UNIVERSITÉ DE RENNES 1

Master de mathématiques

Quantum mechanics
Foundations and applications

Lecture notes

Dimitri Petritis

UFR Mathématiques

Rennes
January 2020

Dimitri Petritis
Institut de recherche mathématique de Rennes
Université de Rennes 1 et CNRS (UMR6625)
Campus de Beaulieu
35042 Rennes Cedex
France

Mathematics subject classification (2010): 81P10, 81P15, 81P13, 81P16, 81P45, 60J05

Warning!

This text is still in a preliminary version.
Even if LaTeX makes it look like a book, **it is not as yet a book!**

Contents

Part I

Introduction to the physical problem and its mathematical formalism

In this part, we make a very short historical review of the scientific problems and experimental facts that led to the development of the quantum theory during the first part of the 20th century. A gentle introduction to the mathematical formalism of quantum theory is given by treating some elementary finite-dimensional examples and exhibiting the analogy there exists between discrete finite classical random systems and discrete finite quantum systems but underlying also the profound differences among them in this setting.

To make the text self-contained, we include some basic facts about Hilbert spaces and linear operators on these spaces and stress on some aspects (spectral theorems, tensor products) that are not always thoroughly treated in introductory texts on Hilbert spaces. We conclude this part by explaining some counter-intuitive phenomena stemming from the quantum formalism.

1

Physics, mathematics, and mathematical physics

"It doesn't matter how beautiful your theory is, it doesn't matter how smart you are. If it doesn't agree with experiment, it's wrong. In that simple statement is the key to science".

Richard P. FEYNMAN, Lecture on *The character of physical law*, Cornell University (1964).

« La mathématique est une science expérimentale. Contrairement en effet à un contresens qui se répand de nos jours (. . .), les objets mathématiques préexistent à leurs définitions ; celles-ci ont été élaborées et précisées par des siècles d'activité scientifique et, si elles se sont imposées, c'est en raison de leur adéquation aux objets mathématiques qu'elles modélisent ».

Michel DEMAZURE, *Calcul différentiel*, Presses de l'École Polytechnique, Palaiseau (1979).

1.1 Experiments

Physics relies ultimately on **experiment**. Observation of many different experiments of similar type establishes a **phenomenology** revealing relations between the experimentally measured physical observables. A phenomenology, even relying on false hypotheses, can still be useful if it **predicts correctly** quantitative relationships occurring in yet unrealised experiments [1]. The experimental nature of Physics implies

1. For instance, the Antikythera mechanism is a mechanical device of the size of a modern laptop constituted of more than 30 bronze gears that has been found in a ship wreck. Its approximate date

the statistical character of its crude experimental results; nevertheless, sound results can be obtained thanks to the statistical reproducibility of the physical experiments.

The next step is inductive: **physical models** are proposed satisfying the phenomenological relations. Then, new phenomenology is predicted, new experiments designed to verify it, and new models are proposed. When sufficient data are available, a **physical theory** is proposed, encompassing all the models that have been developed so far and all the phenomenological relations that have been established. The theory can **deductively** predict the outcome for yet unrealised experiments. If it is technically possible, the experiment is performed. Either the subsequent phenomenology contradicts the theoretical predictions — and the theory must be rejected — or it is in accordance with them — and this precise experiment serves as an additional validity check of the theory. Therefore, physical theories have not a definite status: they are accepted as long as no experiment contradicts them!

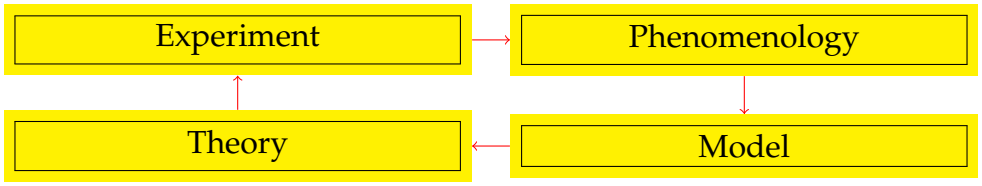


Figure 1.1 – The endless loop of Physics

It is a philosophical debate **how mathematical theories** emerge. Some scientists — among them the author of these lines — share the opinion expressed by Michel Demazure (see quotation on page 5), claiming that Mathematics is as a matter of fact an experimental science. Accepting, for the time being, this view, hypotheses for particular mathematical branches are the pendants of models. What differentiates strongly mathematics from physics is that once the axioms are stated, the proved theorems (phenomenology) need not be experimentally corroborated, they exist *per se*. The experimental nature of mathematics is hidden in the mathematician's intuition that served to propose a given set of axioms instead of another.

Mathematical physics is physics, i.e. its truth relies ultimately on experiment but it is also mathematics, in the sense that physical theories are stated as a set of axioms (called postulates in the physical literature) and the resulting physical phenomenology must derive both as theorems and as experimental truth. Although experimental results can have random outcomes, an important epistemological requirement is that they must exhibit some kind of **statistical reproducibility**. Therefore, all physical theories can be described as a **statistical model** augmented by a **dynamical law**.

of manufacture is estimated between 150 BC and 100 BC. It uses geocentric astronomical knowledge of Ptolemy's era to predict movements of Mercury, Venus, Mars, Jupiter and Saturn. Although the phenomenology prevailing in the Antikythera mechanism is known now to be wrong, the mechanism had nevertheless sufficient predictive power, in line with the technology available at that time.

1.2 A brief history of modern Physics

1.2.1 End of 19th century: the era of false certainties

By the end of 19th century, the success of Physics to describe the phenomena known at that time was such that most physicists acquired the certainty that **all** physical phenomena could be explained by the then known Physics.

— Space was thought as an infinite Euclidean space $\mathbb{R}^3$; time as an one-dimensional space $\mathbb{R}$, independent of space. Space and time were absolute entities, time serving only to describe motion (evolution) in space.
— Matter was thought as a continuum, described by densities, and its motion was precisely described by the equations of motion established 2 centuries ago by Newton that remained invariant under transformations of the Galileo's group.
— Light, like all other electromagnetic phenomena, was governed by Maxwell's equations that remained invariant under transformations of the Poincaré's group.
— Thermodynamics and open thermal systems were phenomenologically understood.

All problems of Physics seemed to reduce in obtaining the correct solution of the adequate underlying differential equation.

Nevertheless, some (considered as) **minor** problems were remaining, like:

— The experimental **spectrum of a radiating black-body** was in disagreement with the theoretical computations in terms of Maxwell equations of electromagnetism.
— When Maxwell equations were considered without sources, they admitted solutions in the form of electromagnetic waves. By analogy with sound or water waves, electromagnetic waves were supposed to require a medium into which they can propagate. The existence of the **luminiferous aether**, as the adequate medium for the propagation of electromagnetic waves, has then been conjectured.

But is was only a matter of time to definitely settle those . . . small vexations. Several senior scientists were supposedly [2] discouraging brilliant young fellows from pursuing studies in Physics since . . . there was nothing interesting that remained to be discovered. It turned out that this false certainty was one of the greatest fallacies in the history of sciences since almost all branches of physics have been revolutionised in the early 20th century.

2. Such a quote is misattributed to Lord Kelvin though there is no evidence that he said anything of the sort. The only historically proven quote on the subject is due — quite ironically — to the American physicist Andrew Abraham Michelson (one of the experimenters who proved that aether does not exist) who — as reported in the University of Chicago Annual Registrer 1894, page 159 — said:

> "While it is never safe to affirm that the future of Physical Science has no marvels in store even more astonishing than those of the past, it seems probable that most of the grand underlying principles have been firmly established and that further advances are to be sought chiefly in the rigorous application of these principles to all the phenomena which come under our notice. It is here that the science of measurement shows its importance — where quantitative work is more to be desired than qualitative work. An eminent physicist remarked that the future truths of physical science are to be looked for in the sixth place of decimals."

1.2.2 1895 – 1932: Everything is falling down

Aether does not exist. We have seen that the existence of the luminiferous aether has been conjectured as a necessary medium ensuring the propagation of electromagnetic waves. But if such a medium existed, it should be possible to detect it experimentally. After a series of ingenious experiments peformed in 1887 and later during the period 1902 – 1905, by Andrew Abraham Michelson [3] and Edward Morley proved that the aether does not exist! Therefore, the then available understanding of Maxwell's equations turned out to be incomplete.

Matter is discontinuous. It is remarkable that already in the 7th century BC, questioning about the organisation of Nature started to occupy philosophers [4]. The existence of atoms has then been conjectured [5] not on the basis of experimental observation but on the basis [6] of logical necessity! However, during the post-renaissance era of science, and until the early 19th century, the atomic hypothesis has been dismissed giving place to a continuum description of matter.

In the beginning of the 19th century, John Dalton, a chemist, showed that chemical reactions were compatible with an atomistic description of matter. In 1827, Robert Brown, a botanist, while looking through a microscope at particles trapped in cavities inside pollen grains in water, noted that the particles moved erratically (performed a called — at present —Brownian motion) through the water but he was not able to determine the mechanisms that caused this motion.

In 1866, Ludwig Boltzmann, in his thesis, establishes a kinetic theory of gases in which he explains the thermodynamic behaviour of gases in terms of mechanical equations of its atomic constituents. Nevertheless, the **atomic hypothesis** — as it is called by that time — is not accepted (if not rejected with sheer hostility) by the scientific establishment. In 1897 Joseph John Thomson discovers the electron and proposes a (wrong) model of the atom. In 1905, Albert Einstein proves mathematically that the erratic motion of a witness particle in a liquid (the Brownian motion) is explained by the random collisions of atoms of the liquid on the witness particle, provided that the witness particle is significantly larger than the atoms of the liquid. He obtains moreover precise quantitative relationships between various physical quantities that were instrumental to Jean Perrin for experimentally [7] proving the **existence of atoms** in 1908. Another of the false certainties of the 19th century felt down .... Matter is not continuous!

Matter is not stable. Modern Chemistry emerged with the work of Antoine Lavoisier

3. Michelson won the 1907 Nobel Prize in Physics.
4. Thales (624 – 546 BC) and Anaximander (ca. 610 – ca. 546 BC)
5. By Leucippus (unknown dates during the 5th century BC) and Democritus (460 – 370 BC) and later Epicurus (341 – 270 BC).
6. The ancient atomists theorised that the two fundamental and oppositely characterised constituents of the natural world are indivisible bodies — atoms, etymologically meaning "that cannot be cut into pieces" — and void. Void is described simply as nothing, or the negation of body. Atoms are by their nature intrinsically unchangeable; they can only move about in the void and combine into different clusters. Since the atoms are separated by void, they cannot fuse, but must rather bounce off one another when they collide. Because all macroscopic objects are in fact combinations of atoms, everything in the macroscopic world is subject to change, as their constituent atoms shift or move away. Thus, while the atoms themselves persist through all time, everything in the world of our experience is transitory and subject to dissolution.
7. And wining the 1927 Nobel Prize in Physics for this discovery.

who cut short, in 1783, the dreams and speculations of generations of alchemists [8] who pretended to transmutate ordinary metals to gold. As a matter of fact, Lavoisier established that substances intervening in a chemical reaction are only recombinations of the participating chemicals [9]. In 1896, Henri Becquerel discovers radioactivity of uranium, a phenomenon confirmed later by Maria Skłodowska-Curie and Pierre Curie on uranium, radium and polonium [10]. Radioactivity appeared then as the transmutation of a chemical consisting of one species of atoms, like radium, to another species [11]. Thus radioactive isotopes $^{238}_{92}$U or $^{234}_{92}$U of uranium, after a sequence of radioactive cascades transmutate eventually to the stable isotope $^{206}_{82}$Pb of lead.

Space and time are not absolute. Equations of classical mechanics are invariant under Galileo group; equations of electromagnetism are invariant under Poincaré group. Why two different invariance groups are needed? In 1905, Albert Einstein starting from two simple principles, namely that the speed of light c is a universal constant, the same in all reference frames, and that the laws of physics must remain identical in all inertial frames, establishes **special relativity**, unifying classical mechanics and electormagnetism. In the framework of special relativity, the notion of aether is no longer needed for light to propagate, at the expense of merging absolute space and time in a single **relative space-time, endowed with a flat pseudo-Euclidean metric** where physical events occur.

Physical space-time is curved. In 1913, Einstein extends the special relativity, he had conceived some eight years earlier, to include gravitational phenomena. The new theory is called the **general relativity**. In this new theory, the space-time becomes a pseudo-Riemannian manifold whose geometry (metric tensor) becomes itself a field. The local curvature of the manifold is determined by the local density of the matter. On a Riemannian manifold, the role of straight lines is played by geodesics. For instance, the Moon is revolving around the Earth because the mass of the Earth curves locally the space-time so that the geodesic followed by the Moon becomes a closed orbit around the Earth. The main idea of General Relativity is that matter (and energy) shapes the space-time geometry and space-time geometry imposes the way matter moves. Most of the predictions of general relativity have been repeatedly tested (e.g. precession of the perihelion of Mercury, gravitational lensing observed during total solar eclipses, etc.). The most decisive test of the theory was the experimental detection of gravitational waves; their existence has been theoretically predicted in 1916 by Einstein but they have been experimentally detected only one century later, on 14 September 2015, when the front of the gravitational wave generated by the merging of two black holes reached the Earth. The article announcing this detection [1] appeared on 11 February 2016 [12]. But one must not think that

8. Even the great Sir Isaac Newton versed in those speculations during the period 1668–1675.

9. Think of the chemical reaction $NaOH + HCl \to NaCl + H_2O$. Sodium (Na), oxygen (O), hydrogen (H), and chlorine (Cl) are only recombined but globally preserved.

10. The 1903 Nobel Prize in Physics has been awarded for the discovery of radioactivity to Antoine Becquerel, Maria Skłodowska-Curie and Pierre Curie.

11. Nowdays, we know that radioactivity is a transmutation of the atomic nucleus.

12. The American physicists Rainer Weiss, Kip Thorne and Barry Barish who made the detection — but, sadly, not the French theoretical physicist Thibault Damour, who made the computations that were essential for rendering the experimental discovery possible — were awarded the Nobel Prize in Physics on 2017.

general relativity is some esoteric discipline only predicting some phenomena totally irrelevant to every-day life. For instance, general relativity is necessary to an every-day life technological application: the **global positioning system** [13].

Energy is not continuous. In 1887, Heinrich Hertz observed that ultraviolet light falling on some electrodes make them sparking more easily **(photoelectric effect)**. In 1900, Max Karl Ernst Planck gives a groundbreaking phenomenological derivation of the **black-body radiation spectrum**. If the energy levels of light wave can only take discrete values, then a perfect agreement between experimental observation and computation can be achieved. In 1905, Albert Einstein — elaborating on the idea of Max Planck — proposes that a beam of light is not a continuous wave propagating through space but a collection of discrete wave packets — he termed *Lichtquanten* (light quanta), presently called the **photons**, — having an energy proportional to their frequency [14]. Under this hypothesis, he gives an explanation of the photoelectric effect and proposes a quantitive estimate of the photoelectric current. These theoretical predictions have been experimentally verified [15] by Robert Andrews Millikan in 1914. Niels Bohr, Louis de Broglie, Werner Heisenberg, Wolfgang Pauli, Paul Adrien Maurice Dirac, Erwin Schrödinger, John von Neumann and others, during the golden era 1913 – 1932, considered Planck's idea seriously and established Quantum Mechanics [16] named after the fact that energy is not continuous but "quantified" (i.e. its possible values arise as integer multiples of a fundamental "quantum" of energy). However, by 1926, two — apparently irreconcilable — theories describe quantitatively atomic phenomena: matrix mechanics, advocated by Heisenberg, and wave mechanics, advocated by Dirac. Pauli argues that the two theories should be equivalent. The equivalence is proved by von Neumann in 1927 by showing that Heisenberg "matrices" are in fact operators acting on a Hilbert space defined as the L^2 space of Dirac waves.

1.2.3 Physics after 1932

A general physical theory must describe all physical phenomena in the **universe**, extending from elementary particles to cosmological phenomena. Numerical values of the fundamental physical quantities, i.e. mass (M), length (L), and time [17] (T), span

13. The GPS performs localisation of a car on the surface of the Earth by measuring its position relative to three satellites whose coordinates are precisely known and proceeding by triangulation. The estimate of the car-satellite distance is obtained by the time needed for an electromagnetic signal to travel to and fro. To be useful, the precision of the localisation must be of the order of metre. Now, the mass of Earth curves the space-time in its vicinity so that time lapses differently near Earth and near the satellites; to achieve the required precision of localisation, this curvature effect must be taken into account!

14. The frequency determines the colour of the light.

15. And allowed Einstein to win the 1921 and Millikan the 1923 Nobel Prize in Physics for the explanation and the experimental confirmation of the photoelectric effect.

16. All founders of Quantum Mechanics, but von Neumann, have been laureates of the Nobel Prize in Physics: Planck in 1918, Bohr in 1922, de Broglie in 1929, Heisenberg in 1932, Schrödinger and Dirac in 1933, Pauli in 1945.

17. The upper bound of physical times (10^{17}s $\simeq 1.4 \times 10^{10}$a) is identified with the "age of the universe". It turns out that the "age of the universe" is a badly defined concept since there is not yet a generally accepted physical/mathematical theory encompassing both quantum field theory and gravi-

vast ranges:

$$10^{-31}\text{kg} \leq M \leq 10^{51}\text{kg};\ \ 10^{-15}\text{m} \leq L \leq 10^{27}\text{m};\ \ 10^{-23}\text{s} \leq T \leq 10^{17}\text{s}.$$

Units used in measuring fundamental quantities, i.e. kilogramme (kg), metre (m), and second (s) respectively, were introduced after the French Revolution so that everyday life quantities are expressed with reasonable numerical values (roughly in the range $10^{-3} - 10^{3}$). The general theory believed to describe the universe [18] is called **quantum field theory**; it contains two fundamental quantities, the speed of light in the vacuum, $c = 2.99792458 \times 10^{8}\text{m/s}$, and the Plank's constant $\hbar = 1.05457 \times 10^{-34}\text{J}\cdot\text{s}$. These constants have extraordinarily atypical numerical values. Everyday velocities are negligible compared to c, everyday actions are overwhelmingly greater than $\hbar$. Therefore, everyday phenomena can be thought as the $c \to \infty$ and $\hbar \to 0$ limits of quantum field theory; the corresponding theory is called **classical mechanics**.

It turns out that considering solely the $c \to \infty$ limit of quantum field theory gives rise to another physical theory called **quantum mechanics**; it describes phenomena for which the action is comparable with $\hbar$. These phenomena are important when dealing with atoms and molecules.

The other partial limit, $\hbar \to 0$, is physically important as well; it describes phenomena involving velocities comparable with c. These phenomena lead to another physical theory called **special relativity**.

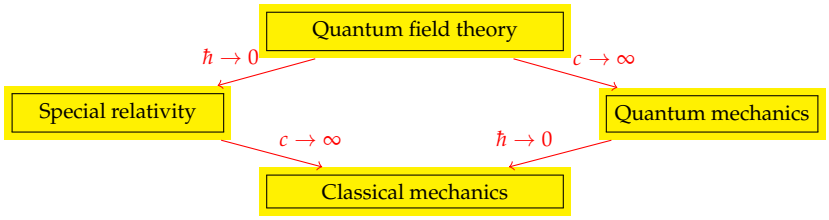


Figure 1.2 – Physical theories (with the exception of gravity) as special cases of more general theories

Although quantum field theory is still mathematically incomplete, the theories obtained by the limiting processes described above, namely quantum mechanics, special relativity, and classical mechanics are **mathematically closed**, i.e. they can be formulated in a purely axiomatic fashion and all the experimental observations made so far (within the range of validity of these theories) are compatible with the derived theorems.

Among the three theories mentioned above, quantum mechanics has a very particular status:

— can be formulated in a totally axiomatic way;
— **all** its predictions have been verified with unprecedented accuracy;
— not a single experiment has ever put the theory in difficulty;

tational phenomena beyond the Planck's scale. When we extrapolate the estimates of the theory valid before the Planck's scale beyond that scale, an initial singularity is predicted, commonly termed Big-Bang. The "age of the universe" is the elapsed time since the *thus determined* initial singularity.

18. This claim is true if gravitational phenomena are not taken into account.

— current technology, developed essentially during the second half of the 20th century, has been shaped by the achievements of quantum physics so that quantum phenomena play a prominent role in the global economy (a very conservative estimate is that 35–40% of the global wealth relies on exploiting quantum phenomena).

1.2.4 Perspectives on the foundational aspects in the 21st century

In spite of the tremendous usefulness, pertinence, predictive power, and its mathematically closed form, quantum theory — almost one century after its conception — has still an awkward and counterintuitive formulation. It remains still difficult to understand what really happens during the measurement process and apprehend phenomena like entanglement, teleportation, decoherence, etc. Contrary to other physical theories — classical mechanics, special and general relativity, electromagnetism, thermodynamics, etc. — whose formulation is based on a small number of physically reasonable postulates that are begging for a specific mathematical formalism, in quantum theory, a mathematical formalism based on the abstract notion of a Hilbert space — emerging out of nowhere — precedes the formulation of the basic postulates. But, as Asher Peres [116, page 373] put it: "quantum phenomena do not occur in a Hilbert space; they occur in a laboratory". We have an extraordinarily predictive theory but we still lack a satisfactory explanation scheme; the theory looks as if a conceptual building block were missing in its description.

During many decades, the core of physicists adopted the "shut up and compute" stance with foundational aspects neglected — if not contemptuously abandoned to the quest of philosophers. The situation is fortunately changing and foundational aspects win renewed interest. Even the philosophical basis of quantum mechanics is questioned by joint efforts of physicists [11] and philosophers.

The main challenge in modern Physics remains the quest for the "big unification", i.e. the conception of a theory encompassing — in a mathematically coherent and physically verifiable way — quantum and gravitational phenomena. Two candidate theories are competing these days: string theory and loop quantum gravity. String theory supposes that the universe holds many dimensions: the four (spatio-temporal) degrees of freedom are unbounded; the other (many) dimensions remain bounded. Loop quantum gravity [126] is more radical in the sense that it predicts that space-time itself is discrete; its continuum appearance is only an illusion because every-day distances contain a tremendous number of **space quanta** [19].

Another theoretical challenge remains the understanding of **decoherence**. Decoherence is the phenomenon responsible for the quantum-to-classical transition occurring in any realistic, i.e. non isolated from its environment, quantum system; it constitutes the main impediment to the physical realisation of large scale quantum computers. Fully incorporating decoherence as a primitive notion into the mathematical founda-

19. The space quantum corresponds to the distance where gravitational and quantum phenomena become of the same order of magnitude. This distance is known as the **Planck scale** and corresponds to 10^{-35}m.

tions of quantum mechanics remains a challenging open problem. Possibly, the full understanding of decoherence will be ultimately achieved only when the gravitational phenomena will be successfully incorporated into quantum theory. In that respect, the discreteness of space-time — advocated by quantum loop gravity — may be the correct idea to understand the mechanisms underlying quantum measurement and decoherence.

1.3 Technological impact of quantum physics

1.3.1 The era of the first quantum revolution

Quantum mechanics intervenes in a decisive manner in the explanation of vast classes of phenomena in other fundamental sciences and in technology. Without being exhaustive, here are some examples of such quantum phenomena:

— atomic and molecular physics (e.g. stability of — non-radioactive — matter, physical properties of matter), quantum optics (e.g. lasers), nuclear magnetic resonance and positron emission tomography (e.g. medical imaging),
— chemistry (e.g. valence theory) and biology (e.g. photosynthesis — including industrially mimicked photosynthesis —, structure of DNA),
— solid state physics (e.g. physics of semiconductors, transistors),
— tunnel effect (e.g. atomic force microscope) and nanotechnology,
— supraconductivity (e.g. magnetic levitation to sustain ultra-fast trains) and superfluidity
— ... and the list keeps growing.

Nevertheless, present time technology is still based on macroscopic systems; for instance we still use currents or laser beams to transport information, solid state devices (transistors) to process information, etc. All these physical systems involve tremendous numbers of particles (10^{15} photons in laser beam of typical power, 10^{23} electrons in a typical current). Therefore, the behaviour of the system must be described statistically, by applying the law of large numbers. This produces an averaging of the behaviour so that we can still use classical reasoning. Our present technology, although relying on quantum achievements is understandable/describable in classical terms. We are still in the era of the **first quantum revolution**.

1.3.2 The second quantum revolution

Starting with some pioneering experiments (like trapping of one single electron [155] in Washington or manipulating an individual pair of photons [7] in Orsay), physicists become able of manipulating various *single microscopic quantum objects*.

There is however another major technological breakthrough that is foreseen with a tremendous socio-economical impact: if the integration of electronic components continues at the present pace (see figure 1.3), within 10–15 years, only some tenths

of silicium atoms [20] will be required to store a single bit of information [21] Classical (Boolean) logics does not apply any longer to describe atomic logical gates, quantum (orthocomplemented lattice) logics is needed instead.

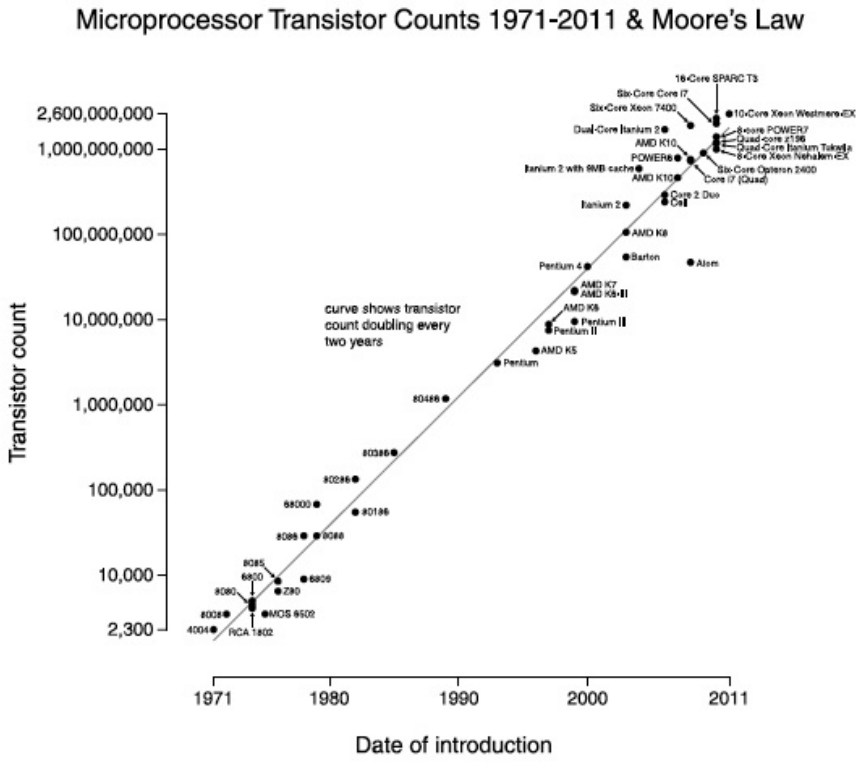


Figure 1.3 – The evolution of the number of transistors on integrated circuits in the period 1971–2011. (Source: Wikipedia, transistor count.)

Theoretical exploration of this new type of informatics has started and it is proven [136] that some algorithmically complex problems, like the integer prime factoring problem — for which the best known classical algorithm [100] requires a time that is superpolynomial in the number of digits — can be achieved in polynomial time using quantum logic. The present time technology does not yet allow the prime factoring of large integers but it demonstrates that there is no fundamental physical obstruction to its achievement for the rapidly improving computer technology. Should such a breakthrough occur, all our electronic transmissions, protected by classical cryptologic methods could become vulnerable. The table 1.1 gives a very rough estimate of the time needed to factor an $n = 1000$ digits numbers, assuming an operation per nanosecond for various hypotheses of algorithmic complexity.

On the other hand, present day technology allows to securely and unbreakably cipher messages using **quantum cryptologic protocols**. For instance, one can buy quantum random generators in the form of USB sticks (see figure 1.4) or general quantum cryptographic devices.

20. The last generation of microprocessors has a etch thickness of some 14 nm while the silicium interatomic distance in the crystal is 0.2 nm.

21. See the video zooming on a micrprocessor prepared by Frank Kusiak of the University of California at Berkeley.

n	$\mathcal{O}(\exp(n))$	$\mathcal{O}(\exp(n^{1/3}(\log n)^{2/3}))$	$\mathcal{O}(n^3)$
100	1.26×10^{21}s $= 4.01 \times 10^{13}$a	3.13s $= 9.93 \times 10^{-8}$a	1×10^{-3}s $= 3.17 \times 10^{-11}$a
500	3.27×10^{141}s $= 1.31 \times 10^{134}$a	6.74×10^{10}s $= 2139$a	0.125s $= 3.96 \times 10^{-9}$a
1000	1.07×10^{292}s $= 3.39 \times 10^{284}$a	6.42×10^{17}s $= 2.03 \times 10^{10}$a	1s $= 3.17 \times 10^{-8}$a

Table 1.1 – A very rough estimate of the order of magnitude of the time needed to factor an n-bit number (with $n = 100, 500, 1000$), under the assumption of execution of the algorithm on a hypothetical computer performing an operation per nanosecond, as a function of the time complexity of the used algorithm. When the cryptologic protocol RSA has been proposed [125] in 1978, the best factoring algorithm had a time complexity in $\mathcal{O}(\exp(n))$. The best known algorithm (the general number field sieve algorithm) reported in [101] requires time $\mathcal{O}(\exp(n^{1/3}\log^{2/3} n))$ to factor a n-bit number. The Shor's quantum factoring algorithm [136] requires time $\mathcal{O}(n^3)$. We recall for comparison: "age of the universe" 1.5×10^{10} a.

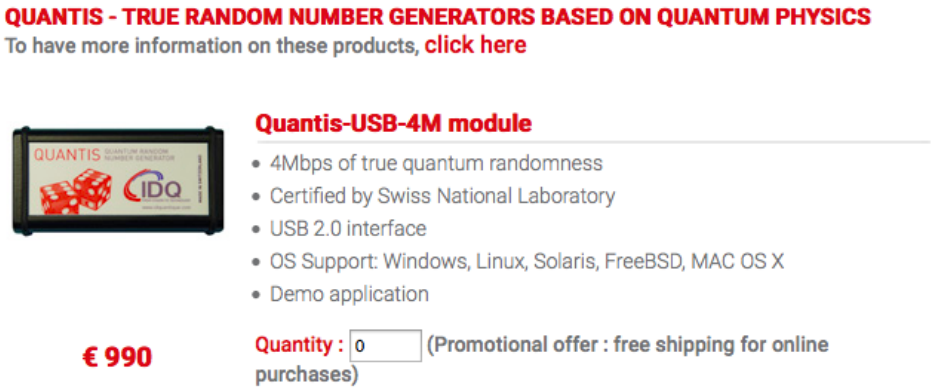


Figure 1.4 – Quantum random number generation and quantum cryptography are not speculative dreams of physicists but already full-fledged pre-industrial applications. In this figure is reproduced a screen copy of the online catalog of the company selling quantum random number generators as well as general quantum cryptographic devices. (By courtesy of Id-Quantique).

The figure 1.5 represents currently foreseen advancements in quantum information technology for the coming years. (Source: Quantum Manifesto 2010 [22]). The same efforts are deployed outside Europe. For instance, on 16 August 2016, at 01:40 local time, China has launched the world's first satellite, Micius, dedicated to testing the fundamentals of quantum communication in space in the framework of the Quantum Experiments at Space Scale (QUESS) mission. On 29 September 2017 the first intercontinental videoconference encrypted by quantum methods has been held between the Austrian and Chinese academies of sciences in Vienna and Beijing (separated by 7400 km), using the Chinese satellite Micius facility. This experiment paves the road for a worldwide quantum communication network foreseen for the forthcoming decade. It proves the possibility of entanglement between particles separated by such a large distance [23].

Companies in the United States are also very actively developing quantum algorithms and test them on prototypal quantum computers. IBM launched, on 4 May

22. http://qurope.eu/manifesto
23. The notion of entanglement is explained in §3.10.

Communication	Simulators	Sensors	Computers
0–5 years			
Quantum repeaters	Simulator of motion of electrons in materials	Quantum sensors for niche applications (gravity and magnetic sensors for health care, geosurvey and security)	Operation of a logical qubit with error correction
Secure point-to-point quantum links	New algorithms for quantum simulators and networks	More precise atomic clocks for synchronisation of future smart networks	New algorithms for quantum computers Small quantum processor executing technologically relevant algorithms
5–10 years			
Quantum networks between distant cities	Development and design of new complex materials	Quantum sensors for larger volume applications (automotive, construction, etc.)	Solving chemistry and materials science problems with special purpose quantum computer > 100 physical qubit
Quantum credit cards	Versatile simulator of quantum magnetism and electricity	Handheld quantum navigation devices	
$\geq$ 10 years			
Quantum repeaters with cryptography and eavesdropping detection	Simulators of quantum dynamics and chemical reaction mechanisms to support drug design	Gravity imaging devices based on gravity sensors	Integration of quantum circuit and cryogenic classical control hardware
Secure Europe-wide internet merging quantum and classical communication		Quantum sensors integrating consumer applications including mobile devices	General purpose quantum computers exceeding computational power of classical computers

Figure 1.5 – Advancement in quantum information technology foreseen for the coming years (extracted from the 2010 Quantum Manifesto). Similar roadmaps have been also established by the NFS. In view of the present achievements, the objectives set for the 10 years — i.e. to be achieved by ca. 2020 — sound quite realistic.

2016, the world's first publicly accessible quantum computer operating on 5 qubits [24]. On 14 November 2017, IBM launched a quantum computer prototype, IBM Q, operating with 50 qubits and constituting an important threshold because the computational power of a quantum computer with 50-qubit registers outperforms all known classical computers; beyond 50 qubits we enter in the zone of **quantum supremacy**. Quantum supremacy is defined as the ability of quantum devices without error correction to perform a well-defined computational task beyond the possibilities of the state of the art of classical computers.

The enthusiasm of achieving large-scale universal computers in the foreseen future seems nevertheless overoptimistic. What sounds more realistic seems to be special purpose machines (like machines exploiting quantum tunnelling phenomena) to perform optimisation tasks. As a matter of fact, Nature, by choosing the lowest energy configurations, performs a non-trivial optimisation task. If this ability of Nature can be tamed, then we can solve complicated optimisation problems by quantum evolution. Such ideas prevailed in the work [2], where DNA-computing has been used to encode and solve the "travelling salesman problem", a problem known to be algorithmically NP-complete. Such methods are used in some commercially available architectures like the D-wave^{TM} computer.

Beyond those foreseen advances in technology, computer science, information transmission and protection, material sciences, etc. another emerging usefulness is the back-action of quantum processes to introduce quantum-inspired methods applied to cognitive and decisional sciences (see e.g. [145, 137, 33, 105]). It is also important to realise that several natural transformations induced by quantum phenomena (eg. photosynthesis) can be formalised as quantum computational tasks.

We start entering into the **second quantum revolution**.

1.4 Plan of the lectures

These lecture notes are divided in three parts:

1. The **mathematical foundations** of quantum mechanics are presented into the simplest **finite-dimensional case**.
2. We then deal with the applications of finite-dimensional quantum mechanics into the rapidly developing field of **quantum information, computing, communication, and cryptology.**
3. Finally, the mathematical foundations are revisited in the general **infinite-dimensional case**. Algebra, analysis, probability, and statistics are necessary to describe and interpret this theory. Its predictions are often totally counter-intuitive. Hence it is interesting to study this theory that provides a useful application of the mathematical tools, a source of inspiration [25] for new developments

24. Qubit is the quantum analog of bit.

25. Recall that entire branches of mathematics have been developed on purpose, to give precise mathematical meaning to — initially — ill-defined mathematical objects introduced by physicists to formulate and handle quantum theory. To mention but the few most prominent examples of such mathematical

for the underlying branches of mathematics, and a description of unusual physical phenomena.

The third part does not depend on the second. Therefore, a course towards applications in quantum information can include only parts 1 and 2. A course orientated to more fundamental aspects can contain only parts 1 and 3.

theories: von Neumann algebras, spectral theory of operators, theory of distributions, non-commutative probabilities.

2

Phase space, observables and effects, states, measurement, probability

> Probability theory did not enter into quantum mechanics at the outset. The pioneers of the field had no reason or intention to make quantum mechanics a probabilistic subject. The stochastic nature of quantum mechanics was reluctantly accepted later when it proved to an intrinsic, inescapable part of the field.
>
> Stanley P. GUDDER: *Stochastic methods in quantum mechanics*, [78].

2.1 Statistical models and measurements

As is the case in all experimental sciences, information on a physical system is obtained through **observation** (also called **measurement**) of the possible values or outcomes — within a prescribed set — that can take the physical **observables**. There exists an abstract set $\mathbf{O}$ of observables; every observable $X \in \mathbf{O}$ has possible outcomes in a given set $\mathbb{X} := \mathbb{X}_X$. The acquisition procedure of the information must be described operationally in terms of

— macroscopic instruments, designed to reveal the outcomes of the observables and

— prescriptions on the application of instruments on the observables of an objectified physical system.

The biggest the set of observables whose values are known, the finest is the knowledge about the physical system. Since crude physical observables (e.g. number of particles, energy, velocity, etc.) can take values in various sets ($\mathbb{N}, \mathbb{R}_+, \mathbb{R}^3$, etc.), a practical way in order to have a unified treatment for general systems is to reduce any physical

experiment into a series of measurements of a special class of observables, called **yes-no experiments** or **(sharp) effects**. This is very reminiscent of the approximation of any integrable random variable by a sequence of step functions. Therefore, ultimately, we can focus on observables taking values in the set $\{0,1\}$. Systems are prepared in some precise **state** ρ in some abstract set **S** of states. **Measurement** of an observable X (by means of the appropriate instrument) consists in registering the outcome of X. In general, an observable can give different outcomes. The formalism provides us with the probability distribution of possible outcomes of X when the system is prepared in state ρ. The process of measurement is summarised in the box on page 21.

It turns out that physical observables for classical systems can be described as random variables while states are probability measures on some measurable space called the phase space. The first mathematically sound description [148] of quantum systems was in the framework of Hilbert spaces. This description is sufficient to describe finite systems and is the only one we shall use in this introductory section. The phase space of a quantum system is a Hilbert space, observables are generally non-commuting Hermitean operators acting on the Hilbert space while states constitute a special subclass of Hermitean operators (postive operators having a normalised trace), known as density operators, on the same Hilbert space. We will show that this description conveys an intrinsically and irreducibly stochastic character to the predictions of quantum mechanics. This stochastic character remains to all other possible formulations — to be developed in later chapters — of quantum mechanics.

2.2 Some reminders from probability theory

2.2.1 Three seemingly anodyne questions of the utmost importance

Start by three very naïve-looking questions:

1. Is it possible to play "heads-or-tails" with the help of a honest die, i.e. simulate the outcome of a single realisation of a honest coin from the outcome of a single realisation of a honest die?
2. Is it possible to play dice with the help of a honest coin, i.e. simulate a single outcome of a honest die from the outcome of a single realisation of a honest coin?
3. More profoundly, how to play a random game having a finite set of outcomes?

The first question has an easy answer: the die outcomes form the space $\Omega = \{1,\dots,6\}$ equipped with the uniform probability determined by the constant probability vector $\rho(\omega) = 1/6$ for all $\omega \in \Omega$. The space of the coin outcomes is $\mathbb{X} = \{0,1\}$; we can obviously silmulate a honest coin with the help of the map $X : \Omega \to \mathbb{X}$, defined, for instance, by

$$X(\omega) = \begin{cases} 0 & \text{if } \omega = \text{even}, \\ 1 & \text{if } \omega = \text{odd}. \end{cases}$$

Measurement

To become quantifiable and theoretically exploitable, experimental observations must be performed under very precise conditions, known as **the experimental protocol**.

— Firstly, the objectified system must be carefully **prepared** in an initial condition known as the **state** of the system. Mathematically, the state ρ incorporates all the a priori information we have on the system, it belongs to some abstract space of states $\mathbf{S}$.

— Secondly, the system enters in contact with a measuring apparatus (instrument), specifically designed to measure the outcomes of a given **observable** X. Observables belong to some abstract space $\mathbf{O}$.

— Interaction of the system with the measuring apparatus returns **outcomes** of the observables; the outcome space is some measurable space $(\mathbb{X}, \mathcal{X})$ with $\mathbb{X}$ some discrete or continuous Borel subset of $\mathbb{R}$. This is precisely the **measurement process.**

— The whole physics relies on the postulate of **statistical reproducibility of experiments**: if the same measurement is performed on a very number of copies of the system prepared in the same state, the experimentally observed data for a given observable take random outcomes in $\mathbb{X}$ scattered with some fluctuations around some central value. However, when the number of repetitions tends to infinity, the empirical distribution of the observed data tends to some **probability distribution** ν on the space of outcomes $(\mathbb{X}, \mathcal{X})$.

Thus, abstractly, a single **measurement** can be thought as a black box assigning to a pair $(\rho, X) \in \mathbf{S} \times \mathbf{O}$

— the outcome of the observable X and

— the probability of the occurrence of the given outcome.

When the experiment is repeated on a large ensemble of identically prepared systems, the probability measure ν_X^ρ on the space of outcomes, i.e. the map ν defined by:

$$\mathbf{S} \times \mathbf{O} \ni (\rho, X) \mapsto \nu(\rho, X) := \nu_X^\rho \in \mathcal{M}_1(\mathbb{X}, \mathcal{X}),$$

whose meaning is, for all $A \in \mathcal{X}$,

$$\nu_X^\rho(A) = \mathbb{P}(X \text{ takes values in } A | \text{system has been prepared at } \rho).$$

is also empirically determined.

The pair $(\mathbf{S}, \mathbf{O})$ is called a **statistical model**. The protocol implemented in order to determine the possible outcomes and the map ν is called **measurement**. Mathematically, ν is fully determined by a **stochastic transformation kernel** expressed in terms of X and ρ. For that reason, very often the measurement is identified with this stochastic kernel.

Then the distribution of X on the space of outcomes $\mathbb{X}$ reads

$$\nu_X^\rho(x) = \sum_{\omega \in X^{-1}(x)} \rho(\omega) = 1/2, \text{ for } x \in \mathbb{X}.$$

The second question sounds awkward: the roles of Ω and $\mathbb{X}$ are now interchanged, reading respectively $\Omega = \{0,1\}$ and $\mathbb{X} = \{1,\dots,6\}$. Obviously any mapping $X : \Omega \to \mathbb{X}$ can take at most 2 distinct values in $\mathbb{X}$, since $|X(\Omega)| \leq 2$. Therefore, the space Ω is not sufficiently large to host all possible outcomes of a die. As a matter of fact, it is possible to simulate a die by throwing 2 or 3 times a honest coin. It can be shown that, in the long run (a very large number N of die outputs), one must throw the honest coin $N \log_2 6$ times (recall that $2 < \log_2 6 < 3$) on average to simulate N realisations of the die, since the entropy of a honest die is $\log_2 6$ bits (see lecture notes [120]).

We come now to the third question. The two previous questions showed that it is possible to choose some space Ω sufficiently large, equipped with a probability vector ρ, and a map X from Ω to a set of possible outcomes $\mathbb{X}$, provided that $X(\Omega) \supseteq \mathbb{X}$. The probability distribution of X is directly determined as the image probability of the vector ρ given by $\nu_X^\rho(x) = \sum_{\omega \in X^{-1}(x)} \rho(\omega)$. But, as the careful reader has already understood, we still need some known probabilistic model Ω equipped with its probability vector ρ, in order to simulate other random games. The above described procedure — known as Kolmogorov's axiomatisation of probability theory [97] — **does** provide an answer to the question whether is it possible to play a random game but **does not** answer the crucial question how to simulate a given random game. All the construction relies on the assumption that an abstract probabilistic model (Ω, ρ) exists; it can then be shown that any other probabilistic game can be built on it. It sounds as if standard probability theory is about transformations of an object we don't know how to construct into concrete realisations. These profound questionings obsessed Kolmogorov and led him to introduce another fundamental concept — known these days as **Kolmogorov's complexity** (see for instance [144] for a detailed exposition of the subject, or [121] for a freely accessible resource) — characterising the nature of truly random sequences. It is astonishing that the far-reaching conclusions of Kolmogorov on this topic are seldom mentioned in standard courses of probability theory. As a matter of fact, an immediate corollary of his approach of complexity is that there does not exist either a computer algorithm (a Turing machine) or a classical finite system allowing to produce a truly random sequence! As a matter of fact, truly random sequences **do exist** in Nature but they are not produced by classical finite systems or by computer algorithms. We shall show in this course that it is very easy to produce a sequence of random bits by a small quantum physical device; you can even buy such a device (see figure 1.4).

2.2.2 Random variables and probability kernels

The mappings X used in the previous subsection are archetypal examples of random variables. Let us recall the mathematical definition of a random variable.

Definition 2.2.1 (Random variable)**.** Let $(\Omega, \mathcal{F})$ be an abstract space of events, and

$(\mathbb{X}, \mathcal{X})$ a concrete space of events [1] (the space of outcomes). A function $X : \Omega \to \mathbb{X}$ such that for every event $A \in \mathcal{X}$ of the space of outcomes, its inverse image is an event of the abstract space (i.e. $X^{-1}(A) \in \mathcal{F}$) is called ($\mathbb{X}$-valued) **random variable**. When the abstract space $(\Omega, \mathcal{F})$ comes equipped with a probability ρ, the random variable X induces a probability ν_X^ρ on $(\mathbb{X}, \mathcal{X})$ (i.e. $\nu_X^\rho(A) = \rho(\{\omega \in \Omega : X(\omega) \in A\})$, for $A \in \mathcal{X}$), called the **law** (or **distribution**) of X.

Notation 2.2.2. The notation ν_X^ρ for the law of the random variable X can be simplified to ν_X or simply ν when, from the context, it is clear which probability ρ and which random variable X we are considering. Note also that in classical probability texts, the probability ρ is usually denoted by $\mathbb{P}$ and the law of the random variable $\mathbb{P}_X$. We stick to the more precise notation introduced in definition 2.2.1. Occasionally we shall also use the notation $X_*\rho$ or $\rho \circ X^{-1}$ as equivalent expressions for ν_X^ρ. Finally recall that on finite spaces $\mathbb{X}$, the probability ν_X^ρ is identified with a probability vector [2] on $\mathbb{X}$, i.e. $\nu_X^\rho : \mathbb{X} \to [0,1]$ with $\sum_{x \in \mathbb{X}} \nu_X^\rho(x) = 1$.

Remark 2.2.3. The careful reader will certainly have noted that the probability measure ρ (or ν_X^ρ) **is not** a constituent of the definition of random variable: the only requirement is $(\mathcal{F}, \mathcal{X})$-measurability of X. Nevertheless, every $\rho \in \mathcal{M}_1(\mathcal{F})$ uniquely determines a $\nu_X^\rho \in \mathcal{M}_1(\mathcal{X})$, the law of X.

Example 2.2.4. Let $\mathbb{X} = \{0,1\}$, $\mathcal{X}$ be the algebra of subsets of $\mathbb{X}$, and $\nu_X(\{0\}) = \nu_X(\{1\}) = 1/2$ the law of a random variable X (the honest coin tossing). A possible realisation of $(\Omega, \mathcal{F}, \rho)$ is $([0,1], \mathcal{B}([0,1]), \lambda)$, where λ denotes the Lebesgue measure, and a possible realisation of the random variable X is

$$X(\omega) = \begin{cases} 0 & \text{if } \omega \in [0, 1/2[\\ 1 & \text{if } \omega \in [1/2, 1]. \end{cases}$$

Notice however that the above realisation of the probability space involves the Borel σ-algebra over an uncountable set, quite complicated an object indeed. A much more economical realisation should be given by $\Omega = \{0,1\}$, $\mathcal{F} = \mathcal{X}$, and $\rho(0) = \rho(1) = 1/2$. In the latter case the random variable X should read $X(\omega) = \omega$: on this smaller probability space, the random variable is the identity function; such a realisation is called **minimal**.

Exercise 2.2.5. (An elementary but important exercise)! Generalise the above minimal construction to the case we consider two random variables $X_i : \Omega \to \mathbb{X}$, for $i = 1, 2$. Are there some plausible requirements on the joint distributions for such a construction to be possible?

Notation 2.2.6. For every abstract space of events $(\Omega, \mathcal{F})$, we denote by

$$m\mathcal{F} = \{f : \Omega \to \mathbb{R}; f \text{ random variable}\} \text{ and } b\mathcal{F} = \{f \in m\mathcal{F} : \sup |f(\omega)| < \infty\}$$

1. Technically, both spaces are measurable spaces, i.e. $\mathcal{F}$ and $\mathcal{X}$ are σ-algebras of events. In order to be able to define regular conditional distributions, we require the space $\mathbb{X}$ to be a Polish space (i.e. a metrisable, complete, and separable space), a requirement that will be automatically be fulfilled since we shall only consider the cases $\mathbb{X} = \mathbb{R}$ or a discrete subset of $\mathbb{R}$, in this course.
2. In the finite case, we often write $\nu_X^\rho(x)$ instead of $\nu_X^\rho(\{x\})$.

the vector spaces of random variables and bounded random variables respectively. We denote by $m\mathcal{F}_+$ or $b\mathcal{F}_+$ non-negative measurable or non-negative bounded measurable functions. $\mathcal{M}_1(\mathcal{F})$ denotes the convex set of probability measures on $\mathcal{F}$; $\mathcal{M}_+(\mathcal{F})$ the set of non-negative σ-finite measures and $\mathcal{M}(\mathcal{F})$ the set of σ-finite measures.

Another important notion in probability theory is that of a stochastic kernel.

Definition 2.2.7 (Stochastic kernel)**.** Let $(\mathbb{W}, \mathcal{W})$ and $(\mathbb{X}, \mathcal{X})$ be two measurable spaces. A map

$$\mathbb{W} \times \mathcal{X} \ni (w, A) \to K(w, A) \in [0, 1],$$

such that

1. for each fixed $w \in \mathbb{W}$, the map $K(w, \cdot)$ is a probability measure on $(\mathbb{X}, \mathcal{X})$, and
2. for each fixed $A \in \mathcal{X}$, the map $K(\cdot, A)$ is $(\mathcal{W}, \mathcal{B}([0, 1])$-measurable,

is termed a **stochastic kernel** (or probability kernel, or transition kernel) from $(\mathbb{W}, \mathcal{W})$ to $(\mathbb{X}, \mathcal{X})$, denoted by $(\mathbb{W}, \mathcal{W}) \overset{K}{\rightsquigarrow} (\mathbb{X}, \mathcal{X})$. Notice that when $\mathbb{W}$ and $\mathbb{X}$ are finite sets, the stochastic kernel K is in fact a matrix.

Definition 2.2.8. Let K be a probability kernel $(\mathbb{W}, \mathcal{W}) \overset{K}{\rightsquigarrow} (\mathbb{X}, \mathcal{X})$. For $f \in m\mathcal{X}_+$, we define a function on $m\mathcal{W}_+$, denoted by Kf, by the formula:

$$\forall w \in \mathbb{W},\ Kf(w) = \int_{\mathbb{X}} K(w, dx) f(x) = \langle K(w, \cdot), f \rangle.$$

The function $f \in m\mathcal{X}_+$ is not necessarily integrable with respect to the measure $K(w, \cdot)$. The function Kf is defined with values in $[0, +\infty]$ by approximating by step functions. The definition can be extended to $f \in m\mathcal{X}$ by defining $Kf = Kf^+ - Kf^-$ provided that the functions Kf^+ and Kf^- do not take simultaneously infinite values.

Definition 2.2.9. Let K be a probability kernel $(\mathbb{W}, \mathcal{W}) \overset{K}{\rightsquigarrow} (\mathbb{X}, \mathcal{X})$. For $\mu \in \mathcal{M}_+(\mathcal{W})$, we define a measure of $\mathcal{M}_+(\mathcal{X})$, denoted by μK, by the formula:

$$\forall A \in \mathcal{X},\ \mu K(A) = \int_{\mathbb{W}} \mu(dw) K(w, A) = \langle \mu, K(\cdot, A) \rangle.$$

Note that the transition kernel $(\mathbb{W}, \mathcal{W}) \overset{K}{\rightsquigarrow} (\mathbb{X}, \mathcal{X})$ acts **contravariantly** on functions and **covariantly** on measures. In the language of categories, the whole picture reads:

$$\begin{array}{ccc}
\mathcal{M}(\mathcal{W}) & \xrightarrow{\mathcal{M}(K) := K} & \mathcal{M}(\mathcal{X}) \\
\mathcal{M} \uparrow & & \uparrow \mathcal{M} \\
(\mathbb{W}, \mathcal{W}) & \overset{K}{\rightsquigarrow} & (\mathbb{X}, \mathcal{X}) \\
b \downarrow & & \downarrow b \\
b\mathcal{W} & \xleftarrow{b(K) := K} & b\mathcal{X}
\end{array}$$

Notation 2.2.10. When the space $\mathbb{X}$ is denumerable (finite or infinite), we assume that the σ-algebra $\mathcal{X}$ is the exhaustive one, i.e. $\mathcal{X} = \mathcal{P}(\mathbb{X})$. Since singletons belong obviously to this $\mathcal{X}$, we simplify notation by denoting $K(w,x) := K(w,\{x\})$. Similarly, if $\rho \in \mathcal{M}_1(\mathcal{X})$, instead of writing $\rho(\{x\})$ we simplify into $\rho(x)$. Therefore, we identify probability measures on denumerable sets with probability row [3] vectors and stochastic kernels between denumerable sets with stochastic matrices $K(w,x)$.

Example 2.2.11. (Kernel of a noisy channel). Suppose that an optical fibre connects two distant positions in a network. Inputs are digitised signals (encoded in a binary alphabet $\mathbb{A} = \{0,1\}$), and outputs are also digitised signals (encoded in a binary alphabet $\mathbb{B} \simeq \mathbb{A} = \{0,1\}$). Since transmission is through a physical device (fibre), single bits suffer a random noise. Thus a 0 input bit will be transmitted correctly to an output bit 0 with probability P_{00} and erroneously to a 1 bit with probability P_{01} (verifying of course $P_{00} + P_{01} = 1$. Similarly, input bit 1 will be transmitted correctly with probability P_{11} and erroneously with probability P_{10}. The matrix $P = (P_{ab})_{a\in\mathbb{A},b\in\mathbb{B}}$ is an archetypal example of a stochastic transformation kernel, i.e. a matrix with non-negative elements, whose every line sums up to 1, otherwise stated, every line is interpreted as a probability on the output space. The matrix elements are interpreted as conditional probabilities:

$$P_{ab} = \mathbb{P}(\text{output bit } = b | \text{input bit } = a).$$

If the input bits are randomly distributed according to the (row) probability vector ρ, then we can compute the joint input-output distribution

$$\kappa(a,b) := \mathbb{P}(\text{input bit } = a, \text{output bit } = b) = \rho(a)P_{ab}$$

and the output (row) probability vector ν as the second marginal of the joint probability: $\nu(b) = \sum_{a\in\mathbb{A}} \kappa(a,b) = \sum_{a\in\mathbb{A}} \rho(a)P_{ab}$, for $b \in \mathbb{B}$.

In the same spirit, the observation of a given output influences the distribution of the input. We can infer on this influence by computing the conditional probability

$$\mathbb{P}(\text{input bit } = a | \text{output bit } = b) = \frac{\rho(a)P_{ab}}{\nu(b)}.$$

The formula of total probability guarantees that we recover

$$\mathbb{P}(\text{input bit } = a) = \sum_b \mathbb{P}(\text{input bit } = a | \text{output bit } = b)\nu(b) = \sum_b \rho(a)P_{ab} = \rho(a),$$

i.e. the marginal probability for the input equals the probability obtained as the weighted sum of conditional probabilities given the possible outputs. The reader with basic knowledge of probability theory may wonder why we are stating such elementary facts here. The answer is "in order to stress them", because this elementary formula will not be any longer valid in the quantum case (see §2.6.2)!

3. The reason we insist in representing probabilities on a denumerable set $\mathbb{W}$ by a **row vector** is that we view probabilities as linear functionals on the vector space of real random variables: the probability measure $\rho \in \mathcal{M}_1(\mathbb{W})$ acts on the real random variable X on $\mathbb{W}$ as the duality product $\langle \rho, X\rangle = \sum_{w\in\mathbb{W}} \rho(w)X(w)$ to give the expectation of X under ρ. In other words, the space of real random variables on $\mathbb{W}$ is identified with $\mathbb{R}^{\mathbb{W}}$ and the expectation of X w.r.t. ρ is nothing else than the product of the vectors ρX.

2.3 Classical physics as a probability theory with a dynamical law

2.3.1 A motivating example: gambling with a classical die

Let $\Omega = \{1, \dots, 6\}$ and $\mathbb{X} = \{-1, 0, 1\}$, thought as finite subsets of $\mathbb{R}$ — assumed equipped with their exhaustive σ-algebras $\mathcal{F} = \mathcal{P}(\Omega)$ and $\mathcal{X} = \mathcal{P}(\mathbb{X})$, thought as sub-algebras of $\mathcal{B}(\mathbb{R})$ — and let $X(\omega) = (\omega - 1) \mod 3 - 1$ be a fixed $\mathbb{X}$-valued random variable on Ω. Think of this random variable as representing a sharp decision rule: if the die shows up face ω, the gambler irrefutably wins $X(\omega)$ €. There are various equivalent descriptions of the random variable X:

1. X can be thought as a vector of $\mathbb{X}^\Omega \subset \mathbb{R}^\Omega$:
$$X = \begin{pmatrix} -1 \\ 0 \\ 1 \\ -1 \\ 0 \\ 1 \end{pmatrix} \in \mathbb{X}^\Omega \subset \mathbb{R}^\Omega.$$
2. Plotting the graph of X, as in figure 2.1, we observe that the graph is also equivalent to the matrix $K \in \mathbb{M}_{|\Omega|\times|\mathbb{X}|}(\{0,1\})$ with elements
$$K = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{with elements} \quad K(\omega, x) = \begin{cases} 1 & \text{if } X(\omega) = x \\ 0 & \text{otherwise.} \end{cases}$$
We see immediately that K is a stochastic matrix (kernel), i.e. for all ω, the ω^{th} line sums up to 1, i.e. $\sum_{x\in\mathbb{X}} K(\omega, x) = 1$. The significance of its matrix elements is of the **conditional probability**
$$K(\omega, x) = \mathbb{P}(\text{gain } = x | \text{ die shows face } \omega).$$
Additionally, the stochastic matrix is of a very special type: in every line, there is exactly one element that is 1, all other elements being 0. Such a stochastic kernel is termed **deterministic stochastic kernel**. We have thus established that a $\mathbb{X}$-valued random variable on Ω is equivalent to a deterministic stochastic kernel K between Ω and $\mathbb{X}$; we denote it by K_X if we wish to stress its equivalence to X.
3. The matrix $K := K_X$ has $|\mathbb{X}|$ columns. Denote by $E[x]$ its x^{th} column (we may write $E_X[x]$ instead of $E[x]$ when we wish to stress that E is a column of the stochastic matrix K_X stemming from the random variable X). Then $E[x]$ is a vector in $\{0,1\}^\Omega \subset \mathbb{R}^\Omega$, i.e. a random variable. The value $E[x](\omega) = \mathbb{1}_{X^{-1}(x)}(\omega)$ represents the decision (yes or no) to the question "does the gambler win x?" taken whenever the die shows up ω. There are some useful identities that we can obtain:

(a) It is immediate to see that the random variable X is reconstructed from the collection of elementary questions $(E[x])_{x\in\mathbb{X}}$ through the formula $X = \sum_{x\in\mathbb{X}} E[x]x$, meaning that for every $\omega \in \Omega$, we have

$$X(\omega) = \sum_{x\in\mathbb{X}} \mathbb{1}_{X^{-1}(x)}(\omega)X(\omega) = \sum_{x\in\mathbb{X}} E_X[x](\omega)x = \sum_{x\in\mathbb{X}} K_X(\omega, x)x.$$

These identities establish the fact that the datum X is equivalent to K_X and to the collection $(E[x])_{x\in\mathbb{X}}$.

(b) Let $(\varepsilon_x)_{x\in\mathbb{X}}$ be the canonical basis of $\mathbb{R}^{\mathbb{X}}$ (written as row vectors), i.e.

$$\varepsilon_{-1} = (1, 0, 0),\ \varepsilon_0 = (0, 1, 0),\ \text{and}\ \varepsilon_1 = (0, 0, 1).$$

These row vectors are probability vectors on $\mathbb{X}$ and as a matter of fact the extreme points of the convex set of probability vectors in $\mathcal{M}_1(\mathbb{X})$. We can now reconstruct K as [4]

$$K = \sum_{x\in\mathbb{X}} E[x] \otimes \varepsilon_x,$$

meaning that for all $(\omega, A) \in \Omega \times \mathcal{X}$, we have

$$K(\omega, A) = \sum_{x\in\mathbb{X}} E[x](\omega)\varepsilon_x(A) = \sum_{x\in A} K(\omega, x).$$

(Recall that K has been defined as a random variable w.r.t. its first argument and as a probability measure w.r.t. its second).

4. Since K represents a conditional probability, if $\rho \in \mathcal{M}_1(\Omega)$ is given (as a row vector of $\mathbb{R}^{\Omega}$), then we can compute the joint probability on $\Omega \times \mathbb{X}$ by:

$$\mathbb{P}(\text{die shows face } \omega,\ \text{gambler wins } x) = \rho(\omega)K(\omega, x).$$

From this formula follow

(a) the second marginal, i.e. the probability on $\mathbb{X}$:

$$\begin{aligned}\mathbb{P}(\text{gambler wins } x) = \nu_X^{\rho}(x) &= \sum_{\omega\in\Omega} \rho(\omega)K(\omega, x) = \sum_{\omega\in\Omega} \rho(\omega)E[x](\omega) \\ &= \langle \rho, E[x]\rangle = \rho E[x] = \mathbb{E}(E[x]),\end{aligned}$$

(b) the expectation of $E[x]$

$$\mathbb{E}(E[x]) = \sum_{\omega\in\Omega} \rho(\omega)E[x](\omega) = \sum_{\omega\in\Omega} \rho(\omega)K(\omega, x) = \nu_X^{\rho}(x),$$

4. The symbol $\otimes$ stands for the tensor product. For $A \in \mathbb{M}_{m,n}(\mathbb{C})$ and $B \in \mathbb{M}_{p,q}(\mathbb{C})$, the tensor product is the matrix $A \otimes B \in \mathbb{M}_{mp,nq}(\mathbb{C})$ that can be written in block form as

$$A \otimes B := \begin{pmatrix} A_{11}B & \dots & A_{1n}B \\ \vdots & \vdots & \vdots \\ A_{m1}B & \dots & A_{mn}B \end{pmatrix} \neq \begin{pmatrix} AB_{11} & \dots & AB_{1q} \\ \vdots & \vdots & \vdots \\ AB_{p1} & \dots & AB_{pq} \end{pmatrix} = B \otimes A.$$

More precisely, the matrix elements of $A \otimes B$ are given by $(A \otimes B)_{rs} = A_{ij}B_{kl}$, where $r = (i-1)p + k$, for $1 \leq k \leq p$ and $s = (j-1)q + l$, for $1 \leq l \leq q$ and $1 \leq i \leq m$, $1 \leq j \leq n$. More details about tensor products are given in §3.8.

(c) the expectation of X

$$\begin{aligned}\mathbb{E}X &= \sum_{\omega\in\Omega}\rho(\omega)\sum_{x\in\mathbb{X}}E[x](\omega)x = \sum_{\omega\in\Omega}\rho(\omega)\sum_{x\in\mathbb{X}}K(\omega,x)x\\ &= \sum_{x\in\mathbb{X}}\rho K_X(x)x = \sum_{x\in\mathbb{X}}\nu_X^\rho(x)x,\end{aligned}$$

(d) the reverse conditional law [5]

$$\mathbb{P}(\text{die shows face }\omega|\text{ gambler won }x) = \frac{\rho(\omega)E[x](\omega)}{\langle\rho, E[x]\rangle},$$

(e) the formula of total probability

$$\begin{aligned}\mathbb{P}(\text{die shows face }\omega) &= \sum_{x\in\mathbb{X}}\mathbb{P}(\text{die shows face }\omega|\text{ gambler won }x)\mathbb{P}(\text{gambler won }x)\\ &= \sum_{x\in\mathbb{X}}\frac{\rho(\omega)E[x](\omega)}{\langle\rho, E[x]\rangle}\langle\rho, E[x]\rangle = \rho(\omega).\end{aligned}$$

The profound meaning of this formula is that **the observation of the output leaves the initial state of the system unchanged.**

5. Denote by O and I the "zero" and "one" random variables respectively, defined by $O(\omega) = 0$ and $I(\omega) = 1$; obviously we have $O \leq E[x] \leq I$ component-wise. If A is an arbitrary subset of $\mathbb{X}$ we write $E[A] = \sum_{x\in A}E[x]$, with $E[\mathbb{X}] = I$ and $E[\emptyset] = O$; if $A\cap B = \emptyset$, then $E[A\sqcup B] = E[A] + E[B]$. As a matter of fact, E is a probability measure taking as values random variables (of a particular type, i.e. random variables that are indicators). Finally $E[A]^2 = E[A]$ (where the square is computed component-wise); therefore $(E[A])_{A\in\mathcal{X}}$ are projections.
6. The random variables $(E[x])_{x\in\mathbb{X}}$ appearing in the above resolution of unity are called **sharp classical effects**. The corresponding random variable $X = \sum_{x\in\mathbb{X}}E[x]$, or equivalently its kernel K (or equivalently the collection of questions $(E[x])_{x\in\mathbb{X}}$), is called a **sharp classical observable**. (See precise definition 2.3.5 below).

Exercise 2.3.1. Denote by A, B, and C three coins: coin A is honest, coin B gives 1 with probability $1/3$ and coin B with probability $7/8$. We toss coin A. If it shows 0, then the second toss is performed again with coin A, else with coin B. If the two tosses have shown equal faces, i.e. if 00 or 11 has occurred, the third tossing is performed with coin C, else with coin A. Let Ω denote the minimal space allowing to model the face outcomes during this experiment.

1. Give precisely Ω (assumed to be equipped with its exhaustive σ-algebra $\mathcal{F}$).
2. Determine the probability vector $\rho\in\mathcal{M}_1(\Omega,\mathcal{F})$ induced by this experiment.
3. Let $X:\Omega\to\mathbb{X} := \{0,1,2,3\}$ be random variable counting the number of 1's. Determine the stochastic kernel K describing this variable.
4. Determine the effects $(E[x])_{x\in\mathbb{X}}$.
5. Determine the probability vector ν_X^ρ.
6. Determine the conditional probability $\rho_x(\cdot)$.

5. We can write $\rho(\omega)E[x](\omega) = E[x](\omega)\rho(\omega)E[x](\omega)$ beacause $E[x](\omega)\in\{0,1\}$, hence $E[x]^2 = E[x]$. The last form will be shown formally equivalent to the form we shall obtain in the quantum case.

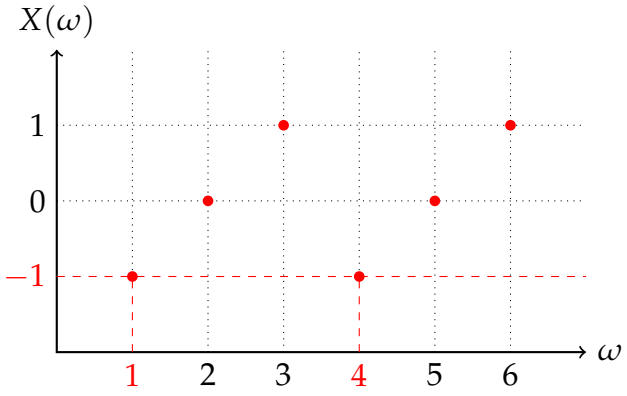


Figure 2.1 – The non-zero elements of the matrix K are depicted as coloured dots. The answer to the question $E[-1]$ (i.e. does the random variable X take the value -1?) is the yes-no-valued random variable $\mathbb{1}_F$, with $F = X^{-1}(\{-1\}) = \{1,4\}$. Obviously, the collection $(E[x])_{x\in\mathbb{X}}$ provides with a partition of unity because $\int_{\mathbb{X}} E[dx] := \sum_{x\in\mathbb{X}} E[x] = E[\mathbb{X}] = \mathbb{1}_\Omega = I$ on Ω.

Exercise 2.3.2. The component-wise partial ordering in the set of indicator-valued random variables $\{0,1\}^\Omega$ (defined by $A \leq B \Leftrightarrow A(\omega) \leq B(\omega), \forall\omega \in \Omega$) turns the set $\{0,1\}^\Omega$ into a partially ordered set or **poset** (for details see chapter 13). For the case $|\Omega| = 3$, propose an arrangement of the elements of $\{0,1\}^\Omega$ on a plane so that the order relation among them becomes *graphically* visible. What is the role played by the random variables O and I?

The ideas developed in the previous paragraph can be extended to arbitrary random variables provided they are defined and take values on adequate measurable spaces. The example 2.3.3 suggests that a bijection between arbitrary random variables and deterministic stochastic kernels prevails in the case $(\Omega,\mathcal{F}) \simeq (\mathbb{X},\mathcal{X}) \simeq (\mathbb{R},\mathcal{B}(\mathbb{R}))$ or more generally whenever these spaces are standard Borel spaces (i.e. isomorphic to Polish spaces).

Example 2.3.3. *(Approximating a measurable function).* Let $(\Omega,\mathcal{F}) \simeq (\mathbb{X},\mathcal{X}) \simeq (\mathbb{R},\mathcal{B}(\mathbb{R}))$ and $X : \Omega \to \mathbb{X}$ a bounded Borel function. Standard integration theory states that X can be approximated by simple functions. More precisely, for every $\varepsilon > 0$, there exists a finite family $(F_i)_i$ of disjoint measurable sets $F_i \in \mathcal{F}$ and a finite family of real numbers $(x_i)_i$ such that $|X(\omega) - \sum_i x_i \mathbb{1}_{F_i}(\omega)| < \varepsilon$ for all $\omega \in \Omega$.

It is instructive to recall the main idea of the proof of this elementary result. Let $m = \inf X(\omega)$, $M = \sup X(\omega)$, and subdivide the interval $[m,M]$ into a finite family of disjoint intervals $(A_j)_j$, with $|A_j| < \varepsilon$ (see figure 2.2).

For each j, select an arbitrary $x_j \in A_j$; in the subset $X^{-1}(A_j) \in \mathcal{F}$, the values of X lie within ε from x_j. Therefore, we get the desired result by setting $F_j = X^{-1}(A_j)$. If for every Borel set $A \in \mathcal{X}$, we define $E[A] = \mathbb{1}_{X^{-1}(A)}$ (this is a random variable!), the approximation result can be rewritten as

$$|X(\omega) - \sum_j x_j E[A_j](\omega)| < \varepsilon,\ \forall\omega \in \Omega.$$

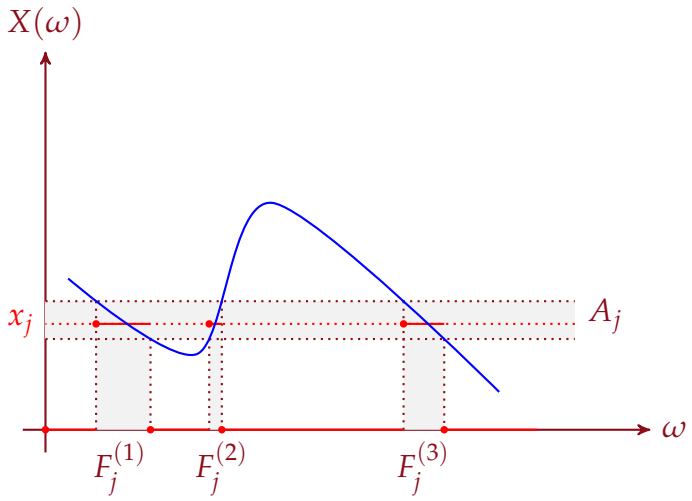


Figure 2.2 – The approximation of a bounded measurable function X by simple functions. Observe that $X^{-1}(A_j) = F_j^{(1)} \cup F_j^{(2)} \cup F_j^{(3)} = F_j$. In the figure, we depict the summand $E[A_j]x_j$ of the decomposition $X = \sum_j E[A_j]x_j$. For any $x_j \in A_j$ and any $\omega \in F_j$ we have $|X(\omega) - x_j| < \varepsilon$.

Now, E is a set function-valued random variable (a probability measure-valued random variable actually) and the sum $\sum_j E[A_j]x_j$ tends to $\int E[dx]x$. More precisely, the function X is equivalent to the deterministic stochastic kernel K from $(\Omega, \mathcal{F})$ to $(\mathbb{R}, \mathcal{B}(\mathbb{R}))$, defined by the formula

$$\Omega \times \mathcal{B}(\mathbb{R}) \ni (\omega, A) \mapsto K(\omega, A) = E[A](\omega) = \mathbb{1}_{X^{-1}(A)}(\omega) = \varepsilon_{X(\omega))}(A) = \varepsilon_\omega(X^{-1}(A)).$$

The kernel K acts (to the right) on positive measurable functions g defined on $\mathbb{X}$ by:

$$Kg(\omega) = \int_{\mathbb{X}} K(\omega, dx)g(x) = \int_{\mathbb{X}} E[dx](\omega)g(x) = \int_{\mathbb{X}} \varepsilon_{X(\omega)}(dx)g(x) = g(X(\omega)).$$

In particular, if $g = \mathrm{id}$ then we recover the formula $X = \int_{\mathbb{X}} E[dx]x$ established above.

If the space $(\Omega, \mathcal{F})$ carries a probability measure $\mathbb{P}$, then the space $(\mathbb{X}, \mathcal{X})$ acquires also a probability measure $\mathbb{P}_X$, the law of X, determined through the standard transport formula

$$\mathbb{P}_X(A) = \mathbb{P}K(A) = \int_\Omega \mathbb{P}(d\omega)K(\omega, A) = \int_\Omega \mathbb{P}(d\omega)E[A](\omega) = \mathbb{E}(E[A]).$$

That means that the law $\mathbb{P}_X$ is disintegrated into $\int_\Omega \mathbb{P}(d\omega)K(\omega, A)$, i.e. conditioning arises as disintegration. Assuming that the spaces $(\Omega, \mathcal{F})$ and $(\mathbb{X}, \mathcal{X})$ are standard Borel spaces, the existence of a disintegration in terms of the conditional probabilities encoded in K_X is proven in [35, theorems 1 and 2].

We are now in position to proceed with the general case.

Remark 2.3.4. As stressed in remark 2.2.3, the pertinent property in the defintion of a random variable X is the measurability of the map $X : \Omega \to \mathbb{X}$. Suppose that the

$\mathcal{X}$ contains all singletons. It is then elementary to show [32] that the datum of X is equivalent to the datum of a **deterministic Markovian kernel** $K_X : \Omega \times \mathcal{X} \to [0,1]$ such that $K_X(\omega, A) = \varepsilon_{X(\omega)}(A) = \mathbb{1}_{X^{-1}(A)}(\omega) = \mathbb{1}_A(X(\omega))$. The kernel $K := K_X$ acts to the right on the vector space $b\mathcal{X}$: $b\mathcal{X} \ni f \mapsto Kf \in b\mathcal{F}$ the right hand side being defined by the formula

$$Kf(\omega) := \int_{\mathbb{X}} K(\omega, dx) f(x) \in b\mathcal{F},\ \forall \omega \in \Omega,$$

and to the left on the convex set $\mathcal{M}_1(\mathcal{F})$, by

$$\mathcal{M}_1(\mathcal{F}) \ni \mu \mapsto \mu K(A) := \int_{\Omega} \mu(d\omega) K(\omega, A) \in \mathcal{M}_1(\mathcal{X}),\ \forall A \in \mathcal{X}.$$

Now for every $A \in \mathcal{X}$, the kernel $K(\cdot, A)$ is a random variable defined on $(\Omega, \mathcal{F})$. On denoting $E[A] := E_X[A]$ the random variable [6] defined by

$$E[A](\omega) := K(\omega, A) = \mathbb{1}_A(X(\omega)) = \mathbb{1}_A \circ X(\omega), A \in \mathcal{X},$$

we verify that the set function defined on $\mathcal{F} = \mathcal{B}(\mathbb{R})$ by

$$\mathcal{B}(\mathbb{R}) \ni A \mapsto E[A] = \mathbb{1}_{X^{-1}(A)} \in b\mathcal{F}$$

is positive, majorised by $E[\mathbb{X}] = I$, where I is the constant 1 random variable $I(\omega) = 1$, and by monotone convergence σ-additive. Hence, $E[\cdot]$ is a random-variable-valued probability. Morover, E has the following properties

1. E is multiplicative: i.e. $E[B \cap C] = E[B]E[C]$ for all $B, C \in \mathcal{B}(\mathbb{R})$ (hence E is idempotent),
2. E is supported by $\mathsf{Ran}(X)$: i.e. $E[A] \equiv 0$ for all $A \in \mathcal{B}(\mathbb{R})$ such that $A \cap \mathsf{Ran}(X) = \emptyset$.

Therefore E is a projection and, in particular, from 2, if $B \cap C = \emptyset$ then $E[B]E[C] = 0$.

2.3.2 Sharp classical effects and observables

Definition 2.3.5. Let $(\Omega, \mathcal{F})$ be an abstract measurable space and $(\mathbb{R}, \mathcal{B}(\mathbb{R}))$ the concrete Borel space on the reals.

1. Define a set function [7] $E : \mathcal{B}(\mathbb{R}) \to b\mathcal{F}$ by

$$\mathcal{B}(\mathbb{R}) \ni A \mapsto E[A] \in \{0,1\}^{\Omega} \subset b\mathcal{F}$$

such that E is

(a) normalised: $E[\mathbb{R}] = I$.
(b) multiplicative: $E[B \cap C] = E[A]E[B]$ (hence idempotent: $E[A]^2 = E[A]$ for all Borel sets A).

6. We use this special notation to remind constantly to the reader that $E[A]$ is still a function — a random variable actually — that must be evaluated at a given point ω to give the number $E[A](\omega) \in \{0,1\}$.

7. This function verifies, for all $A \in \mathcal{B}(\mathbb{R})$, the inequalities $O \leq E[A] \leq I$ (the inequalities holding component-wise).

(c) σ-additive: for any disjoint sequence $(A_n)_{n\in\mathbb{N}}$ of Borel sets, we have $E[\sqcup_{n\in\mathbb{N}} A_n] = \sum_{n\in\mathbb{N}} E[A_n]$,

The probability measure E on$(\mathbb{R}, \mathcal{B}(\mathbb{R}))$ — defined above — taking as values $\{0,1\}$-valued random variables, is called a **sharp classical effect** over $(\Omega, \mathcal{F})$. The set of sharp classical effects over $(\Omega, \mathcal{F})$ is denoted by $\mathbf{E}_s(\Omega, \mathcal{F})$. If $E \in \mathbf{E}_s(\Omega, \mathcal{F})$ is a fixed sharp classical effect, then $X = \int_{\mathbb{R}} E[dx]x$ defines a real valued random variable on $(\Omega, \mathcal{F})$ by $X(\omega) = \int_{\mathbb{R}} E[dx](\omega)x$. Such a random variable is called a **sharp classical observable**. The set of sharp classical observables over $(\Omega, \mathcal{F})$ is denoted by $\mathbf{O}_s(\Omega, \mathcal{F})$; it is isomorphic to the vector space $\mathbb{R}^\Omega$.

2. If $E \in \mathbf{E}_s(\Omega, \mathcal{F})$ is a fixed sharp classical effect (or equivalently X a sharp classical observable), the stochastic kernel defined in the previous item, can be reconstructed [8] as $K = \int_{\mathbb{R}} E[dx] \otimes \varepsilon_x$. Since deterministic kernels are in bijection with random variables, the kernel is also called sharp classical observable.
3. Reciprocally, when a real valued random variable X is given on $(\Omega, \mathcal{F})$, then there exists a sharp effect E associated with X defined by $E[A] = \mathbb{1}_{X^{-1}(A)}$.
4. If X is the observable associated with the effect E, then the measure E is supported by the set of outcomes $\mathbb{X} = \mathsf{im}(X) = X(\Omega)$, i.e. $E[A] = O$ for all Borel sets A, such that $A \cap \mathsf{im}(X) = \emptyset$.

The quantity $E[A]$ appears in various disciplines; what renders it a little mysterious is that every discipline uses a different term for it. Depending on the context, $E[A]$ is called

— a **question** or a **sharp effect** or a **yes-no experiment** (in quantum mechanics) because the random variable $E[A]$ can be interpreted as questioning whether the event $\{X \in A\}$ occurs and its possible values (answers) are 0 or 1,
— a **projective resolution of the identity** (in measure theory) since $E[A]^2 = E[A]$ for all $A \in \mathcal{B}(\mathbb{R})$ (hence it is a projection) and $\int_{\mathbb{R}} E[dx] = E[\mathbb{R}] = I$, where I is the constant random variable defined by $I(\omega) = 1$ for all $\omega \in \Omega$ (hence it is a resolution of identity),
— a **spectral projection** (in functional analysis) because it is a projection and its "spectral" nature will become apparent later (see a simple example in the subparagraph *Interpretation of postulate* 2.6.4 and a more general development in §12.5),
— a **deterministic decision rule** (in mathematical statistics) for reasons that will become apparent later (see question 2 of exercise 2.5.3),
— a **crisp set** (in fuzzy logic); since for all $A \in \mathcal{B}(\mathbb{R})$, the indicator-function-valued probability $E[A]$ can be interpreted as the membership in the set A, the set A is a crisp set. (See remark 2.3.9 below).

2.3.3 Unsharp classical effects and observables

This paragraph is a motivation for the notions of unsharp quantum effects and observables introduced in page 52. In quantum cryptography, contrary to classical one, an eavesdropper intrusion in the communication channel disturbs necessarily the

8. The meaning of this formula is that when applied on $(\omega, A) \in \Omega \times \mathcal{X}$, we get $K(\omega, A) = \int_{\mathbb{X}} E[dx](\omega)\varepsilon_x(A)$.

transmitted message; to analyse precisely the relationship between information gain and induced disturbance the notion of quantum unsharp effect is needed. Since these notions will not be used before §6.5, this paragraph can be omitted in first reading.

Suppose now that K is a genuine (non-deterministic) stochastic kernel between $(\Omega, \mathcal{F})$ and $(\mathbb{X}, \mathcal{X})$, i.e. for every $\omega \in \Omega$, the probability $K(\omega, \cdot) \in \mathcal{M}_1(\mathcal{X})$ is not extremal. We can again consider for each $A \in \mathcal{X}$ the random variable $E[A]$ defined by $E[A](\omega) = K(\omega, A)$. For $\mathbb{X} \subset \mathbb{R}$ and $\mathcal{X} \subseteq \mathcal{B}(\mathbb{R})$, the map $E : \mathcal{B}(\mathbb{R}) \to b\mathcal{F}$ defined by

$$\mathcal{B}(\mathbb{R}) \ni A \mapsto E[A] \in [0,1]^{\Omega} \subset b\mathcal{F}$$

verifies the properties of a sharp effect *but* multiplicativity (hence projection).

Definition 2.3.6. Let $(\Omega, \mathcal{F})$ be an abstract measurable space and $(\mathbb{R}, \mathcal{B}(\mathbb{R}))$ the concrete Borel space on the reals.

1. Define a set function E by

   $$\mathcal{B}(\mathbb{R}) \ni A \mapsto E[A] \in b\mathcal{F}$$

   verifying $O \leq E[A] \leq I$ for all $A \in \mathcal{B}(\mathbb{R})$ such that
   (a) E is normalised: $E[\mathbb{R}] = I$.
   (b) E is supermultiplicative: $E[A \cap B] \geq E[A]E[B]$ (hence powers are contracting: $E[A]^2 \leq E[A]$ for all Borel sets A).
   (c) E is σ-additive: for any disjoint sequence $(A_n)_{n\in\mathbb{N}}$ of Borel sets, we have $E[\sqcup_{n\in\mathbb{N}} A_n] = \sum_{n\in\mathbb{N}} E[A_n]$,

   The probability measure E defined on $(\Omega, \mathcal{F})$ taking as values $[0,1]$-valued random variables is called a **(unsharp) classical effect** over $(\Omega, \mathcal{F})$. The set of classical effects over $(\Omega, \mathcal{F})$ is denoted by $\mathbf{E}(\Omega, \mathcal{F})$, with $\mathbf{E}_s(\Omega, \mathcal{F}) \subset \mathbf{E}(\Omega, \mathcal{F})$.
2. With any fixed classical effect $E \in \mathbf{E}(\Omega, \mathcal{F})$ we can associate a genuine (generally non-deterministic) stochastic kernel K, defined by $K = \int_{\mathbb{R}} E[dx] \otimes \varepsilon_x$. (The meaning of this formula is that when applied on $(\omega, A) \in \Omega \times \mathcal{B}(\mathbb{R})$, we get $K(\omega, A) = \int_{\mathbb{R}} E[dx](\omega)\varepsilon_x(A)$). The kernel K is termed an $\mathbb{R}$-valued **(unsharp) classical observable**. The set of classical observables over $(\Omega, \mathcal{F})$ is denoted by $\mathbf{O}(\Omega, \mathcal{F})$.

Remark 2.3.7. If $E \in \mathbf{E}(\Omega, \mathcal{F}) \setminus \mathbf{E}_s(\Omega, \mathcal{F})$, the random variable $X = \int_{\mathbb{X}} E[dx]x$ — provided that the function $x \mapsto x$ is integrable with respect to the probability E — can again be constructed. Nevertheless, X **is not** any longer in bijection with $K = \int_{\mathbb{R}} E[dx] \otimes \varepsilon_x$; instead, X is corresponds to a conditional expectation (see exercise 2.3.8).

Exercise 2.3.8. (Gambling with a die according to a randomised decision rule). Consider the spaces Ω and $\mathbb{X}$ introduced in §2.3.1 but with a genuine stochastic matrix [9]

$$K = \begin{pmatrix} 2/3 & 0 & 1/3 \\ 0 & 1 & 0 \\ 1/3 & 0 & 2/3 \\ 2/3 & 0 & 1/3 \\ 0 & 1 & 0 \\ 1/3 & 0 & 2/3 \end{pmatrix} \text{ leading to the effects } E[-1] = \begin{pmatrix} 2/3 \\ 0 \\ 1/3 \\ 2/3 \\ 0 \\ 1/3 \end{pmatrix}, E[0] = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, E[1] = \begin{pmatrix} 1/3 \\ 0 \\ 2/3 \\ 1/3 \\ 0 \\ 2/3 \end{pmatrix}.$$

9. Think of a randomised decision rule as induced by an experimental uncertainty. Suppose that every time the die is thrown, a LED display marks $-1, 0$, or 1, but the $-$ sign LED of the display is defunct: when a $-$ sign must be displayed, with probability $1/3$ the LED stays off, and conversely, when it must not be displayed with probability $1/3$ the LED turns on.

1. Determine the random variable $X = \sum_{x\in\mathbb{X}} E[x]x$.
2. Determine the deterministic stochastic kernel L associated with X and verify that $L \neq K$.
3. Show that along with the column decomposition $K = \sum_{x\in\mathbb{X}} E[x] \otimes \varepsilon_x$, we can also decompose K line-wise: $K = \sum_{\omega\in\Omega} e_\omega \otimes \nu[\omega]$, where $\nu[\omega]$ is the row probabilty vector on $\mathbb{X}$ associated with the ω^{th} line of K and $e_\omega \in \mathbb{R}^\Omega$ the ω^{th} column unit vector of $\mathbb{R}^\Omega$.
4. Use the previous line decomposition of K to interpret the values $-1, 0, 1$ as a randomised gain G corresponding to the gambling with this die.
5. Show that $X = \mathbb{E}(G|\mathcal{F})$.

Remark 2.3.9. In set theory, a (crisp) set A is a precisely determined collection of elements, i.e. for any a, we can unambiguously determine whether it belongs to A or not. It is therefore clear that a set A can be *identified* with its indicator $\mathbb{1}_A$, taking values in $\{0, 1\}$. The sharp effects being precisely indicators, they correspond to a crisp delimitation of the indexing set A.

Now, when sets are used to model physical objects, things may be less clear-cut than the previous situation. Think, for instance, of the atmosphere: it is usually stated that the atmosphere is a thin [10] gaseous mantle with a thickness of 10 km above Earth's surface. Does it mean that a molecule of oxygen at 9999.9999 m from the surface belongs to the atmosphere and another at 10000.0001 m not? If you have some doubts look at the photograph 2.3 of a sunset taken from ISS and read carefully the caption of that figure.

Figure 2.3 – Photograph of a sunset taken from the International Space Station. The atmosphere is the blueish mantle above the Earth's surface. Instead of a membership function associated with an indicator falling sharply from 1 to 0, a more appropriate description of the membership function is that of a function falling smoothly from 1 to 0, the point where its value is 1/2 corresponding to approximately a distance of 10 km from Earth. Identification of a (fuzzy) set with its smooth membership function is known as **fuzzification**.

In summarising, any sharp classical observable X on $(\Omega, \mathcal{F}, \rho)$ is associated with a projection-valued probability measure (PVM) $E := E_X$ supported by the set $\mathbb{X} = X(\Omega)$, also known as the **spectrum** of X. Conversely, any PVM E supported on some set $\mathbb{X} \subseteq \mathbb{R}$ uniquely determines a sharp classical observable X. Therefore, for classical sharp

10. Its thickness of 10 km must be compared with the radius of the Earth, ca. 6000 km.

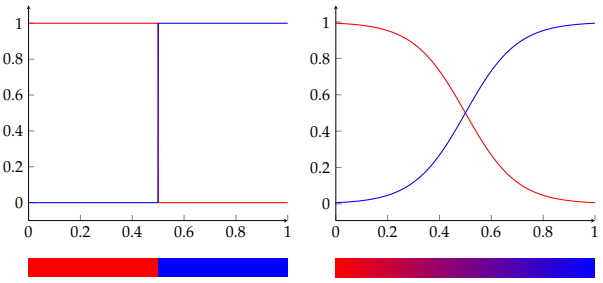


Figure 2.4 – Example of sharp (left) and fuzzy (right) effects $(E[c])_{c\in\{\text{red, blue}\}}$ on $\Omega = [0,1]$.

observables, X and the corresponding PVM E_X are both called abusively sharp classical observables. Unsharp classical observables on the contrary are merely defined in terms of their stochastic kernel (or equivalently in terms of the corresponding unsharp effect E that is a positive random variable valued measure. This distinction will remain valid in the quantum case.

2.3.4 Postulates for classical systems

To describe a physical system, we need a scene on which the system is physically realised and where all legitimate questions we can ask about the system receive definite answers. This scene is called phase space in classical physics. Nevertheless, the only objects having physical pertinence are the family of questions we can formulate about the system and the answers we receive in some very precise preparation of the system. From this conceptual view, the classical phase space shares the same indeterminacy as the probability space. The only objects having physical relevance are the physical observables (as is the case for random variables in probability theory). In the same way a random variable is determined merely through its space of outcomes and its law, a given physical system can be described by different phase spaces; if the questions formulated about the system are identically answered within the two descriptions, then we say the system admits different but mathematically equivalent physical realisations.

Example 2.3.10. (Dice rolling by the mathematician) Let the physical system be a die and the complete set of questions to be answered the family $(E[x])_{x=1,\dots,6}$ where $E[x]$ stands for the question: "When the die lies at equilibrium on the table, does the top face read x?" An obvious choice for the phase space is $\Omega = \{1,\dots,6\}$. The random variable X corresponding to the physical observable "value of the top face" is realised by $X(\omega) = \omega, \omega \in \Omega$, the questions read then $E[x] = \mathbb{1}_{\{X=x\}}$, for $x = 1,\dots,6$, and $X = \sum_{x\in\mathbb{X}} E[x]x$.

Example 2.3.11. (Dice rolling by the layman) Consider the same space of outcomes as in example 2.3.10 and the same set of questions but think of the die as a solid body that can evolve in the space. To completely describe its state, we need 3 coordinates for its barycentre, 3 coordinates for the velocity of the barycentre, 3 coordinates for the angular velocity, and the direction of the unit exterior normal at the centre of face "6". Thus, $\Omega = \mathbb{R}^9 \times \mathbb{S}^2$. Now the realisation $X : \Omega \to \{1,\dots,6\}$ is much more involved (but still possible in principle) and the questions are again represented by

$E[x] = \mathbb{1}_{\{X=x\}}$, for $x = 1, \ldots, 6$. Additionally, again $X = \sum_{x\in\mathbb{X}} E[x]x$, but we don't even dare to write down the explicit function $X : \Omega \to \mathbb{X}$ realising this experiment. Yet, the phase spaces given here and given in example 2.3.10 provide us with two different but mathematically equivalent physical realisations of the system "die".

Postulate 2.3.12 (Phase-space)**.** *The **phase space** of a classical system is an abstract measurable space $(\Omega, \mathcal{F})$. Events of this space correspond to measurable sets $F \in \mathcal{F}$. When two systems, respectively described by $(\Omega_1, \mathcal{F}_1)$ and $(\Omega_2, \mathcal{F}_2)$ are merged and considered as a single system, their phase space is $(\Omega_1 \times \Omega_2, \mathcal{F}_1 \otimes \mathcal{F}_2)$, where $\mathcal{F}_1 \otimes \mathcal{F}_2$ is the σ-algebra generated by $\mathcal{F}_1 \times \mathcal{F}_2$.*

Before continuing with the postulates, it is instructive to study the convexity properties of the set of probability measures $\mathcal{M}_1(\Omega, \mathcal{F})$. Obviously, it is a **convex set**, i.e. of $\mu_1, \mu_2 \in \mathcal{M}_1(\Omega, \mathcal{F})$ and $\alpha \in [0, 1]$ then $\mu = \alpha\mu_1 + (1-\alpha)\mu_2 \in \mathcal{M}_1(\Omega, \mathcal{F})$.

Definition 2.3.13. A probability $\mu \in \mathcal{M}_1(\Omega, \mathcal{F})$ is called **extremal** if it cannot be non-trivially written as a convex combination of other probability measures, i.e. if $\mu = \alpha\mu_1 + (1-\alpha)\mu_2 \in \mathcal{M}_1(\Omega, \mathcal{F})$ with some $\alpha \in]0, 1[$, then necessarily $\mu_1 = \mu_2 = \mu$. The set of extremal points is denoted by $\partial_e\mathcal{M}_1(\Omega, \mathcal{F})$ or extr $\mathcal{M}_1(\Omega, \mathcal{F})$.

The following lemma gives a practical method to test extremality.

Lemma 2.3.14. *A probability μ is extremal if, and only if, for all $F \in \mathcal{F}$ we have $\mu(F) \in \{0, 1\}$.*

Proof. [$\Leftarrow$:] Suppose that for all $F \in \mathcal{F}$ we have $\mu(F) \in \{0, 1\}$ and μ is non-trivially decomposable $\mu = \alpha\mu_1 + (1-\alpha)\mu_2$ for some $\alpha \in]0, 1[$ and $\mu_1, \mu_2 \in \mathcal{M}_1(\Omega, \mathcal{F})$. Now, if F is such that $\mu(F) = 0$, then $0 = \mu(F) = \alpha\mu_1(F) + (1-\alpha)\mu_2(F)$ and both terms in the last part of the equality are non-negative. Hence both must vanish and since neither α nor $1-\alpha$ vanish, it must be $\mu_1(F) = \mu_2(F) = \mu(F) = 0$. If F is such that $\mu(F) = 1$, then again the equality $1 = \mu(F) = \alpha\mu_1(F) + (1-\alpha)\mu_2(F)$ can be satisfied only if $\mu_1(F) = \mu_2(F) = \mu(F) = 1$ because both α and $1-\alpha$ are strictly less than 1. In summarising, for every $F \in \mathcal{F}$, we have $\mu_1(F) = \mu_2(F) = \mu(F)$, concluding to the extremality of μ.

[$\Rightarrow$:] If $\mu \in \partial_e\mathcal{M}_1(\Omega, \mathcal{F})$, without verifying $\mu(F) \in \{0, 1\}$ for every $F \in \mathcal{F}$, then there exists some F_0 with $0 < \alpha := \mu(F_0) < 1$. Define then for all $F \in \mathcal{F}$,

$$\mu_1(F) = \frac{1}{\mu(F_0)}\mu(F \cap F_0) \quad \text{and} \quad \mu_1(F) = \frac{1}{1-\mu(F_0)}\mu(F \cap F_0^c).$$

With these definitions, we can write $\mu(F) = \alpha\mu_1(F) + (1-\alpha)\mu_2(F)$ for all $F \in \mathcal{F}$, with $\alpha \in]0, 1[$. Now $\mu_1(F_0) = 1$ while $\mu_2(F_0) = 0$ meaning that $\mu_1 \neq \mu_2$ and we have a non-trivial convex decomposition of μ. But this constitutes a contradiction because μ has been supposed extremal.

□

Corollary 2.3.15. *We have that $\{\varepsilon_\omega, \omega \in \Omega\} \subseteq \partial_e\mathcal{M}_1(\Omega, \mathcal{F})$.*

Nevertheless, we have not the converse inclusion in general. For instance consider the case where $\mathcal{F} = \{\emptyset, F, F^c, \Omega\}$ with $|F| \geq 2$ and $|F^c| \geq 2$. Then the probability verifying $\mu(F) = 1$ and $\mu(F^c) = 0$ is extremal but it cannot be written as a Dirac mass.

The following proposition gives the conditions under which the reverse inclusion holds.

Proposition 2.3.16. *If $\mathcal{F}$*

1. *is separable — or denumerably generated — (i.e. there exists a sequence*[11] *$(F_n)_{n\in\mathbb{N}}$ such that $\mathcal{F} = \sigma\{F_n, n \in \mathbb{N}\}$) and*
2. *contains all singletons $\{\omega\}$,*

then $\{\varepsilon_\omega, \omega \in \Omega\} = \partial_e \mathcal{M}_1(\Omega, \mathcal{F})$.

Proof. It is enough to show the inclusion $\partial_e \mathcal{M}_1(\Omega, \mathcal{F}) \subseteq \{\varepsilon_\omega, \omega \in \Omega\}$. We shall show in fact that any $\mu \in \partial_e \mathcal{M}_1(\Omega, \mathcal{F})$ coincides with a Dirac mass.

Suppose $\mu \in \partial_e \mathcal{M}_1(\Omega, \mathcal{F})$. Then, for all $n \in \mathbb{N}$, we have $\mu(F_n) \in \{0, 1\}$. Define

$$G_n = \begin{cases} F_n & \text{if } \mu(F_n) = 1 \\ F_n^c & \text{if } \mu(F_n) = 0. \end{cases}$$

Consequently, $\mu(G_n) = 1$ for all n, hence $\mu(\cap_{n\in\mathbb{N}} G_n) = 1$, i.e. $H := \cap_{n\in\mathbb{N}} G_n \neq \emptyset$. We shall show that the set H, supporting the measure μ, cannot contain more than one element either. Consider in fact the family of sets $\mathcal{G}$ (a sub-σ-algebra of $\mathcal{F}$ as a matter of fact) verifying

$$\{F_n, n \in \mathbb{N}\} \subset \mathcal{G} := \{A \in \mathcal{F} : A \cap H = \emptyset \text{ or } H \subseteq A\} \subseteq \mathcal{F}.$$

Since $\mathcal{F} = \sigma\{F_n, n \in \mathbb{N}\}$, it follows that $\mathcal{G} = \mathcal{F}$. Now $\mathcal{F}$ contains all singletons. Hence for every ω either $\{\omega\} \cap H = \emptyset$ or $H \subseteq \{\omega\}$. Hence H must be a singleton. □

Corollary 2.3.17. *If $(\Omega, \mathcal{F}) = (\mathbb{R}^d, \mathcal{B}(\mathbb{R}^d))$ or Ω is finitely or infinitely denumerable and $\mathcal{F} = \mathcal{P}(\Omega)$ then $\{\varepsilon_\omega, \omega \in \Omega\} = \partial_e \mathcal{M}_1(\Omega, \mathcal{F})$. More generally, the same result holds if $(\Omega, \mathcal{F})$ is a standard Borel space.*

In the sequel, only phase spaces in one of the class covered by the previous corollary 2.3.17 will be considered.

Postulate 2.3.18 (States)**.** *The set* **S** *of* ***states*** *of a classical system is the convex set of probability measures on $(\Omega, \mathcal{F})$. Pure states $\mathbf{S}_p$ are the extremal points of* **S***; they correspond to Dirac masses, i.e. $\mathbf{S}_p \cong \{\varepsilon_\omega, \omega \in \Omega\}$.*

Postulate 2.3.19 (Evolution)**.** *Any* ***time evolution*** *of an isolated classical system is implemented by an invertible measurable transformation $T : \Omega \to \Omega$ leaving the set of states invariant, i.e. for every $\rho \in \mathbf{S}$, we have $T_*\rho := \rho \circ T^{-1} \in \mathbf{S}$.*

In 2.3.19, the measurability of T is required but not of T^{-1}. It is not generally true that the inverse map is also measurable. However, for T bijective (in fact injective) and $(\Omega, \mathcal{F})$ a standard Borel space, one can show — though not so straightforwadly (see [93, §15.A], for instance) — that T^{-1} is also measurable.

11. Note that such a sequence is not unique!

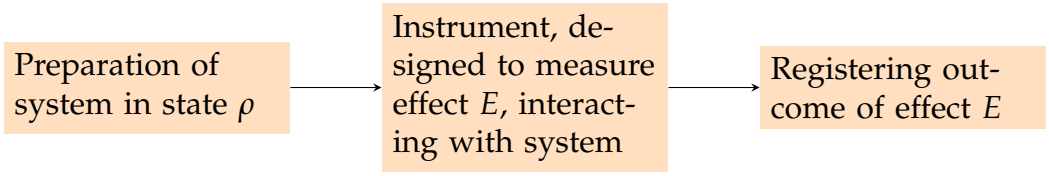


Figure 2.5 – A large ensemble of N identical systems are prepared in the same state ρ. Every system interacts with an *ad hoc* instrument specially designed to measure the possible outcomes of a given effect E. A single system of the ensemble gives a single outcome possibly different from another system of the ensemble. The frequencies of outcomes falling in the set A converge, when $N \to \infty$, towards the probability $\nu_E^\rho(A)$.

Postulate 2.3.20 (Effects and observables)**.** *The sets of **effects** and **observables** are respectively the sets* $\mathbf{E}(\Omega, \mathcal{F})$ *and* $\mathbf{O}(\Omega, \mathcal{F})$ *defined in 2.3.6. The set* $\mathbf{O}_s(\Omega, \mathcal{F})$ *of **sharp observables** of a classical system is the set of real random variables* $X \in m\mathcal{F}$ *(with space of outcomes* $(\mathbb{X}, \mathcal{X}) = (\mathbb{R}, \mathcal{B}(\mathbb{R}))$*). The corresponding set* $\mathbf{E}_s(\Omega, \mathcal{F})$ *of **sharp effects or questions** are the extremal points of* $\mathbf{E}(\Omega, \mathcal{F})$*; they are of the form* $E[A] : \Omega \to \{0, 1\}$ *and any* $X \in \mathbf{O}_s(\Omega, \mathcal{F})$ *can be decomposed into its complete set of questions through* $X = \int_{x \in \mathbb{R}} E[dx]x$*.*

Postulate 2.3.21 (Measurement)**.** ***Measuring** an effect* $E \in \mathbf{E}$ *when the system is prepared in state* $\rho \in \mathbf{S}$ *corresponds in determining the possible values of its outcomes — i.e. answers 0 or 1 — and the distribution with which those outcomes occur, given by the probability measure* $\nu_E^\rho \in \mathcal{M}_1(\mathcal{X})$*, defined by* $\nu_E^\rho(A) = \mathbb{E}(E[A]) = \int_\Omega \rho(d\omega) E[A](\omega) = \langle \rho, E[A] \rangle =: \rho E[A]$*, for all* $A \in \mathcal{X}$*.*

Hence a classical experiment designed to measure an effect E can always be thought as as the sequence of operations shown in the figure 2.5.

Exercise 2.3.22. (Convexity of the set of effects). Let $(\Omega, \mathcal{F})$ be an abstract measurable space. Show that

1. $\mathbf{E}(\Omega, \mathcal{F})$ is convex and
2. $\mathrm{extr}(\mathbf{E}(\Omega, \mathcal{F})) = \mathbf{E}_s(\Omega, \mathcal{F})$.

Exercise 2.3.23. Let $\rho \in \mathbf{S}$ be a state on $(\Omega, \mathcal{F})$, $X \in \mathbf{O}_s$ a $\mathbb{X}$-valued random variable ($\mathbb{X} \subseteq \mathbb{R}$), and $E[A]$ the question $\mathbb{1}_A \circ X$ for some fixed $A \in \mathcal{B}(\mathbb{R})$.

1. Compute the expectation of $E[A]$ w.r.t. ρ.
2. What happens if ρ is a pure state?
3. What happens if $(\Omega, \mathcal{F})$ is minimal for the random variable X?

Solution: We have already established in example 2.3.3 that $\mathbb{E}(E[A]) = \nu_X^\rho(A)$. We compute further:

1. $\rho E[A] = \int_\Omega \mathbb{1}_{\{X \in A\}}(\omega) \rho(d\omega) = \int_\Omega \mathbb{1}_A(X(\omega)) \rho(d\omega)$.
2. If $\rho = \varepsilon_{\omega_0}$ for some ω_0, then $\rho E[A] = \int_\Omega \mathbb{1}_{\{X \in A\}}(\omega) \varepsilon_{\omega_0}(d\omega) = \mathbb{1}_A(X(\omega_0)) = \nu_X^\rho(A) \in \{0, 1\}$. This result means that when measuring a sharp observable in a pure state, any measurable set of the space of outcomes, either occurs with certainty or almost surely does not occur. This is a far reaching result establishing the **reducibility of the classical randomness**.

3. If the space is minimal for X, then $X(\omega) = \omega$ and we get respectively: $\rho E[A] = \int_\Omega \mathbb{1}_A(X(\omega))\rho(d\omega) = \rho(A)$ for arbitrary state $\mathbb{P}$ and $\rho E[A] = \varepsilon_{\omega_0}(A)$ in case of a pure state $\rho = \varepsilon_{\omega_0}$. □

Exercise 2.3.24. What is the minimal phase space for a mechanical system composed by N point particles in dimension 3?

2.3.5 Interpretation of the postulates for classical systems

We stick to example provided by the physical system "die".

Phase space. From what is explained previously, we can use as phase space the set $\Omega = \{1, \ldots, 6\}$, equipped with its exhaustive σ-algebra $\mathcal{F} = \mathcal{P}(\Omega)$. All pertinent questions we can formulate on the system "die" can thus receive a definite answer. Events correspond to $\mathcal{F}$-measurable subsets of Ω.

States. The state of the system corresponds to the preparation of the physical system, i.e. the precise probability measure $\rho \in \mathcal{M}_1(\Omega, \mathcal{F})$. A die is called honest if it comes out from the factory prepared in the state ρ with $\rho(\omega) = 1/6$, for all $\omega \in \Omega$. But any other probability is an admissible state of the die. There is a statistical way to describe the state ρ: if we receive a load of N identically prepared dice, throw them, and denote by $N(\omega)$ the number of dice having given outcome ω, with $\omega \in \Omega$, when they were thrown. Then, $\lim_{n\to\infty} \frac{N(\omega)}{N} = \rho(\omega)$, by the law of large numbers.

Suppose now that we have two types of loads of dice delivered by the factory, N_1 in state ρ_1 and N_2 in state ρ_2 and mix all $N = N_1 + N_2$ of them in an urn. Dice are chosen randomly from the urn, thrown, and the numbers $N(\omega)$ where the face ω is observed are registered. Then $\lim_{N\to\infty} \frac{N(\omega)}{N} = p\rho_1(\omega) + (1-p)\rho_2(\omega)$, where $p = \lim_{N\to\infty} \frac{N_1}{N}$ and $1 - p = \lim_{N\to\infty} \frac{N_2}{N}$, with $p \in [0, 1]$. We have thus prepared a new die system into a state, convex combination of the two previous ones. Therefore convexity of $\mathcal{M}_1(\Omega, \mathcal{F})$ is not merely a mathematical property of the set of states, it is associated directly with the physical preparation of the system; it allows by mixing in different proportions systems prepared in given states, to obtain statistical ensembles that can be in any possible state.

Evolution. The physical realisation of the system die is irrelevant. Usually a die is thought as a standard cubic die. However, throwing a cubic die and waiting for its stopping on the table does not describe an isolated system! The solid body "die" must lose all its kinetical energy by transforming it into heat when it meats the plastic surface of the table. To speak about an isolated system, we have to think of another realisation. For instance, a frictionless hexachromatic perfectly rigid ball whose 6 coloured regions on its surface have equal area is another possible physical realisation of a honest die [12]. Isolated evolution of this die, corresponds to gently rolling the ball on a frictionless table. The "output"

12. Another possible realisation of an isolated system correspond to a cubic die launched in the outer space from the spatial station. The die rotates about itself without friction in the interstellar space. The outcome of the die is identified with the face of the die having the largest projection area on the space station window. Since the motion of the die is free, the sequence of the "outcomes" are a permutation over the states $\{1, \ldots, 6\}$.

of this new "die" is the colour of the area containing at each moment the unique point of the ball in contact with the table. Sampling the colour of the contact point at every second — say — implements a mapping $T : \Omega \to \Omega$ that is measurable and reversible. Reversible means that if a film shows this evolution as the time passes or during its rewinding, the two animations are physically indistinguishable. There is no physical way to distinguish the evolution T from its inverse T^{-1}. Now since T is a measurable map from Ω into Ω, it is a Ω-valued random variable on Ω. Hence it can also be represented by a stochastic kernel — in fact a matrix if Ω is finite — K_T that must invertible; hence a permutation.

Effects and observables. The example of gambling with a classical die, presented in §2.3.1, gives a precise description of what a sharp effect is, while the example of a randomised die given in §2.3.3, of what an unsharp effect is.

Measurement. As explained in §2.3.1, the probability, ν^ρ_X, on the outcome space $\mathbb{X} \subseteq \mathbb{R}$ is given, for a sharp observable X, by

$$\nu^\rho_{E[x]}(x) = \rho(X^{-1}(x)) = \sum_{\omega\in\Omega} \rho(\omega)E[x](\omega) = \langle \rho, E[x]\rangle.$$

Consider now the significance of the quantity

$$\rho(\omega)E[x](\omega) = \rho(\omega)K(\omega, x) = \mathbb{P}(\text{die shows face } \omega;\ \text{gain is } x\};$$

i.e. it represents the joint distribution of die outcome and gambler's gain. With this interpretation, we can compute
— the *a posteriori* probability on $\mathbb{X}$ as second marginal: $\nu^\rho_X(x) = \sum_{\omega\in\Omega} \rho(\omega)E[x](\omega)$,
— the *a priori* probability on Ω as the first marginal: $\rho(\omega) = \sum_{x\in\mathbb{X}} \rho(\omega)E[x](\omega)$,
— the conditional probability for the die showing face ω given that the gain has been x:

$$\rho_x(\omega) := \mathbb{P}(\text{die shows } \omega | X = x) = \frac{\rho(\omega)E[x](\omega)}{\langle \rho, E[x]\rangle} = \frac{E[x]\rho(\omega)E[x](\omega)}{\langle \rho, E[x]\rangle}.$$

Thus the joint probability can also be expressed through the formula

$$\mathbb{P}(\text{die shows } \omega; X = x) = \rho_x(\omega)\langle \rho, E[x]\rangle$$

so that by applying the formula of total probability we get consistently

$$\begin{aligned}\mathbb{P}(\text{die shows } \omega) &= \sum_{x\in\mathbb{X}} \mathbb{P}(\text{die shows } \omega; X = x)\\ &= \sum_{x\in\mathbb{X}} \rho_x(\omega)\langle \rho, E[x]\rangle = \sum_{x\in\mathbb{X}} \rho(\omega)E[x](\omega) = \rho(\omega).\end{aligned}$$

With this formula, it becomes apparent that $\nu^\rho_{E[x]}$ is obtained as the second marginal of the joint probability and we get a totally coherent system of probabilities thanks to the formula of total probability that holds in the classical setting. It is precisely this statement that fails in the quantum setting and gives so an unusual and counter-intuitive interpretation of quantum mechanics.

We conclude this paragraph by another extremely trivial looking example. Its *raison d'être* here is that it will turn to the most awkward example when considered in the quantum setting (see example 2.6.6).

Example 2.3.25. (A classical *Gedankenexperiment*[13]). Suppose a lorry has uncharged a huge amount, N, of dice, guaranteed by the producing factory to give outcomes distributed according to a known probability vector ρ (e.g. uniform). Consider the following experiment. We consider the random variable $X : \Omega \to \mathbb{X} \simeq \Omega$ defined by $X(\omega) = \omega$ and for some fixed $x \in \{1, \ldots, 6\}$, ask the question $E[x]$ meaning "does the die show face x?" We group dice according to the response we got to the previous question. If we got answer "yes", we place the die in the group of "yes answerers" and if not to the group of "no-nswerers". When the question has been asked to all the N dice, we get a group of $N[x]$ yes-answerers and a group of $N - N[x]$ no-answerers. Of course, both experimental practice and elementary probabilistic reasoning show that the proportion $N[x]/N$ is approximately equal to $\rho(x)$. Now, ask the same question but only to the subgroup of "yes-answerers". (Assume that the initial amount N was so large that $N[x]$ is also a huge number and proceed as before to form a sub-group of "yes-yes-answerers" and a subgroup of "yes-no-answerers" according to the their response to the second question and denote by $N[xx]$ the number of yes-yes answers. Experimental practice and standard probabilistic reasoning give of course $N[xx]/N[x]$ approximately equal to $\rho(x)$ and $N[xy]/N[x] \simeq \rho(y)$.

2.4 Classical physics does not suffice to describe Nature!

Quantum mechanics has been introduced in the 1930's to explain physical phenomena without classical description. Therefore, there are numerous experiments in the early years of the 20th century having only quantum explanation. The present notes are not intending to present an historical development of quantum theory but to provide the (non-physicist) reader with a feeling of the deadlocks reached by classical physics. The most famous experiment of this type is the "double slit" experiment, popularised by the Nobel Prize winner — and unparalleled pedagogue — Richard Feynman in his memorable[14] 6th (out of a series of seven "Messenger lectures") he gave at Cornell university in 1964 and intended to more "profane" an audience than his Lectures on Physics taught at Caltech [58].

Suppose that a plane wave of wavelength λ reaches a wall pierced with two slits whose distance is of the order of magnitude λ. Suppose further that a screen is placed parallel to the wall at a large distance D from it (see figure 2.6). Classical wave propagation predicts that the amplitude (hence intensity) of the wave at different points of the screen follows a standard interference fringes pattern.

Now suppose that macroscopic classical material particles, for instance gun bullets, are sent on the wall. If the lower slit is closed and the upper open, then on the screen, we observe a Gaussian distribution of the density of particle impacts centred at the point in front of the open slit as depicted in figure 2.7 below. When the two slits are open the density of the impact points follows a distribution obtained as a superposition

13. The term *Gedankenexperiment* — introduced by Einstein — means literally thought experiment. It is used to describe a powerful epistemological method of logically inferring on the possible results one would obtain if the experiment should be actually performed.

14. Whose video recording can be found on https://www.youtube.com/watch?v=f27bh4CIky4.

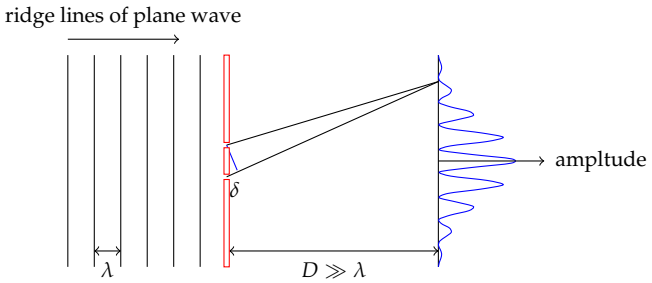


Figure 2.6 – *Schematic setting of the double-slit experiment for waves.* The amplitude of the wave at every point of the screen depends on the difference δ between the lengths of the paths between the slits and the screen. When $\delta = n\lambda$ (for integer n), the amplitude has a local maximum, when $\delta = (n + \frac{1}{2})\lambda$ then the amplitude vanishes. The continuous variation of the amplitude between these extremes gives rise to the built-up of the characteristic interference fringes observed in the wave scattering case. Notice that the picture above is not in scale! The distance between two successive maxima of the amplitude should be equal to λ.

of two Gaussians.

Turn now to the experiment where instead of macroscopic gun bullets we use electrons as projectiles [15], sent one by one to the screen. If only one slit is open, then the density of individual impact points follows a Gaussian distribution. Therefore, we have the confirmation that electrons are material particles that hit the screen individually. Now, when the two slits are open, we get the very awkward distribution of impact points depicted in figure 2.8. A recent realisation of the experiment is described in [6], where a video recording of the impact points on the screen is proposed. We observe that the number of impacts per unit area tends to a continuous distribution reminiscent of the interference fringes observed for waves. Therefore, microscopic particles (electrons) behave in some respects as particles (when only one slit is open) and in some other as waves (when the two slits are open). This behaviour cannot be explained by classical physics but is perfectly explainable by the formalism of quantum physics. Of course, there exists a long list of other experiments unexplainable in classical physics but perfectly well explained within quantum physics (e.g. EPR correlations, tunnel effect, stability of atoms, laser — i.e. light amplification by stimulated emission of radiation —, superconductivity, superfluidity etc.).

2.5 Classical probability does not suffice to describe Nature!

The previous section gave an example of experiment not explicable in terms of classical physics. Since classical physics can be formulated as a classical probability theory augmented by a dynamical law, it is not surprising that classical probability turns out to be not sufficient to explain Nature. So, the careful reader may wonder why to include the present section. The reason is that in the historical development of quan-

15. Electrons are sub-atomic particles with mass $9.10938215(45) \times 10^{-31}$ kg.

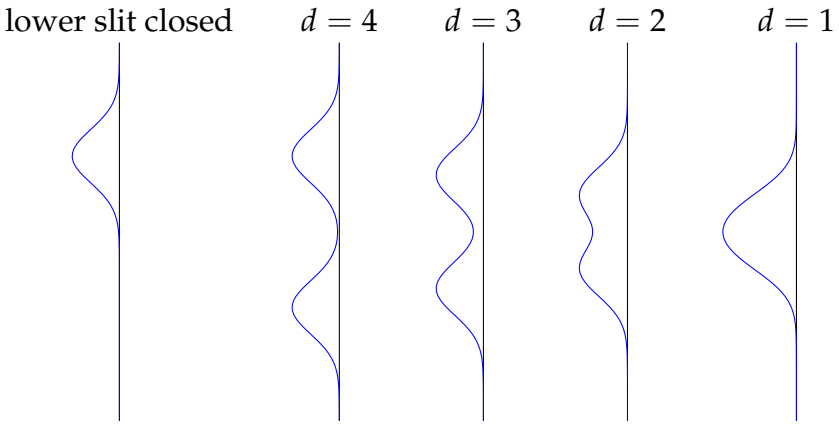


Figure 2.7 – *Schematic setting of the double-slit experiment for gun bullets.* When only the upper slit is open, we observe a Gaussian distribution of the density of impact points on the screen, centred in front of the upper slit. When the two slits are open, the density of impact points follows a distribution obtained as the superposition of two Gaussians centred in front of the slits. Depending on the distance among the slits the superposition can appear as unimodal or bimodal. In the above figure, the distance d among slits is given in *ad hoc* units (mutiples of the standard deviation of the Gaussian).

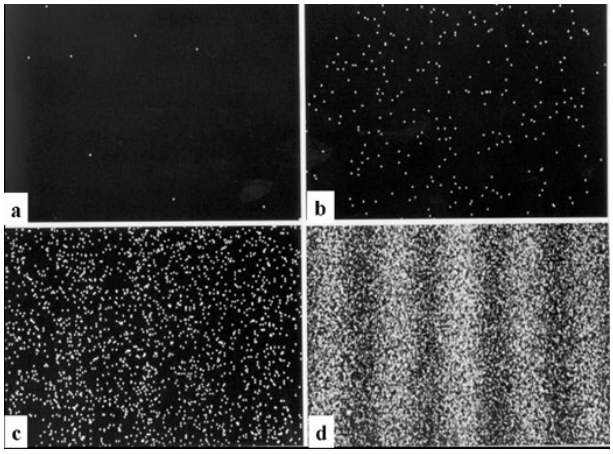


Figure 2.8 – *Experimental observation of the impact points left on the screen by electrons in a double slit experiment.* The four pictures a) – d) correspond at different instants of the experimental process. Picture a) corresponds to an early snapshot having accumulated only 11 impacts of individual electrons on the screen, picture b) has 200, c) has 600, and d) has 40000. Continuing the accumulation of impact points, we get a continuous density of impacts that follows a pattern of interference fringes as is classically the case for waves! Source of pictures: Wikipedia, distributed under Creative Commons Licence BY-SA 3.0.

tum mechanics, the statement about insufficiency of probability theory turned out to be more controversial than the experimental evidence of the insufficiency of classical physics!

Quantum mechanics has been proposed as a theory explaining physical phenomena occurring mainly in microscopic systems. The formalism of quantum mechanics in use these days has been successfully tested in **all known** experimental situations; not a single prediction made by quantum theory has ever been falsified by an experiment! Nevertheless, the quantum formalism remains highly counter-intuitive and several physicists have advocated the hypothesis that the theory is incomplete. The most prominent among those physicists was Einstein who refused to admit the intrinsically stochastic nature of quantum mechanics. In the last paragraph of his 52nd letter to Max Born — written in a joking mood on 4th December 1926 — he states [55]:

> „Die Quantenmechanik ist sehr achtunggebietend. Aber eine innere Stimme sagt mir, daß das noch nicht der wahre Jakob ist. Die Theorie liefert viel, aber dem Geheimnis des Alten bringt sie uns kaum näher. Jedenfalls bin ich überzeugt, daß *der* nicht würfelt[a] (...)".

a. Quantum mechanics is certainly imposing. But an inner voice tells me that it is not yet the real thing. The theory says a lot, but does not really bring us any closer to the secret of the "old one". I, at any rate, am convinced that *He* is not playing at dice [55].

This quotation remained in the folklore of Quantum Mechanics paraphrased into the short aphorism „Gott würfelt nicht" (or translated as "God does not play dice").

In 1935, Einstein writes, jointly with Podolsky and Rosen, a seminal and influential paper [54], based on a *Gedankenexperiment* and known as the EPR paradox[16]. This paradox will be presented and explained in §3.10.

When dealing with physical theories, we are confronted with two basic notions, locality and realism. **Locality** means that we can always take actions that have consequences only within a small region of space. In physics, locality stems from the finiteness of the speed of light. Since no interaction can propagate faster than light, no influence can be sensed in space points lying beyond the wave front of light. **Realism** means that although experiments have always random outputs, the observed randomness is nothing else than the reflection of the imperfection of the measuring instruments. In a theory where realism applies, there is no conceptual obstruction to think that there exists a state in which the system can be perfectly described in principle, i.e. the observables have determinate values before they have been measured. The observed randomness reflects only the fact that information is missing preventing us from having complete knowledge of the precise state of the system. As we shall see later, when the standard formalism of quantum mechanics will be introduced, this is not any longer the case for quantum systems: quantum systems exhibit an **irreducible randomness**, a randomness that cannot be removed by better describing the state. The role of the EPR paradox was to show the incompleteness of the quantum theory be-

16. See the "Analyse" item at http://bibnum.education.fr/physique/physique-quantique/le-paradoxe-epr for the unconventional beginnings and fate of the EPR paper.

cause a physical theory — as Einstein, Podolsky, and Rosen conceived it — ought to be realist. As the authors put it:

> "From this follows that either (1) the quantum mechanical description of reality given by the wave function is not complete or (2) when the operators corresponding to two physical quantities do not commute the two quantities cannot have simultaneous reality. For if both of them had simultaneous reality — and thus definite values — these values would enter into the complete description, according to the condition of completeness. If then the wave function provided such a complete description of reality, it would contain these values; these would then be predictable. This not being the case, we are left with the alternatives stated."

This paper triggered extremely fruitful (although sometimes epic) discussions between the tenants and the opponents of quantum formalism. Schrödinger, in a letter (in German) addressed to Einstein on 7 June 1935, uses for the first time the term *Verschränkung*; he translates it into **entanglement**[17] in the two papers he published [131, 132] to give a quantum explanation of "the EPR paradox". In [131], Schrödinger realised that entanglement refutes any paradoxical aspect of the EPR correlations. He has been led to consider entanglement as **the distinctive future** of quantum mechanics. In his own words:

> "When two systems (...) enter into temporary physical interaction (...) and when after a time of mutual influence the systems separate again, then they can no longer be described in the same way as before, viz. by endowing each of them with a representative of its own. I would not call that **one** but rather **the** characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought. **By the interaction the two representatives have become entangled.**"

Based on Einstein's refutations, Bohm proposed, in [25, 26], a new formalism of quantum mechanics, expanded by postulating the existence of — unobserved — "hidden variables", allowing to describe the same phenomenology as quantum mechanics without postulating an intrinsically stochastic nature of the theory. Therefore, the hidden variables formalism intended to restore the realism of quantum mechanics. The introduction of hidden variables did not predict any new phenomenon beyond those predicted by standard quantum theory and for many years, it was the root of a mainly philosophical controversy between the tenants of standard quantum theory (the only one we shall present in the sequel of this course) and the tenants of the hidden variables description.

A long-lasted and widely spread popular belief among physicists was that John von Neumann had refuted the possibility of existence of hidden variables in his seminal foundations of 1932 (reprinted in [149]). However, the hypotheses he did were too strong to be realisable in physical systems[18], as discovered by John Bell some thirty years later, in [18].

17. This notion will be defined in §3.10.
18. The result shown by von Neumann will be given in proposition 4.5.3.

The first mathematically sound refutation of hidden variables has been provided by John Bell, in the seminal paper [17], where he established the so-called Bell's inequalities (these inequalities are proven in proposition 2.5.2). This result established that if we impose the existence of hidden variables (i.e. classical — Kolmogorovian — unobserved variables) to assign determinate values to the quantum observables prior to the measurement process, their existence induces classical statistical correlations incompatible with the statistical predictions of quantum mechanics. The major conceptual step performed by Bell was that if hidden variables existed then they should have predictable consequences that could be experimentally tested.

In spite of the fundamental interest such an experiment would have in the conceptual foundations of the theory, during several years it was dismissed by the scientific establishment — in another outburst of arrogance — as an uninteresting philosophical quest not worth the efforts of respectable scientists [19]. Due to the enormous success of quantum mechanics to quantitatively predict all observed phenomena, a utilitarian attitude condensed into the motto "shut up and compute" prevailed in the scientific circles. It was only thanks to the ingeniousness of several groups of physicists around the world (Clauser, Shimony, Horne, Holt, Aspect, Dalibard, Roger who persevered in willing to experimentally test the hypothesis of hidden variables) that the existence of both local and realistic physical theories has been refuted in the three seminal papers [8, 9, 7] of the group at the *Université d'Orsay*. This experiment, of the utmost fundamental importance, is described in paragraph 2.5.2. It establishes that a theory that is simultaneously local and realistic cannot reproduce all the predictions of quantum mechanics (hence cannot explain experimental observations either). Phrased differently, assuming realism, the phenomenon observed in this experience — when interpreted within classical probability — appears as non-local. This fact is sometimes **wrongly** termed quantum non-locality in the literature. This term will never be used in the sequel of this course.

Therefore, before presenting the form of quantum mechanics accepted at the present time, we spend some lines to describe Bell's inequalities and explain in some details the Orsay experiment (see §2.5.2 below) that has been designed in order to check whether a Kolmogorovian theory is compatible with experimental observation or, else, refute the hidden variables hypothesis. We follow the exposition of [104]. The quantum mechanical explanation of the Orsay experiment — postponed after the introduction of the quantum formalism — will be given in §4.4.

2.5.1 Bell's inequalities

Proposition 2.5.1 (The three-variable Bell's inequality). *Let X_1, X_2, X_3 be an arbitrary triple of $\{0,1\}$-valued random variables defined on some probability space $(\Omega, \mathcal{F}, \mathbb{P})$. Then*

$$\mathbb{P}(X_1 = 1, X_3 = 0) \leq \mathbb{P}(X_1 = 1, X_2 = 0) + \mathbb{P}(X_2 = 1, X_3 = 0).$$

19. Readers so inclined to philosophical meditation are invited to consider the ravages "fashion-led" a.k.a. "project-oriented" research can cause to the advancement of science.

Proof:

$$\begin{aligned}\mathbb{P}(X_1 = 1, X_3 = 0) &= \mathbb{P}(X_1 = 1, X_2 = 0, X_3 = 0) + \mathbb{P}(X_1 = 1, X_2 = 1, X_3 = 0) \\ &\leq \mathbb{P}(X_1 = 1, X_2 = 0) + \mathbb{P}(X_2 = 1, X_3 = 0).\end{aligned}$$

□

Proposition 2.5.2 (The four-variable Bell's inequality)**.** *Let X_1, X_2, Y_1, Y_2 be an arbitrary quadruple of $\{0,1\}$-valued random variables defined on some probability space $(\Omega, \mathcal{F}, \mathbb{P})$. Then*

$$\mathbb{P}(X_1 = Y_1) \leq \mathbb{P}(X_1 = Y_2) + \mathbb{P}(X_2 = Y_2) + \mathbb{P}(X_2 = Y_1).$$

Proof: The random variables being $\{0,1\}$-valued, it is enough to check on all 16 possible realisations of the quadruple $(X_1(\omega), X_2(\omega), Y_1(\omega), Y_2(\omega))$ that

$$\{X_1 = Y_1\} \subseteq \{[X_1 = Y_2] \vee [X_2 = Y_2] \vee [X_2 = Y_1]\}.$$

□

2.5.2 The Orsay experiment(s)

The idea behind what remained in the quantum folklore as "the Orsay experiment" [20] is to associate precise physical observables with the $\{0,1\}$-valued quantities occurring in Bell's inequalities. Classical theory describes light as an electromagnetic wave; the electric field oscillates in a plane perpendicular to the propagation direction known as **polarisation**. (Some additional details on the nature and properties of light are given in appendix A). When monochromatic light emitted from a random source (i.e. unpolarised) of some intensity I passes through a polariser, the emerging beam is polarised in the direction of the polariser and has intensity $I/2$. Now, it has been established that a light beam is composed of a great number of elementary **light quanta** called **photons**. Therefore, the statement on intensities made above has only a statistical meaning; if a photon passing through a polariser oriented in a given direction α encounters a second polariser oriented in a direction β, it has probability $\frac{1}{2}\cos^2(\alpha - \beta)$ to pass through (see figure 2.9). This is an experimental fact, in accordance with both quantum mechanical prescriptions and with classical electromagnetic theory of light.

If the experiment is to be explained in terms of classical probability, with every polariser in direction $\alpha \in [0, \pi/2]$ is associated a random variable $X_\alpha \in \{0,1\}$; the random variables X are defined on a probability spaces $(\Omega, \mathcal{F}, \mathbb{P})$ where $\omega \in \Omega$ represent the microscopic state of the photon. Now for the experimental setting depicted in figure 2.9, the random variables X are correlated as

$$\mathbb{E}(X_\alpha X_\beta) = \mathbb{P}(X_\alpha = 1, X_\beta = 1) = \frac{1}{2}\cos^2(\alpha - \beta).$$

But now there is a problem because this correlation cannot be that of classical random variables. Choosing in fact three polarisations α_1, α_2, and α_3, we have $\mathbb{P}(X_{\alpha_i} = 1, X_{\alpha_j} =$

20. As a matter of fact, there has been two experiments.

Figure 2.9 – When a photon passes through the first polariser — oriented in direction α — emerges polarised in **that** direction. When it encounters a second polariser — oriented in direction β — passes through with probability $\cos^2(\alpha-\beta)$. If the photon is initially already polarised in direction α, nothing changes if the first polariser is removed.

$0) = \mathbb{P}(X_{\alpha_i}=1) - \mathbb{P}(X_{\alpha_i}=1, X_{\alpha_j}=1) = \frac{1}{2}(1-\cos^2(\alpha_i-\alpha_j)) = \frac{1}{2}\sin^2(\alpha_i-\alpha_j)$ for $i,j \in \{1,2,3\}$. The three-variable Bell inequality 2.5.1 reads then

$$\frac{1}{2}\sin^2(\alpha_1-\alpha_3) \leq \frac{1}{2}\sin^2(\alpha_1-\alpha_2) + \frac{1}{2}\sin^2(\alpha_2-\alpha_3).$$

The choice $\alpha_1 = 0$, $\alpha_2 = \pi/6$, and $\alpha_3 = \pi/3$ leads to the impossible inequality $3/8 \leq 1/8+1/8$. Therefore, classical probability cannot describe this simple experiment.

On a second reading, this experiment is not very convincing because on arranging polarisers on the optical table as described above, there is nothing preventing conceptually the second random variable X_β to depend in fact on both α and β. But then the correlation reads $\mathbb{E}(X_\alpha X_{\alpha,\beta}) = \mathbb{P}(X_\alpha = 1, X_{\alpha,\beta}=1) = \frac{1}{2}\cos^2(\alpha-\beta)$ and this can be satisfied by choosing, for instance, X_α and $X_{\alpha,\beta}$ independent with $\mathbb{P}(X_\alpha = 1) = 1/2$ and $\mathbb{P}(X_{\alpha,\beta}=1) = \cos^2(\alpha-\beta)$ which of course can be easily conceived.

The irrefutable evidence of the impossibility of describing Nature with merely classical probability is provided through the second experiment Aspect, Dalibard and Roger performed in 1982, [7], schematically described in figure 2.10. (Please carefully read the caption of this figure where the precise experimental setting is described). The same analysis can be made as in the previous experimental setting. Denoting by X_α the $\{0,1\}$-valued random variable quantifying the passage of the photon through the left polariser and Y_β through the right one, it is experimentally established in [7] that,

$$\mathbb{P}(X_\alpha = Y_\beta) = \frac{1}{2}\sin^2(\alpha-\beta),$$

for every choice of α and β. (Note incidentally that the same conclusion is obtained using — the not yet presented — quantum formalism). Now the choice $\alpha_1 = 0$, $\alpha_2 = \pi/3$, $\beta_1 = \pi/2$, and $\beta_2 = \pi/6$, should read $1 \leq 1/4+1/4+1/4$, manifestly violating the four variable Bell's inequality 2.5.2.

To better grasp the significance of this experiment, it has been proposed, see [104] for instance, to think of it as a card game between two players X and Y who can preagree on any conceivable strategy in order to win the game. The game is described in the following

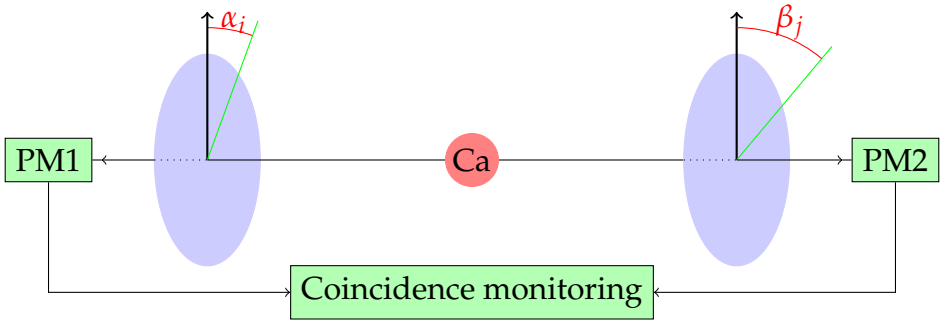


Figure 2.10 – Schematic view of the Orsay experiment [9]. A beam of calcium (Ca) atoms is triggered by a laser. When thus excited, a calcium atom emits simultaneously two photons (at different frequencies) in opposite directions and having correlated polarisations. Two polarisers stand to the left and to the right the calcium beam, at equal optical distances from it. An ingenious system of rapid optical switches is used whose net effect can be described by the following equivalent description. After the two photons have been emitted, the left polariser is oriented according to an angle randomly chosen in the set $\{\alpha_1, \alpha_2\}$, the right polariser according to an angle randomly chosen in the set $\{\beta_1, \beta_2\}$. The optical distance between the beam and the polarisers is sufficiently large to allow enough time for the switching to take place **after** the emission of the photons and **before** their reaching the polarisers (so that any causal influence of the choice of orientations on the manner the photons are emitted is safely excluded). After passing through the polarisers, the photons are detected by photomultipliers (PM1) and (PM2) and only photons in synchronisation are recorded.

Exercise 2.5.3. (The Orsay experiment as a card game [104]) The game is played between players X, Y (see figure 2.10), and A (like ... Aspect) who acts as an arbiter and as game leader.

Description of the game

— A disposes of a well shuffled deck of red and black cards (consider it as an infinite sequence of i.i.d. $\{\text{red}, \text{black}\}$-valued random variables uniformly distributed on $\{\text{red}, \text{black}\} := \{r, b\}$).
— X and Y are free to use random resources (e.g. dice) if they wish.
— Before the game starts, X and Y agree on given strategy (deterministic, non-deterministic, or random) how to determine a $\{\text{yes}, \text{no}\}$-valued variable out of the colour of the card they will be presented. Once the game starts, the players are not allowed any longer to communicate.
— A picks two cards from the deck and presents the one to X and the other to Y (mind that X and Y don't know each other's card).
— X and Y apply their own pre-agreed strategy to the colour they are presented and **simultaneously** say yes or no.
— After the announcement of the players, the cards are laid on the table. Four different card pairs are possible $(rr), (rb), (br), (bb)$, where the first colour refers to the colour of the X's card and the second to the Y's one (consider these colour pairs as boxes in a 2×2 board). If both players have given the same answer then 1 is written in the corresponding box, else 0 is marked.
— In the course of the game, the boxes get filled by sequences of 0's and 1's.
— Let $\pi_{cc'}$, with $c, c' \in \{r, b\}$, be the limit of the empirical probability of 1's in the box corresponding to colours (cc') when the game runs indefinitely. The players

win the game if $\pi_{rr} > \pi_{rb} + \pi_{br} + \pi_{bb}$. The purpose is to show that there exists no strategy (deterministic or random) allowing the players to win the game.

Questions

1. Suppose that X and Y have agreed on the following strategy: X always says "yes", independently of the colour of the card presented to her/him and Y answers the question "is my card red?". Compute explicitly the values of $\pi_{cc'}$ for $c, c' \in \{r, b\}$ and show that with this deterministic strategy, the numbers $\pi_{cc'}$ satisfy the four variable Bell's inequality $\pi_{rr} \leq \pi_{rb} + \pi_{br} + \pi_{bb}$.
2. In the above strategy, the decision making process is described through the matrices D_X and D_Y with $D_X : \{r, b\} \times \{0, 1\} \to [0, 1]$ (and similarly for D_Y), defined respectively by

$$D_X = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } D_Y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

   interpreted as meaning $\mathbb{P}(\text{Answer of } X \text{ is } a \mid \text{card colour is } c) = D_X(c, a)$ for $c \in \{r, b\}$ and $a \in \{0, 1\}$ (and similarly for Y). Hence the previously described strategies are termed **deterministic strategies**. There are 4 deterministic strategies for every player. Determine all 16 pairs of deterministic strategies and show that for all of them, Bell's inequality is verified.
3. Propose a plausible parametrisation of the space of all strategies (deterministic and random) and show that this space is convex. Is it a simplex? Show that the previous deterministic strategies are extremal points of this space.
4. Conclude that in general any strategy can be written as a convex combination of deterministic strategies. Is this decomposition unique? How such a convex combination is related to **hidden variables?** Conclude that no classical strategy exists allowing to win this game.

Some hints concerning convexity and convex decomposition of stochastic matrices needed for the the two last questions can be found in the chapter "Markov chains on finite state spaces" of the lecture notes [119].

This exercise shows that **any** system described in terms of classical probabilities, even augmented to incorporate hidden variables, cannot win this game. But the Orsay experiment proved that Nature wins! Therefore, the quantum strategy used by Nature is strictly more powerful than any classical strategy. Probably the first person to really understand this power was Feynman (see [83, chap. 7 and 15] for instance), who first conjectured the computational power of quantum mechanics and was the first who proposed to use atoms as quantum computers.

Later on, many other experiments have been performed to refute the hidden variables hypothesis. We shall present in §**??** the most recent one based on the violation of Bell's test in the form of the so called CHSH inequalities.

2.6 Quantum systems (elementary formulation)

Quantum mechanics emerged thanks to various experimental and theoretical advances, due mainly to Bohr, Planck, Schrödinger, Heisenberg, Dirac, and many others. Various formulations of quantum mechanics are possible. We start from the most straightforward one [149], based on the Hilbert space formalism, introduced by von Neumann in 1932. It turns out that shortly after the publication of this text, von Neumann confessed that he was not satisfied with the Hilbert space formulation of quantum mechanics (see [122] for a review of the ideas of von Neumann on quantum mechanics that pays due attention to historical facts). Later on, a more general formulation [146], based on quantum logics and C^*-algebras, will be given; this formulation has the advantage of allowing a unified treatment for both classical and quantum systems. Another possible formulation is provided by the operational formulation of quantum mechanics, based on the notion of instrument (see [45, 112, 114, 115]) or informational formulation (see [36, 37] for instance). The reader may wonder why so many formulations have been proposed so far. The answer is that although all the formulations are totally satisfactory from the computational point of view, their predictive power, and their adaptedness to explain diverse experiments, none of the existing ones is philosophically and epistemologically satisfactory. Quantum mechanics is a partial theory, describing fragile systems, i.e. systems that eventually leave the quantum realm to enter the classical one; such a fragility demands for a unified treatment of classical and quantum formalism, not guaranteed by any of the existing formalisms. The most counter-intuitive postulate of quantum mechanics is the measurement postulate that obsessively tormented physicists since the early days of quantum mechanics (see [141, 139, 140] or [12] for a critical account of the previous references).

2.6.1 Postulates of quantum mechanics (sharp effects and pure states)

For the time being, we proclaim that a quantum system verifies the following postulates, given in the same order as the postulates for classical systems. These postulates hold for very simple quantum systems (mainly for systems with finite degrees of freedom with non-degenerate observables). They will be completed and extended later to cover more complicated systems.

Postulate 2.6.1 (Phase space)**.** *The phase space of a quantum mechanical system is a separable complex Hilbert space* $\mathbb{H}$*. Events are associated with Hilbert subspaces of* $\mathbb{H}$*. When two systems, respectively described by Hilbert spaces* $\mathbb{H}_1$ *and* $\mathbb{H}_2$*, are considered as a single system, the composite system is described by the Hilbert space* $\mathbb{H}_1 \otimes \mathbb{H}_2$ *where* $\otimes$ *denotes the tensor product.*

The notion of tensor product will be precisely defined in §3.8. For the time being, it must be thought as a means to construct composite systems from simpler ones. However, at this point, an important remark must be made. A system composed from two different subsystems, described respectively by Hilbert spaces $\mathbb{H}_1$ and $\mathbb{H}_2$, is well described by the Hilbert space $\mathbb{H}_1 \otimes \mathbb{H}_2$. But if the subsystems describe identical (i.e. indistinguishable) systems, not the whole tensor product is physically accessible but only

either the symmetric or the antisymmetric component of it, depending on the precise nature of the subsystems. Their is one kind of systems (called bosonic) where symmetric subspaces are relevant and another kind of systems (called fermionic) where only antisymmetric subspaces are relevant. What determines the bosonic or fermionic character of the system is its spin, a quantity introduced defined in §16.4.29. However, the connection between the bosonic/fermionic character and the relevance of symmetric/antisymmetric subspace of the tensor product space is a much deeper result that can only be obtained in the more general setting of quantum field theory. The connection is shown there to be a theorem, known as **spin-statistics theorem**. For a thorough study of this theorem, the reader can consult the book [47], where the detailed proof is provided together with many historical remarks. Since this important result lies outside the scope of this course, we supplement the previous postulate by the following

Supplement to postulate 2.6.1 (Symmetrisation postulate). The phase space of a system containing 2 identical (i.e. indistinguishable) particles is either the antisymmetric subspace of $\mathbb{H}_1 \otimes \mathbb{H}_2$ or the symmetric one (with respect to permutation of the particles).

Postulate 2.6.2 (States). *Unit vectors*[21] *of* $\mathbb{H}$ *correspond to* ***pure***[22] ***quantum states*** $\mathbf{S}_p$. *More precisely, with a unit vector* ψ, *we associate the spanned one-dimensional Hilbert subspace* $\mathbb{C}\psi$ *and we denote by* $\rho = \rho_\psi$ *the orthoprojection onto* $\mathbb{C}\psi$. *The set of pure states is then identified with* $\mathbf{S}_p = \{\rho_\psi, \psi \in \mathbb{H}, \|\psi\| = 1\} \simeq \mathbb{C}\psi$.

Postulate 2.6.3 (Evolution). *Any time* ***evolution*** *of an isolated quantum system is described by a unitary operator acting on* $\mathbb{H}$. *Conversely, any unitary operator acting on* $\mathbb{H}$ *corresponds to a possible invariance*[23] *of the system.*

Postulate 2.6.4 (Observables). *The set* $\mathbf{O}_s$ *of* ***sharp observables*** *of a quantum system is the set of bounded self-adjoint operators* X *acting on the phase space* $\mathbb{H}$ *of the system. The space of outcomes of a sharp observable* X *is its spectrum, i.e.* $\mathbb{X} = \mathsf{spec}(X)$. ***Sharp effects*** $E[A]$ *are special self-adjoint operators occurring as spectral projections of an observable. The set of sharp effects is denoted by* $\mathbf{E}_s$. *Conversely, if a projective resolution of unity* $E : \mathcal{B}(\mathbb{R}) \to \mathfrak{P}(\mathbb{H})$ *is given*[24], *we can associate the self-adjoint operator* X *having* E *as spectral projections. The set of all effects* $\mathbf{E}$ ***effects (unsharp or fuzzy ones)*** *is the closed convex hull of* $\mathbf{E}_s$.

Postulate 2.6.5 (Measurement). ***Measuring*** *a sharp observable represented by its spectral projectors (effects)* E, *in the pure state* ρ_ψ *described by the unit vector* ψ, *corresponds to determining the possible outcomes and the probability measure* $\nu_E^{\rho_\psi}$ *on the real line induced by the spectral projectors through the formula*

$$\nu_E^{\rho_\psi}(B) = \mathsf{tr}(\rho_\psi E[B]) = \langle\, \psi \,|\, E[B]\psi \,\rangle, \forall B \in \mathcal{B}(\mathbb{R}) = \mathsf{tr}(\rho_\psi E[B]) = \langle \rho_\psi, E[B] \rangle,$$

where $\langle \cdot, \cdot \rangle$ *denotes the duality bracket on* $\mathbf{S}_p \times \mathbf{O}_s$

21. Strictly speaking, equivalence classes of unit vectors differing by a global phase, called **rays**. For the sake of simplicity we stick to unit vectors in this introductory section.

22. The structure of the set of arbitrary states is postponed to postulate 3.12.17 that generalises the present one.

23. The time evolution of an isolated system leaves the physical quantity "energy" invariant. Unitary operators are associated with conserved quantities. See definition 13.5.4 and the reformulation of the present postulate as postulate 13.5.5 for precise statements.

24. We denote by $\mathfrak{P}(\mathbb{H})$ the set of orthoprojections onto subspaces of $\mathbb{H}$.

2.6.2 Interpretation of the basic postulates

These postulates will be revisited later, after some basic notions on Hilbert spaces have been reminded. For the time being, it is instructing to illustrate the implications of these axioms on a very simple non-trivial quantum system and interpret their significance. Beyond its pedagogical interest, this simple example has also an intrinsic interest since it describes any physical system with two internal degrees of freedom serving to model a **qubit**, the quantum analog of a bit.

Phase space. We study a quantum system whose phase space $\mathbb{H} = \mathbb{C}^2$. This is the simplest non-trivial situation that might occur and could describe, for instance, the internal degrees of freedom of an atom having two states. In spite of its apparent simplicity, the systems carries already very interesting features. Notice however that in general, even for very simple finite systems, the phase space is not necessarily finite-dimensional.

Every $f \in \mathbb{H}$ can be decomposed into the canonical basis $(\varepsilon_1, \varepsilon_2)$ as $f = f_1\varepsilon_1 + f_2\varepsilon_2$ with $f_1, f_2 \in \mathbb{C}$. If $\|f\| \neq 0$, denote by $\phi = f/\|f\|$ the corresponding normalised vector[25].

(Pure) states. Now $\phi = \phi_1\varepsilon_1 + \phi_2\varepsilon_2$ with $|\phi_1|^2 + |\phi_2|^2 = 1$ corresponds to a pure state. The numbers $|\phi_1|^2$ and $|\phi_2|^2$ are non-negative reals summing up to 1; therefore, they are interpreted as a probability on the finite set of coordinates $\{1, 2\}$. Consequently, the complex numbers $\phi_1 = \langle\, \varepsilon_1 \,|\, \phi \,\rangle$ and $\phi_2 = \langle\, \varepsilon_2 \,|\, \phi \,\rangle$ are complex probability amplitudes, their squared moduli represent the probability that a system in a pure state ϕ is in the pure state ε_1 or ε_2.

Notice that pure states can be written as linear superpositions $\phi = \phi_1\varepsilon_1 + \phi_2\varepsilon_2$ meaning that a pure state ϕ can have components in two other pure states ε_1 and ε_2. But this **does not mean** that the pure state ϕ can be written as a convex combination of the pure states ε_1 and ε_2. The complex numbers ϕ_1 and ϕ_2 have no direct probabilistic interpretation; only their squared amplitudes have.

Evolution. A unitary operator on $\mathbb{H}$ is a 2×2 matrix U, verifying $UU^* = U^*U = I$. If ϕ is a pure state, then $\psi = U\phi$ verifies $\|\psi\|^2 = \langle\, U\phi \,|\, U\phi \,\rangle = \langle\, \phi \,|\, U^*U\phi \,\rangle = \|\phi\|^2$. Therefore quantum evolution transforms pure states into pure states (preserves purity of states). Moreover, due to the unitarity of U, we have $\phi = U^*\psi$, and since U^* is again unitary, it corresponds to a possible time evolution (as a matter of fact to the time reversed evolution of the one corresponding to U.) This shows that time evolution of isolated quantum systems is reversible.

(Sharp) effects and observables. Recall that any normal operator X admits a spectral decomposition $X = \int_{\mathsf{spec}(X)} E[dx]x$. If X is self-adjoint, then $\mathsf{spec}(X) \subseteq \mathbb{R}$. Let us illustrate with a very simple example: chose for X the matrix

$$X = \begin{pmatrix} 1 & 2i \\ -2i & -2 \end{pmatrix}.$$

We compute easily

25. General (unnormalised) vectors of $\mathbb{H}$ are denoted by small Latin letters f, g, h, etc.; normalised vectors, representing rays, by small Greek letters ϕ, χ, ψ, etc.

Eigenvalues x	Eigenvectors $\zeta[x]$	Projectors $E[x]$
-3	$\frac{1}{\sqrt{5}}\begin{pmatrix} -i \\ 2 \end{pmatrix}$	$\frac{1}{5}\begin{pmatrix} 1 & -2i \\ 2i & 4 \end{pmatrix}$
2	$\frac{1}{\sqrt{5}}\begin{pmatrix} 2i \\ 1 \end{pmatrix}$	$\frac{1}{5}\begin{pmatrix} 4 & 2i \\ -2i & 1 \end{pmatrix}$

Hence

$$X = \sum_{x\in\{-3,2\}} E[x]x = (-3)\frac{1}{5}\begin{pmatrix} 1 & -2i \\ 2i & 4 \end{pmatrix} + 2\frac{1}{5}\begin{pmatrix} 4 & 2i \\ -2i & 1 \end{pmatrix}.$$

Since the operator X is self-adjoint (hence normal), eigenvectors associated with different eigenvalues are orthogonal (see §3.7, corollary 3.7.4). The operators $E[-3]$ and $E[2]$ are self-adjoint (hence they correspond to observables) and othoprojectors to mutually orthogonal subspaces. Since their spectrum is $\{0,1\}$, they play the role of yes-no questions for a quantum system.

Measurement. This axiom in some respects generalises straightforwardly the classical case; in some other it has the most counter-intuitive consequences.

Straightforward generalisation of classical case: Let $\psi \in \mathbb{H}$ be a pure phase; since $\zeta[-3]$ and $\zeta[2]$ are two orthonormal vectors of $\mathbb{H}$ (hence also pure phases), they serve as basis to decompose $\psi = z_{-3}\zeta[-3] + z_2\zeta[2]$, with $\|\psi\|^2 = |z_{-3}|^2 + |z_2|^2 = 1$. Thus any pure state ψ, with probability $|\langle\, \psi \,|\, \zeta[-3] \,\rangle|^2$ is in the pure state $\zeta[-3]$ and with probability $|\langle\, \psi \,|\, \zeta[2] \,\rangle|^2$ is in the pure state $\zeta[2]$.

Compute further

$$\begin{aligned} \nu_X^{\rho_\psi}(x) &= \mathsf{tr}(\rho_\psi E[x]) = \langle\, \psi \,|\, E[x]\psi \,\rangle \\ &= \sum_{x',x''\in\mathsf{spec}(X)} \bar{z}_{x'} z_{x''} \langle\, \zeta[x'] \,|\, E[x]\zeta[x''] \,\rangle = |z_x|^2 \in [0,1]. \end{aligned}$$

Thus $(|z_x|^2)_{x\in\mathsf{spec}(X)}$ can be interpreted as a probability on the set of the spectral values. Hence, the scalar product $\langle\, \psi \,|\, X\psi \,\rangle = \sum_{x\in\mathsf{spec}(X)} x|z_x|^2$ is the expectation of the spectral values with respect to the decomposition of ψ on the basis of eigenvectors. It is worth noticing that expectation of a classical random variable X taking values in a finite set $\{x_1,\dots,x_n\}$ with probabilities $p_1,\dots,p_n$ respectively, is

$$\mathbb{E}X = \sum_{k=1}^n x_k p_k = \sum_{k=1}^n \sqrt{p_k} x_k \sqrt{p_k} = \sum_{k=1}^n \sqrt{p_k}\exp(-i\theta_k) x_k \sqrt{p_k}\exp(i\theta_k),$$

with arbitrary $\theta_k \in \mathbb{R}, k = 1,\dots,n$. Hence, classically, $\mathbb{E}X = \langle\, \psi \,|\, X\psi \,\rangle$ with $\psi = \begin{pmatrix} \sqrt{p_1}\exp(i\theta_1) \\ \vdots \\ \sqrt{p_n}\exp(i\theta_n) \end{pmatrix}$, verifying $\|\psi\| = 1$ and with $X = \begin{pmatrix} x_1 & & 0 \\ & \ddots & \\ 0 & & x_n \end{pmatrix}$.

We have moreover seen that classical probability is equivalent to classical physics; thanks to the previous lines, it turns out that it is also equivalent to quantum physics involving solely diagonal self-adjoint operators as observables. The full flavour of quantum physics is obtained only when the observables are represented by non-diagonal self-adjoint operators.

Counter-intuitive consequences: Consider now,

$$f[x] = E[x]\psi = \begin{cases} \langle\, \zeta[x] \,|\, \psi \,\rangle \zeta[x] & \text{if } x \in \mathsf{spec}(X) \\ 0 & \text{otherwise.} \end{cases}$$

The vector $f[x]$ is in general unnormalised; the corresponding normalised state $\phi[x] = \frac{E[x]\psi}{\|E[x]\psi\|}$, well defined whenever $x \in \mathsf{spec}(X)$ and ψ has a non-zero $\zeta[x]$-component, has a very particular interpretation. Suppose we ask the question: "does the physical observable take the value -3?" The answer, as in the classical case, is a probabilistic one:

$$\mathbb{P}(\{X = -3\}) = \nu_X^{\rho_\psi}(-3) = |z_{-3}|^2 = \langle\, f[-3] \,|\, f[-3] \,\rangle = \|E[-3]\psi\|^2 = \mathsf{tr}(\rho_\psi E[-3]).$$

What is new, is that once we have asked this question, the state ψ is projected on the eigenspace $E[-3]\mathbb{H}$ and is represented by the state $\phi[-3]$. This means that asking a question on the system has irreversibly changed its state! The conditional state $\rho_{\phi[x]}$ given that we have asked the question $E[x]$ reads now

$$\rho_{\phi[x]} = \frac{E[x]\rho_\psi E[x]}{\mathsf{tr}(\rho_\psi E[x])}.$$

But now, the state has been irreversibly modified. If we apply the total probability formula, we obtain

$$\sum_{x \in \mathsf{spec}(X)} \rho_{\phi[x]}\, \mathsf{tr}(\rho_\psi E[x]) = \sum_{x \in \mathsf{spec}(X)} E[x]\rho_\psi E[x] \neq \rho_\psi,$$

due to the non-commutativity of ρ_ψ and $E[x]$. This is a totally new phenomenon without classical counterpart. Asking questions about a quantum system corresponds to a **quantum measurement** and the above formula shows that measurement irreversibly changes (projects) the state of the system. It will be shown later that the above averaging over the possible outcomes of a sharp observable X irreversibly transforms the quantum state ρ_ψ into the state $\sum_{x \in \mathsf{spec}(X)} E[x]\rho_\psi E[x]$ that is isomorphic to a classical state.

Example 2.6.6. (A quantum *Gedankenexperiment*). Suppose that a a huge number, N, of copies of a "quantum die" has been prepared in a quantum state ρ guaranteed to give output x with probability $\mathsf{tr}(E[x]\rho)$ and repeat the experiment as described in the classical setting of the example 2.3.25. Then of course, $N[x]/N$ will tend to $\mathsf{tr}(E[x]\rho)$ as was the case in the classical situation. But now it follows from the formalism and is experimentally verified that $N[xx]/N[x] \to 1$! This is a totally new phenomenon, without classical counterpart. It is termed **collapse of the quantum state** after a sharp measurement.

There are many other counter-intuitive quantum phenomena; we shall study some of them in this course.

Summarising the interpretation of these axioms, we have leapro:linear-hidden-donot-existrnt that

— quantum mechanics has a probabilistic interpretation, generalising the classical probability theory to a quantum (non-Abelian) one,
— quantum evolution is reversible (as is the classical one),
— quantum measurement is irreversible and this constitutes a highly counter-intuitive aspect of quantum mechanics.

Were only to consider this generalisation of probability theory to a non-commutative setting and to explore its implications for explaining quantum physical phenomena, should the enterprise be already a fascinating one. But there is even much more fascination about it: there has been demonstrated lately that quantum phenomena can serve to cipher messages in an unbreakable way and these theoretical predictions have already been exemplified by currently working pre-industrial prototypes [26].

In a more speculative perspective, it is even thought that in the near future there will be manufactured computers capable of performing large scale computations using quantum algorithms [27]. Should such a construction be realised, a vast family of problems in the (classical) complexity class of "exponential time" could be solved in polynomial time on a quantum computer.

2.7 Some complements on effects

2.7.1 Necessity of considering quantum unsharp effects

We have seen that the set $\mathbf{E}_s$ of sharp effects of a system (classical or quantum) is is the set of **projection-valued measures** on $(\mathbb{R}, \mathcal{B}(\mathbb{R}))$

$$\mathbf{E}_s := \{E : \mathcal{B}(\mathbb{R}) \to \mathsf{Proj}\},$$

where $\mathcal{B}(\mathbb{R})$ stands for the Borel σ-algebra on $\mathbb{R}$ and Proj for the set of projections on the adequate space.

In the classical case — where the phase space is a measurable space $(\Omega, \mathcal{F})$ — the set Proj stands for the set $\mathcal{I} := \mathcal{I}(\Omega, \mathcal{F})$ of $\{0,1\}$-valued random variables (indicators)

$$\mathsf{Proj} = \{\iota : \Omega \to \{0,1\},\ \iota \text{ measurable}\} =: \mathcal{I}(\Omega, \mathcal{F}),$$

endowed with componentwise multiplication.

In the quantum case — where the phase space is a Hilbert space $\mathbb{H}$ — the set Proj stands for the set $\mathfrak{P} := \mathfrak{P}(\mathbb{H})$ of orthoprojections to Hilbert subspaces of $\mathbb{H}$

$$\mathsf{Proj} = \{P : \mathbb{H} \to \mathbb{H},\ P \text{ orthoprojection}\} =: \mathfrak{P}(\mathbb{H}).$$

In both classical and quantum cases, the set of effects $\mathbf{E}$ is defined as the closed convex hull of $\mathbf{E}_s$, i.e. $\mathbf{E} = \overline{\mathsf{co}}(\mathbf{E}_s)$.

26. See the article [70], articles in *Le Monde* (they can be found on the website of this course), the website www.idquantique.com of the company commercialising quantum cryptologic and teleporting devices, etc.

27. Contrary to the quantum transmitters and cryptologic devices that are already available (within pre-industrial technologies), the prototypes of quantum computers that have been manufactured so far have still extremely limited scale capabilities.

In the classical situation, unsharp effects have been motivated by the introduction of randomised decision rules or by the weakening of crisp membership functions (corresponding to indicator functions) to fuzzy ones. Therefore, in the classical case, unsharp effects correspond to some generalisation of the theory to encompass these new decision rules or memberships.

It turns out that in the quantum case, unsharp effects show up both as a consequence of the mathematical formalism (even at its simplest level presented in this chapter) and as a sheer experimental necessity. As a matter of fact, there are experiments involving two successive projective measurements that cannot be described by a projective measurement. This phenomenon is purely quantum (has no classical counterpart) and is illustrated in the following example occurring when the spin of an electron is measured by two successive Stern-Gerlach apparatus in general positions. The notion of spin and the functioning of the Stern-Gerlach apparatus will be explained much later in this text (in §16.7). For the time being, just keep in mind that in a Stern-Gerlach experiment, silver atoms are sent through a strong inhomogeneous magnetic field caused by a magnet (see figure 2.11 and carefully read its caption).

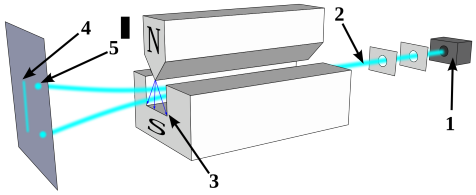


Figure 2.11 – Schematic view of the experimental setting of Stern-Gerlach experiment. Silver atoms emerge from a furnace (1) and are collimated (2) to form a beam entering a strongly inhomogeneous magnetic field (3). Atoms are detected on the screen at the left. Only the trajectories of the atoms having travelled in the vertical plane passing through the middle of the magnet are shown in the figure. If the atoms were classical particles, they should reach the screen at any position within the segment (4). Instead, atoms emerging from the magnet hit the screen only at two possible positions (5) corresponding to the upper and lower extrema of the previous segment. Source: from file provided by Theresa Knott on Wikipedia; distributed under licence CC BY-SA 4.0.

Quantum mechanically the above experiment can be described by asking a question (measuring a sharp effect that will be specified shortly) on a quantum system in a two-dimensional Hilbert space $\mathbb{H} = \mathbb{C}^2$.

Rays of $\mathbb{C}^2$ are classes of unit vectors differing by a global phase factor, i.e. $\psi \in \mathbb{C}^2$, with $\|\psi\| = 1$, where vectors ψ and $\exp(i\gamma)\psi$, with $\gamma \in \mathbb{R}$, are identified. It turns out that the set of rays is isomorphic to the unit sphere of $\mathbb{R}^3$. In fact, let $(\varepsilon_1, \varepsilon_2)$ denote the canonical basis of $\mathbb{C}^2$. Since for every $\psi = \psi_1\varepsilon_1 + \psi_2\varepsilon_2$, the condition $\|\psi\|^2 = 1$ implies $|\psi_1|^2 + |\psi_2|^2 = 1$, we can chose $\psi_1 = \cos(\theta)\exp(i\alpha)$ and $\psi_2 = \sin(\theta)\exp(i\beta)$, $\alpha, \beta \in \mathbb{R}$. Omission of global phase implies that any ray can be reparametrised by

Euclidean points on the unit sphere [28] in $\mathbb{R}^3$:

$$\psi := \psi(\theta,\phi) = \begin{pmatrix} \cos(\theta)e^{i\phi/2} \\ \sin(\theta)e^{-i\phi/2} \end{pmatrix}, \theta \in [0,\pi], \phi \in [0,2\pi],$$

as shown in figure 2.12.

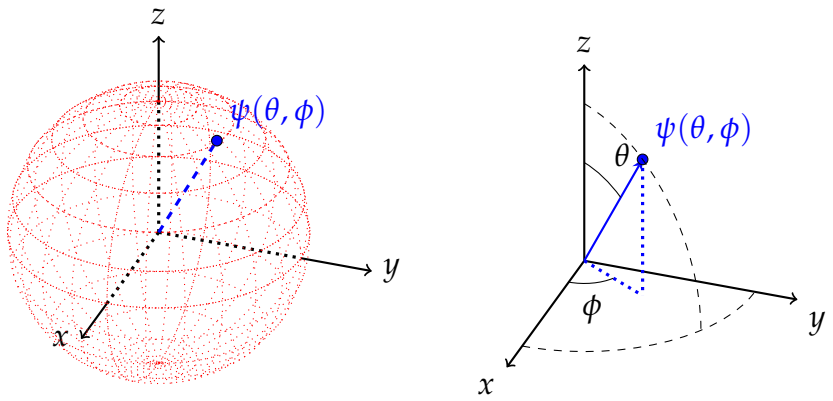


Figure 2.12 – The set of rays in $\mathbb{C}^2$ is isomorphic to the Euclidean sphere $\mathbb{S}^2$ (left figure). The ray corresponding to the point having spherical coordinates $(r = 1, \theta, \phi)$ is represented by the vector $\psi := \psi(\theta,\phi) = \cos(\theta)e^{i\phi/2}\varepsilon_1 + \sin(\theta)e^{-i\phi/2}\varepsilon_2 \in \mathbb{C}^2$, where $\varepsilon_1, \varepsilon_2$ are the canonical basis vectors of $\mathbb{C}^2$. The right figure depicts the convention used to name angles.

With any point in $\mathbb{R}^3$ with spherical coordinates $(1,\theta,\phi)$, is associated a vector $\psi := \psi(\theta,\phi)$: we denote by $P := P(\theta,\phi)$ the orthoprojector onto the one dimensional space $\mathbb{C}\psi$ spanned by ψ. It reads [29]

$$P := P(\theta,\phi) = \begin{pmatrix} \cos^2(\theta) & \cos(\theta)\sin(\theta)\exp(i\phi) \\ \cos(\theta)\sin(\theta)\exp(-i\phi) & \sin^2(\theta) \end{pmatrix}.$$

Return now to the Stern-Gerlach experiment. Suppose that the electron is sent through a first Stern-Gerlach apparatus oriented as shown in the picture and we ask the question "does the electron hit the screen at the upper point"? It corresponds to the sharp effect $E_A := E_A[\text{up}] = P(0,0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Suppose now that instead of placing a screen after the first apparatus, we stop the electrons emerging in the lower beam and let the electrons emerging in the upper beam pass through a second Stern-Gerlach magnet oriented so that the upper beam emerging from the first magnet enters the second magnet at its axis. Then again only two possible beams will emerge in directions "up" or "down" w.r.t. the new north-south pole orientation. Ask again the question "does the electron hit the screen at the upper point (w.r.t. the new north-south orientation)"? It corresponds to a sharp effect. For the sake of concreteness [30], suppose that

28. This sphere is known as the **Bloch sphere** in Quantum Physics, as the **Poincaré sphere** in Optics, and as the **Riemann sphere** in Projective Geometry.

29. In §3.9 it is explained how to compute easily the expression of the orthoprojector onto the subspace spanned by a given vector. For the time being, it is enough to verify that the proposed operator P orhtoprojects an arbitrary vector $h \in \mathbb{H}$ to $Ph = \langle \psi \mid h \rangle \psi \in \mathbb{C}\psi$.

30. As a matter of fact, we can arrange the two experiments so that to make the second effect correspond to an arbitrary value of (θ,ϕ).

the new effect reads $E_B := E_B[\text{up}] = P(\pi/3, \pi/4) = \begin{pmatrix} 1/4 & (1+i)\sqrt{6}/8 \\ (1-i)\sqrt{6}/8 & 3/4 \end{pmatrix}$. Now the electrons emerging in the "upper" beam from the second magnet are those that emerged surely from the upper beam of the first magnet. Suppose that the incoming electron is in an arbitrary state ρ_ξ, where $\xi = a\varepsilon_1 + b\varepsilon_2$ with $|a|^2 + |b|^2$. Following the formalism introduced in the previous section, the state of the electron after having passed through the first magnet is $\rho_A = \frac{E_A \rho_\xi E_A}{\mathsf{tr}(\rho_\xi E_A)}$. Hence, the probability that the electron emerges ultimately from the upper beam in the composite experiment is

$$\mathsf{tr}(\rho_A E_B)\,\mathsf{tr}(\rho_\xi E_A) = \mathsf{tr}(E_A \rho_\xi E_A E_B) = \langle\, \xi \,|\, E_A E_B E_A \xi \,\rangle.$$

If we suppose that he composite experiment can be described by some sharp effect F, we must have $\mathsf{tr}(\rho_\xi F) = \langle\, \xi \,|\, F\xi \,\rangle = \langle\, \xi \,|\, E_A E_B E_A \xi \,\rangle$ for an arbitrary ξ. But $Q = E_A E_B E_A = \begin{pmatrix} 1/4 & 0 \\ 0 & 0 \end{pmatrix}$ is not a projector since $Q^2 \neq Q$. Nevertheless it is a positive operator (since[31] $\mathsf{spec}\, Q = \{0, 1/4\}$), verifying $O \leq Q \leq I$. Hence, the product of quantum sharp effects is in general an unsharp effect. This is a purely quantum phenomenon — in the classical situation, the product of two indicators $\mathbb{1}_F \mathbb{1}_G$ is always the indicator $\mathbb{1}_{F\cap G}$ — that is due to the non-commutative nature of quantum effects. As a matter of fact, the product of two sharp effects E_A and E_B remains a sharp effect, if, and only if, they commute, i.e. $[E_A, E_B] = O$. We conclude that considering unsharp effects is a necessity in quantum theory, imposed both by the mathematical formalism and the experimental observation.

2.7.2 Effect algebras and states

Sharp effects are measures defined on the Borel σ-algebra $\mathcal{B}(\mathbb{R})$ and take values in the set of projections; general effects take values in $\overline{\mathsf{co}}(\mathsf{Proj})$. Now, technically, the σ-algebra $\mathcal{B}(\mathbb{R})$ is a σ-complete Boolean algebra; a Boolean algebra of subsets is also a poset (partially ordered set) of subsets ordered by inclusion and is also a lattice since every two sets have an upper bound (their union) and a lower bound (their intersection). The same observations hold for the set of (classical or quantum) projectors. Hence effects appear as morphisms between very closely related algebraic structures. Those ideas will be developed in chapter 13. The purpose of this subsection is to strip $\mathcal{B}(\mathbb{R})$ and $\mathsf{co}(\mathsf{Proj})$ from all superstructures in order to get their quintessential elementary algebraic properties encoded into a — so called — **effect algebra** introduced in [62] and further developed in [49, 48, 77] among others).

Presently, Boolean algebras are thought as algebraic structures $(B, +, \cdot, ', 0, 1)$ on a set B endowed with a unary operation denoted $'$, two binary operations $+$ and $\cdot$, and two particular elements 0 et 1, such that $(B, +, 0)$ is an Abelian group with neutral element 0, $(B, \cdot, 1)$ is a commutative monoid with neutral element 1, binary operations are distributive with respect to one another and the unary operation is such that $a + a' = 1$ and $a \cdot a' = 0$, for every $a \in B$. These rules imply that both addition and multiplication are idempotent.

31. See §3.11.

This definition of Boolean algebra is efficient and instrumental since it encompasses its essential properties. However, Boole used to think of Boolean algebra as a structure with *partially defined operations*. In his own words [30, chap. II, pp. 32–33]:

> "We are not only capable of entertaining the conceptions of objects, as characterized by names, qualities, or circumstances, applicable to each individual of a group of objects consisting of partial groups, each of which is separately named and described. For this purpose we use the conjunctions "and," "or," &c (sic). [...] In strictness, the words "and," "or," interposed between the terms descriptive of two or more classes of objects, imply that those classes are quite distinct, so that **no member of one is found in another. In this and in all other respects the words "and" "or" are analogous with the sign $+$ in algebra, and their laws are identical."**

Definition 2.7.1. An **effect algebra** is a structure $(E, \boxplus, 0, 1)$ where E is a set endowed with a *partially defined* binary operation $\boxplus$ and two particular elements 0 et 1 such that, for all $a, b, c \in E$, the following laws are satisfied:

Commutativity: $a \boxplus b$ is defined if, and only if, $b \boxplus a$ is defined, and in that case $a \boxplus b = b \boxplus a$.

Associativity: $a \boxplus b$ and $(a \boxplus b) \boxplus c$ are defined if, and only if, $b \boxplus c$ and $a \boxplus (b \boxplus c)$ are defined, and in that case $a \boxplus (b \boxplus c) = (a \boxplus b) \boxplus c$.

Complementation: For any a, there exists a unique a' such that $a \boxplus a'$ is defined and $a \boxplus a' = 1$.

Zero-one law: If $a \boxplus 1$ is defined in E, then $a = 0$.

Writing $a \boxplus b$ in the sequel, implies that $a \boxplus b$ is defined in E. An effect algebra can be naturally endowed with a partial order $\leq$ defined by

$$[a \leq b] \Leftrightarrow [\exists c \in E : a \boxplus c = b].$$

We write then $c = b \boxminus a$. In particular, $a' = 1 \boxminus a$ and if $a \leq b$ then $b \boxminus a = (b' \boxplus a)'$. A partially ordered set is termed **poset**.

Example 2.7.2.

1. Let $(\Omega, \mathcal{F})$ be a measurable space and $\mathcal{I}(\Omega, \mathcal{F}) = \{\iota : \Omega \to \{0,1\},\ \iota \text{ measurable}\}$ the set of measurable indicators on Ω. On denoting o the constant zero function $o(\omega) = 0, \forall \omega \in \Omega$, and u the constant one function $u(\omega) = 1, \forall \omega \in \Omega$, the set $\mathcal{I}$, endowed with a partial pointwise addition $\iota_1 \boxplus \iota_2$ defined if, and only if, ι_1 and ι_2 are disjointly supported, becomes an effect algebra $(\mathcal{I}(\Omega, \mathcal{F}), \boxplus, o, u)$.
2. Le $\mathbb{H}$ be a Hilbert space and $\mathfrak{P}(\mathbb{H}) = \{P : \mathbb{H} \to \mathbb{H},\ P \text{ orthoprojection}\}$ the set of orthoprojections to Hilbert subspaces of $\mathbb{H}$. On denoting O the orthoprojection to the trivial subspace $\{0\}$ and I the identity on $\mathbb{H}$, the set $\mathfrak{P}(\mathbb{H})$ endowed with a partial addition $P_1 \boxplus P_2$ defined if, and only if, P_1 and P_2 commute, becomes an effect algebra $(\mathfrak{P}(\mathbb{H}), \boxplus, O, I)$.
3. Let $(G, +)$ be a partially ordered Abelian group, i.e. an Abelian group endowed with a translation invariant partial order $\leq$. Choose an element $u \neq 0$ in its positive cone, i.e. $u \in G_{\geq} := \{g \in G : g \geq 0\}$ and denote by $\Gamma(G, u) := \{g \in G : 0 \leq g \leq u\}$. Then, endowed with a partial addition $g_1 \boxplus g_2$ defined if, and only

if, $g_1 + g_2 \leq u$, this set becomes an effect algebra $(\Gamma(G,u), \boxplus, 0, u)$, called an **interval effect algebra**. In particular if $G = \mathbb{R}$ and $u = 1$, then $\Gamma(\mathbb{R}, 1) = [0,1]$ gives rise to an interval effect algebra.

4. Let $\mathbb{X}$ be a set and $\mathcal{X} \subseteq \mathcal{P}(\mathbb{X})$ a family of subsets of $\mathbb{X}$ that contains the empty set and is closed by complementation and finite union; then $(\mathcal{X}, \cup, \cap, (\cdot)^c, \emptyset, \mathbb{X})$ is a Boolean algebra. On denoting by $\boxplus$ the partially defined operation of disjoint union, i.e. $a \boxplus b$ is defined on $\mathcal{X}$ if, and only if, $a \cap b = \emptyset$ as $a \boxplus b = a \sqcup b$, this **Boolean algebra can be viewed as an effect algebra** $(\mathcal{X}, \boxplus, \emptyset, \mathbb{X})$.

Definition 2.7.3. A **lattice** L is a non-empty poset in which any two elements a and b have a greatest lower bound or **meet**, denoted by $a \wedge b$, and a least upper bound or **join**, denoted by $a \vee b$.

Lemma 2.7.4. *In a lattice $(L, \vee, \wedge)$, the following laws are satisfied, for all $a, b, c \in L$:*

Idempotence: $a \wedge a = a$ *and* $a \vee a = a$.
Commutativity: $a \wedge b = b \wedge a$ *and* $a \vee b = b \vee a$.
Associativity: $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ *and* $a \vee (b \vee c) = (a \vee b) \vee c$.
Absorption: $a \wedge (a \vee b) = a \vee (a \wedge b) = a$.

*Moreover, the condition $a \leq b$ is equivalent to each of the following **consistency** conditions*

$$a \wedge b = a \quad \text{and} \quad a \vee b = b.$$

Definition 2.7.5. Let E be an effect algebra.

1. If E is also endowed with a lattice structure, we speak about a **lattice effect algebra**.
2. The algebra E is a **convex effect algebra** if for any $a, b \in E$ and $\lambda, \mu \in [0,1]$, the following laws are satisfied:
   (a) $\lambda a \in E$,
   (b) $\lambda(\mu a) = (\lambda\mu)a$,
   (c) if $a \boxplus b$ is well defined in E, then $(\lambda a) \boxplus (\lambda b)$ is also well defined in E and moreover, $(\lambda a) \boxplus (\lambda b) = \lambda(a \boxplus b)$,
   (d) $1a = a$.

Example 2.7.6.

1. The effect algebras introduced in the example 2.7.2 are all lattice effect algebras. Among them, only the case 3 constitutes a convex effect algebra.
2. Let $(\Omega, \mathcal{F})$ be a measurable set. The set $(\mathbf{E}(\Omega, \mathcal{F}), \boxplus, o, u)$, where $\mathbf{E} := \mathbf{E}(\Omega, \mathcal{F})$ stands for the set of measurable fuzzy membership functions $\mathbf{E} := \{\phi : \Omega \to [0,1];\ \phi \text{ measurable}\}$ on Ω, and $\boxplus$ a partial addition such that $\phi_1 \boxplus \phi_2$, defined if, and only if, for all $\omega \in \Omega$, $\phi_1(\omega) + \phi_2(\omega) \leq 1$, constitutes a convex lattice effect algebra. Remark that $\mathbf{E} = \overline{\text{co}}\mathcal{I}$.
3. Let $\mathbb{H}$ be a Hilbert space and $\mathbf{E} := \mathbf{E}(\mathbb{H}) = \{X \in \mathcal{L}(\mathbb{H}) : O \leq X \leq I\}$ the set of linear operators that satisfy the claimed inequalities for the natural ordering of operators (see definition 3.11.1). On denoting $\boxplus$ the binary operation defined if, and only if, $X + Y \in \mathbf{E}$, by $X \boxplus Y = X + Y$ is a convex effect algebra, called **Hilbert space effect algebra**.

Definition 2.7.7. Let E be an effect algebra. A morphism $\mu : E \to [0,1]$ from the effect algebra E to the interval effect algebra $[0,1]$ is called a **state** on E. The set of states on E is denoted by $S := S(E)$.

An **effect-state space** is a triple (E, S, F), where F is a map $F : E \times S \to [0,1]$ satisfying the following conditions for $a, b \in E$:

1. there exist $0, 1 \in E$ such that
$$F(0,\mu) = 0 \text{ and } F(1,\mu) = 1, \forall \mu \in S;$$
2. if $F(a,\mu) \leq F(b,\mu)$, forall $\mu \in S$, then there exists a unique $c \in E$, such that $F(a,\mu) + F(c,\mu) = F(b,\mu)$;
3. if $\lambda \in [0,1]$, then $\lambda a \in E$ and $F(\lambda a, \mu) = \lambda F(a,\mu)$, for all $\mu \in S$.

We conclude this introductory section on effect algebras and states on them by underlying that they provide a very general and versatile framework for applications by
— identifying Boolean algebras [32] and the $[0,1]$ as effect algebras,
— proving that unsharp observations correspond to convex effect algebras,
— identifying states (probability charges or measures) as morphisms between effect algebras.

These ideas will be further developed in chapter 13 to offer a unified treatment to both classical and quantum systems. State-effect spaces can be even extended beyond classical and quantum theories by providing richer (although unphysical) structures on which we can test ideas and better apprehend the specificities of physical theories making them so special.

32. The same holds true for σ-algebras.

3

Short resumé of Hilbert spaces

Hilbert spaces have been introduced during the period 1890–1932. The early steps of their development have been initiated by the need to give a rigorous status to the computation of extrema arising in the calculus of variations. In [67], Fredholm generalises the results of Cramér in linear algebra to an "infinite dimensional algebra" and shows what is known these days as the "Fredholm alternative" by inverting a mathematical object to obtain what is called the resolvent of an integral operator. Between 1904 and 1910 Hilbert (see [85, pp. 56–72 and 94–145] for a more easily accessible reference than the original articles) develops these ideas and introduces the spaces — now denoted $\ell^2(\mathbb{N})$ — of square summable sequences as archetypes of such infinite dimensional algebras. Between 1905 and 1908 Fischer [60, 59], Riesz [124], Schmidt [130], and Fréchet [63, 64, 65, 66] complete the geometrisation of spaces of square summable sequences and introduce vectors and scalar products. These methods were subsequently generalised to arbitrary normed spaces in [13]. In their infinite-dimensional variety, Hilbert spaces are generalisations of the vector spaces $\mathbb{R}^d$ or $\mathbb{C}^d$ studied in introductory linear algebra courses. They are endowed with rich structures (geometrical, topological, metric, probabilistic) that make them very versatile.

During the years 1926–1932, the Hilbert space formalism of quantum mechanics, initiated in [84], is worked out systematically by von Neumann and culminated with his seminal book on the "Mathematical foundations of quantum mechanics" in 1932 (reprinted later in [149] and translated into French in 1946 [152] and into English in [150]) in 1955. [1] For this reason, von Neumann continued in searching for a better formulation of quantum mechanics that led him to develop the lattice theoretic approach (explained in chapter 13) and later to introduce the concept of what is presently nowadays known as "von Neumann algebras" (presented in chapter 11) as better adapted

1. Quite ironically, after having completed the Hilbert space formulation of quantum mechanics, von Neumann proved dissatisfied with his wonderful achievement. The following quotation is from Redei's historical account [122] on von Neumann's work:

to the formulation of quantum mechanics.

Despite the afterthoughts made by von Neumann, Hilbert space formulation of quantum mechanics remains a powerful tool allowing an elementary and pedagogical introduction to the topic. For the sake of completeness, some standard results on Hilbert spaces are reminded in this chapter. Most of the proofs in this chapter are omitted because they are considered as exercises; they can be found in the classical textbooks [3, 79, 87, 123, 127, 157] which are strongly recommended for further reading.

This chapter is written with two different readerships in mind: those interested solely in finite dimensional applications of quantum mechanics and those interested in full-fledged applications. The former can skip the passages printed in colour.

3.1 Scalar products and Hilbert spaces

Hilbert spaces have many distinct features. They are $\mathbb{C}$-vector spaces (hence are algebraic objects) equipped with a Hermitean scalar product (hence angles and geometry follow) from which a Hilbert norm can be defined (they thus become analytic objects) for which they are complete (hence a unit vector ψ has components on an orthonormal basis (e_n) reading $\sum_n |\psi_n|^2 = 1$; therefore its components can be interpreted as probability amplitudes).

Definition 3.1.1. Let $\mathbb{V}$ be a $\mathbb{C}$-vector space, $u, v, w \in \mathbb{V}$, and $\alpha, \beta \in \mathbb{C}$. A form $s : \mathbb{V} \times \mathbb{V} \to \mathbb{C}$ is

- **sesquilinear** if it is
  - linear with respect to the second [2] argument: $s(u, \alpha v + \beta w) = \alpha s(u, v) + \beta s(u, w)$, and
  - antilinear with respect to first argument: $s(\alpha u + \beta v, w) = \overline{\alpha} s(u, w) + \overline{\beta} s(v, w)$;
- **Hermitean** if it is sesquilinear and $\overline{s(u, v)} = s(v, u)$,
- **positive** if $s(v, v) \geq 0$, and
- **definite** if $s(v, v) = 0 \Leftrightarrow v = 0$.

A Hermitean positive definite form is a **a scalar product**. The scalar product s is denoted usually $\langle \cdot \,|\, \cdot \rangle$ and the pair $(\mathbb{V}, \langle \cdot \,|\, \cdot \rangle)$ is called a **pre-Hilbert space**. Two vectors v and w are called **orthogonal** if $\langle v \,|\, w \rangle = 0$.

> "I would like to make a confession which may seem immoral: I do not believe absolutely in Hilbert space any more. After all, Hilbert space (as far as quantum mechanical things are concerned) was obtained by generalizing Euclidean space, footing on the principle of conserving the validity of all formal rules. Now we begin to believe that it is not the vectors which matter, but the lattice of all linear (closed) subspaces. Because:
>
> 1. The vectors ought to represent the physical states, but they do it redundantly, up to a complex factor, only
> 2. and besides, the states are merely a derived notion, the primitive (phenomenologically given) notion being the qualities which correspond to the linear closed subspaces."

2. Notice that very often in the mathematical literature, the scalar product is defined to be linear with respect to its first argument. This is only a matter of taste that must be consistently kept in the whole formalism. We stick in the definition given here because it greatly simplifies formulæ arising in the quantum mechanical setting.

Lemma 3.1.2. *Let $(\mathbb{V}, \langle \cdot \,|\, \cdot \rangle)$ be a pre-Hilbert space and $u, v \in \mathbb{V}$. The following hold:*

- — ***Buniakowski-Cauchy-Schwarz inequality:*** $|\langle u \,|\, v \rangle| \leq \sqrt{\langle u \,|\, u \rangle}\sqrt{\langle v \,|\, v \rangle}$,
- — *The scalar product defines uniquely a norm $\|v\| = \sqrt{\langle v \,|\, v \rangle}$, called the **Hilbert norm**; the scalar product is recovered from the Hilbert norm through the **polarisation equality***

$$\langle u \,|\, v \rangle = \frac{1}{4}\sum_{k=0}^{3} i^k \|u + i^k v\|^2.$$

- — *The function $\langle \cdot \,|\, \cdot \rangle : \mathbb{V} \times \mathbb{V} \to \mathbb{C}$ (hence the norm) is continuous.*
- — *The **parallelogram rule** holds, i.e.*

$$\|u - v\|^2 + \|u + v\|^2 = 2\|u\|^2 + 2\|v\|^2.$$

Lemma 3.1.3. *[153, Th. 1.6, p. 9]: Let $(\mathbb{V}, \|\cdot\|)$ be a normed space. The norm is stemming from a scalar product on $\mathbb{V}$ if, and only if, the norm satisfies the parallelogram rule.*

Exercise 3.1.4. (Pythagoras theorem). Let $(\mathbb{V}, \langle \cdot \,|\, \cdot \rangle)$ be a vector space equipped with a scalar product and denote by $\|\cdot\|$ the corresponding Hilbert norm.

1. Show that if u and v are orthogonal then

$$\|u + v\|^2 = \|u\|^2 + \|v\|^2.$$

2. Is the condition of orthogonality necessary for the above equality to hold. *Hint:* consider $\mathbb{V}$ a *complex* pre-Hilbert space.

As stated above, the scalar product of a pre-Hilbert space $(\mathbb{V}, \langle \cdot \,|\, \cdot \rangle)$ induces a Hilbert norm $\|v\| = \sqrt{\langle v \,|\, v \rangle}$ turning $(\mathbb{V}, \|\cdot\|)$ into a **normed space**; furthermore, the Hilbert norm defines a distance $d(x, y) = \|x - y\|$, turning thus $(\mathbb{V}, d)$ into a **metric space**. We can therefore define the notion of a **fundamental (Cauchy) sequence** on $\mathbb{V}$ as being a sequence $\mathbf{v} = (v_n)_{n\in\mathbb{N}}$ of vectors $v_n \in \mathbb{V}$ such that for every $\varepsilon > 0$ there exists $N = N(\varepsilon) \in \mathbb{N}$ such that for $m, n \geq N$, we have $d(v_n, v_m) < \varepsilon$. Nevertheless, nothing imposes that any fundamental sequence converges within $\mathbb{V}$. If such is the case, the metric space $(\mathbb{V}, d)$ (or the normed space $(\mathbb{V}, \|\cdot\|)$ is termed **complete** or **Banach space**. A pre-Hilbert space that is complete for the metric induced by its Hilbert norm is called a **Hilbert space**. A subset $A \subset \mathbb{V}$ of a Banach space is termed **closed** if it contains the limits of all Cauchy sequences constructed from elements of A.

Usually we use the symbols $\mathbb{F}, \mathbb{G}, \mathbb{H}$ to denote Hilbert spaces instead of the generic symbol $\mathbb{U}, \mathbb{V}, \mathbb{W}, \mathbb{X}, \mathbb{Y}$, used for arbitrary spaces, i.e. when no further precision is given, $\mathbb{F}, \mathbb{G}, \mathbb{H}$ will stand for Hilbert spaces. In the same vein, vectors of a Hilbert space are usually denoted by e, f, g, h, etc. or $\varepsilon, \zeta, \eta, \phi, \psi$, etc. instead of the generic notation u, v, w, x, y, z, etc. for vectors in an arbitrary vector space.

Definition 3.1.5. Let $(\mathbb{V}, \|\cdot\|)$ be a normed space and $A \subset \mathbb{V}$. The **linear span** of A, denoted $\mathrm{vect}(A)$, is the intersection of all subspaces of $\mathbb{V}$ which contain A; the **closed linear span** of A, denoted $\overline{\mathrm{vect}}(A)$, is the intersection of all closed subspaces of $\mathbb{V}$ which contain A.

We recall that a complete metric space $(\hat{\mathbb{V}}, \hat{d})$ is called a **completion** of a metric space $(\mathbb{V}, d)$ if there exists an isometric embedding $\iota : \mathbb{V} \to \hat{\mathbb{V}}$ such that the image $\iota(\mathbb{V})$ is dense in $\hat{\mathbb{V}}$. An arbitrary normed space (not necessarily complete) can be completed via a standard procedure we recall here briefly. Let $\mathrm{CS}(\mathbb{V})$ be the set of Cauchy sequences on $\mathbb{V}$, $\sim$ an equivalence relation on $\mathrm{CS}(\mathbb{V})$ defined, for sequneces $\mathbf{v} = (v_n)$ and $\mathbf{w} = (w_n)$, by

$$\mathbf{v} \sim \mathbf{w} \iff \lim_{n\to\infty} \|v_n - w_n\| = 0,$$

and $\hat{\mathbb{V}} = \mathrm{CS}(\mathbb{V})/\sim$ the set of equivalence classes of $\sim$. The space $\hat{\mathbb{V}}$ has a natural vector space structure and through the definition

$$\hat{\mathbb{V}} \ni [\mathbf{v}] \mapsto \|[\mathbf{v}]\| = \lim_{n\to\infty} \|v_n\|$$

— that can be shown to be independent of the representative $\mathbf{v}$ of $[\mathbf{v}]$ — becomes a complete normed space. On identifying elements of $\mathbb{V}$ with constant sequences in $\hat{\mathbb{V}}$ we establish a canonical embedding $\iota : \mathbb{V} \to \hat{\mathbb{V}}$.

Theorem 3.1.6. *For each normed (pre-Hilbert) vector space $\mathbb{V}$, there exists a completion $\hat{\mathbb{V}}$. Two arbitrary completions (stemming from the same norm) are isomorphic.*

Proof. See [87, §1.6, pp. 17–21] or [153, Th. 4.11, p. 64]. □

Exercise 3.1.7. The following are classical examples of normed spaces.

1. The finite-dimensional vector space $\mathbb{V} = \mathbb{C}^d$ with the ordinary scalar product $\langle u \,|\, v \rangle = \sum_{n=1}^{d} \overline{u}_n v_n$ is obviously a Hilbert space.
2. Let $\mathbb{V} = \mathbb{M}_{d,d'}(\mathbb{C})$ the set of $d \times d'$ matrices with complex coefficients. Then $\langle u \,|\, v \rangle = \mathrm{tr}(u^* v)$, where u^* denotes the transposed complex conjugate matrix of u, is a scalar product.
3. On defining $\|\mathbf{v}\|_p = (\sum_{n\in\mathbb{N}} |v_n|^p)^{1/p}$ for $1 \le p < \infty$ and $\|\mathbf{v}\|_\infty = \sup_{n\in\mathbb{N}} |v_n|$, the spaces $\mathbb{V} = \ell^p(\mathbb{N})$ are complete normed (Banach) spaces [3] for all $1 \le p \le \infty$. The case $p = 2$ is very special, since $\ell^2(\mathbb{N})$ a Hilbert space with a scalar product, compatible with $\|\cdot\|_2$, defined by $\langle u \,|\, v \rangle = \sum_{n\in\mathbb{N}} \overline{u}_n v_n$. It is the infinite-dimensional generalisation of the example 1.
4. A finer classification of sequence spaces is possible. Let

$$\begin{aligned}
\ell^\infty &= \{v : \mathbb{N} \to \mathbb{C} \text{ s.t. } \|v\|_\infty := \sup_{n\in\mathbb{N}} |v_n| < \infty\},\\
c_0 &= \{v : \mathbb{N} \to \mathbb{C} \text{ s.t. } \lim_{n\in\mathbb{N}} v_n = 0\},\\
\ell^p &= \{v : \mathbb{N} \to \mathbb{C} \text{ s.t. } \|v\|_p^p := \sum_{n\in\mathbb{N}} |v_n|^p < \infty\}, 1 \le p < \infty,\\
s &= \{v : \mathbb{N} \to \mathbb{C} \text{ s.t. } \forall p \le 0, \lim_{n\in\mathbb{N}} n^p v_n = 0\},\\
f &= \{v : \mathbb{N} \to \mathbb{C} \text{ s.t. } v_n = 0 \text{ for all but finitely many } n\}.
\end{aligned}$$

3. Note that $\|\mathbf{v}\|_p = (\sum_{n\in\mathbb{N}} |v_n|^p)^{1/p}$ is well defined also for $0 < p < 1$; nevertheless, in those cases, $\|\mathbf{v}\|_p$ **is not a norm**. The spaces $(\ell^p(\mathbb{N}), d_p)$ with $d_p(\mathbf{v}, \mathbf{w}) = \sum_{n\in\mathbb{N}} |v_n - w_n|^p$ are metric spaces for $0 < p < 1$.

The following inclusions are in force for $1 \leq p < \infty$:

$$f \subset s \subset \ell^p \subset c_0 \subset \ell^\infty.$$

Moreover, the spaces ℓ^∞ and c_0 are Banach for the norm $\|\cdot\|_\infty$, ℓ^p is Banach for the norm $\|\cdot\|_p$, and s is a Fréchet space[4]. The interest of this cascade of inclusions is that f is dense in ℓ^p (for the norm $\|\cdot\|_p$, $p < \infty$) and dense in c_0 for the $\|\cdot\|_\infty$) norm. Even the set f of sequences with only rational coefficients is dense on ℓ^p and c_0 with the above norms; this result establishes the separability of ℓ^p and c_0. The space ℓ^∞ is not separable (see [123, page 69] for instance).

5. More generally, let $\mathbb{A}$ be an arbitrary set (not necessarily countable), $\mu : \mathbb{A} \to]0, \infty[$, and $p \in [1, \infty[$. Consider functions $v : \mathbb{A} \to \mathbb{C}$ vanishing outside a countable set (that generally depends on v) and denote by

$$\ell^p(\mathbb{A}, \mu) = \{v : \mathbb{A} \to \mathbb{C}, \text{ s.t. } v \equiv 0 \text{ but on a countable set, } \sum_{a \in \mathbb{A}} |v(a)|^p \mu(a) < \infty\} \subseteq \mathbb{C}^{\mathbb{A}}.$$

On defining $\|v\|_p := (\sum_{a \in \mathbb{A}} |v(a)|^p \mu(a))^{1/p}$, the space $\ell^p(\mathbb{A}, \mu)$ becomes a normed space. In particular, $\ell^2(A, \mu)$ is a Hilbert space.

6. The space $\mathbb{V} = L^p([a, b], \lambda)$ with $1 \leq p < \infty$ can be equipped with a norm $\|\cdot\|_p$ defined by $\|v\|_p = \left(\int_{[a,b]} |v(t)|^p \lambda(dt)\right)^{1/p}$. Then $(\mathbb{V}, \|\cdot\|_p)$ is a Banach space. For $p = 2$, it becomes also a Hilbert space for the scalar product $\langle u \,|\, v \rangle = \int_{[a,b]} \overline{u(t)} v(t) \lambda(dt)$.
7. The space $\mathbb{V} = C^k([a, b])$ can be equipped with a scalar product $\langle u \,|\, v \rangle = \sum_{j=0}^k \int_{[a,b]} \overline{u^{(j)}(t)} v^{(j)}(t) dt$. The corresponding norm is denoted $\|\cdot\|_{W^{k,2}}$ but the normed space $(\mathbb{V}, \|\cdot\|_{W^{k,2}})$ is not complete. Its completion is called **Sobolev space** $W^{k,2}([a, b])$ and is a Hilbert space. In particular, $W^{0,2}([a, b]) = L^2([a, b])$.

Recall that a subset C of a real or complex vector space $\mathbb{V}$ is **convex** if for all point (vectors) $x, y \in C$ and all $\lambda \in [0, 1]$, the point $\lambda x + (1 - \lambda) y$ belongs to C.

Theorem 3.1.8. *Let C be a non-empty, closed, convex set in a Hilbert space $\mathbb{H}$. For any $h \in \mathbb{H}$, there exists a unique point $c \in C$ lying closer to h than any other point of C, i.e.*

$$\forall h \in \mathbb{H}, \exists! c := c(h) \in C : \|h - c\| = \inf_{a \in C} \|h - a\|.$$

Corollary 3.1.9. *Let $\mathbb{G}$ be a Hilbert subspace of $\mathbb{H}$. Then, for all $h \in \mathbb{H}$, there exists a unique $g \in \mathbb{G}$, such that*

$$\|h - g\| = \inf_{f \in \mathbb{G}} \|h - f\| \text{ and } h - g \perp \mathbb{G}.$$

Exercise 3.1.10 (An important one for probabilists)**.** Let $\mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P}; \mathbb{R})$ denote the vector space of integrable random variables over some probability space $(\Omega, \mathcal{F}, \mathbb{P})$ and $\mathcal{G}$ a sub-σ-algebra of $\mathcal{F}$. Denote by $\mathbb{F} = \mathcal{L}^2(\Omega, \mathcal{F}, \mathbb{P}; \mathbb{R})$ and $\mathbb{G} = \mathcal{L}^2(\Omega, \mathcal{G}, \mathbb{P}; \mathbb{R})$. On $\mathbb{F}$ a sesquilinear form s can be defined by $s(X, Y) = \int_\Omega X(\omega) Y(\omega) \mathbb{P}(d\omega)$ that can be turned into a scalar product by considering the space L^2 instead of $\mathcal{L}^2$.

4. A Fréchet space is a locally convex topological vector space (i.e. a topological vector space which has a 0-neighborhood basis consisting of convex sets) whose topology 0-neighborhood basis is countable.

1. Use corollary 3.1.9 to establish that for every $X \in \mathbb{F}$ there exists a $Y \in \mathbb{G}$ (unique up to modifications differing from X on $\mathbb{P}$-negligible sets), such that $X - Y \perp Z$ for all $Z \in \mathbb{G}$.
2. Use the previous result, with $Z = \mathbb{1}_G$ for an arbitrary $G \in \mathcal{G}$, to establish that Y is a version of the **(classical) conditional expectation** $\mathbb{E}(X|\mathcal{G})$.
3. Use the density of $\mathcal{L}^2$ into $\mathcal{L}^1$ and the monotone convergence theorem to establish that for every random variable $X \in \mathcal{L}^1(\Omega, \mathcal{F}, \mathbb{P}; \mathbb{R})$, there exists a random variable $Y \in \mathcal{L}^1(\Omega, \mathcal{G}, \mathbb{P}; \mathbb{R})$ verifying

$$\forall G \in \mathcal{G}, \int_G X(\omega)\mathbb{P}(d\omega) = \int_G Y(\omega)\mathbb{P}(d\omega).$$

3.2 Orthogonal and orthonormal systems; orthogonal complements

Lemma 3.2.1. *Let $(e_i)_{i=1,\dots,n}$ be a collection of vectors of a Hilbert space $\mathbb{H}$.*

1. *If the collection are orthogonal, then $\| \sum_{i=1}^n e_i\|^2 = \sum_{i=1}^n \|e_i\|^2$.*
2. *If the collection are orthonormal, $(\lambda_i)_{i=1,\dots,n}$ are arbitrary complex numbers and $h \in \mathbb{H}$ arbitrary, then*

$$\|h - \sum_{i=1}^n \lambda_i e_i\|^2 = \|h\|^2 + \sum_{i=1}^n |\lambda_i - c_i|^2 - \sum_{i=1}^n |c_i|^2,$$

where $c_i = c_i(h) := \langle e_i \,|\, h \rangle$.

The significance of the previous result is better grasped in the following:

Theorem 3.2.2. *If $(e_i)_{i=1,\dots,n}$ is an orthonormal collection of vectors in $\mathbb{H}$, the vector $g \in \mathrm{vect}(e_1, \dots, e_n)$ lying closest to h is the vector $g = \sum_{i=1}^n \langle e_i \,|\, h \rangle e_i$, verifying $\|h - g\|^2 = \|h\|^2 - \sum_{i=1}^n |\langle e_i \,|\, h \rangle|^2$.*

In particular, if $h \in \mathrm{vect}(e_1, \dots, e_n)$, then $h = g = \sum_{i=1}^n \langle e_i \,|\, h \rangle e_i$. These results extend to the case of an infinitely denumerable orthonormal system.

Theorem 3.2.3 (Bessel inequality). *If $(e_n)_{n\in\mathbb{N}}$ is an orthonormal system in $\mathbb{H}$, then*

$$\forall h \in \mathbb{H}, \sum_{n\in\mathbb{N}} |\langle e_n \,|\, h \rangle|^2 \leq \|h\|^2.$$

Theorem 3.2.4. *Let $(e_n)_{n\in\mathbb{N}}$ be an orthonormal system in $\mathbb{H}$, and $(\lambda_n)_{n\in\mathbb{N}}$ a sequence of arbitrary complex numbers. Then $\sum_{n\in\mathbb{N}} \lambda_n e_n$ converges — in Hilbert norm — towards a vector $h \in \mathbb{H}$ if, and only if, $\sum_{n\in\mathbb{N}} |\lambda_n|^2 < \infty$.*

The complex numbers $\langle e_n \,|\, h \rangle$ are known as **Fourier coefficients** of h. Combined with Bessel's inequality, the previous theorem states that the Fourier series of any $h \in \mathbb{H}$ converges towards a vector of $g \in \mathbb{H}$. Without any additional condition however, it is not guaranteed that $g = h$. This additional condition is completeness of the orthonormal system $(e_n)_{n\in\mathbb{N}}$, defined in the following

Definition 3.2.5. Let $\mathbb{H}$ be a Hilbert space.

— A family (not necessarily countable) $(e_a)_{a\in A}$ of vectors (not necessarily orthonormal) of $\mathbb{H}$ is said to be **total** if

$$[\,\forall a \in A, \langle\, h \,|\, e_a \,\rangle = 0\,] \Rightarrow [\,h = 0\,].$$

— The space $\mathbb{H}$ is **separable** if it contains an at most infinitely countable dense subset.

Theorem 3.2.6. *If a Hilbert space $\mathbb{H}$ is separable, then the indexing set A of every orthonormal system $(e_a)_{a\in A}$ is countable, i.e. $|A| \leq \aleph_0$.*

Very often it is required the space to be separable, i.e. to possess a denumerable dense subset, but this requirement is not technically part of the definition of a Hilbert space. And as a matter of fact, there exist non separable Hilbert spaces as the following example shows.

Example 3.2.7. [See [3, §15, p. 49] or [154, Beispiel V.1(f), page 208] for instance]. Consider the family of functions $(e_\lambda)_{\lambda\in\mathbb{R}}$ defined, for $t \in \mathbb{R}$, by $e_\lambda(t) = \exp(i\lambda t)$. Form the linear hull $L = \text{vect}\{e_\lambda, \lambda \in \mathbb{R}\}$. For $f, g \in L$, define the scalar product $\langle\, g \,|\, h \,\rangle = \lim_{T\to\infty} \frac{1}{2T} \int_{-T}^{T} \overline{g}(t)h(t)\mathrm{d}t$. Since g and h are finite sums of vectors e_λ, i.e. $g(t) = \sum_{k=1}^{m} a_k e_{\lambda_k}(t)$ and $h(t) = \sum_{s=1}^{n} b_s e_{\mu_s}(t)$, their scalar product reads:

$$\begin{aligned}
\langle\, g \,|\, h \,\rangle &= \lim_{T\to\infty} \frac{1}{2T} \int_{-T}^{T} \overline{g}(t)h(t)\mathrm{d}t \\
&= \sum_{k=1}^{m}\sum_{s=1}^{n} \overline{a}_k b_s \left(\lim_{T\to\infty} \frac{1}{2T} \int_{-T}^{T} \exp(-it(\lambda_k - \mu_s))\mathrm{d}t \right) \\
&= \sum_{k=1}^{m}\sum_{s=1}^{n} \overline{a}_k b_s \delta_{\lambda_k,\mu_s}.
\end{aligned}$$

This scalar product induces a norm $\|g\|^2 = \sum_{k=1}^{m} |a_{\lambda_k}|^2$ because $\|g\|^2 \Leftrightarrow g = 0$. On completing L for the norm stemming from the above scalar product, we get a Hilbert space, denoted $\mathsf{AP}^2(\mathbb{R})$, which is not separable because it contains the uncountable orthonormal system $(e_\lambda)_{\lambda\in\mathbb{R}}$ (notice that $\|e_\lambda - e_\mu\| = \sqrt{2}$ for $\lambda \neq \mu$).

The mathematician Harald Bohr[5] [27] (see also [23]) showed that a continuous function g belongs to $\mathsf{AP}^2(\mathbb{R})$ if, and only if, is **almost-periodic**, i.e. for every $\varepsilon > 0$, there exists an $l := l(\varepsilon)$ such that in every interval of length l there exist a number τ: $|g(t+\tau) - g(t)| < \varepsilon$, for all $t \in \mathbb{R}$.

In the sequel, when we say Hilbert space **we always mean separable Hilbert space**. If $\mathbb{H}$ is separable, every total orthonormal system is denumerable (finite or infinite). An infinite sequence of vectors is total if and only if the sequence are closed in $\mathbb{H}$. For separable Hilbert spaces, the following theorem characterises total systems.

Theorem 3.2.8 (Characterising total systems for separable spaces)**.** *Let $(e_n)_{n\in\mathbb{N}}$ be an orthonormal system in $\mathbb{H}$. The following are equivalent:*

5. Brother of the physicist Niels Bohr, one of the prominent founders of quantum mechanics.

1. *The system $(e_n)_{n\in\mathbb{N}}$ in $\mathbb{H}$ is total.*
2. $\overline{\text{vect}}(e_n, n \in \mathbb{N}) = \mathbb{H}$.
3. *For all $h \in \mathbb{H}$, $\|h\|^2 = \sum_{n\in\mathbb{N}} |\langle e_n \,|\, h\rangle|^2$ (Parseval's equality).*
4. *For all $h \in \mathbb{H}$, $h = \sum_{n\in\mathbb{N}} \langle e_n \,|\, h\rangle e_n$, equality holding in Hilbert norm.*

Exercise 3.2.9. If $(e_n)_{n\in\mathbb{N}}$ is a total orthonormal system in $\mathbb{H}$, then for all $g, h \in \mathbb{H}$, $\langle g \,|\, h\rangle = \sum_{n\in\mathbb{N}} \langle g \,|\, e_n\rangle\langle e_n \,|\, h\rangle$.

Definition 3.2.10.
1. Two vectors $g, h \in \mathbb{H}$ are **orthogonal** if $\langle g \,|\, h\rangle = 0$.
2. Two subsets $A, B \subset \mathbb{H}$ are called **orthogonal** if $\forall a \in A$ and $\forall b \in B$, we have $\langle a \,|\, b\rangle = 0$.
3. If $A \subset \mathbb{H}$, its **orthogonal complement** is defined as

$$A^\perp := \{h \in \mathbb{H} : \forall a \in A, \langle a \,|\, h\rangle = 0\}.$$

Theorem 3.2.11. *If $A \subset \mathbb{H}$, then $A^\perp$ is a Hilbert subspace (closed vector subspace) of $\mathbb{H}$.*

Theorem 3.2.12. *Let $\mathbb{G}$ be a Hilbert subspace of $\mathbb{H}$ and $h \in \mathbb{H}$. Then $h \in \mathbb{G}^\perp$ if, and only if, for all $g \in \mathbb{G}$, we have $\|h - g\| \geq \|h\|$.*

Definition 3.2.13. Let $\mathbb{V}$ be a vector space and $\mathbb{X}, \mathbb{Y}$ vector subspaces of $\mathbb{V}$.

1. If for every $v \in \mathbb{V}$, there exists a unique $x \in \mathbb{X}$ (and consequently a unique $y \in \mathbb{Y}$) such that $v = x + y$, we say that $\mathbb{V}$ is the **direct sum** of $\mathbb{X}$ and $\mathbb{Y}$ and write $\mathbb{V} = \mathbb{X} \oplus \mathbb{Y}$.
2. If $\mathbb{X}$ is a Hilbert space (or at least is equipped with a scalar product) and $\mathbb{Y} = \mathbb{X}^\perp$, then $\mathbb{V} = \mathbb{X} \oplus \mathbb{X}^\perp$ is an **orthogonal direct sum**.

Example 3.2.14.
1. As special cases of the above example, consider, for instance, $\mathbb{V} = L^2([a,b])$ and $-\infty \leq a \leq c \leq b \leq \infty$, and $\mathbb{X} = \{f \in L^2(\mathbb{R}) : f = 0 \text{ for a.e. } x \in [a,c]\}$ and $\mathbb{Y} = \{f \in L^2(\mathbb{R}) : f = 0 \text{ for a.e. } x \in [c,b]\}$. Then $\mathbb{V} = \mathbb{X} \oplus \mathbb{Y}$ is an orthogonal direct sum.
2. In the same vein, let $\mathbb{V} = L^2([-a,a])$ for some $a > 0$, and $\mathbb{X}_\pm = \{f \in L^2([-a,a]) : f(x) = \pm f(-x), x \in [-a,a]\}$. Then $\mathbb{V} = \mathbb{X}_- \oplus \mathbb{X}_+$ is also an orthogonal direct sum.
3. Let $\mathbb{A}$ be an arbitrary set (not necessarily countable) and $(\mathbb{H}_\alpha)_{\alpha\in\mathbb{A}}$ a family of pre-Hilbert spaces. Define

$$\mathbb{H} = \{h = (h_\alpha)_{\alpha\in\mathbb{A}} \in \times_{\alpha\in\mathbb{A}}\mathbb{H}_\alpha, h_\alpha = 0 \text{ for all but countably many } \alpha, \sum_{\alpha\in\mathbb{A}} \|h_\alpha\|^2 < \infty\}.$$

Then $\langle h \,|\, h'\rangle = \sum_{\alpha\in\mathbb{A}} \langle h_\alpha \,|\, h'_\alpha\rangle$ is a scalar product on $\mathbb{H}$. $\mathbb{H}$ is Hilbert if, and only if, all spaces $\mathbb{H}_\alpha$ are Hilbert. On identifying

$$\mathbb{H}_\alpha \simeq \{(h_\beta)_{\beta\in\mathbb{A}} : h_\beta \in \mathbb{H}_\beta, \beta \in \mathbb{A}, \text{ and } h_\beta = 0 \text{ if } \beta \neq \alpha\},$$

the family $(\mathbb{H}_\gamma)_{\gamma\in\mathbb{A}}$ are mutually orthogonal subspaces of $\mathbb{H}$. The decomposition

$$\mathbb{H} = \oplus_{\alpha\in\mathbb{A}}\mathbb{H}_\alpha$$

provides with an orthogonal direct sum.

Exercise 3.2.15. Consider the space $\mathbb{H} = \ell^2(\mathbb{Z})$, endowed with an orthonormal basis $(\varepsilon_k)_{k\in\mathbb{Z}}$, and two sequences $\alpha, \beta \in \mathbb{H}$. For a $k \in \mathbb{Z}$, define $T_k : \mathbb{H} \to \mathbb{H}$ by the formula $(T_k\alpha)_n = \alpha_{n-k}$. Assume that α and β constitute **quadrature mirror filtres**, i.e. the family $(T_{2k}\alpha, T_{2k}\beta)_{k\in\mathbb{Z}}$ are an orthonormal basis of $\mathbb{H}$. For simplicity, we can assume that α and β are finitely supported.

1. Show that the sequence $\zeta = (\zeta_k)_{k\in\mathbb{Z}}$, with $\zeta_{2k} = \sum_{l\in\mathbb{Z}} \alpha_{2k-l}\varepsilon_l$ and $\zeta_{2k+1} = \sum_{l\in\mathbb{Z}} \beta_{2k-l}\varepsilon_l$, for $k \in \mathbb{Z}$ are a new orthonormal basis.
2. Denote by $\mathbb{H}_0 = \text{vect}(\zeta_{2k}, k \in \mathbb{Z})$ and $\mathbb{H}_1 = \text{vect}(\zeta_{2k+1}, k \in \mathbb{Z})$ (hence $\mathbb{H} = \mathbb{H}_0 \oplus \mathbb{H}_1$). This splitting can be iterated to get $\mathbb{H} = (\mathbb{H}_{00} \oplus \mathbb{H}_{01}) \oplus (\mathbb{H}_{10} \oplus \mathbb{H}_{11})$ and then a finite number of times. Show that these splittings generate new orthonormal bases of $\mathbb{H}$.

3.3 Duality

Definition 3.3.1. Let $\mathbb{V}$ be a $\mathbb{C}$-vector space. A map $F : \mathbb{V} \to \mathbb{C}$ such that for all $u, v \in \mathbb{V}$ and all $\lambda, \mu \in \mathbb{C}$,

$$F(\lambda u + \mu v) = \lambda F(u) + \mu F(v),$$

is called a **linear functional**. The space of all linear functionals on $\mathbb{V}$ is called the **(algebraic) dual** of $\mathbb{V}$. (It is itself a $\mathbb{C}$-vector space).

Example 3.3.2.
1. Let $\mathbb{V} = \mathbb{C}^n$ and $c_1, \dots, c_n$ be fixed complex numbers and $(e_1, \dots, e_n)$ a fixed basis of $\mathbb{V}$. The map F defined by $F(v) = \sum_{i=1}^n c_i v_i$ where (v_i) denote the components of v in the basis (e_i) is a linear functional.
2. $\mathbb{V} = C([0,1]; \mathbb{R})$ and $\mu \in \mathcal{M}_1(\mathcal{B}([0,1]))$ a probability measure on $[0,1]$ having a density ρ. The map $F(v) = \int_{[0,1]} v(t)\rho(t)dt$ is a linear functional.
3. $\mathbb{V} = L^1(\Omega, \mathcal{F}, \mathbb{P})$. The expectation of every integrable real random variable is a linear functional.
4. $\mathbb{V} = \mathbb{H}$ a Hilbert space and g a fixed vector in $\mathbb{H}$. The map $F(h) = \langle g \,|\, h \rangle$ is a linear functional.

When the vector space $\mathbb{V}$ is equipped with a norm $\|\cdot\|$, with which it is complete (Banach space), we can consider continuous linear functionals.

Theorem 3.3.3. *Let F be a linear functional on a complex Banach space $(\mathbb{V}, \|\cdot\|)$. The following are equivalent:*

1. *F is continuous everywhere.*
2. *F is continuous at point 0.*
3. $\sup\{|F(v)|, v \in \mathbb{V}, \|v\| \leq 1\} < \infty$.

The previous theorem establishes continuity of F provided it is bounded on the unit ball of $\mathbb{V}$. The bound $\sup\{|F(v)|, v \in \mathbb{V}, \|v\| \leq 1\}$ constitutes a norm, denoted $\|F\|$.

Theorem 3.3.4. *Let $(\mathbb{V}, \|\cdot\|)$ be a Banach space. The space of continuous linear functionals*

$$\mathbb{V}' = \{F : F \text{ continuous linear functional on } \mathbb{V}\}$$

*is called the **(topological) dual** of $\mathbb{V}$. When equipped with the norm $\|F\| = \sup\{|F(x)|, x \in \mathbb{V}, \|x\| \leq 1\}$, it becomes a Banach space on its own.*

Remark 3.3.5. The topological dual space of a Banach space $\mathbb{V}$ is usually (especially in the French and German literature) denoted by $\mathbb{V}'$. Mind however that this notation is not universal; in the Anglo-Saxon literature the dual is usually denoted by $\mathbb{V}^*$. There does not exist a universal convention for denoting the algebraic dual. The action of a linear form F on a vector $v \in \mathbb{V}$ is often denoted $\langle F, v\rangle$ and called the **duality pairing**. In finite dimension the algebraic and topological duals of a normed space coincide.

Example 3.3.6.
1. Let $\ell^p(\mathbb{N};\mathbb{R})$, with $1 \leq p < \infty$, and q the conjugate exponent verifying $1/p + 1/q = 1$. Then $(\ell^p)' = \ell^q$.
2. $c_0' = \ell^1$.
3. Let $\mathbb{X}$ be a metric (or topological) compact space and $\mathcal{X}$ its Borel σ-algebra. Then $C(\mathbb{X})' = \mathcal{M}(\mathbb{X}, \mathcal{X})$, where $\mathcal{M}(\cdot)$ denotes the set of regular (signed) Borel measures of finite variation (see for instance [154, Th. II.2.5, p. 62]).

Exercise 3.3.7. Show that if $F \in \mathbb{V}'$, then $|F(v)| \leq \|F\|\|v\|$.

The **bi-dual** $\mathbb{V}''$ of $\mathbb{V}$ is defined as $\mathbb{V}'' = (\mathbb{V}')'$. For every $v \in \mathbb{V}$, define $\iota(v) : \mathbb{V}' \to \mathbb{C}$ by $\iota(v)(F) = F(v)$, for all $F \in \mathbb{V}'$. Then the canonical linear map $\iota : \mathbb{V} \to \mathbb{V}''$ defined above is a (generally non-surjective) linear isometry.

The **pre-dual** of a space $\mathbb{W}$ is a space $\mathbb{V}$ whose dual is $\mathbb{W}$, i.e. verifying $\mathbb{V}' = \mathbb{W}$.

When the Banach space is a Hilbert space, we have a result generalising the corresponding result on finite dimensional Euclidean spaces, namely:

Theorem 3.3.8 (Fréchet-Riesz)**.** *For every continuous linear functional F on a Hilbert space $\mathbb{H}$, there exists a unique vector $f \in \mathbb{H}$ such that for all $h \in \mathbb{H}$, $F(h) = \langle f \,|\, h\rangle$. Additionally, $\|F\| = \|f\|$.*

The previous theorem establishes the existence of a map $T : \mathbb{H} \to \mathbb{H}'$ defined by the formula $Tf(\cdot) := \langle f \,|\, \cdot\rangle$. This mapping is antilinear (i.e. $T(\lambda f + \mu g) = \overline{\lambda} Tf + \overline{\mu} Tg$), isometric (i.e. $\|Tf\| = \|f\|$), and bijective. Therefore, T isometrically identifies $\mathbb{H}$ with its dual $\mathbb{H}'$; for this reason, we say that the Hilbert space is **self-dual**.

3.4 Linear operators, inverses, adjoints

Definition 3.4.1. Let $\mathbb{V}, \mathbb{W}$ be $\mathbb{C}$-vector spaces. A linear map $X : \mathbb{V} \to \mathbb{W}$ — i.e. satisfying for all $u, v \in \mathbb{V}$ and all $\lambda, \mu \in \mathbb{C}$, the linearity condition $X(\lambda u + \mu v) = \lambda Xu + \mu Xv$ — is called a **linear operator** (or simply operator) from $\mathbb{V}$ to $\mathbb{W}$.

1. The set of linear operators from $\mathbb{V}$ to $\mathbb{W}$ is denoted $\mathfrak{L}(\mathbb{V}, \mathbb{W})$ and is itself a $\mathbb{C}$-vector space; when $\mathbb{V} = \mathbb{W}$ we denote this set simply by $\mathfrak{L}(\mathbb{V})$. An operator $X \in \mathfrak{L}(\mathbb{V})$ is called (linear) operator on $\mathbb{V}$.

2. For $X \in \mathfrak{L}(\mathbb{V}, \mathbb{W})$, we define the **kernel** and the **range** respectively by

$$\ker X = \{v \in \mathbb{V} : Xv = 0\} \subset \mathbb{V} \quad \text{and} \quad \operatorname{im} X = \{Xv, v \in \mathbb{V}\} \subset \mathbb{W}.$$

3. When $(\mathbb{V}, \|\cdot\|_{\mathbb{V}})$ and $(\mathbb{W}, \|\cdot\|_{\mathbb{W}})$ are normed spaces, we can define

$$\|X\| = \|X\|_{\mathbb{V},\mathbb{W}} := \sup\{\|Xv\|_{\mathbb{W}}, v \in \mathbb{V}, \|v\|_{\mathbb{V}} \leq 1\}.$$

$\|\cdot\|$ is a norm, called **operator norm** [6]. The set

$$\mathfrak{B}(\mathbb{V}, \mathbb{W}) := \{X \in \mathfrak{L}(\mathbb{V}, \mathbb{W}) : \|X\| < \infty\},$$

(or simply $\mathfrak{B}(\mathbb{V})$ when $\mathbb{V} = \mathbb{W}$), is called the space of **bounded operators**. Equipped with the operator norm, it becomes a normed vector space on its own.

Exercise 3.4.2. Let $\mathbb{V}$ and $\mathbb{W}$ be normed spaces. Any bounded operator $X \in \mathfrak{B}(\mathbb{V}, \mathbb{W})$ is continuous.

Example 3.4.3.
1. $\mathfrak{L}(\mathbb{C}^m, \mathbb{C}^n) = \mathfrak{B}(\mathbb{C}^m, \mathbb{C}^n) = \mathbb{M}_{n\times m}(\mathbb{C})$.
2. For any vector space $\mathbb{V}$, its algebraic dual is $\mathfrak{L}(\mathbb{V}, \mathbb{C})$ and for any normed space $(\mathbb{V}, \|\cdot\|)$, $\mathbb{V}' = \mathfrak{B}(\mathbb{V}, \mathbb{C})$.
3. Let $\mathbb{H} = L^2([a,b];\mathbb{C})$ with $a < b$. For any function $f \in C([a,b];\mathbb{C})$ define the operator $M := M_f : \mathbb{H} \to \mathbb{H}$ by $Mh(t) = f(t)h(t), t \in [a,b]$. Then $M \in \mathfrak{B}(\mathbb{H})$, with $\|M\| = \|f\|_{\sup} = \sup_{t\in[a,b]} |f(t)|$, is called the **multiplication operator**.

As item 1 of the above example shows, all linear operators over finite dimensional Hilbert spaces are bounded. A natural question then arises: do there exist unbounded operators? The answer is yes but this can occur only on infinite dimensional spaces as the following example shows.

Example 3.4.4. Let $\mathbb{H} = \ell^2(\mathbb{N})$ and consider the multiplication operator $X \in \mathfrak{L}(\mathbb{H})$ defined by $Xh(n) = nh(n)$. Then X is not well defined on the whole space $\mathbb{H}$ but only on the set

$$D = \{h \in \mathbb{H} : \sum_{n\in\mathbb{N}} n^2|h(n)|^2 < \infty\} \subset \mathbb{H}.$$

For instance, although the sequence h with $h(n) = 1/n$ for $n \geq 1$ and $h(0) = 1$ belongs to $\mathbb{H}$, its image $Xh \notin \mathbb{H}$. The subset D is called the **domain** of X and denoted by $\mathsf{Dom}(X)$.

The above example is a general result: an unbounded operator on a vector space $\mathbb{V}$ can only be defined on a domain strictly smaller than $\mathbb{V}$. The operator is said to be **essentially defined** on $\mathbb{V}$ if $\mathsf{Dom}(X)$ is dense in $\mathbb{V}$.

In general, $\mathsf{im}(X)$ is not necessarily a (closed) subspace of $\mathbb{W}$. However, $\mathsf{im}(X)^\perp$ is always a closed subspace. This subspace is known as the **support** of X and denoted by $\mathsf{supp}(X)$. The **rank** of X is defined as $\mathsf{rank}(X) = \dim \mathsf{supp}(X)$.

Theorem 3.4.5. *If $(\mathbb{W}, \|\cdot\|)$ is a Banach space, then for every normed space $(\mathbb{V}, \|\cdot\|)$, the space $\mathfrak{B}(\mathbb{V}, \mathbb{W})$, equipped with the operator norm, is a Banach space.*

6. Sometimes, the operator norm is denoted $|||\cdot|||$.

Theorem 3.4.6. *If $\mathbb{U}, \mathbb{V}, \mathbb{W}$ are normed spaces, $X \in \mathfrak{B}(\mathbb{U}, \mathbb{V})$, and $Y \in \mathfrak{B}(\mathbb{V}, \mathbb{W})$, then $XY \in \mathfrak{B}(\mathbb{U}, \mathbb{W})$ and $\|XY\| \leq \|X\|\|Y\|$.*

Definition 3.4.7. An operator $X \in \mathfrak{B}(\mathbb{V}, \mathbb{W})$ is **invertible** if there exists an operator $Y \in \mathfrak{B}(\mathbb{W}, \mathbb{V})$, such that $YX = I_{\mathbb{V}}$ and $XY = I_{\mathbb{W}}$. The operator Y is then termed the **inverse** of X and is denoted by X^{-1}.

Remark 3.4.8. Notice that in the above definition X^{-1} is required to be bounded in order to be considered as the inverse of X. For instance, on $\mathbb{H} = \ell^2(\mathbb{N})$, let $(e_n)_{n\in\mathbb{N}}$ be a total orthonormal system and define the operator X by its action on it, e.g. $Xe_n = \lambda_n e_n$, with $\lambda_n \in \mathbb{C} \setminus \{0\}$ and $\sup_n |\lambda_n| < \infty$ (for instance if $\lambda_n = \frac{1}{n+1}$). Then $X \in \mathfrak{B}(\mathbb{H})$ and X^{-1} is well defined as an element of $\mathfrak{L}(\mathbb{H})$ but not necessarily of $\mathfrak{B}(\mathbb{H})$ since it may happen that $\|X^{-1}\| = \infty$; in that case, X **is not invertible**.

Exercise 3.4.9. If $\dim \mathbb{H} < \infty$ and $X \in \mathfrak{B}(\mathbb{H})$, the the following are equivalent:

1. X is invertible.
2. X is injective.
3. X is surjective.
4. $\exists Y \in \mathfrak{B}(\mathbb{H}) : XY = I$,
5. $\exists Y \in \mathfrak{B}(\mathbb{H}) : YX = I$.

Remark 3.4.10. In infinite dimension the above claims are not equivalent. Provide with an example!

Theorem 3.4.11. *Let $X \in \mathfrak{B}(\mathbb{H}, \mathbb{F})$. There exists a unique operator $Y \in \mathfrak{B}(\mathbb{F}, \mathbb{H})$ such that*

$$\forall f \in \mathbb{F}, \forall h \in \mathbb{H}, \langle f \,|\, Xh \rangle_{\mathbb{F}} = \langle Yf \,|\, h \rangle_{\mathbb{H}}.$$

*The operator Y is then denoted X^* and called the **adjoint operator** of X.*

Exercise 3.4.12. For $\mathbb{H} = \ell^2(\mathbb{N})$, show that the adjoint of the right shift is the left shift.

Theorem 3.4.13. *For any pair of Hilbert spaces $\mathbb{F}$ and $\mathbb{H}$, and any $X \in \mathfrak{B}(\mathbb{F}, \mathbb{H})$, we have $X^{**} = X$, where $X^{**} = (X^*)^*$. Moreover, $\|X^*\| = \|X\|$.*

Exercise 3.4.14. For $\mathbb{F}, \mathbb{G}, \mathbb{H}$ arbitrary Hilbert spaces, $X, X_1, X_2 \in \mathfrak{B}(\mathbb{F}, \mathbb{G})$, $Y \in \mathfrak{B}(\mathbb{G}, \mathbb{H})$, and $\lambda_1, \lambda_2 \in \mathbb{C}$, show that

1. $(YX)^* = X^*Y^*$.
2. $(\lambda_1 X_1 + \lambda_2 X_2)^* = \overline{\lambda_1} X_1^* + \overline{\lambda_2} X_2^*$.
3. $\|XY\| \leq \|X\|\|Y\|$.
4. $\|X\| = \|X^*\| = \|X^*X\|^{1/2}$.
5. If X is invertible, then X^* is invertible and $(X^*)^{-1} = (X^{-1})^*$.

3.5 Classes of operators

3.5.1 Normal operators

Definition 3.5.1. Let $X \in \mathfrak{B}(\mathbb{H})$ and X^* its adjoint. The operator X is termed

1. **normal** if $[X, X^*] := XX^* - X^*X = 0$,
2. **self-adjoint** if $X^* = X$,
3. **skew-adjoint** if $X^* = -X$ (hence iX is self-adjoint),
4. **unitary** if $XX^* = X^*X = I$.

Self-adjoint, skew-adjoint, and unitary operators are all normal; nevertheless there exist normal operators that are of none of those types. Consider, for example, $X = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$.

Exercise 3.5.2. Show that $X \in \mathfrak{B}(\mathbb{H})$ is normal if, and only if, $\|Xh\| = \|X^*h\|$ for all $h \in \mathbb{H}$.

Definition 3.5.3. Two Hilbert spaces are **isomorphic** if there exists $U : \mathbb{H}_1 \to \mathbb{H}_2$ that is unitary, i.e.

$$\langle Uh \,|\, Ug \rangle_{\mathbb{H}_2} = \langle h \,|\, g \rangle_{\mathbb{H}_1}, \forall h, g \in \mathbb{H}_1.$$

Corollary 3.5.4. *There exist only two types of separable spaces, those isomorphic to $\mathbb{C}^n$ (for some $n \in \mathbb{N}$) and those isomorphic to $\ell^2(\mathbb{N})$.*

Exercise 3.5.5. Show that if X is normal and U unitary, then $Y = UXU^*$ is normal.

3.5.2 Projections

Definition 3.5.6. Let $\mathbb{V}$ be a vector space and decomposed as a direct sum $\mathbb{V} = \mathbb{X} \oplus \mathbb{Y}$ into two vector subspaces $\mathbb{X}$ and $\mathbb{Y}$. Define a linear operator $P : \mathbb{V} \to \mathbb{X}$ by

$$\mathbb{V} \ni v = x + y \mapsto Pv = P(x + y) := x \in \mathbb{X}.$$

Remark 3.5.7. If P is the operator defined in 3.5.6, obviously $P^2v = P^2(x + y) = Px = x = Pv$. Hence $P^2 = P$. Additionally $\mathsf{im}\, P = \mathbb{X}$ and $\ker P = \mathbb{Y}$.

Definition 3.5.8. A **projection** on a vector space $\mathbb{V}$ is a linear operator $P \in \mathfrak{L}(\mathbb{V})$ satisfying the condition $P^2 = P$.

There exists a bijection between projections and decompositions in direct sums as stated in the following important

Theorem 3.5.9. *Let $\mathbb{V}$ be a vector space.*

1. *If an operator $P \in \mathfrak{L}(\mathbb{V})$ is a projection on $\mathbb{V}$, then $\mathbb{V} = \mathsf{im}\, P \oplus \ker P$.*
2. *If $\mathbb{X}$ and $\mathbb{Y}$ are vector subspaces of $\mathbb{V}$ such that $\mathbb{V} = \mathbb{X} \oplus \mathbb{Y}$, then there exists a projection P on $\mathbb{V}$ such that $\mathsf{im}\, P = \mathbb{X}$ and $\ker P = \mathbb{Y}$.*

When the vector space is a Hilbert space $\mathbb{H}$ (hence equipped with a scalar product) and $\mathbb{F}$ a Hilbert subspace of $\mathbb{H}$, obviously we can decompose the space into the orthogonal direct sum $\mathbb{H} = \mathbb{F} \oplus \mathbb{F}^\perp$. The projection operator is then defined analogously, thanks to the theorem 3.5.9, but now we have for $h = f + g$ and $h' = f' + g'$ that

$$\langle Ph \,|\, h' \rangle = \langle h \,|\, f' + g' \rangle = \langle f \,|\, f' \rangle = \langle f \,|\, Ph' \rangle = \langle h \,|\, Ph' \rangle.$$

We have thus:

Definition 3.5.10. A linear operator $P : \mathbb{H} \to \mathbb{H}$ is an **orthoprojection** on $\mathbb{H}$ if P is a projection (i.e. $P^2 = P$) and for every pair $h, h' \in \mathbb{H}$, we have $\langle Ph \,|\, h' \rangle = \langle h \,|\, Ph' \rangle$ (i.e. $P^* = P$). The set of orthoprojections of $\mathbb{H}$ is denoted by $\mathfrak{P}(\mathbb{H})$.

Again we can establish a bijection between orthoprojections and decompositions into orthogonal Hilbert subspaces as shown in the next

Theorem 3.5.11.
1. *If P is an orthoprojection on $\mathbb{H}$, then* $\mathsf{im}\, P$ *is closed and* $\mathbb{H} = \mathsf{im}\, P \oplus \ker P$.
2. *If $\mathbb{V}$ is a Hilbert subspace of $\mathbb{H}$ then there exists an orthoprojection P on $\mathbb{H}$ such that* $\mathsf{im}\, P = \mathbb{V}$ *and* $\ker P = \mathbb{V}^\perp$.

Exercise 3.5.12. Let $\mathbb{H} = L^2(\mathbb{R})$.

1. If $\mathbb{V}$ is the Hilbert subspace of even square integrable functions, then $\mathbb{V}^\perp$ is the Hilbert subspace of odd square integrable functions, then P, Q defined by
$$Ph(x) = \frac{h(x) + h(-x)}{2} \text{ and } Qh(x) = \frac{h(x) - h(-x)}{2},$$
are orthoprojections on $\mathbb{H}$.
2. If $A \in \mathcal{B}(\mathbb{R})$ and $\mathbb{V} = \{h \in \mathbb{H} : h = \mathbb{1}_A h\}$, then $\mathbb{V}$ is a vector subspace of $\mathbb{H}$ not necessarily closed. Nevertheless, an orthoprojection P can be associated with the decomposition $\mathbb{H} = \overline{\mathbb{V}} \oplus \mathbb{V}^\perp$, where $\overline{\mathbb{V}}$ is the Hilbert subspace of functions with support contained in $\overline{A}$.

Exercise 3.5.13. An orthoprojection $P \neq 0$ on $\mathbb{H}$ has norm $\|P\| = 1$. Therefore, any orthoprojection belongs to $\mathfrak{B}(\mathbb{H})$.

3.6 Various topologies on operator spaces

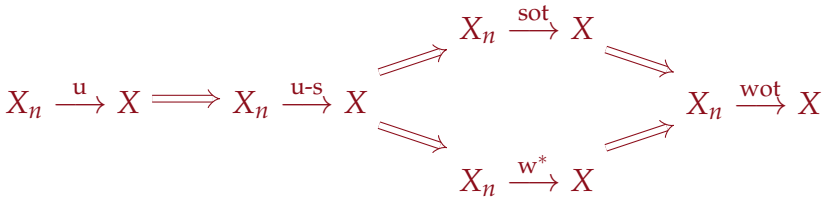
We shall consider limits of sequences of operators in $\mathcal{B}(\mathbb{H})$ and we have seen that this space is a Banach space for the operator norm. Nevertheless, the topology induced by the Hilbert norm is too fine for certain important sequences. For instance, let $(\varepsilon_n)_{n\in\mathbb{N}}$ be an orthonormal basis of $\mathbb{H}$ and E_n the orthoprojection on the one-dimensional space $\mathbb{C}\varepsilon_n$. Although the sum $\sum_n E_n$ does not converge in Hilbert norm, we can nevertheless show that $\lim_{N\to\infty} \| \sum_{n=1}^N E_n h - h\| = 0$ for every $h \in \mathbb{H}$. For many practical purposes, it is therefore important to have alternative ways to study asymptotic behaviour.

Definition 3.6.1. [Topologies]. Let $\mathbb{H}$ be a Hilbert space; denote by $(X_n)_{n\in\mathbb{N}}, X$ operators in $\mathcal{B}(\mathbb{H})$ and $g, h, (g_n)_{n\in\mathbb{N}}, (h_n)_{n\in\mathbb{N}}$ vectors in $\mathbb{H}$.

1. (X_n) converges **uniformly** or **in the operator norm topology** to X, if
$$\lim_{n\to\infty} \|X_n - X\| = 0.$$
We denote this convergence by $\lim_{n\to\infty} X_n \overset{\mathrm{u}}{=} X$.

2. (X_n) converges **ultrastrongly** or **in the ultrastrong operator topology** to X, if
$$\lim_{n\to\infty} \sum_{k\in\mathbb{N}} \|(X_n - X)h_k\| = 0,$$
for all sequences $(h_k) \in \mathbb{H}$ of vectors such that $\sum_{k\to\infty} \|h_k\|^2 < \infty$. We denote this convergence by $\lim_{n\to\infty} X_n \overset{\text{u-s}}{=} X$.
3. (X_n) converges **strongly** or **in the strong operator topology** to X, if
$$\lim_{n\to\infty} \|(X_n - X)h\| = 0,$$
for all $h \in \mathbb{H}$. We denote this convergence by $\lim_{n\to\infty} X_n \overset{\text{sot}}{=} X$.
4. (X_n) converges **weakly** or **in the weak operator topology** to X, if
$$\lim_{n\to\infty} |\langle g \,|\, (X_n - X)h \,\rangle| = 0,$$
for all $g, h \in \mathbb{H}$. We denote this convergence by $\lim_{n\to\infty} X_n \overset{\text{wot}}{=} X$.
5. (X_n) converges $*$**-weakly** or **in the weak* topology** to X, if
$$\sum_{k\to\infty} |\langle g_k \,|\, (X_n - X)h_k \,\rangle| = 0,$$
for all sequences of vectors $(g_k), (h_k) \in \mathbb{H}$, such that $\sum_{k\to\infty} \|g_k\|^2 < \infty$ and $\sum_{k\to\infty} \|h_k\|^2 < \infty$. We denote this convergence by $\lim_{n\to\infty} X_n \overset{\text{w}^*}{=} X$.

Sometimes, the term "ultraweak" is used in the literature instead of weak*. This choice is unfortunate since we have the following implications:



Hence the term ultraweak will be not used in this course.

It is also useful to have in mind bases of open neighborhoods for these topologies.

Uniform: $\mathcal{V}_\varepsilon(X) = \{Y \in \mathfrak{B}(\mathbb{H}) : \|X - Y\| < \varepsilon\}$.

Ultrastrong: $\mathcal{V}_\varepsilon(X, (h_k)_{k\in\mathbb{N}}) = \{Y \in \mathfrak{B}(\mathbb{H}) : \sum_{k\in\mathbb{N}} \|(X - Y)h_k\|^2 < \varepsilon\}$, where $(h_k)_{k\in\mathbb{N}}$ is an arbitrary sequence of vectors of $\mathbb{H}$ such that $\sum_{k\in\mathbb{N}} \|h_k\|^2 < \infty$.

Strong: $\mathcal{V}_\varepsilon(X, F) = \{Y \in \mathfrak{B}(\mathbb{H}) : \|(X - Y)f\| < \varepsilon, \forall f \in F\}$ where F is a finite subset of $\mathbb{H}$.

Weak*: $\mathcal{V}_\varepsilon(X, (g_k)_{k\in\mathbb{N}}, (h_k)_{k\in\mathbb{N}}) = \{Y \in \mathfrak{B}(\mathbb{H}) : \sum_{k\in\mathbb{N}} |\langle g_k \,|\, (X - Y)h_k \,\rangle|^2 < \varepsilon\}$, where $(g_k)_{k\in\mathbb{N}}$ and $(h_k)_{k\in\mathbb{N}}$ are an arbitrary sequences of vectors of $\mathbb{H}$ such that $\sum_{k\in\mathbb{N}} \|g_k\|^2 < \infty$ and $\sum_{k\in\mathbb{N}} \|h_k\|^2 < \infty$.

Weak: $\mathcal{V}_\varepsilon(X, F, G) = \{Y \in \mathfrak{B}(\mathbb{H}) : |\langle f \,|\, (X - Y)g \,\rangle| < \varepsilon, \forall f \in F, \forall g \in G\}$ where F and G are a finite subsets of $\mathbb{H}$.

3.7 Spectral theorem for normal operators ($\dim \mathbb{H} < \infty$)

The spectral theorem for infinite dimensional spaces is postponed until chapter 12. Here only the very basic notions are given for normal matrices.

Exercise 3.7.1. Let X be a $d \times d$ matrix with complex coefficients. Show that

1. If the matrix is diagonal, then is normal;
2. (by induction on the dimension) if the matrix is normal and upper triangular, then it is diagonal.
3. Conclude that a triangular matrix is normal if, and only if, it is diagonal.

We recall also Schur's theorem, a classical result in linear algebra (see [71, Proposition 18.3, p. 421] for instance):

Theorem 3.7.2 (Schur's theorem)**.** *Every $X \in \mathfrak{L}(\mathbb{C}^d)$ is unitarily similar to an upper triangular matrix*[7]*.*

Theorem 3.7.3 (Spectral theorem)**.** *Let $X \in \mathfrak{L}(\mathbb{C}^d)$. The following statements are equivalent:*

1. *X is normal.*
2. *X is unitarily similar to a diagonal matrix.*
3. *$\sum_{1\leq i,j\leq d} |X_{ij}|^2 = \sum_{1\leq i\leq d} |\lambda_i|^2$, where $\lambda_1, \ldots, \lambda_d$ are the eigenvalues of X counted with their multiplicity.*

Proof. $1 \Leftrightarrow 2$: By proposition 3.7.2, X is unitarily similar to an upper triangular matrix T. By exercise 3.5.5, normality of X is equivalent to normality of T. By exercise 3.7.1, T is equivalently diagonal. So X is unitarily similar to the diagonal matrix T.

$2 \Rightarrow 3$: Suppose X is unitarily similar to a diagonal matrix D. Hence the diagonal elements of D are the eigenvalues of X. We have thus:

$$\sum_{1\leq i,j\leq d} |X_{ij}|^2 = \mathrm{tr}(X^*X) = \mathrm{tr}(D^*D) = \sum_{1\leq i\leq d} |\lambda_i|^2.$$

$3 \Rightarrow 2$: By Schur's theorem 3.7.2, X is unitarily similar to an upper triangular matrix T. Hence,

$$\mathrm{tr}(X^*X) = \sum_{1\leq i,j\leq d} |X_{ij}|^2 = \mathrm{tr}(T^*T) = \sum_{1\leq i,j\leq d} |T_{ij}|^2.$$

But the triangular normal matrix T is in fact diagonal and its diagonal entries are the eigenvalues of X, i.e. $\sum_{1\leq i,j\leq d} |T_{ij}|^2 = \sum_{1\leq i\leq d} |T_{ii}|^2 = \sum_{1\leq i\leq d} |\lambda_i|^2$ because the non-diagonal entries of T vanish. Hence, X is unitarily similar to a diagonal matrix.

□

Corollary 3.7.4. *Let $\mathbb{H} \simeq \mathbb{C}^d$ for some d and $X \in \mathfrak{L}(\mathbb{H})$. X is normal if and only if there exists an orthonormal basis of $\mathbb{H}$ composed solely of eigenvectors of X.*

7. I.e. there exists a unitary matrix U such that $X = UTU^*$, where T is upper triangular.

If X is normal, on denoting $E[\lambda]$ the orthoprojection on the space spanned by the eigenvectors associated with the eigenvalue λ, the previous results mean that X is equal to $\sum_{\lambda\,\mathsf{spec}(X)} \lambda E[\lambda]$, where $\mathsf{spec}(X)$ is the set of eigenvalues of X. It will be established in 12 that this formula has an infinite dimensional generalisation to the expression $\int_{\mathsf{spec}(X)} \lambda E[\lambda]$, where E denotes now the spectral measure of X and $\mathsf{spec}(X)$ the spectrum of X.

Speaking of **spectral theory** for an operator X, we mean
— determining its spectrum,
— determining a spectral measure E on $(\mathbb{C}, \mathcal{B}(\mathbb{C}))$, and
— establishing that $X = \int_{\mathsf{spec}\,X} xE[dx]$.

3.8 Tensor product of Hilbert spaces

Tensor products appear naturally in quantum mechanics in order to deal with composite systems. Since this topic is scarcely touched in functional analysis courses, some precisions are due.

3.8.1 Algebraic aspects

In all this section, $\mathbb{V}, \mathbb{W}, \mathbb{X}$ denote $\mathbb{C}$-vector spaces and $\mathsf{Bil}(\mathbb{V} \times \mathbb{W}; \mathbb{X})$ the set of $\mathbb{X}$- valued bilinear mappings on $\mathbb{V} \times \mathbb{W}$ [8]. When $\mathbb{X} = \mathbb{C}$ we simplify notation for the set of bilinear forms to $\mathsf{Bil}(\mathbb{V} \times \mathbb{W})$. The symbols v, v_i will denote generically vectors of $\mathbb{V}$ and w, w_i vectors of $\mathbb{W}$. The symbols a, a_i, c, c_i, d, d_i denote generically complex numbers while β, b, B, τ denote bilinear forms.

Remark 3.8.1. Let $\beta \in \mathsf{Bil}(\mathbb{V} \times \mathbb{W}; \mathbb{X})$ and $S = \{\beta(v, w), v \in \mathbb{V}, w \in \mathbb{W}\}$. Note that in general S is a mere subset of $\mathbb{X}$ (i.e. S is not in general a vector subspace of $\mathbb{X}$) as the example [9] 3.8.2 shows. The vector subspace spanned by S is termed **image** of β, i.e.

$$\mathsf{im}\,\beta = \mathsf{vect}S = \mathsf{vect}\{\beta(v, w), v \in \mathbb{V}, w \in \mathbb{W}\}.$$

Example 3.8.2. Let $\mathbb{V} \simeq \mathbb{W} \simeq \mathbb{C}^2$, $\mathbb{X} \simeq \mathbb{C}^4$, and $(\varepsilon_0, \varepsilon_1)$ a basis of $\mathbb{C}^2$ and $(\zeta_0, \zeta_1, \zeta_2, \zeta_3)$ a basis of $\mathbb{C}^4$. Let $\beta \in \mathsf{Bil}(\mathbb{V} \times \mathbb{W}; \mathbb{X})$ be defined by its action on the basis vectors of $\mathbb{V}$ and $\mathbb{W}$ through the relationship $\beta(\varepsilon_i, \varepsilon_j) = \zeta_{\mathsf{num}(ij)}$, $i, j \in \{0, 1\}$. A vector $x \in \mathbb{X}$ will belong to S if, and only if, there exist two vectors $v \in \mathbb{V}$ and $w \in \mathbb{W}$ such that, on decomposing $v = \sum_{i=0}^{1} v_i \varepsilon_i$, $w = \sum_{i=0}^{1} w_i \varepsilon_i$, we have $x_{\mathsf{num}(ij)} = v_i w_j$ or, equivalently, that $x_0 x_3 - x_1 x_2 = 0$. We conclude that both vectors $x = 2\zeta_0 + 2\zeta_1 + \zeta_2 + \zeta_3$ and $y = \zeta_0 + \zeta_2$ of $\mathbb{X}$ fulfil the previous condition, hence $x \in S$ and $y \in S$. Nevertheless $x - y = \zeta_0 + 2\zeta_1 + z_3 \notin S$. Thus, S is not a subspace of $\mathbb{X}$.

Remark 3.8.3. Observe that

8. Recall that a mapping $\beta : \mathbb{V} \times \mathbb{W} \to \mathbb{X}$ is **bilinear** if it is separately linear with respect to both arguments.
9. From [73].

1. The set $\mathcal{L}(\mathbb{V},\mathbb{X})$ is isomorphic to the set $\mathsf{Hom}(\mathbb{V};\mathbb{X})$.
2. The set $\mathbb{V}\times\mathbb{W}$ can be endowed with a natural linear structure on defining
$$(v_1,w_1)+(v_2,w_2)=(v_1+v_2,w_1+w_2)$$
$$a(v,w)=(av,aw).$$
3. Nevertheless $\mathsf{Bil}(\mathbb{V}\times\mathbb{W};\mathbb{X})$ fails to be isomorphic to $\mathsf{Hom}(\mathbb{V}\times\mathbb{W};\mathbb{X})$.

In view of this remark, the natural question that arises is: does there exist a vector space $\mathbb{Y}$, somehow canonically derived from $\mathbb{V}$ and $\mathbb{W}$, such that $\mathsf{Bil}(\mathbb{V}\times\mathbb{W};\mathbb{X})$ becomes isomorphic to $\mathsf{Hom}(\mathbb{Y};\mathbb{X})$? As we shall see, the answer to this question is yes, at the expense of dealing with some space, provisionally denoted by $\mathbb{Y}$, that is much larger than $\mathbb{V}\times\mathbb{W}$. As a matter of fact, the space $\mathbb{Y}$ will be denoted later $\mathbb{V}\otimes\mathbb{W}$ and will be called the tensor product of $\mathbb{V}$ and $\mathbb{W}$. We follow the approach of [143, Chap. 39, pp. 403–410] in this section.

Definition 3.8.4. Let $\beta:\mathbb{V}\times\mathbb{W}\to\mathbb{X}$ be a bilinear map. The spaces $\mathbb{V}$ and $\mathbb{W}$ are **β-linearly disjoint** if, for any $n\in\mathbb{N}$ and for any two subsets $\{v_1,\dots,v_n\}\subset\mathbb{V}$ and $\{w_1,\dots,w_n\}\subset\mathbb{W}$ such that the $\sum_{i=1}^n\beta(v_i,w_i)=0$, it follows that the two conditions below hold:

1. if $(v_i)_{i=1,\dots,n}$ are linearly independent on $\mathbb{V}$, then $w_i=0,\forall i=1,\dots,n$,
2. if $(w_i)_{i=1,\dots,n}$ are linearly independent on $\mathbb{W}$, then $v_i=0,\forall i=1,\dots,n$.

The *raison d'être* of the technical definition 3.8.4 is justified by the instrumental definition 3.8.5 and notation 3.8.9.

Definition 3.8.5. An **algebraic tensor product** between the $\mathbb{K}$-vector spaces $\mathbb{V}$ and $\mathbb{W}$ is a pair $(\mathbb{Y},\tau)$ composed of a $\mathbb{K}$-vector space $\mathbb{Y}$ and a bilinear map $\tau:\mathbb{V}\times\mathbb{W}\to\mathbb{Y}$ such that

1. the image $\mathsf{im}\,\tau$ is exhaustive, i.e. $\tau(\mathbb{V}\times\mathbb{W})=\mathbb{Y}$, and
2. the spaces $\mathbb{V}$ and $\mathbb{W}$ are τ-linearly disjoint.

The rest of this subsection is devoted in establishing the existence of a tensor product, its uniqueness up to isomorphisms, and its, so-called, "universality", as formulated in the theorem 3.8.7 below. We start by an equivalent definition of linear disjointness.

Proposition 3.8.6. *Let $\mathbb{V},\mathbb{W}$, and $\mathbb{X}$ be three vector spaces and β a bilinear map between $\mathbb{V}\times\mathbb{W}$ and $\mathbb{X}$. The spaces $\mathbb{V}$ and $\mathbb{W}$ are β-linearly disjoint if, and only if, the following condition holds: for arbitrary linearly independent sets $\{v_1,\dots,v_m\}\subset\mathbb{V}$ and $\{w_1,\dots,w_n\}\subset\mathbb{W}$, with $m,n\in\mathbb{N}$, the set $\{x_{ij}=\beta(v_i,w_j),i=1,\dots,m,j=1,\dots,n\}\subset\mathbb{X}$ consists of linearly independent vectors.*

Proof. **[⇒]:** Let $\{v_1,\dots,v_m\}\subset\mathbb{V}$ and $\{w_1,\dots,w_n\}\subset\mathbb{W}$ be independent sets in their respective spaces and
$$\sum_{i=1}^m\sum_{j=1}^n c_{ij}x_{ij}=\sum_{i=1}^m\sum_{j=1}^n c_{ij}\beta(v_i,w_j)=0.$$

Bilinearity of β implies that $\sum_{i=1}^{m} \beta(v_i, W_i) = 0$ with $W_i = \sum_{j=1}^{n} c_{ij} w_j$, for $i = 1, \ldots, m$. Since the vectors (v_i) are linearly independent, linear disjointness implies that $W_1 = \ldots = W_m = 0$, i.e. for all $i = 1, \ldots, m$, $\sum_{j=1}^{n} c_{ij} w_j = 0$. But the vectors (w_j) are independent, therefore all $c_{ij} = 0$. Hence (x_{ij}) are linearly independent.

[⇐]: Suppose that $(v_i)_{i=1,\ldots,m}$ and $(w_i)_{i=1,\ldots,m}$ are vectors such that $\sum_{i=1}^{m} \beta(v_i, w_i) = 0$ and assume that the vectors $(v_i)_{i=1,\ldots,m}$ are independent (the case where the vectors $(w_i)_{i=1,\ldots,m}$ are assumed independent is treated analogously). Denote by $(z_j)_{j=1,\ldots,n}$ a basis (hence a linearly independent set) of the linear span $\mathrm{vect}(w_1, \ldots, w_m)$; hence every w_i, $i = 1, \ldots, m$, is expressible as a linear combination $w_i = \sum_{j=1}^{n} c_{ij} z_j$. We have then

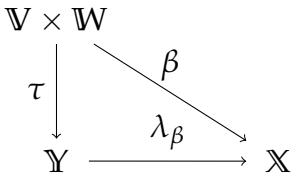
$$0 = \sum_{i=1}^{m} \beta(v_i, w_i) = \sum_{i=1}^{m} \beta(v_i, \sum_{j=1}^{n} c_{ij} z_j) = \sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} \beta(v_i, z_j) = \sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} y_{ij},$$

where $y_{ij} = \beta(v_i, z_j)$. Assume now that (y_{ij}) are independent; we conclude then that all coefficients $c_{ij} = 0$. But this implies that $w_i = 0$ for all $i = 1, \ldots, m$. We have thus established β-linear disjointness of $\mathbb{V}$ and $\mathbb{W}$.

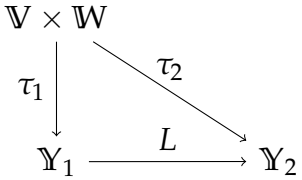
□

Theorem 3.8.7. *Let $\mathbb{V}$ and $\mathbb{W}$ be $\mathbb{K}$-vector spaces.*

1. *A tensor product $(\mathbb{Y}, \tau)$ of $\mathbb{V}$ and $\mathbb{W}$ always exists.*
2. *Let $(\mathbb{Y}, \tau)$ be a tensor product, $\mathbb{X}$ an arbitrary $\mathbb{K}$-vector space, and $\beta : \mathbb{V} \times \mathbb{W} \to \mathbb{X}$ an arbitrary bilinear map. Then there exists a unique linear map $\lambda := \lambda_\beta : \mathbb{Y} \to \mathbb{X}$ such that the following diagram commutes.*



3. *If $(\mathbb{Y}_1, \tau_1)$ and $(\mathbb{Y}_2, \tau_2)$ are two tensor products, then there exists a linear map $L : \mathbb{Y}_1 \to \mathbb{Y}_2$ such that the following diagram commutes.*



The item 2 of this theorem establishes a **universality property** of the map τ, in the sense that the same map τ serves to linearise any bilinear map β into a linear map λ_β. The vector space $\mathbb{Y}$, whose existence is proclaimed in the theorem 3.8.7, will be denoted $\mathbb{V} \otimes \mathbb{W}$ (and occasionally $\mathbb{V} \otimes_{\mathrm{alg}} \mathbb{W}$) in the sequel.

Definition 3.8.8. Let S be a fixed non empty set. A complex **formal sum** over S is an expression $\sum_{s\in S} a_s \cdot s$, in which only finitely many a_s are non-zero complex numbers. The set of all these formal sums become a vector space, called the **free vector space** over S, if addition and scalar multiplication is defined by

$$\sum_{s\in S} a_s \cdot s + \sum_{s\in S} a'_s \cdot s = \sum_{s\in S} (a_s + a'_s) \cdot s \text{ and } c \cdot \sum_{s\in S} a_s \cdot s = \sum_{s\in S} (ca_s) \cdot s.$$

This space is denoted by $\mathbb{F} := \mathbb{F}(S)$. Notice that $\mathbb{F}(S) \simeq \mathbb{C}^S$.

One can identify $\mathbb{F}(S)$ with

$$\hat{\mathbb{F}} := \hat{\mathbb{F}}(S) = \{f : S \to \mathbb{C} : f \equiv 0 \text{ outside a finite subset } F := F_f \text{ of } S\}.$$

On defining

$$e_s(s') = \begin{cases} 1 & \text{if } s = s' \\ 0 & \text{otherwise,} \end{cases}$$

we can write $f = \sum_{s\in F_f} a_s e_s$, i.e. $(e_s)_{s\in S}$ is a basis of $\hat{\mathbb{F}}$.

If $\mathbb{V}$ and $\mathbb{W}$ are two vector spaces, their Cartesian product $\mathbb{V} \times \mathbb{W}$ can be given a natural vector product structure as pointed out in remark 3.8.3. Nevertheless, we regard this product here as a *mere set of pairs* (v, w) *without any further structure.* In the free vector space $\mathbb{F} := \mathbb{F}(\mathbb{V} \times \mathbb{W})$ we cannot claim that $(v_1, w) + (v_2, w) = (v_1 + v_2, w)$ or that $a(v, w) = (a \cdot v, w)$ because these equalities *are not implied by the definition* 3.8.8.

The idea of the construction of the tensor product is to introduce a relation $\mathcal{R} \subset \mathbb{F} \times \mathbb{F}$, tailored to be the equivalence relation [10] that identifies naturally the following pairs

$$\begin{aligned} (v_1, w) + (v_2, w) &\text{ and } (v_1 + v_2, w), \\ (v, w_1) + (v, w_2) &\text{ and } (v, w_1 + w_2), \\ a \cdot (v, w) &\text{ and } (a \cdot v, w), \\ a \cdot (v, w) &\text{ and } (v, a \cdot w). \end{aligned}$$

The tensor product of $\mathbb{V}$ and $\mathbb{W}$ will be eventually defined as its equivalence classes $\mathbb{V} \otimes \mathbb{W} = \mathbb{F} \times \mathbb{F}/\mathcal{R}$.

Proof of theorem 3.8.7. 1. We start henceforth the explicit construction of a pair $(\mathbb{Y}, \tau)$, having the properties of a tensor product. It proves more convenient to work with $\hat{\mathbb{F}} := \hat{\mathbb{F}}(\mathbb{V} \times \mathbb{W})$. Consider the basis $(e_{(v,w)})_{(v,w)\in\mathbb{V}\times\mathbb{W}}$ of $\hat{\mathbb{F}}(\mathbb{V} \times \mathbb{W})$ and define

$$\hat{\mathbb{F}}_0 := \text{vect}\{e_{(\sum_{i=1}^m a_i v_i, \sum_{i=1}^n c_j w_j)} - \sum_{i=1}^m \sum_{i=1}^n a_i c_j e_{(v_i, w_j)}\},$$

with $m, n \in \mathbb{N}$, $(a_i), (b_j) \in \mathbb{C}$, $(v_i) \in \mathbb{V}$, and $(w_j) \in \mathbb{W}$. Denote further by $\mathbb{Y} = \hat{\mathbb{F}}/\hat{\mathbb{F}}_0$ the set of equivalence classes, by $\pi : \hat{\mathbb{F}} \to \mathbb{Y}$ the canonical projection and

10. Recall that a relation is an equivalence if it is reflexive ($I \subseteq \mathcal{R}$), symmetric ($\mathcal{R}^{-1} \subseteq \mathcal{R}$), and transitive ($\mathcal{R}^2 \subseteq \mathcal{R}$).

define $\tau : \mathbb{V} \times \mathbb{W} \to \mathbb{Y}$ by $\tau(v,w) := \pi(e_{(v,w)})$. Since the canonical projection is a linear map, the map τ is easily checked to be bilinear. As a matter of fact, $e_{(av+cv',w)} - ae_{(v,w)} - ce_{(v',w)} \in \ker(\pi)$. Therefore

$$\begin{aligned} 0 &= \pi(e_{(av+cv',w)} - ae_{(v,w)} - ce_{(v',w)}) \\ &= \pi(e_{(av+cv',w)}) - a\pi(e_{(v,w)}) - c\pi(e_{(v',w)}) \\ &= \tau(av+cv',w) - a\tau(v,w) - b\tau(v',w) \end{aligned}$$

establishes the linearity with respect to the first argument; the linearity with respect to the second one is obtained similarly.
We focus now on the linear span of τ. We have

$$\mathrm{vect}\{\tau(v,w), v \in \mathbb{V}, w \in \mathbb{W}\} = \mathrm{vect}\{\pi(e_{(v,w)}), v \in \mathbb{V}, w \in \mathbb{W}\} = \pi(\hat{\mathbb{F}}) = \mathbb{Y}.$$

Therefore item 1) of the definition 3.8.5 is satisfied.
It remains to establish the τ-linear disjointness of $\mathbb{V}$ and $\mathbb{W}$. Let $r \in \mathbb{N}$ and $(v_1, \ldots, v_r) \subset \mathbb{V}$, $(w_1, \ldots, w_r) \subset \mathbb{W}$ be such that $\sum_{i=1}^r \tau(v_i, w_i) = 0$ and suppose that $(w_1, \ldots, w_r)$ are linearly independent. For every linear form $f \in \mathbb{V}'$, define the linear map $L_f : \hat{\mathbb{F}} \to \mathbb{W}$ by its action on the basis elements: $L_f(e_{v,w}) = f(v)w$. We remark that the map L_f vanishes on $\hat{\mathbb{F}}_0$ since, by linearity of f,

$$L_f(e_{av+cv',w} - ae_{v,w} - ce_{v',w}) = f(av+cv')w - af(v)w - cf(v')w = 0.$$

Consequently, L_f induces a map $\tilde{L}_f : \mathbb{Y} \to \mathbb{W}$ such that for all $\psi \in \hat{\mathbb{F}}$, we have $\tilde{L}_f(\pi(\psi)) = L_f(\psi)$. Now $0 = \sum_{i=1}^r \tau(v_i, w_i) = \pi(\sum_{i=1}^r e_{v_i,w_i})$. Hence

$$0 = \tilde{L}_f(\pi(\sum_{i=1}^r e_{v_i,w_i})) = L_f(\sum_{i=1}^r e_{v_i,w_i}) = \sum_{i=1}^r f(v_i)w_i.$$

But $(w_i)_i$ are supposed linearly independent. Therefore the previous equality means that $\forall i = 1, \ldots, r : f(v_i) = 0$. But this conclusion holds for arbitrary $f \in \mathbb{V}'$; consequently $\forall i = 1, \ldots, r : v_i = 0$. We have thus established item 2) of he definition 3.8.5. Interchanging the roles of $(v_i)_i$ and $(w_i)_i$, we establish similarly item 1). Thus the spaces are τ-linearly disjoint. This result, combined with the exhaustivity of the image of τ, proves the existence of the tensor product $(\mathbb{Y}, \tau)$.

2. Let $(\mathbb{Y}, \tau)$ be a tensor product of spaces $\mathbb{V}$ and $\mathbb{W}$, $\mathbb{X}$ a vector space, and $\beta : \mathbb{V} \times \mathbb{W} \to \mathbb{X}$ a bilinear form. Denote by $(v_i)_{i\in I}$ and $(w_j)_{j\in J}$ two bases of $\mathbb{V}$ and $\mathbb{W}$. We know that $(\tau(v_i, w_j))_{i\in I, j\in J}$ is total in $\mathbb{Y}$ because $\mathrm{vect}(\tau(\mathbb{V} \times \mathbb{W})) = \mathbb{Y}$; by proposition 3.8.6, we know further that $(\tau(v_i, w_j))_{i\in I, j\in J}$ are linearly independent. Hence they form a basis of $\mathbb{Y}$. We construct thus the map λ_β as the unique linear map $\mathbb{Y} \to \mathbb{X}$ such that

$$\forall i \in I, \forall j \in J, \lambda_\beta(\tau(v_i, w_j)) := \beta(v_i, w_j).$$

We have thus proven the commutativity of the diagram.

3. It remains to establish uniqueness (up to isomorphisms) of the tensor product. Let $(\mathbb{Y}_1, \tau_1)$ and $(\mathbb{Y}_2, \tau_2)$ be two tensor products of the spaces $\mathbb{V}$ and $\mathbb{W}$. We denote by λ_{12} the map linearising the bilinear form $\tau_2 : \mathbb{V} \times \mathbb{W} \to \mathbb{Y}_2$ and by

λ_{21} the map linearising the bilinear form $\tau_1 : \mathbb{V} \times \mathbb{W} \to \mathbb{Y}_1$. Applying twice the commutativity of the diagrams, we get

$$\lambda_{12} \circ \tau_1 = \tau_2$$
$$\lambda_{21} \circ \tau_2 = \tau_1.$$

We conclude that $\lambda_{12} = \lambda_{21}^{-1}$, establishing thus the isomorphism of $\mathbb{Y}_1$ and $\mathbb{Y}_2$.

□

Notation 3.8.9. The $\mathbb{K}$-vector space $\mathbb{Y}$, introduced in 3.8.7, will henceforth be denoted $\mathbb{V} \otimes \mathbb{W}$ and termed the **algebraic tensor product** of the vector spaces $\mathbb{V}$ and $\mathbb{W}$. The map τ assigns to every pair of vectors (v, w) their tensor product $\tau(v, w) = v \otimes w$.

Note that $\forall v \in \mathbb{V}$ and $\forall w \in \mathbb{W}$

$$0_{\mathbb{V}} \otimes w = v \otimes 0_{\mathbb{W}} = 0_{\mathbb{V}\otimes\mathbb{W}}.$$

Similarly, for all $a, c \in \mathbb{C}$ such that $ac = 1$, we have

$$v \otimes w = (av) \otimes (cw).$$

In the same vein, any $\Psi = \sum_j c_j g_j \otimes h_j \in \mathbb{G} \otimes \mathbb{H}$ can be rewritten as

$$\Psi = \sum_k \varepsilon_k \otimes \psi_k = \sum_l \phi_l \otimes \zeta_l,$$

where $(\varepsilon_k)_k$ is an orthonormal system in $\mathrm{vect}\{g_j, j = 1, \ldots, m\}$ and $(\zeta_l)_l$ is an orthonormal system in $\mathrm{vect}\{h_j, j = 1, \ldots, m\}$ respectively.

Definition 3.8.10. Elements of $\mathbb{V} \otimes \mathbb{W}$ are called **tensors**. The set $\mathbb{T} = \{v \otimes w : v \in \mathbb{V}, w \in \mathbb{W}\}$ generates $\mathbb{V} \otimes \mathbb{W}$. Elements of $\mathbb{T}$ are called **simple or factored tensors** while the elements of $(\mathbb{V} \otimes \mathbb{W}) \setminus \mathbb{T}$ are the **entangled tensors**.

Since the set $\mathbb{T}$ generates $\mathbb{V} \otimes \mathbb{W}$, it follows that every tensor $t \in \mathbb{T}$ admits a representation $t = \sum_{i\in I} v_i \otimes w_i$, with a finite family I. As no condition is imposed on the vectors v_i and w_i, this representation is not unique.

The tensor product between vectors defined above satisfies obviously the following equalities:

$$(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w,$$
$$v \otimes (w_1 + w_2) = v \otimes (w_1 + w_2)$$
$$\lambda \cdot v \otimes w = (\lambda \cdot v) \otimes w) = v \otimes (\lambda \cdot w).$$

Corollary 3.8.11. $\dim(\mathbb{V} \otimes \mathbb{W}) = \dim \mathbb{V} \dim \mathbb{W}$.

Exercise 3.8.12. Let $X : \mathbb{V} \to \mathbb{X}$ and $Y : \mathbb{W} \to \mathbb{Y}$ be linear maps. Define the bilinear map B by

$$(v, w) \mapsto B(v, w) = Xv \otimes Yw.$$

Let L be the linearising map of B. Show [11] that $L(v \otimes w) = Xv \otimes Yw$.

11. We write $X \otimes Y$ instead of L for this linear map.

Definition 3.8.13. If $X : \mathbb{V} \to \mathbb{X}$ and $Y : \mathbb{W} \to \mathbb{Y}$ are linear operators, we define $X \otimes Y : \mathbb{V} \otimes \mathbb{W} \to \mathbb{X} \otimes \mathbb{Y}$ by

$$(X \otimes Y)(v \otimes w) = (Xv) \otimes (Yw).$$

Example 3.8.14. (Tensor product of finite dimensional spaces). If $\mathbb{V} = \mathbb{C}^m$ and $\mathbb{W} = \mathbb{C}^n$, then $\mathbb{V} \otimes \mathbb{W} = \mathbb{C}^{mn}$. Denote by $(v_i)_{i\in\{1,\dots,m\}}$ and $(w_j)_{j\in\{1,\dots,n\}}$ the Fourier coefficients of two arbitrary vectors $v \in \mathbb{V}$ and $w \in \mathbb{W}$ in arbitrary (fixed) bases of $\mathbb{V}$ and $\mathbb{W}$. Then, in the derived basis of $\mathbb{V} \otimes \mathbb{W}$, the canonical map τ is defined by

$$\tau\left((v_i)_{i\in\{1,\dots,m\}}, (w_j)_{j\in\{1,\dots,n\}}\right) = \left((v_i w_j)_{i\in\{1,\dots,m\}, j\in\{1,\dots,n\}}\right) \in \mathbb{V} \otimes \mathbb{W}.$$

Example 3.8.15. (Tensor product of functions). Let A and B be two sets, and f, g complex-valued functions on A and B. Denote by $f \otimes g$ the function on $A \times B$ defined by

$$A \times B \ni (a, b) \mapsto f \otimes g(a, b) := f(a)g(a) \in \mathbb{C}.$$

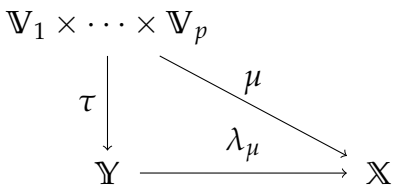
Denote by $\mathbb{F} = \{f : A \to \mathbb{C}\}$ and $\mathbb{G} = \{g : B \to \mathbb{C}\}$. On defining $\mathbb{F} \otimes \mathbb{G} = \mathsf{vect}\{f \otimes g : f \in \mathbb{F}, g \in \mathbb{G}\}$, we see immediately that $\mathbb{F} \otimes \mathbb{G}$ is the tensor product of $\mathbb{F}$ and $\mathbb{G}$. If both A and B are topological spaces, and recalling that the support of a function is the closure of the set of points on which the function does not vanish, we verify immediately that $\mathsf{supp}(f \otimes g) = \mathsf{supp}(f) \times \mathsf{supp}(g)$.

3.8.2 Extension by multi-linearity

The notion of tensor product between two vector spaces can be extended to a tensor product among an arbitrary number of spaces by multilinearity. More specifically, we have the following

Definition 3.8.16. Let $(\mathbb{V}_i)_{i=1,\dots,p}$ be a family of $\mathbb{K}$-vector spaces and $\mathbb{X}$ a vector space. A tensor product of the family $(\mathbb{V}_i)_{i=1,\dots,p}$ is a pair $(\mathbb{Y}, \tau)$ composed of a $\mathbb{K}$-vector space $\mathbb{Y}$ and a multilinear map (p-linear) $\tau := \tau_p : \mathbb{V}_1 \times \cdots \times \mathbb{V}_p \to \mathbb{Y}$ such that

1. $\mathsf{im}\,\tau$ is exhaustive, i.e. $\tau(\mathbb{V}_1 \times \cdots \times \mathbb{V}_p) = \mathbb{Y}$, and
2. their exists a unique (up to isomorphisms) universal linear map $\lambda_\mu : \mathbb{Y} \to \mathbb{X}$, such that, for every multilinear (p-linear) mapping $\mu : \mathbb{V}_1 \times \cdots \times \mathbb{V}_p \to \mathbb{X}$ on an arbitrary $\mathbb{K}$-vector space $\mathbb{X}$, the universality property



holds.

The tensor product space $\mathbb{Y} = \tau_p(\mathbb{V}_1 \times \cdots \times \mathbb{V}_p)$ is usually denoted $\mathbb{V}_1 \otimes \cdots \otimes \mathbb{V}_p$ and when $\mathbb{V}_1 = \ldots = \mathbb{V}_p = \mathbb{V}$, the tensor product $(\mathbb{Y}, \tau)$ is denoted $(\mathbb{V}^{\otimes p}, \otimes^p)$.

Remark 3.8.17. The mappings τ_p can be defined inductively: $\tau_2 \equiv \tau$ and, for $p \geq 3$, $\tau_p(v_1, v_2, v_3) = \tau_2(\tau_{p-1}(v_1, \dots, v_{p-1}), v_p)$.

3.8.3 Symmetric and skew-symmetric tensors

As stated in the symmetrisation postulate (supplement to postulate 2.6.1), important classes of tensors are the symmetric and the skew-symmetric ones since they serve as state representatives of particular quantum systems (bosons and fermions respectively).

Let $\mathbb{S}_p$ denote the symmetric group on p objects and $\mathbb{V}^{\otimes p}$ the p-fold tensor product of a vector space $\mathbb{V}$, $p \geq 2$. Define, for every $\sigma \in \mathbb{S}_p$, an operator U_σ acting on $\mathbb{V}^{\otimes p}$ by its action on factored tensors $t = v_1 \otimes \cdots \otimes v_p$:

$$U_\sigma(t) = U_\sigma(v_1 \otimes \cdots \otimes v_p) = v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(p)}.$$

Obviously, $U \in \mathsf{Aut}(\mathbb{V}^{\otimes p})$. Moreover, for $\sigma, \sigma' \in \mathbb{S}_p$, $U_\sigma U_{\sigma'} = U_{\sigma\sigma'}$ and if σ' is the identity permutation $\mathbb{1}$, then $U_{\sigma\mathbb{1}} = U_\sigma$, hence U is a representation of $\mathbb{S}_p$.

Consider now the subspace $\mathcal{N}^p(\mathbb{V}) \subseteq \mathbb{V}^{\otimes p}$ generated by products $v_1 \otimes \cdots \otimes v_p$ such that $v_i = v_j$ for at least one pair $i \neq j$, with $1 \leq i, j \leq p$.

Lemma 3.8.18. *For all $t \in \mathbb{V}^{\otimes p}$ and all $\sigma \in \mathbb{S}_p$,*

$$t - \mathrm{sign}(\sigma) U_\sigma t \in \mathcal{N}^p(\mathbb{V}).$$

Proof. It is enough to establish the result for factored tensors $t = v_1 \otimes \cdots \otimes v_p \in \mathbb{V}^{\otimes p}$.

Step 1: Assume that σ is the transposition $i \leftrightarrow j$. We have then

$$\begin{aligned} t - \mathrm{sign}(\sigma) U_\sigma t &= v_1 \otimes \cdots \otimes v_i \otimes \cdots \otimes v_j \otimes \cdots \otimes v_p \\ &\quad + v_1 \otimes \cdots \otimes v_j \otimes \cdots \otimes v_i \otimes \cdots \otimes v_p \\ &= v_1 \otimes \cdots \otimes (v_i + v_j) \otimes \cdots \otimes (v_i + v_j) \otimes \cdots \otimes v_p \\ &\quad - v_1 \otimes \cdots \otimes v_i \otimes \cdots \otimes v_i \otimes \cdots \otimes v_p \\ &\quad - v_1 \otimes \cdots \otimes v_j \otimes \cdots \otimes v_j \otimes \cdots \otimes v_p \in \mathcal{N}^p(\mathbb{V}). \end{aligned}$$

Step 2: Assume that the result has been established for all $\sigma \in \mathbb{S}_p$ such that σ is the product of m ($m < p$) transpositions. We shall establish that the result holds for $\sigma\sigma'$, where σ' is a transposition. By the reccurrence hypothesis, $t - \mathrm{sign}(\sigma) U_\sigma t \in N_p(\mathbb{V})$. Since $\mathcal{N}^p(\mathbb{V})$ is stable under transpositions, we have further that $U_{\sigma'} t - \mathrm{sign}(\sigma) U_{\sigma'} U_\sigma t \in \mathcal{N}^p(\mathbb{V})$. Multiplying by $\mathrm{sign}(\sigma')$ we get $\mathrm{sign}(\sigma') U_{\sigma'} t - \mathrm{sign}(\sigma'\sigma) U_{\sigma'\sigma} t \in \mathcal{N}^p(\mathbb{V})$. On the other hand, $t - \mathrm{sign}(\sigma') U_{\sigma'} t \in \mathcal{N}^p(\mathbb{V})$. Adding the above relations, we get $t - \mathrm{sign}(\sigma'\sigma) U_{\sigma'\sigma} t \in \mathcal{N}^p(\mathbb{V})$.

The claimed result holds by induction. □

Definition 3.8.19. Define the linear operator $A_p : \mathbb{V}^{\otimes p} \to \mathbb{V}^{\otimes p}$ by

$$A_p = \frac{1}{p!} \sum_{\sigma \in \mathbb{S}_p} \mathrm{sign}(\sigma) U_\sigma.$$

This operator is called the **anti-symmetriser**; the subspace $\mathcal{A}^p(\mathbb{V}) = \mathsf{im}(A_p) \subseteq \mathbb{V}^{\otimes p}$ is the **subspace of skew-symmetric tensors**.

Lemma 3.8.20. *The anti-symmetriser is a projector; moreover*

$$\ker A_p = \mathcal{N}^p(\mathbb{V}).$$

Proof. Let $v_1, \ldots, v_p$ be linearly independent vectors of $\mathbb{V}$. Then, for every $\sigma \in \mathbb{S}_p$, the vectors $v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(p)}$ are linearly independent in $\mathbb{V}^{\otimes p}$. It follows that

$$A_p(v_1 \otimes \cdots v_p) = \sum_{\sigma \in \mathbb{S}_p} \mathrm{sign}(\sigma) v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(p)} \neq 0.$$

Hence, we have

$$A_p U_\sigma = \mathrm{sign}(\sigma) A_p, \forall \sigma \in \mathbb{S}_p.$$

Suppose now that $t = v_1 \otimes \cdots v_p$ is a generator of $\mathcal{N}^p(\mathbb{V})$, i.e. $v_i = v_j$ for some pair i, j with $i \neq j$. Let σ be the transposition $i \leftrightarrow j$. Then $U_\sigma t = t$. Hence, $A_p U_\sigma t = A_p t = \mathrm{sign}(\sigma) A_p t = -A_p t$. Therefore $A_p t = -A_p t \Rightarrow A_p t = 0 \Rightarrow \mathcal{N}^p(\mathbb{V}) \subseteq \ker A_p$.

To establish the reverse inclusion, observe that, for all $t \in \mathbb{V}^{\otimes p}$, we have

$$A_p t - t = \frac{1}{p!} \sum_{\sigma \in \mathbb{S}_p} (\mathrm{sign}(\sigma) U_\sigma t - t) \in \mathcal{N}^p(\mathbb{V}).$$

Now, if $t \in \ker A_p$, then $A_p t = 0$ and consquently $t \in \mathcal{N}^p(\mathbb{V})$.

To prove the projective nature of A_p, in view of the previous result, we have,

$$A_p^2 t - A_p t = 0, \forall t \in \mathbb{V}^{\otimes p}$$

because $\mathcal{N}^p(\mathbb{V}) = \ker \mathbb{A}_p$. Hence $A_p^2 = A_p$. □

Remark 3.8.21. We conclude that the following direct decomposition holds:

$$\mathbb{V}^{\otimes p} = \ker A_p \oplus \mathrm{im}\, A_p = \mathcal{N}^p(\mathbb{V}) \oplus \mathcal{A}^p(\mathbb{V}).$$

For every $t \in \mathbb{V}^{\otimes p}$, the vector $A_p t$ is the skew-symmetric part of t.

In the same vein, define

$$\mathcal{M}^p(\mathbb{V}) = \mathrm{vect}\{t - U_\sigma t, t \in \mathbb{V}^{\otimes p}, \sigma \in \mathbb{S}_p \text{ a transposition}\}.$$

Using similar arguments as in the proof of lemma 3.8.18, we establish the following

Lemma 3.8.22. *For all $t \in \mathbb{V}^{\otimes p}$ and all $\sigma \in \mathbb{S}_p$, we have*

$$t - U_\sigma t \in \mathcal{M}^p(\mathbb{V}).$$

Definition 3.8.23. The linear operator $S_p : \mathbb{V}^{\otimes p} \to \mathbb{V}^{\otimes p}$ defined by

$$S_p = \frac{1}{p!} \sum_{\sigma \in \mathbb{S}_p} U_\sigma$$

is called the **symmetriser**; the image of the symmetriser $\mathcal{S}^p(\mathbb{V}) = \mathrm{im}\, S_p \subseteq \mathbb{V}^{\otimes p}$ is the **subspace of symmetric tensors**.

Lemma 3.8.24. *The symmetriser is a projector; moreover*

$$\ker S_p = \mathcal{M}^p(\mathbb{V}).$$

Remark 3.8.25. We conclude that the following direct decomposition holds:

$$\mathbb{V}^{\otimes p} = \ker S_p \oplus \operatorname{im} S_p = \mathcal{M}^p(\mathbb{V}) \oplus \mathcal{S}^p(\mathbb{V}).$$

For every $t \in \mathbb{V}^{\otimes p}$, the vector $S_p t$ is the symmetric part of t.

Notation 3.8.26. Let $\mathbb{V}$ be a vector space with $d = \dim(\mathbb{V})$, $\mathbb{B} \simeq \{0, \dots, d-1\}$ an indexing set for any basis of $\mathbb{V}$, and $\{v_1, \dots, v_d\}$ a set of d (distinct) non null vectors of $\mathbb{V}$.

— Write as usual

$$\mathbb{B}^p = \{\boldsymbol{\beta} = (\beta_1, \dots, \beta_p) \text{ s.t. } \forall i = 1, \dots, p, \beta_i \in \mathbb{B}\}.$$

— Similarly, write $\mathbb{B}^p_{\neq} = \emptyset$ when $p > d$, and

$$\mathbb{B}^p_{\neq} = \{\boldsymbol{\beta} = (\beta_1, \dots, \beta_p) \text{ s.t. } \forall i = 1, \dots, p, \beta_i \in \mathbb{B} \text{ and } \beta_i \neq \beta_j, \text{ for } i \neq j\} \subset \mathbb{B}^p,$$

when $p \leq d$.

— We define now an equivalence relation on $\mathbb{B}^p$ (or $\mathbb{B}^p_{\neq}$) by identifying words $\boldsymbol{\beta}$ and $\boldsymbol{\gamma}$ when they are connected by a permutation, i.e. $\exists \sigma \in \mathrm{S}_p$, such that $\gamma_i = \beta_{\sigma(i)}$. We write

$$\mathbb{B}^p_B = \mathbb{B}^p/\mathrm{S}_p = \{[\boldsymbol{\beta}] = [\beta_1 \cdots \beta_p], 0 \leq \beta_1 \leq \cdots \leq \beta_p \leq d-1\}$$
$$\mathbb{B}^p_F = \mathbb{B}^p_{\neq}/\mathrm{S}_p = \{[\boldsymbol{\beta}] = [\beta_1 \cdots \beta_p], 0 \leq \beta_1 < \cdots < \beta_p \leq d-1\},$$

for the indistinguishable p-uples of elements of $\mathbb{B}$, i.e. the set of equivalence classes of words identified by permutations. We denote by $\mathbb{B}^p_B$ those where the same letter can be re-used — i.e. letters are sampled with replacement (without exclusion) — and by $\mathbb{B}^p_F$ those where each letter can be used at most once — i.e. letters are sampled without replacement (with exclusion). The subscripts B et F stand for **bosonic** and **fermionic** statistics.

— Given a set $\{v_1, \dots, v_p\}$ of distinct vectors and $\boldsymbol{\beta} \in \mathbb{B}^p$ we write $\mathbf{v}(\boldsymbol{\beta}) := v_{\beta_1} \otimes \cdots \otimes v_{\beta_p}$.

— Let now $(\varepsilon_0, \dots, \varepsilon_{d-1})$ be a basis of $\mathbb{V}$. Then,

$$\forall \boldsymbol{\beta} \in \mathbb{B}^p : S_p(\varepsilon_{\beta_1} \otimes \cdots \otimes \varepsilon_{\beta_p}) = \frac{1}{p!} \sum_{\sigma \in \mathrm{S}_p} U_\sigma\left(\boldsymbol{\varepsilon}(\boldsymbol{\beta})\right) = \frac{1}{p!} \sum_{\boldsymbol{\gamma} \in [\boldsymbol{\beta}]} \boldsymbol{\varepsilon}(\boldsymbol{\gamma})$$

$$\forall \boldsymbol{\beta} \in \mathbb{B}^p_{\neq} : A_p(\varepsilon_{\beta_1} \otimes \cdots \otimes \varepsilon_{\beta_p}) = \frac{1}{p!} \sum_{\sigma \in \mathrm{S}_p} \operatorname{sign}(\sigma) U_\sigma\left(\boldsymbol{\varepsilon}(\boldsymbol{\beta})\right) = \frac{1}{p!} \sum_{\boldsymbol{\gamma} \in [\boldsymbol{\beta}]} \operatorname{sign}(\boldsymbol{\gamma}) \boldsymbol{\varepsilon}(\boldsymbol{\gamma}).$$

— Since the equivalence classes $[\boldsymbol{\beta}] \in \mathbb{B}^p_B$ (or in $\mathbb{B}^p_F$) do not depend on the order of the letters appearing in $[\boldsymbol{\beta}]$ but only on the number of appearances of each letter, on defining $\boldsymbol{\nu} : \mathbb{B}^p \to \mathbb{N}^d$ by $\boldsymbol{\nu}(\boldsymbol{\beta}) = \sum_{i=1}^p \mathbb{1}_{\{b\}}(\beta_i)$, for $b \in \mathbb{B}$, we see that $S_p(\boldsymbol{\varepsilon}(\boldsymbol{\beta}))$ can be uniquely determined by $\boldsymbol{\nu}(\boldsymbol{\gamma})$, for an aribtrary $\boldsymbol{\gamma} \in [\boldsymbol{\beta}]$ and similarly for $A_p(\boldsymbol{\varepsilon}(\boldsymbol{\beta}))$. Such a representation is termed **number representation** and plays an important role in second quantisation. For every $b \in \mathbb{B}$, we have

— in the bosonic case: $0 \leq \nu_b \leq p$,
— in the fermionic case: $0 \leq \nu_b \leq 1$.
Obviously in both cases $\sum_{b\in\mathbb{B}} \nu_b(\boldsymbol{\beta}) = p$. Moreover, the equivalence class $[\boldsymbol{\beta}]$ is uniquely determined by the vector $\boldsymbol{\nu}(\boldsymbol{\gamma})$, for an arbitrary $\boldsymbol{\gamma} \in [\boldsymbol{\beta}]$. Moreover, given an arbitrary decomposition of p into d non-negative integers $p = p_1 + \ldots + p_d$, there exists a (unique) equivalence class $[\boldsymbol{\beta}] \in \mathbb{B}^p_B$ such that $\nu_b([\boldsymbol{\beta}]) = p_b, \forall b \in \mathbb{B}$.

Example 3.8.27. For $d = 3$ and $p = 2$, we get

$$\begin{aligned}
\mathbb{B}^p &= \{00, 01, 02, 10, 11, 12, 20, 21, 22\}\\
\mathbb{B}^p_B &= \{[00], [01], [02], [11], [12], [22]\}\\
\mathbb{B}^p_{\neq} &= \{01, 02, 10, 12, 20, 21\}\\
\mathbb{B}^p_F &= \{[01], [02], [12]\}.
\end{aligned}$$

$[\boldsymbol{\beta}] \in \mathbb{B}^p_B$	$\gamma \in [\boldsymbol{\beta}]$	$\boldsymbol{\nu}(\boldsymbol{\beta})$	$S_p(\boldsymbol{\varepsilon}([\boldsymbol{\beta}]))$	$[\boldsymbol{\beta}] \in \mathbb{B}^p_F$	$\gamma \in [\boldsymbol{\beta}]$	$\boldsymbol{\nu}(\boldsymbol{\beta})$	$A_p(\boldsymbol{\varepsilon}([\boldsymbol{\beta}]))$
[00]	00	200	$\varepsilon_0 \otimes \varepsilon_0$	$\emptyset$			
[01]	01 10	110	$\frac{1}{2!}(\varepsilon_0 \otimes \varepsilon_1 + \varepsilon_1 \otimes \varepsilon_0)$	[01]	01 10	110	$\frac{1}{2!}(\varepsilon_0 \otimes \varepsilon_1 - \varepsilon_1 \otimes \varepsilon_0)$
[02]	02 20	101	$\frac{1}{2!}(\varepsilon_0 \otimes \varepsilon_2 + \varepsilon_2 \otimes \varepsilon_0)$	[02]	02 20	101	$\frac{1}{2!}(\varepsilon_0 \otimes \varepsilon_2 - \varepsilon_2 \otimes \varepsilon_0)$
[11]	11	020	$\varepsilon_1 \otimes \varepsilon_1$	$\emptyset$			
[12]	12 21	011	$\frac{1}{2!}(\varepsilon_1 \otimes \varepsilon_2 + \varepsilon_2 \otimes \varepsilon_1)$	[12]	12 21	011	$\frac{1}{2!}(\varepsilon_1 \otimes \varepsilon_2 - \varepsilon_2 \otimes \varepsilon_1)$
[22]	22	002	$\varepsilon_2 \otimes \varepsilon_2$	$\emptyset$			

Exercise 3.8.28. Let $d = \dim \mathbb{V}$ and $(\varepsilon_1, \ldots, \varepsilon_d)$ a basis of $\mathbb{V}^{\otimes p}$ and $\mathbb{B} \simeq \{0, \ldots, d-1\}$ an indexing set for the basis. It is evident then that
— $\big(A_p(\boldsymbol{\varepsilon}(\boldsymbol{\beta}))\big)_{\boldsymbol{\beta}\in\mathbb{B}^p}$ is a total set $\mathcal{A}^p(\mathbb{V})$ and
— $\big(S_p(\boldsymbol{\varepsilon}(\boldsymbol{\beta}))\big)_{\boldsymbol{\beta}\in\mathbb{B}^p}$ is a total set in $\mathcal{S}^p(\mathbb{V})$.
However these sets are not necessarily independent.

1. Show that
   (a) $|\mathbb{B}^p| = d^p$,
   (b) $|\mathbb{B}^p_{\neq}| = \frac{d!}{(d-p)!}$ for $p \leq d$ (and 0 otherwise),
   (c) $|\mathbb{B}^p_B| = C^p_{p+d-1}$, and
   (d) $|\mathbb{B}^p_F| = C^p_d$ for $p \leq d$ (and 0 otherwise).
2. Show that for every $\boldsymbol{\gamma} \in [\boldsymbol{\beta}]$, and every $[\boldsymbol{\beta}] \in \mathbb{B}^p_B$, the vector $S_p(\boldsymbol{\varepsilon}(\boldsymbol{\gamma}))$ is constant, i.e. $S_p(\boldsymbol{\varepsilon}(\boldsymbol{\beta}))$ depends only on $[\boldsymbol{\beta}] \in \mathbb{B}^p_B$.
3. Similarly, for every $\boldsymbol{\gamma} \in [\boldsymbol{\beta}]$, and every $[\boldsymbol{\beta}] \in \mathbb{B}^p_F$, the vector $A_p(\boldsymbol{\varepsilon}(\boldsymbol{\gamma}))$ is constant, i.e. $A_p(\boldsymbol{\varepsilon}(\boldsymbol{\beta}))$ depends only on $[\boldsymbol{\beta}] \in \mathbb{B}^p_F$.
4. Conclude that

$$\dim \mathcal{S}^p(\mathbb{V}) = C^p_{p+d-1} \quad \text{and} \quad \dim \mathcal{A}^p(\mathbb{V}) = \begin{cases} C^p_d & \text{if } p \leq \dim \mathbb{V} \\ 0 & \text{otherwise.} \end{cases}$$

5. Conclude that if $d = 2$ then $\mathbb{V}^{\otimes 2} = \mathcal{A}^2(\mathbb{V}) \oplus \mathcal{S}^2(\mathbb{V})$.

3.8.4 Tensor product of Hilbert spaces: the finite dimensional case

Consider the case of finite dimensional Hilbert spaces $\mathbb{G}$ and $\mathbb{H}$ with bases $(\varepsilon_i)_{i=1,\dots,m}$ and $(\zeta_j)_{j=1,\dots,n}$ respectively. Decomposing arbitrary vectors $g \in \mathbb{G}$ and $h \in \mathbb{H}$ on these bases, $g = \sum_{i=1}^m g_i \varepsilon_i$ and $h = \sum_{j=1}^n h_i \zeta_j$, and using the bilinearity of the map τ, we get

$$\tau(g,h) = g \otimes h = \sum_{i=1}^m \sum_{j=1}^n g_i h_j \varepsilon_i \otimes \zeta_j,$$

where $\varepsilon_i \otimes \zeta_j := \tau(\varepsilon_i, \zeta_j)$. Since $(\varepsilon_i \otimes \zeta_j)_{i,j}$ span the space $\mathbb{G} \otimes \mathbb{H}$ and they are independent, they form a basis of $\mathbb{G} \otimes \mathbb{H}$. Unless otherwise stated, the standard ordering of the basis elements of the tensor product space will be chosen as the **lexicographic** ordering of the individual vectors.

We can now extend the notion of scalar product on $\mathbb{G} \otimes \mathbb{H}$.

Proposition 3.8.29. *Let $\mathbb{G}, \mathbb{H}$ be given finite-dimensional Hilbert spaces and $s : (\mathbb{G} \otimes \mathbb{H}) \times (\mathbb{G} \otimes \mathbb{H}) \to \mathbb{C}$ be given by*

$$s(\sum_{j=1}^m a_j g_j \otimes h_j, \sum_{k=1}^n c_k g_k \otimes h_k) = \sum_{j=1}^m \sum_{k=1}^n \overline{a}_j c_k \langle\, g_j \,|\, g_k \,\rangle \langle\, h_j \,|\, h_k \,\rangle.$$

Then

1. *s is sesquilinear,*
2. *s is a scalar product.*

Proof. 1. Obvious!

2. To show that s is a scalar product, we must show that, for $\Psi \in \mathbb{G} \otimes \mathbb{H}$, the fact $s(\Psi, \Psi) = 0$ implies $\Psi = 0$. Let $\Psi = \sum_{j=1}^n c_j g_j \otimes h_j \in \mathbb{G} \otimes \mathbb{H}$ and $(\varepsilon_a)_{a=1,\dots,p}$ an orthonormal basis of $\mathrm{vect}\{g_1, \dots, g_m\}$ and $(\zeta_b)_{b=1,\dots,q}$ an orthonormal basis of $\mathrm{vect}\{h_1, \dots, h_n\}$. Then

$$\begin{aligned} s(\varepsilon_a \otimes \zeta_b, \Psi) &= \sum_{j=1}^n c_j s(\varepsilon_a \otimes \zeta_b, g_j \otimes h_j) \\ &= \sum_{j=1}^n c_j \langle\, \varepsilon_a \,|\, g_j \,\rangle \langle\, \zeta_b \,|\, h_j \,\rangle \\ &=: d_{ab}. \end{aligned}$$

Since $(\varepsilon_a \otimes \zeta_b)_{ab}$ is a basis of the subspace in which lives Ψ, the quantities d_{ab} defined above are the Fourier coefficients of Ψ in that basis, i.e. $\Psi = \sum_{a,b} d_{ab} \varepsilon_a \otimes \zeta_b$. Hence $s(\Psi, \Psi) = \sum_{a,b} |d_{ab}|^2$ and

$$[s(\Psi, \Psi) = 0] \Longrightarrow [\forall a, b,\ d_{ab} = 0] \Longrightarrow [\Psi = 0].$$

□

If $\mathbb{G}$ and $\mathbb{H}$ are finite-dimensional, the previous result shows that $\mathbb{G} \otimes \mathbb{H}$ is also a Hilbert space for the scalar product defined by s.

Example 3.8.30. Let $\mathbb{G} \cong \mathbb{H} \cong \mathbb{C}^2$ equipped with orthonormal bases $(\varepsilon_1, \varepsilon_2)$ and (ζ_1, ζ_2) respectively. The operators $X \in \mathfrak{L}(\mathbb{G})$ and $Y \in \mathfrak{L}(\mathbb{H})$ are represented in the respective bases of $\mathbb{G}$ and $\mathbb{H}$ by the matrices

$$X = \begin{pmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{pmatrix} \text{ and } Y = \begin{pmatrix} Y_{11} & Y_{12} \\ Y_{21} & Y_{22} \end{pmatrix},$$

where $X_{ij} = \langle \varepsilon_i \,|\, X\varepsilon_j \rangle$ and $Y_{ij} = \langle \zeta_i \,|\, Y\zeta_j \rangle$, for $i, j = 1, 2$. The operator $X \otimes Y \in \mathfrak{L}(\mathbb{G} \otimes \mathbb{H})$ will be represented on the lexicographically ordered basis $(\varepsilon_1 \otimes \zeta_1, \varepsilon_1 \otimes \zeta_2, \varepsilon_2 \otimes \zeta_1, \varepsilon_2 \otimes \zeta_2)$ by the matrix

$$X \otimes Y = \begin{pmatrix} X_{11}Y_{11} & X_{11}Y_{12} & X_{12}Y_{11} & X_{12}Y_{12} \\ X_{11}Y_{21} & X_{11}Y_{22} & X_{12}Y_{21} & X_{12}Y_{22} \\ X_{21}Y_{11} & X_{21}Y_{12} & X_{22}Y_{11} & X_{22}Y_{12} \\ X_{21}Y_{21} & X_{21}Y_{22} & X_{22}Y_{12} & X_{22}Y_{22} \end{pmatrix} = \begin{pmatrix} X_{11}Y & X_{12}Y \\ X_{21}Y & X_{22}Y \end{pmatrix} \neq \begin{pmatrix} XY_{11} & XY_{12} \\ XY_{21} & XY_{22} \end{pmatrix} = Y \otimes X,$$

i.e. $(X \otimes Y)_{ij,kl} := \langle \varepsilon_i \otimes \zeta_j \,|\, X \otimes Y\varepsilon_k \otimes \zeta_l \rangle = X_{ik}Y_{jl}$, for $i, j, k, l = 1, 2$.

3.8.5 Tensor product of Hilbert spaces: the infinite dimensional case

In the infinite dimensional case, we can still introduce the sesquilinear form of proposition 3.8.29 and establish that it defines a scalar product on the algebraic tensor product of the Hilbert spaces. However, the completion of $\mathbb{H}_1 \otimes \mathbb{H}_2$, denoted $\mathbb{H}_1 \widehat{\otimes} \mathbb{H}_2$, by the corresponding norm fails to verify the universality property in the categorical sense [12].

This impossibility led Grothendieck to introduce the notion of nuclear spaces in [74, 75, 76] in order to give a satisfactory general definition of the tensor product of topological spaces.

In the sequel, we follow the construction of [92, pp. 125–139] (where detailed proofs can be found) of a Hilbert space with a tensor product satisfying the universality property.

Definition 3.8.31. Let $\mathbb{H}_1, \ldots, \mathbb{H}_n$ be Hilbert spaces. A **bounded multilinear functional** is a map $\phi : \mathbb{H}_1 \times \cdots \times \mathbb{H}_n \to \mathbb{C}$ a map that is linear in each of its arguments (while the other arguments remain fixed), verifying

$$|\phi(h_1, \ldots, h_n) \leq C\|h_1\| \cdots \|h_n\|, \quad h_1 \in \mathbb{H}_1, \ldots, h_n \in \mathbb{H}_n$$

for some real constant C. The least such constant is called the norm of ϕ and is denoted $\|\phi\|$.

12. If $\mathbb{V}$ and $\mathbb{W}$ are topological vector spaces, a tensor product in the categorical sense should be the pair $(\mathbb{Y}, \tau)$ composed by a topological vector space $\mathbb{X}$ and a unique continuous bilinear map $\tau = \mathbb{V} \times \mathbb{W} \to \mathbb{Y}$, such that for every continuous bilinear map $\beta : \mathbb{V} \times \mathbb{W} \to \mathbb{X}$ into an arbitrary topological space $\mathbb{X}$, there exists a unique continuous linear map $\lambda := \lambda_\beta : \mathbb{Y} \to \mathbb{X}$ such that $\beta = \lambda \circ \tau$, verifying thus the universality propoerty. It will be shown in §3.12 that such a construction is impossible in the case the two Hilbert spaces $\mathbb{V}$ and $\mathbb{W}$ are infinite-dimensional.

Obviously a bounded multilinear functional is continuous w.r.t. the product of the norm topologies on the Hilbert spaces.

Proposition 3.8.32. *Let $\mathbb{H}_1, \dots, \mathbb{H}_n$ be Hilbert spaces and ϕ a bounded multilinear functional on $\mathbb{H}_1 \times \cdots \times \mathbb{H}_n$.*

1. *The sum*
$$\sum_{b_1 \in B_1, \dots b_n \in B_n} |\phi(b_1, \dots, b_n|^2$$
has the same (finite or infinite) value for all orthonormal bases B_1 of $\mathbb{H}_1$, …, B_n of $\mathbb{H}_n$.
2. *If $\mathbb{G}_1, \dots, \mathbb{G}_n$ are Hilbert spaces, $X_m \in \mathfrak{B}(\mathbb{H}_m, \mathbb{G}_m)$ for $m = 1, \dots, n$, $\psi : \mathbb{G}_1 \times \cdots \times \mathbb{G}_n \to \mathbb{C}$ a bounded multilinear functional and*
$$\phi(h_1, \dots, h_n) = \psi(X_1 h_1, \dots, X_n h_n), \quad \forall h_1 \in \mathbb{H}_1, \dots, h_n \in \mathbb{H}_n,$$
then
$$\sum_{b_1 \in B_1, \dots b_n \in B_n} |\phi(b_1, \dots, b_n|^2 \leq \|X_1\|^2 \cdots \|X_n\|^2 \sum_{c_1 \in C_1, \dots c_n \in C_n} |\psi(c_1, \dots, c_n|^2,$$
for arbitrary bases B_m of $\mathbb{H}_m$ and C_m of $\mathbb{G}_m$ for $m = 1, \dots, n$.

Definition 3.8.33. A **Hilbert-Schmidt functional** is a bounded multilinear functional such that the sum in item 1 of proposition 3.8.32 is finite for one choice (hence for all) of bases $B_1, \dots, B_n$. The set of Hilbert-Schmidt functionals on $\mathbb{H}_1 \times \cdots \times \mathbb{H}_n$ is denoted HSF (or $\mathsf{HSF}(\mathbb{H}_1 \times \cdots \times \mathbb{H}_n)$ when disambiguation is necessary).

Proposition 3.8.34. *Let HSF be the set of Hilbert-Scmidt functionals on $\mathbb{H}_1 \times \cdots \times \mathbb{H}_n$. Equip the set HSF with:*

A linear structure *defined by $(a\phi + b\psi)(h_1, \dots, h_n) = a\phi(h_1, \dots, h_n) + b\psi(h_1, \dots, h_n)$.*
An inner product *by $\langle \phi \,|\, \psi \rangle = \sum_{b_1 \in B_1} \cdots \sum_{b_n \in B_n} \overline{\phi(b_1, \dots, b_n)} \psi(b_1, \dots, b_n)$ for arbitrary orthonormal bases $B_1, \dots, B_n$.*
A norm *by $\|\phi\|_2 = (\langle \phi \,|\, \phi \rangle)^{1/2}$.*

Then:

1. *The sum defining the inner product is independent of the choice of the bases.*
2. *The set HSF becomes a Hilbert space on its own.*
3. *For each choice $v_1 \in \mathbb{H}_1, \dots, v_n \in \mathbb{H}_n$, the equation $\phi_{v_1,\dots,v_n}(h_1, \dots, h_n) = \langle v_1 \,|\, h_1 \rangle \cdots \langle v_n \,|\, h_n \rangle$ defines an element of HSF and*
$$\langle \phi_{v_1,\dots,v_n} \,|\, \phi_{w_1,\dots,w_n} \rangle = \langle w_1 \,|\, v_n \rangle \cdots \langle w_n \,|\, v_n \rangle$$
$$\|\phi_{v_1,\dots,v_n}\|_2 = \|v_1\| \cdots \|v_n\|.$$
4. *The collection $(\phi_{b_1,\dots,b_n})_{b_1 \in B_1, \dots, b_n \in B_n}$ is an orthonormal basis of HSF.*
5. *There is a unitary transformation $U : \mathsf{HSF} \twoheadrightarrow \ell^2(B_1 \times \cdots \times B_n)$ defined by $U\phi = \phi\restriction_{B_1 \times \cdots \times B_n}$.*

The results concerning multilinear functionals are immediately generalised to multilinear mappings.

Definition 3.8.35. Let $\mathbb{H}_1, \dots, \mathbb{H}_n, \mathbb{G}$ be Hilbert spaces.

1. A **bounded multilinear mapping** is a map $M : \mathbb{H}_1 \times \cdots \times \mathbb{H}_n \to \mathbb{G}$ that is linear in each of its arguments (while the other arguments remain fixed), verifying

$$\|M(h_1, \ldots, h_n)\| \leq C\|h_1\| \cdots \|h_n\|, \quad h_1 \in \mathbb{H}_1, \ldots, h_n \in \mathbb{H}_n$$

for some real constant C. The least such constant is called the norm of M and is denoted $\|M\|$.
2. A **weak Hilbert-Schmidt mapping** is a bounded multilinear mapping such that for every $g \in \mathbb{G}$, the functional defined by

$$M_g(h_1, \ldots, h_n) = \langle\, g \,|\, M(h_1, \ldots, h_n) \,\rangle$$

belongs to HSF. (Additionally, there exists a real number D such that $\|M_g\|_2 \leq D\|g\|$). The least D for which these conditions are satisfied is denoted $\|M\|_2$.

Theorem 3.8.36. *Let $\mathbb{H}_1, \ldots, \mathbb{H}_n, \mathbb{G}$ be Hilbert spaces.*

1. *There is a Hilbert space $\mathbb{H}$ and a weak Hilbert-Schmidt mapping $\tau : \mathbb{H}_1 \times \cdots \times \mathbb{H}_n \to \mathbb{H}$ with the following universality property: for any weak Hilbert-Schmidt mapping $\beta : \mathbb{H}_1 \times \cdots \times \mathbb{H}_n \to \mathbb{G}$, there exists a unique bounded linear mapping $L : \mathbb{H} \to \mathbb{G}$, such that $\beta = L \circ \tau$; moreover $\|L\| = \|\beta\|_2$.*
2. *If $\mathbb{H}'$ and τ' have the properties attributed to $\mathbb{H}$ and τ in the previous item, there is a unitary $U : \mathbb{H} \twoheadrightarrow \mathbb{H}'$ such that $\tau' = U\tau$.*
3. *If $v_m, w_m \in \mathbb{H}_m$ and B_m is an orthonormal basis of $\mathbb{H}_m$, for $m = 1, \ldots, n$, then*

$$\langle\, \tau(v_1, \ldots, v_n) \,|\, \tau(w_1, \ldots, w_n) \,\rangle = \langle\, v_1 \,|\, w_1 \,\rangle \cdots \langle\, v_n \,|\, w_n \,\rangle,$$

and the family $(\tau(b_1, \ldots, b_m)_{b_1 \in B_1, \ldots, b_n \in B_n}$ is an orthonormal basis of $\mathbb{H}$ with $\|\tau\|_2 = 1$.

Remark 3.8.37. The pair $(\mathbb{H}, \tau)$ defined in item 1 of theorem 3.8.36 is defined (up to isomorphisms) by the universal property. It is termed the **Hilbert tensor product** of $\mathbb{H}_1, \ldots, \mathbb{H}_n, \mathbb{G}$, denoted $\mathbb{H}_1 \otimes \cdots \otimes \mathbb{H}_n$. The vector $\tau(h_1, \ldots, h_n)$ is denoted $h_1 \otimes \cdots \otimes h_n$. Finite linear combinations of such simple tensors form an everywhere dense subspace $\mathbb{H}_0$ of $\mathbb{H}_1 \otimes \cdots \otimes \mathbb{H}_n$.

Theorem 3.8.38. *Let $\mathbb{H}_1$ and $\mathbb{H}_2$ be Hilbert spaces.*

1. *If B_1 and B_2 are total systems of vectors respectively from $\mathbb{H}_1$ and $\mathbb{H}_2$, then the system $\{g \otimes h : g \in B_1, h \in B_2\}$ is total in $\mathbb{H}_1 \overline{\otimes} \mathbb{H}_2$.*
2. *If $(\varepsilon_j)_{j \in J}$ and $(\zeta_k)_{k \in K}$ are orthonormal bases of $\mathbb{H}_1$ and $\mathbb{H}_2$, then $(\varepsilon_j \otimes \zeta_k)_{j \in J, k \in K}$ is an orthonormal basis of $\mathbb{H}_1 \overline{\otimes} \mathbb{H}_2$.*

We conclude by a standard example-exercise on tensor products.

Exercise 3.8.39. Let $\mathbb{G} = L^2(\mathbb{X}, \mathcal{X}, \mu; \mathbb{C})$ and $\mathbb{H} = L^2(\mathbb{Y}, \mathcal{Y}, \nu; \mathbb{C})$ two separable Hilbert spaces with respective orthonormal bases $(\phi^{(k)})_{k \in \mathbb{N}}$ and $(\psi^{(l)})_{l \in \mathbb{N}}$. Consider for $k, l \in \mathbb{N}$, the family of functions $\Phi^{(k,l)} \in \mathbb{F} := L^2(\mathbb{X} \times \mathbb{Y}, \mathcal{X} \otimes \mathcal{Y}, \mu \otimes \nu; \mathbb{C})$ defined by $\Phi^{(k,l)} = \phi^{(k)}(x)\psi^{(l)}(y)$.

1. Show that $(\Phi^{(k,l)})_{(k,l) \in \mathbb{N}^2}$ is an orthonormal system.

2. Suppose that a function $f \in \mathbb{F}$ verifies, for all $k, l \in \mathbb{N}$,
$$\int_{\mathbb{X}\times\mathbb{Y}} \overline{f}(x,y)\phi^{(k)}(x)\psi^{(l)}(y)\mu(\dot{x})\nu(\dot{y}) = 0.$$
Use Fubini's theorem to show that $f = 0$ for $\mu\otimes\nu$-almost all $(x,y) \in \mathbb{X}\times\mathbb{Y}$.
3. Define the linear operator $U : \mathbb{G}\overline{\otimes}\mathbb{H} \to \mathbb{F}$ by its action on basis elements:
$$U : \phi^{(k)}\psi^{(l)} \mapsto \Phi^{(k,l)}.$$
Show that U is unitary.
4. On extending U by linearity, establish that $U(g\otimes h)(x,y) = g(x)h(y)$, for all $(x,y) \in \mathbb{X}\times\mathbb{Y}$ and all $g \in \mathbb{G}, h \in \mathbb{H}$.
5. Conclude that U induces a natural isomorphism between $L^2(\mathbb{X},\mathcal{X},\mu;\mathbb{C})\otimes L^2(\mathbb{Y},\mathcal{Y},\nu;\mathbb{C})$ and $L^2(\mathbb{X}\times\mathbb{Y},\mathcal{X}\otimes\mathcal{Y},\mu\otimes\nu;\mathbb{C})$.

Remark 3.8.40. (A classical case). The previous exercise establishes the fact that $L^2(\mathbb{R},\lambda_1)\otimes L^2(\mathbb{R},\lambda_1) = L^2(\mathbb{R}^2,\lambda_2)$, where λ_d is the d-dimensional Lebesgue measure on $\mathcal{B}(\mathbb{R}^d)$. Suppose now that $g, h \in L^2(\mathbb{R},\lambda_1)$ are non-negative such that both
$$\int_{\mathbb{R}} g(x)\lambda_1(\mathrm{d}x) = 1 \text{ and } \int_{\mathbb{R}} h(y)\lambda_1(\mathrm{d}y) = 1.$$
These functions define probabilities $\mathbb{P}_1$ and $\mathbb{P}_2$ absolutely continuous w.r.r. λ_1 such that g and h are their Radon-Nikodým derivatives. Similarly, a $f \in L^2(\mathbb{R},\lambda_2)$ such that $f \geq 0$ and $\int_{\mathbb{R}^2} f(x,y)\lambda_2(\mathrm{d}x\mathrm{d}y) = 1$ defines a probability $\mathbb{P} \ll \lambda_2$ whose Radon-Nikodým derivative is f. Now, f is a general vector (tensor) of $L^2(\mathbb{R},\lambda_2)$. In the particular case where $f = gh$ (i.e. the tensor f is **factored**) then $\mathbb{P}$ has marginals $\mathbb{P}_1$ and $\mathbb{P}_2$ and is a determined through its marginals as a product measure $\mathbb{P} = \mathbb{P}_1\otimes\mathbb{P}_2$.

Remark 3.8.41. (The quantum analog). Let $\mathbb{G} \simeq \mathbb{H} \simeq \mathbb{C}^2$ and $\mathbb{F} = \mathbb{G}\otimes\mathbb{H}$. Assume that $G \in \mathbf{E}(\mathbb{G}), H \in \mathbf{E}(\mathbb{H})$ and ϕ and ψ are unit vectors respectively in $\mathbb{G}$ and $\mathbb{H}$. For $B \in \mathcal{B}(\mathbb{R})$, denote by $\nu_G^\phi(B) = \langle\,\phi\,|\,G[B]\phi\,\rangle$ and $\nu_H^\psi(B) = \langle\,\psi\,|\,H[B]\psi\,\rangle$. Let now $\Phi \in \mathbb{F}$ be the **factored** tensor $\Phi = \phi\otimes\psi$. We compute immediately
$$\begin{aligned}\langle\,\phi\otimes\psi\,|\,(G[B]\otimes I)\phi\otimes\psi\,\rangle &= \nu_G^\phi(B)\\ \langle\,\phi\otimes\psi\,|\,(I\otimes H[B])\phi\otimes\psi\,\rangle &= \nu_H^\psi(B)\\ \langle\,\phi\otimes\psi\,|\,(G[B]\otimes H[B])\phi\otimes\psi\,\rangle &= \nu_G^\phi(B)\nu_H^\psi(B).\end{aligned}$$
Exactly as in the classical situation of remark 3.8.40 a factored tensor f led to product probability measure $\mathbb{P} = \mathbb{P}_1\otimes\mathbb{P}_2$, a factored tensor $\Phi = \phi\otimes\psi$ in the quantum case leads to a product probability measure $\nu_{G\otimes H}^\Psi = \nu_G^\phi\nu_H^\psi$. Similarly, as in the classical case entangled tensors ($f \neq gh$) give rise to general joint non-product measures, in the quantum case **entangled tensors** ($\Phi \neq g\otimes h$) give rise to general joint **non-product measures**.

3.8.6 Fock space

Assume in this subsection that we are interested in a system holding an indeterminate number of indistinguishable particles. Further, each individual particle is described by a (separable) Hilbert space $\mathbb{H}$. If the number of particles were fixed, p say,

then the p-particle system should be described by a subset of the p-fold tensor product $\mathbb{H}^{\otimes p}$. (In the infinite dimensional case we assume that the tensor product is always completed). We have already mentioned that only the symmetrised $\mathcal{S}^p(\mathbb{H})$ or anti-symmetrised $\mathcal{A}^p(\mathbb{H})$ tensor products occur as phase space of bosonic or fermionic indistinguishable particles. In this subsection, we treat the case where the particles are bosons and their number is indeterminate. The solution to this problem was given by Fock in 1932 [61]; more easily accessible sources are [78, pp. 189–193] and [22, pp. 1–6].

Let $\mathbb{B}$ be the indexing set ($\mathrm{card}\mathbb{B} = d \in \mathbb{N} \cup \{\infty\}$) of an orthonormal basis $(\varepsilon_b)_{b\in\mathbb{B}}$ of $\mathbb{H}$, $\boldsymbol{\beta} \in \mathbb{B}^p$, and $\boldsymbol{\nu}([\boldsymbol{\beta}])$ the number representation [13] of $S_p(\boldsymbol{\varepsilon}(\boldsymbol{\beta}))$. (As a matter of fact, we tacitly — but straightforwardly (please work out the details) — extended the definition of number representation to the infinite-dimensional case.

Exercise 3.8.42. For the above setting,

— show that
$$\|S_p(\boldsymbol{\varepsilon}(\boldsymbol{\beta}))\|^2 = \frac{\prod_{b\in\mathbb{B}}(\nu_b(\boldsymbol{\beta})!)}{p!}.$$

— Consider an arbitrary decomposition of p into d ($d \in \mathbb{N} \cup \{+\infty\}$ non-negative integers $p = \sum_{b\in\mathbb{B}} p_b$ and denote by $\mathbf{p} = (p_b)_{b\in\mathbb{B}}$. Then, there exists a unique equivalence class $[\boldsymbol{\beta}] \in \mathbb{B}_B^p$ such that $\forall\gamma \in [\boldsymbol{\beta}]$, we have $\boldsymbol{\nu}(\gamma) = \mathbf{p}$. Show that the set of vectors, indexed by the set number vectors,
$$\Psi_{\mathbf{p}} = \Big(\frac{p!}{\prod_{b\in\mathbb{B}}(p_b!)}\Big)^{1/2} S_p \varepsilon_{\beta_1} \otimes \cdots \otimes \varepsilon_{\beta_p},$$
constitutes an orthonormal basis of $\mathbb{B}_B^p$.

Definition 3.8.43. Let $\mathbb{H}$ be a separable Hilbert space. The **Fock space** associated with $\mathbb{H}$ is the direct sum
$$\mathsf{Fock}(\mathbb{H}) = \oplus_{p\in\mathbb{N}} \mathbb{H}^{\otimes p},$$
with $\mathbb{H}^0 = \mathbb{C}$. Similarly, we define the bosonic sector of the Fock space
$$\mathsf{Fock}_B(\mathbb{H}) = \oplus_{p\in\mathbb{N}} \mathcal{S}^p(\mathbb{H}).$$
A vector $\Psi \in \mathsf{Fock}_B(\mathbb{H})$ will be identified with the sequence $\Psi = (\psi^{(p)})_{p\in\mathbb{N}}$, where $\psi^{(p)} \in \mathcal{S}^p(\mathbb{H})$ and $\sum_{p\in\mathbb{N}} \|\psi^{(p)}\|^2 < \infty$.

We wish now define the number (of particles) operator N acting on $\mathsf{Fock}(\mathbb{H})$. If N is to be interpreted as the number of particles, intuitively we expect that an *arbitrary* unit vector of $\mathbb{H}^{\otimes p}$ is an eigenvector of N with eigenvalue p. Now we are facing some subtleties because N is not necessarily a bounded operator, even in the case where $\mathbb{H}$ is finite-dimensional.

Definition 3.8.44. We define
$$\mathsf{Dom}(N) = \{\Psi = (\psi^{(p)})_{p\in\mathbb{N}} \in \mathsf{Fock}(\mathbb{H}) : \sum_{p\in\mathbb{N}} \|p\psi^{(p)}\|^2 < \infty\} \subset \mathsf{Fock}(\mathbb{H})$$

13. Recall that this number depends only on the equivalence class $[\boldsymbol{\beta}]$ and not on the individual configuration $\boldsymbol{\beta}$ (see exercise 3.8.28).

and, for $\Psi \in \mathsf{Dom}(N)$, the **number of particles operator** N by

$$N\Psi = \sum_{p\in\mathbb{N}} p\psi^{(p)}.$$

For a $\psi, \psi_1, \ldots, \psi_p \in \mathbb{H}$, define the (bounded) operator $C(\psi) : \mathbb{H}^{\otimes p} \to \mathbb{H}^{\otimes(p+1)}$ by

$$C(\psi)\psi_1 \otimes \cdots \otimes \psi_p := \psi \otimes \psi_1 \otimes \cdots \otimes \psi_p.$$

Obviously $\|C(\psi)\| = \|\psi\|$. When all $\psi, \psi_1, \ldots, \psi_p \in \mathbb{H}$ are unit vectors (i.e. they correspond to pure states on $\mathbb{H}$) the operator $C(\psi)$ is interpreted as the creation of an additional particle in state ψ. The adjoint operator $C(\psi)^* : \mathbb{H}^{\otimes p} \to \mathbb{H}^{\otimes(p-1)}$ is immediately determined: $C(\psi)^*\mathbb{H}^0 = 0$ and

$$C(\psi)^*\psi_1 \otimes \cdots \otimes \psi_p := \langle\, \psi \,|\, \psi_1 \,\rangle \psi_2 \otimes \cdots \otimes \psi_p, p \geq 1.$$

The operator $C(\psi)^*$ is interpreted as the annihilation of a particle from the p-tuple. The operators $C(\psi)$ and $C(\psi)^*$ can be extended on the whole space $\mathsf{Fock}(\mathbb{H})$ by

$$C(\psi)\Psi = \sum_{p\in\mathbb{N}} C(\psi)\psi^{(p)}$$
$$C(\psi)^*\Psi = \sum_{p\in\mathbb{N}} C(\psi)^*\psi^{(p)}.$$

Let now

$$D_0 = \{\Psi \in \mathsf{Fock}_B : \psi^{(p)} = 0 \text{ but for a finite number of } p\} \subset \mathsf{Dom}(N) \subset \mathsf{Fock}(\mathbb{H})$$

and for $\psi \in \mathbb{H}$ and $\Psi \in D_0$, define

$$a(\psi)\Psi = \sum_{p\geq 1} \sqrt{p} S_{p-1}\left(C(\psi)^*\psi^{(p)}\right)$$
$$a(\psi)^*\Psi = \sum_{p\geq 0} \sqrt{p+1} S_{p+1}\left(C(\psi)\psi^{(p)}\right).$$

These operators verify (please check!) the commutation relations:

$$[a(\psi), a(\psi')] = [a^*(\psi), a^*(\psi')] = 0 \text{ and } [a(\psi), a^*(\psi')] = \langle\, \psi' \,|\, \psi \,\rangle I.$$

It is then straightforward to show that the vectors $(\Psi_{\mathbf{p}})_{\mathbf{p}}$, where $\mathbf{p}$ stands for the number representation, are obtained by

$$\Psi_{\mathbf{p}} = \left(\prod_{b\in\mathbb{B}} (p_b!)\right)^{-1/2} \otimes_{b\in\mathbb{B}} a^*(\varepsilon_{\beta_b})\psi^{(0)}$$

are orthonormal and since D_0 is dense in $\mathsf{Fock}(\mathbb{H})$, we conclude that this set is an orthonormal basis. We see that the whole space $\mathsf{Fock}_B(\mathbb{H})$ is spanned by vectors obtained by action of appropriate a^* operators acting on a single vector $\psi^{(0)}$; the latter is called the **vacuum vector**, the operator a^* a **creation operator** and the operator a an **annihilation operator**.

3.9 Dirac's bra and ket notation

Dirac's notation transforms an astonishingly simple idea into a remarkably powerful and convenient shorthand notation for dealing with all standard objects in Hilbert spaces: scalar products, tensor products, operators, projections, and forms occurring in quantum mechanics. The idea behind this notation is to consider the scalar product $\langle \phi \,|\, \psi \rangle$ of two vectors of a Hilbert space as the application of the linear form $F_\phi \in \mathbb{H}' = \mathbb{H}$ — defined by $F_\phi(h) = \langle \phi \,|\, h \rangle$ through the Fréchet-Riesz theorem 3.3.8 — on the vector ψ. Since F_ϕ is uniquely determined by ϕ, Dirac had the idea of splitting the bracket $\langle \phi \,|\, \psi \rangle$ into the linear form — called bra — $\langle \phi \,|$ and the vector — called ket — $|\, \psi \rangle$. The action of the bra on the ket $\langle \phi \,||\, \psi \rangle$ is simplified into the scalar product bra(c)ket $\langle \phi \,|\, \psi \rangle$. The box on page 97 summarises the main features of Dirac's notation.

Usual vs. Dirac's notation

Usual notation	Dirac's notation
Orthonormal basis, linear combinations, scalar product	
$(e_1, \dots, e_n)$ $\psi = \sum_i \psi_i e_i$ $\langle \phi \vert \psi \rangle = \sum \overline{\phi}_i \psi_i$	$(\vert e_1 \rangle, \dots \vert e_n \rangle)$ $\vert \psi \rangle = \sum_i \psi_i \vert e_i \rangle$ $\langle \phi \vert \psi \rangle = \sum \overline{\phi}_i \psi_i$
Duality	
$\mathbb{H}^* = \{f : \mathbb{H} \to \mathbb{C}, \text{linear}\}$ $\dagger : \mathbb{H} \to \mathbb{H}^*$ $\dagger : \phi \mapsto f_\phi(\cdot) = \langle \phi \vert \cdot \rangle$ $\langle \phi \vert \psi \rangle = f_\phi(\psi)$	$\mathbb{H}^* = \{f : \mathbb{H} \to \mathbb{C}, \text{linear}\}$ $\dagger : \mathbb{H} \to \mathbb{H}^*$ $\dagger : \vert \phi \rangle \mapsto \langle \phi \vert$ $\langle \phi \vert \psi \rangle = \langle \phi \vert \vert \psi \rangle = \langle \phi \,|\, \psi \rangle$
Self-adjoint operators	
$X = X^*$ $\langle \phi \vert X\psi \rangle = \langle X^*\phi \vert \psi \rangle = \langle X\phi \vert \psi \rangle$	$X = X^*$ $\langle \phi \,|\, X\psi \rangle = \langle X^*\phi \vert \psi \rangle = \langle X\phi \vert \psi \rangle$
Spectral decomposition	
$X\zeta[x] = x\zeta[x]$ $E[x]$ projection on $\mathbb{C}\zeta[x]$ $X = \sum_x xE[x]$	$X\vert \zeta[x] \rangle = x\vert \zeta[x] \rangle$ $E[x] = \vert \zeta[x] \rangle\langle \zeta[x] \vert$ $X = \sum_x x \vert \zeta[x] \rangle\langle \zeta[x] \vert$
Tensor products	
$\phi \otimes \psi$ $\phi \otimes \psi^*$	$\vert \phi \rangle \otimes \vert \psi \rangle = \vert \phi\psi \rangle$ $\vert \phi \rangle \otimes \langle \psi \vert = \vert \phi \rangle\langle \psi \vert$

Remark 3.9.1. Very often, in the Physics literature, only the indexing set is considered. In that case, the basis is denoted $|\, 1 \rangle, \dots |\, n \rangle$. This simplified notation will be occasionally used in the later sections, especially in those devoted to quantum computing. Mind however that within this simplified notation, the right hand side of $|\, 0 \rangle + |\, 1 \rangle$, namely $|\, 0 + 1 \rangle$ becomes ambiguous because $|\, 0 + 1 \rangle \neq |\, 1 \rangle$. To avoid this pitfall, a slightly more extended notation where vectors are used as indexing set; in that case $|\, \varepsilon_0 \rangle + |\, \varepsilon_1 \rangle = |\, \varepsilon_0 + \varepsilon_1 \rangle$ is perfectly legal and unambiguous.

Exercise 3.9.2. Let $(e_n)_{n \in \mathbb{N}}$ be an orthonormal basis of a Hilbert space $\mathbb{H}$.

1. What is the interpretation of $|\, e_n \rangle\langle\, e_n \,|$ for some n?

2. If ϕ and ψ are unit vectors of $\mathbb{H}$, what is the interpretation of $|\,\phi\,\rangle\langle\,\psi\,|$? What is the significance of $|\,e_m\,\rangle\langle\,e_n\,|$?
3. What is the interpretation of the identity $\sum_{n\in\mathbb{N}} |\,e_n\,\rangle\langle\,e_n\,| \overset{s}{=} I$ (where $\overset{s}{=}$ denotes the strong limit of the partial sums)?
4. Let $\mathbb{H} = L^2(\mathbb{T})$ and (e_n) the basis of trigonometric polynomials $e_n(t) = \exp(int)$. Derive the Parseval formula using the Dirac formalism.

3.10 Bipartite entanglement

Entanglement [14] constitutes a distinctive property of quantum mechanics, without classical analogue, undoubtably the most counter-intuitive one. It fuelled the most passionate discussions among physicists in the early years of quantum physics. The most critical opponent to the the mere philosophical possibility of entanglement was Einstein who wrote (with Podolsky and Rosen) an influential paper (see comment and footnote on page 44). Entanglement is the crux quantum property for most of the informational applications of quantum mechanics (quantum computing, quantum cryptography, quantum communication, etc.). Students are urged to work completely exercise 3.12.20 (if they haven't yet done so) before continuing to read.

Definition 3.10.1. A vector $\Psi \in \mathbb{H}_1 \otimes \mathbb{H}_2$ is called

1. **factored** if there exist vectors $\phi^{(1)} \in \mathbb{H}_1$ and $\phi^{(2)} \in \mathbb{H}_2$ such that $\Psi = \phi^{(1)} \otimes \phi^{(2)}$,
2. **entangled** if the vector Ψ cannot be factored into a tensor product of vectors as above.

Example 3.10.2. Let $n = 2$ and $\mathbb{H}_1 = \mathbb{H}_2 = \mathbb{C}^2$. If we denote by $(\varepsilon_0, \varepsilon_1)$ a basis of $\mathbb{H}_1$ and by (ζ_0, ζ_1) a basis of $\mathbb{H}_2$. A basis of $\mathbb{H}_1 \otimes \mathbb{H}_2$ is given by $(\varepsilon_0 \otimes \zeta_0, \varepsilon_0 \otimes \zeta_1, \varepsilon_1 \otimes \zeta_0, \varepsilon_1 \otimes \zeta_1)$. An arbitrary vector $\Psi \in \mathbb{H}_1 \otimes \mathbb{H}_2$ is decomposed as

$$\Psi = \psi_0\varepsilon_0 \otimes \zeta_0 + \psi_1\varepsilon_0 \otimes \zeta_1 + \psi_2\varepsilon_1 \otimes \zeta_0 + \psi_3\varepsilon_1 \otimes \zeta_1.$$

If $\psi_2 = \psi_3 = 0$ while $\psi_1\psi_1 \neq 0$, then $\psi = \psi_0\varepsilon_0 \otimes \zeta_0 + \psi_1\varepsilon_0 \otimes \zeta_1 = \varepsilon_0 \otimes (\psi_0\zeta_0 + \psi_1\zeta_1)$ and the state can still be written as a tensor product. If $\psi_1 = \psi_2 = 0$ while $\psi_0\psi_3 \neq 0$ then the state cannot be written as a tensor product.

In the previous example, the space has small dimensionality and it is easy to check manually whether a given vector is entangled or not. In more complicated situations, it is useful to have more an algorithmic tool to decide of entanlement. This tool is provided by the Schmidt decomposition (see definition **??** below).

Theorem 3.10.3. *Let $\Psi \in \mathbb{H}_1 \otimes \mathbb{H}_2$ and $d_i = \dim \mathbb{H}_i$, for $i = 1, 2$. There exist orthonormal bases $(\varepsilon_i)_{i=1,\dots,d_1}$ and $(\zeta_j)_{j=1,\dots,d_2}$ respectively of $\mathbb{H}_1$ and $\mathbb{H}_2$ such that*

$$\Psi = \sum_{k=1}^{d} s_k \varepsilon_k \otimes \zeta_k,$$

14. The notion has been introduced by Erwin Schrödinger who named this property *Verschränkung* in German in 1935. The term has been translated into English (by Schrödinger himself in 1936) as *entanglement*. Although the author of these lines advocates the term *enchevêtrement* as the French translation of this term, the French community of physicists have adopted the translation *intrication*.

where $d = \min\{d_1, d_2\}$, *and* $s_1 \geq s_2 \ldots \geq s_d \geq 0$.

Definition 3.10.4. The decomposition — whose existence is guaranteed by theorem 3.10.3 — is called **Schmidt decomposition**; the real d-dimensional vector $\mathbf{s} = (s_1, s_2, \ldots, s_d)$ is called Schmidt vector; $\mathsf{rank}(\mathbf{s}) = \max\{k : s_k > 0\}$ is called the Schmidt rank of the decomposition.

Note that only $d = \min(d_1, d_2)$ elements of the largest (i.e. of size $\max(d_1, d_2)$) basis are used in Schmidt decomposition. When $\|\Psi\|^2 = 1$, then $\sum_{k=1}^{d} s_k^2 = 1$.

Lemma 3.10.5. *Let* $W \in \mathbb{M}_{d_1,d_2}(\mathbb{C})$ *be a matrix and* $d = \min\{d_1, d_2\}$. *Then there exist unitary matrices* $U \in \mathbb{M}_{d_1}(\mathbb{C})$ *and* $V \in \mathbb{M}_{d_2}(\mathbb{C})$ *and a diagonal matrix* $S = \mathsf{diag}(s_1, \ldots, s_d)$, *with* $s_1 \geq \ldots \geq s_r > s_{r-1} = \ldots = s_d = 0$, *such that*

$$W = USV^*.$$

The index r *equals the rank of* W.

Proof. The decomposition is called singular value decomposition of M. The proof is a standard result in linear algebra (see for instance [133, Theorem 11.4, p. 276]). □

Remark 3.10.6. Although the diagonal matrix S is uniquely determined, the matrices U and V are not.

Proof of theorem 3.10.3. Let (ε'_i) and (ζ'_j) be orthonormal bases of $\mathbb{H}_1$ and $\mathbb{H}_2$. For $\Psi \in \mathbb{H}_1 \otimes \mathbb{H}_2$, denote by $W = (W_{ij}) \in \mathbb{M}_{d_1,d_2}(\mathbb{C})$ the matrix of its Fourier coefficients, i.e. $\Psi = \sum_{i,j} W_{ij} \varepsilon'_i \otimes \zeta'_j$, with $W_{ij} = \langle\, \varepsilon'_i \otimes \zeta'_j \,|\, \Psi \,\rangle$. Now wirte the singular value decomposition of $W = USV^*$ with matrices U, S, V as in the lemma 3.10.5. Then $W_{ij} = (USV^*)_{ij} = \sum_{k=1}^{d} U_{ik} s_k \overline{V}_{jk}$. Denote by $\varepsilon_l = \sum_{i=1}^{d_1} U_{il} \varepsilon'_i$ for $l = 1, \ldots, d_1$ and $\sum_{j=1}^{d_2} \overline{V}_{jm} \zeta'_j = \zeta_m$, for $m = 1, \ldots, d_2$, new orthonormal bases of $\mathbb{H}_1$ and $\mathbb{H}_2$, obtained from the previous ones in terms of the unitary passage matrices U and V^*. Replacing in the expansion of Ψ, we get

$$\Psi = \sum_{k=1}^{d} s_k \left(\sum_{i=1}^{d_1} U_{ik} \varepsilon'_i \right) \otimes \left(\sum_{j=1}^{d_2} \overline{V}_{jk} \zeta'_j \right) = \sum_{k=1}^{d} s_k \varepsilon_k \otimes \zeta_k.$$

□

Proposition 3.10.7. *Let* $\mathbb{H} = \mathbb{H}_1 \otimes \mathbb{H}_2$ *and* $\Psi \in \mathbb{H}$, *a unit norm vector, and* $\rho = |\, \Psi \,\rangle\langle\, \Psi \,|$ *the pure state corresponding to* Ψ. *Let* $(\varepsilon_k)_k$ *and* $(\zeta_k)_k$ *be the orthonormal vectors of* $\mathbb{H}_1$ *and* $\mathbb{H}_2$ *entering in the Schmidt decomposition of* Ψ. *Then the quantum marginals read*

$$\rho_1 = \mathsf{tr}_{\mathbb{H}_2} \rho = \sum_{k=1}^{d} s_k^2 |\, \varepsilon_k \,\rangle\langle\, \varepsilon_k \,|$$

$$\rho_2 = \mathsf{tr}_{\mathbb{H}_1} \rho = \sum_{k=1}^{d} s_k^2 |\, \zeta_k \,\rangle\langle\, \zeta_k \,|,$$

i.e. the density matrices ρ_1 *and* ρ_2 *have the same eigenvalues, possibly with different multiplicity.*

Proof. Write $\rho = |\Psi\rangle\langle\Psi| = \sum_{k,l=1}^{d} s_k s_l |\varepsilon_k\zeta_k\rangle\langle\varepsilon_l\zeta_l|$. Then, for every $\phi, \phi' \in \mathbb{H}_1$, we get

$$\begin{aligned}\langle\phi|\,\mathrm{tr}_{\mathbb{H}_2}(\rho)\phi'\rangle &= \sum_{k,l=1}^{d} s_k s_l \sum_{m=1}^{d_2} \langle\phi\zeta_m|\varepsilon_k\zeta_k\rangle\langle\varepsilon_l\zeta_l|\phi'\zeta_m\rangle \\ &= \sum_{k,l=1}^{d} s_k s_l \sum_{m=1}^{d_2} \langle\phi|\varepsilon_k\rangle\delta_{mk}\langle\varepsilon_l|\phi'\rangle\delta_{lm} \\ &= \sum_{k=1}^{d} s_k^2 \langle\phi|\varepsilon_k\rangle\langle\varepsilon_k|\phi'\rangle,\end{aligned}$$

hence we get the claimed form. The second marginal is obtained similarly □

Definition 3.10.8. Let $\rho \in \mathfrak{D}(\mathbb{H}_1 \otimes \mathbb{H}_2)$.

1. The state ρ is called **uncorrelated** or **factored** if there exist states $\rho_1 \in \mathfrak{D}(\mathbb{H}_1)$ and $\rho_2 \in \mathfrak{D}(\mathbb{H}_2)$ such that $\rho = \rho_1 \otimes \rho_2$.
2. A state ρ is called **classically correlated** if it can be written as a convex combination of factored states, i.e. there exist a family, indexed by $\alpha \in A$, of pairs of states $\rho_i^{(\alpha)}$, $i = 1, 2$ and a family of non-negative numbers $p_\alpha, \alpha \in A$, such that
$$\rho = \sum_{\alpha\in A} p_\alpha \rho_1^{(\alpha)} \otimes \rho_2^{(\alpha)}.$$
3. If the state ρ is not classically correlated, then it is called **entangled**.

The components of the Schmidt vector of a given unit vector Ψ are obtained as square roots of the eigenvalues of the quantum marginals of the state $\rho = |\Psi\rangle\langle\Psi|$. The marginal ρ_1 (hence also the marginal ρ_2) will be pure, i.e. $\mathrm{tr}(\rho_1^2) = \mathrm{tr}(\rho_1) = 1$, if, and only if, $s_1 = 1$ and all other components of $\mathbf{s}$ are zero. But thanks to the Schmidt decomposition of Ψ this occurs if and only if Ψ is factored. Therefore, a pure state will be uncorrelated if and only if its marginals are pure. For mixed composite states, the situation is much more complicated. In general the notion of **entanglement witness** and a precise analysis of the properties of the convex cone of states are needed. The notion of entanglement can be extended to multipartite systems. However, the mathematical analysis is much more involved. Full classification of multipartite entangled states is still an open problem.

Remark 3.10.9. If $\rho = \rho_1 \otimes \rho_2$ (uncorrelated) then the quantum marginals verify $\mathrm{tr}_{\mathbb{H}_1}(\rho) = \rho_2$ and $\mathrm{tr}_{\mathbb{H}_2}(\rho) = \rho_1$, i.e. ρ conveys the notion of uncorrelated joint probability. In fact, if X_1 and X_2 are self-adjoint operators on $\mathbb{H}_1$ and $\mathbb{H}_2$, then

$$\mathbb{E}(X_1X_2) = \mathrm{tr}(\rho X_1 \otimes X_2) = \mathrm{tr}(\rho_1 X_1)\,\mathrm{tr}(\rho_2 X_2) = \mathbb{E}(X_1)\mathbb{E}(X_2).$$

3.11 Positive operators

Definition 3.11.1. An operator $X \in \mathfrak{B}(\mathbb{H})$ is called **positive**, denoted $X \geq 0$, if $\forall h \in \mathbb{H}$, we have $\langle h|Xh\rangle \geq 0$. Positivity induces a partial order on $\mathfrak{B}(\mathbb{H})$: we say that $X \leq Y$ if $Y - X \geq 0$.

Remark 3.11.2. Self-adjointness is a necessary but not sufficient condition for positivity.

Example 3.11.3. Let $\mathbb{V}$ be a vector subspace of $\mathbb{H}$ and P be the orthoprojection on $\mathbb{V}$. Then P is positive.

In fact, decompose $\mathbb{H}$ into the orthogonal direct sum: $\mathbb{H} = \mathbb{V} \oplus \mathbb{V}^\perp$ and for $h = v + v^\perp$, define P by $Ph = v$. Obviously $P^2 = P$ because P is a projection and $P^* = P$ because P is an orthoprojection. We get then

$$\langle\, h \,|\, Ph \,\rangle = \langle\, h \,|\, P^2 h \,\rangle = \langle\, h \,|\, P^* Ph \,\rangle = \langle\, Ph \,|\, Ph \,\rangle \geq 0.$$

Proposition 3.11.4. *Let $X \in \mathfrak{B}(\mathbb{H})$. The following are equivalent:*

1. *X is positive.*
2. *$\operatorname{spec} X \subset \mathbb{R}_+$.*
3. *There exists a $Y \in \mathfrak{B}(\mathbb{H})$ such that $X = Y^*Y$.*

Lemma 3.11.5. *Let $X \in \mathfrak{B}(\mathbb{H})$ be positive. Then there exists $Y \in \mathfrak{B}(\mathbb{H})$ positive such that $X = Y^2$. Moreover, Y commutes with every bounded operator commuting with X.*

Definition 3.11.6. For $X \in \mathfrak{B}(\mathbb{H})$, we call **absolute value** of X, the operator $|X| := \sqrt{X^*X}$.

Remark 3.11.7. Beware of the symbol $|\cdot|$ used for the absolute value of the operator. Although it is true that for every $\lambda \in \mathbb{C}$, we have $|\lambda X| = |\lambda||X|$ as is the case for scalars, other fundamental properties of scalar absolute values are not valid in the non-commutative case. Namely,

1. $|XY| = |X||Y|$ **does not hold in general**,
2. $|X| = |X^*|$ **does not hold in general**,
3. $|X + Y| \leq |X| + |Y|$ **does not hold in general**.

Exercise 3.11.8. Give counter-examples for items 1 and 2 of remark 3.11.7.

Example 3.11.9. (Item 3 of remark 3.11.7) Let

$$X = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } Y = \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}.$$

It is an elementary computation to show that, since X is positive,

$$|X| = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}.$$

As for $|Y|$, first remark that Y is normal, hence diagonalisable. The eigenvalues of Y are 0 and -2 with corresponding normalised eigenvectors

$$|\, \varepsilon[0] \,\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \text{ and } |\, \varepsilon[-2] \,\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

Normality of Y implies orthogonality of the eigenvectors. The corresponding spectral orthoprojectors are the (self-adjoint) operators

$$E[0] = |\, \varepsilon[0] \,\rangle\langle\, \varepsilon[0] \,| = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \text{ and } E[-2] = |\, \varepsilon[-2] \,\rangle\langle\, \varepsilon[-2] \,| = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}.$$

The spectral decomposition $Y = \sum_{\lambda\in\mathsf{spec}\,Y} \lambda E[\lambda]$ implies that

$$Y^* = \sum_{\lambda\in\mathsf{spec}\,Y} \overline{\lambda} E[\lambda]^* = \sum_{\lambda\in\mathsf{spec}\,Y} \lambda E[\lambda].$$

Hence $Y^*Y = Y^2 = \sum_{\lambda\in\mathsf{spec}\,Y} \lambda^2 E[\lambda] = 4E[-2]$ and consequently

$$|Y| = 2E[-2] = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}.$$

Similarly, we compute $Z = X + Y$. Be cautious however, that although the spectral decompositions of X and Y are already established, they **cannot be used** to obtain the spectral decomposition of Z because the eigenspaces of X are different from those of Y. The computation of the spectral decomposition of Z requires computation of eigenspaces afresh! Doing so, we compute

$$|Z| = \begin{pmatrix} \sqrt{2} & 0 \\ 0 & \sqrt{2} \end{pmatrix}.$$

But now the operator $W = |X| + |Y| - |X + Y|$ has $\mathsf{spec}\,W = \{2(1-\sqrt{2}), 2\}$ and since there is a strictly negative eigenvalue, the operator W is not positive, therefore the triangular inequality fails.

3.12 Compact, Hilbert-Schmidt and trace class operators; partial trace

We denote by $\mathbb{B}$ the set indexing the elements of an arbitrary orthonormal basis of $\mathbb{H}$. More precisely, let $K = \mathsf{card}\mathbb{H}$. If $K < \infty$, then $\mathbb{B} = \{0, \dots, K-1\}$ while in case $K = \aleph_0$, the indexing set reads $\mathbb{B} = \mathbb{N}$. This notation allows to treat similarly finite and infinite dimensional cases.

Definition 3.12.1. Let $\mathbb{V}$ be a Banach space.

— The set of **finite rank** operators is

$$\mathfrak{B}_{00}(\mathbb{V}) = \{X \in \mathfrak{B}(\mathbb{V}) : \dim X(\mathbb{V}) < \infty\}.$$

— The set of **compact** operators is

$$\mathfrak{B}_0(\mathbb{V}) = \{X \in \mathfrak{B}(\mathbb{V}) : \overline{\{Xh : \|h\| \leq 1\}} \text{ is compact}\}.$$

Needless to stress that in finite dimension, all operators are of finite rank and compact.

Theorem 3.12.2. *Let $\mathbb{V}$ be a Banach space. If $X \in \mathfrak{B}_{00}(\mathbb{V})$ and $(v_j)_{j\in\mathbb{B}}$ is a basis for the vector space $X(\mathbb{V})$, there exist uniquely determined linear forms $(\phi_j)_{j\in\mathbb{B}}$, $\phi_j \in \mathbb{V}'$, such that*

$$X = \sum_{j\in\mathbb{B}} v_j \otimes \phi_j.$$

In the case of a Hilbert space $\mathbb{H}$ and using Dirac's notation, the previous formula reads $X = \sum_{j\in\mathbb{B}} |\, v_j \,\rangle\langle\, \phi_j \,|$ where $|\, v_j \,\rangle, |\, \phi_j \,\rangle \in \mathbb{H}$ (hence $\langle\, \phi_j \,| = (|\, \phi_j \,\rangle)^\dagger$).

Definition 3.12.3. Let $\mathfrak{I}$ be a vector subspace of $\mathfrak{B}(\mathbb{V})$ and $X \in \mathfrak{I}, Y \in \mathfrak{B}(\mathbb{H})$.

1. If $XY \in \mathfrak{I}$, the set $\mathfrak{I}$ is a **left ideal** of $\mathfrak{B}(\mathbb{H})$.
2. If $YX \in \mathfrak{I}$, the set $\mathfrak{I}$ is a **right ideal** of $\mathfrak{B}(\mathbb{H})$.
3. If $X^* \in \mathfrak{I}$, the set $\mathfrak{I}$ is a $*$**-ideal** of $\mathfrak{B}(\mathbb{H})$.

If $\mathfrak{I}$ is a left $*$-ideal, then since XY and X^* belong to $\mathfrak{I}$, it follows that also $YX = (X^*Y^*)^*)$ belong to $\mathfrak{I}$.

Theorem 3.12.4. *The sets $\mathfrak{B}_{00}(\mathbb{V})$ and $\mathfrak{B}_0(\mathbb{V})$ are bilateral $*$-ideals of $\mathfrak{B}(\mathbb{V})$.*

Theorem 3.12.5. *Let $\mathbb{H}$ be a Hilbert space and $X \in \mathfrak{B}(\mathbb{H})$. The following statements are equivalent:*

1. *$X \in \mathfrak{B}_0(\mathbb{H})$,*
2. *for any sequence $(h_n)_{n\in\mathbb{N}}$ in $\mathbb{H}$, with $\|h_n\| \leq 1$ for all $n \in \mathbb{N}$, the sequence $(Xh_n)_{n\in\mathbb{N}}$ has a convergent subsequence,*
3. *for any sequence $(h_n)_{n\in\mathbb{N}}$ in $\mathbb{H}$ with $\|h_n\| < \infty$ for all $n \in \mathbb{N}$, the sequence $(Xh_n)_{n\in\mathbb{N}}$ has a convergent subsequence,*
4. *for any bounded subset $B \subset \mathbb{H}$, the set $\overline{X(B)}$ is compact.*

Definition 3.12.6. Let $(\varepsilon_n)_{n\in\mathbb{B}}$ be an arbitrary orthonormal basis in a Hilbert space $\mathbb{H}$ and X a bounded operator on $\mathbb{H}$. We define the **Hilbert-Schmidt norm** of X the quantity

$$\|X\|_2 = \sum_{n\in\mathbb{N}} \|X\varepsilon_n\|^2 \in \mathbb{R}_+ \cup \{+\infty\}.$$

An operator X is called **Hilbert-Schmidt operator** if $\|X\|_2 < \infty$. The family of Hilbert-Schmidt operators is denoted by $\mathfrak{B}_2(\mathbb{H})$.

Proposition 3.12.7. *Let $\mathbb{H}$ be a Hilbert space.*

1. *$\mathfrak{B}_2(\mathbb{H})$ is a bilateral $*$-ideal of $\mathfrak{B}(\mathbb{H})$.*
2. *If $X \in \mathfrak{B}_2(\mathbb{H})$ then $\|X\| \leq \|X\|_2$.*
3. *$\mathfrak{B}_{00}(\mathbb{H})$ is a dense subset of the normed space $\mathfrak{B}_2(\mathbb{H})$ for the Hilbert-Schmidt norm.*

Definition 3.12.8. Let $(\varepsilon_n)_{n\in\mathbb{B}}$ be an arbitrary orthonormal basis in a Hilbert space $\mathbb{H}$ and X a positive operator. We define the **trace** of X the quantity

$$\mathrm{tr}\, X = \sum_{n\in\mathbb{B}} \langle\, \varepsilon_n \,|\, X\varepsilon_n \,\rangle \in \mathbb{R}_+ \cup \{+\infty\}.$$

An operator X is called of **trace class** if $\mathrm{tr}\,|X| < \infty$. The family of trace class operators is denoted by $\mathfrak{B}_1(\mathbb{H})$.

Remark 3.12.9. In finite dimension, all operators are Hilbert-Schmidt and trace class.

Proposition 3.12.10. *Let $X, Y \geq 0$. The trace is independent of the basis used to compute it. Additionally,*

1. *$\mathrm{tr}(X + Y) = \mathrm{tr}(X) + \mathrm{tr}(Y)$.*

2. *For all* $\lambda \geq 0$, $\mathsf{tr}(\lambda X) = \lambda\,\mathsf{tr}(X)$.
3. *For every unitary operator* U, $\mathsf{tr}(UXU^*) = \mathsf{tr}(X)$.
4. *If* $0 \leq X \leq Y$, *then* $0 \leq \mathsf{tr}(X) \leq \mathsf{tr}(Y)$.

Theorem 3.12.11. *The space of trace class operators* $\mathfrak{B}_1(\mathbb{H})$ *is*

1. *a two-sided* $*$*-ideal in* $\mathfrak{B}(\mathbb{H})$,
2. *the pre-dual of* $\mathfrak{B}(\mathbb{H})$.

Theorem 3.12.12. *Let* $X \in \mathfrak{B}(\mathbb{H})$. *The following assertions are equivalent.*

1. $X \in \mathfrak{B}_1(\mathbb{H})$.
2. $|X|^{1/2} \in \mathfrak{B}_2(\mathbb{H})$,
3. $X = YZ$, *where* $Y, Z \in \mathfrak{B}_2(\mathbb{H})$.
4. $|X| = VW$, *where* $V, W \in \mathfrak{B}_2(\mathbb{H})$.

Theorem 3.12.13. *On defining* $\|X\|_1 = \mathsf{tr}(|X|)$, *the vector space* $\mathfrak{B}_1(\mathbb{H})$ *becomes a Banach space. Additionally* $\|X\| \leq \|X\|_1$. *The class* $\mathfrak{B}_{00}(\mathbb{H})$ *is dense in* $\mathfrak{B}_1(\mathbb{H})$ *for the* $\|\cdot\|_1$ *norm.*

Theorem 3.12.14. *Define* $\langle X, Y\rangle = \mathsf{tr}(X^*Y)$ *for* $X, Y \in \mathfrak{B}_2(\mathbb{H})$. *Then* $\langle\cdot,\cdot\rangle$ *is a scalar product on* $\mathfrak{B}_2(\mathbb{H})$, *for which the Hilbert-Schmidt class of operators becomes a Hilbert space on its own. Hilbert-Schmidt norm of the space stems from the scalar product* $\langle X, Y\rangle$.

Proposition 3.12.15. *Let* $(\varepsilon_n)_{n\in\mathbb{B}}$ *be an orthonormal basis in* $\mathbb{H}$ *and denote, for every* $n \in \mathbb{B}$, *by* $E[n] = |\,e_n\,\rangle\langle\,e_n\,|$ *the orthoprojection onto the one-dimensional subspace* $\mathbb{C}\varepsilon_n$. *If* $\psi \in \mathbb{H}$ *is an arbitrary unit vector, then the family* $(p_n)_{n\in\mathbb{B}}$, *where* $p_n := \langle\,\psi\,|\,E[n]\psi\,\rangle$, *constitute a probability vector and* $\rho = \sum_n p_n E[n]$ *is a positive operator of trace 1. Conversely, if* ρ *is a positive operator such that* $\mathsf{tr}(\rho) = 1$, *then its spectral decomposition reads* $\rho = \sum_{n\in\mathbb{B}} p_n E[n]$, *where* $(p_n)_{n\in\mathbb{B}}$ *is a probability vector.*

Definition 3.12.16. A positive operator of trace 1 is called a **density operator**. The family of density operators on $\mathbb{H}$ is denoted by $\mathfrak{D}(\mathbb{H})$.

A classical probability $\mathbb{P}$ on $(\mathbb{X}, \mathcal{X})$, for $\mathbb{X}$ a denumerable set, is equivalent to a probability vector $(p_x)_{x\in\mathbb{X}}$, with $p_x \geq 0$ and $\sum_{x\in\mathbb{X}} p_x = 1$, through the bijection $\mathbb{P} = \sum_x p_x\varepsilon_x$, where ε_x is the Dirac mass at x. Recall that for any $A \in \mathcal{X}$, Dirac masses verify $\varepsilon_x(A) = \mathbb{1}_A(y)$ hence $\varepsilon_x^2 = \varepsilon_x$, i.e. ε_x is a projector; Dirac masses are extremal points of the convex set $\mathcal{M}_1(\mathcal{X})$ of probability measures on $\mathbb{X}$. All other probability measures $\mathbb{P} \in \mathcal{M}_1(\mathcal{X})$, obtained as non-trivial convex combinations of Dirac masses, verify $\mathbb{P}^2 < \mathbb{P}$ (component-wise).

The proposition 3.12.15 shows that density operators are non-commutative generalisations of probability measures in the following sense. First observe that $\mathfrak{D}(\mathbb{H})$ is a convex set. If $\psi \in \mathbb{H}$ is a unit vector, then $\rho = |\,\psi\,\rangle\langle\,\psi\,| \in \mathfrak{D}(\mathbb{H})$ and verifies $\rho^2 = \rho$, while all other elements of $\mathfrak{D}(\mathbb{H})$, expressed as non-trivial convex combinations $\rho = \sum_n p_n E[n]$ of one-dimensional projections, verify $\rho^2 < \rho$.

These remarks allow to generalise the postulate 2.6.2 into the following form:

Postulate 3.12.17 (Generalisation of the states postulate 2.6.2)**.** *Density operators* $\mathfrak{D}(\mathbb{H})$ *constitute the (convex) set of quantum states* $\mathbf{S}$. *The set of one dimensional projectors in* $\mathfrak{D}(\mathbb{H})$ *are isomorphic to unit vectors of* $\mathbb{H}$ *and constitute extremal elements of* $\mathbf{S}$ *corresponding to pure states* $\mathbf{S}_p$.

Since density operators are the generalisations of states (probability measures) in the quantum case and since composite systems are described by tensor products, a density operator on a tensor product will be interpreted as a joint probability on the composite system. It is therefore natural to ask which are the marginals of the joint probability on the Hilbert spaces of the constituent systems (see postulate 2.6.1). The notion of marginal is naturally implemented by the operation of **partial trace.**

Definition 3.12.18. Let $X \in \mathfrak{B}_1(\mathbb{H}_1 \otimes \mathbb{H}_2)$ and suppose that $(\varepsilon_n)_{n\in\mathbb{B}_1}$ and $(\zeta_n)_{n\in\mathbb{B}_2}$ are orthonormal bases of $\mathbb{H}_1$ and $\mathbb{H}_2$ respectively. We call **partial traces** with respect to the second (respectively first) system the operators $Z_1 := \mathrm{tr}_{\mathbb{H}_2}(X) \in \mathfrak{B}_1(\mathbb{H}_1)$ and $Z_2 := \mathrm{tr}_{\mathbb{H}_1}(X) \in \mathfrak{B}_1(\mathbb{H}_2)$ defined for all $\phi, \phi' \in \mathbb{H}_1$ and all $\psi, \psi' \in \mathbb{H}_2$ by

$$\langle\, \phi \,|\, Z_1\phi' \,\rangle := \sum_{k\in\mathbb{B}_2} \langle\, \phi\otimes\zeta_k \,|\, X(\phi'\otimes\zeta_k)\,\rangle \text{ and } \langle\, \psi \,|\, Z_2\psi' \,\rangle := \sum_{k\in\mathbb{B}_1} \langle\, \varepsilon_k\otimes\psi \,|\, X(\varepsilon_k\otimes\psi')\,\rangle.$$

Definition 3.12.19. If $\rho \in \mathbf{S}(\mathbb{H}_1 \otimes \mathbb{H}_2)$ the partial traces $\rho_1 = \mathrm{tr}_{\mathbb{H}_2}(\rho)$ and $\rho_2 = \mathrm{tr}_{\mathbb{H}_1}(\rho)$ are called **(quantum) marginals.**

Exercise 3.12.20. A very important one!

1. Show that if $X \in \mathfrak{B}_1(\mathbb{H}_1 \otimes \mathbb{H}_2)$ then $\mathrm{tr}_{\mathbb{H}_2}(X) \in \mathfrak{B}_1(\mathbb{H}_1)$ and $\mathrm{tr}_{\mathbb{H}_1}(X) \in \mathfrak{B}_1(\mathbb{H}_2)$. Additionally, if $X \in \mathfrak{D}(\mathbb{H}_1 \otimes \mathbb{H}_2)$ so are its partial traces.
2. Let $\Psi \in \mathbb{H}_1 \otimes \mathbb{H}_2$ be a unit vector and $\rho = |\,\Psi\,\rangle\langle\,\Psi\,| \in \mathbf{S}_p(\mathbb{H}_1 \otimes \mathbb{H}_2)$. Determine its quantum marginals in terms of the components of the vector Ψ. *Hint:* It is enough to consider the example $\mathbb{H}_1 \equiv \mathbb{H}_2 \equiv \mathbb{C}^2$ and the two cases (with $|a|^2 + |b|^2 = 1$)

$$\Psi = a\varepsilon_0\otimes\varepsilon_0 + b\varepsilon_0\otimes\varepsilon_1 \text{ and } \Psi = a\varepsilon_0\otimes\varepsilon_0 + b\varepsilon_1\otimes\varepsilon_1.$$

3. **What do you conclude?**

Exercise 3.12.21. (Tedious but very useful one!) This exercise aims at establishing useful parametrisations for self-adjoint and unitary operators in the special case of $\mathbb{H} = \mathbb{C}^2$. The results obtained here shed new light on the parametrisation of rays in $\mathbb{H}$ used on pages 57–59. They will be also instrumental in §ssec:bell-hidden-variable-model and §16.4.2.

Notation: In this exercise, $\mathbb{H} = \mathbb{C}^2$. The set of (trivially bounded) operators $\mathfrak{B}(\mathbb{H})$ is isomorphic to $\mathbb{M}_{2\times2}(\mathbb{C}) \simeq \mathbb{C}^4$. The space $\mathfrak{B}(\mathbb{H})$ is a complex vector space in its own and, equipped with the Hilbert-Schmidt scalar product $\langle X, Y\rangle = \mathrm{tr}(X^*Y)$, becomes a Hilbert space. Greek indices α, β are running over the set $\{0,1,2,3\}$ while Latin indices k, l, m run over $\{1,2,3\}$. Vectors in $\mathbb{C}^4$ are denoted in sanserif font, e.g. a, b, u, v, x, y, z while vectors in $\mathbb{C}^3$ in bold font **a, b, u, v, x, y, z**; we have, for instance, the equality $\mathsf{a} = (a_0, \mathbf{a})$. The **Pauli matrices** $(\sigma_\alpha)_{\alpha\in\{0,\dots,3\}}$ are given by

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

We denote by $\boldsymbol{\sigma} := (\sigma_1, \sigma_2, \sigma_3)$.

1. Show that
   — for all $\alpha = 0, \dots, 3$, we have $\sigma_\alpha^2 = \sigma_0$,

— $\sigma_k\sigma_l = \delta_{kl}\sigma_0 + i\sum_{m\in\{1,2,3\}} \varepsilon_{klm}\sigma_m$, where ε_{klm} is the totally antisymmetric tensor.

2. Conclude that the family $(\sigma_\alpha)_{\alpha\in\{0,\dots,3\}}$ is an orthogonal basis of $\mathfrak{B}(\mathbb{H})$.
3. In view of the previous result, any $X \in \mathfrak{B}(\mathbb{H})$ can be written as a linear combination of Pauli matrices: $X = \sum_{\alpha=0}^{3} x_\alpha\sigma_\alpha$. Which constraints are imposed on the 4-vector x for X to be
   — self-adjoint $X^* = X$,
   — positive $X \geq 0$,
   — normalised $\mathrm{tr}(X) = 1$.
4. Establish the identity: $(\mathbf{a}\cdot\boldsymbol{\sigma})(\mathbf{b}\cdot\boldsymbol{\sigma}) = (\mathbf{a}\cdot\mathbf{b})\sigma_0 + i(\mathbf{a}\wedge\mathbf{b})\cdot\boldsymbol{\sigma}$.
5. Let U be a unitary operator on $\mathbb{H}$. Show that unitarity imposes that $U = u_0\sigma_0 + i\mathbf{u}\cdot\boldsymbol{\sigma}$, with $u \in \mathbb{R}^4$, verifying $u_0^2 + \|\mathbf{u}\|^2 = 1$. Conclude that the unitary operator can also be written as
$$U = \exp(i\chi\mathbf{n}\cdot\boldsymbol{\sigma}),$$
with $\mathbf{n} \in \mathbb{S}^2$ and $\chi \in [0, 2\pi]$.
6. For arbitrary vectors $\mathbf{a}, \mathbf{b} \in \mathbb{R}^3$ and an arbitrary unitary operator U, let $A = \mathbf{a}\cdot\boldsymbol{\sigma}$, $A' = UAU^*$, and $B = \mathbf{b}\cdot\boldsymbol{\sigma}$.
   — Show that $\mathrm{tr}(A) = \mathrm{tr}(A') = 0$, and conclude that $A' = \mathbf{a}\cdot\boldsymbol{\sigma}$, for some $\mathbf{a}' \in \mathbb{R}^3$.
   — Show that $U(\mathbf{a}\cdot\boldsymbol{\sigma})(\mathbf{b}\cdot\boldsymbol{\sigma})U^* = (\mathbf{a}'\cdot\boldsymbol{\sigma})(\mathbf{b}'\cdot\boldsymbol{\sigma})$ for some $\mathbf{a}, \mathbf{b} \in \mathbb{R}^3$ such that $\mathbf{a}\cdot\mathbf{b} = \mathbf{a}'\cdot\mathbf{b}'$, i.e. U induces some transformation R_U on $\mathbb{R}^3$ that preserves Euclidean scalar product.
   — Show that R_U is linear.
   — Choose a unit vector $\mathbf{m}$ perpendicular to $\mathbf{n}$. A rotation around the axis $\mathbf{n}$ by an angle θ will bring $\mathbf{m}$ into $\mathbf{m}' = R_U\mathbf{m}$, with $\mathbf{m}'\cdot\mathbf{m} = \cos\theta$. Show that $\cos\theta = \mathbf{m}'\cdot\mathbf{m} = \frac{1}{2}\mathrm{tr}[(\mathbf{m}'\cdot\boldsymbol{\sigma})(\mathbf{m}\cdot\boldsymbol{\sigma})]$ and conclude that $U = \exp(i\frac{\theta}{2}\mathbf{n}\cdot\boldsymbol{\sigma})$.
   — Use the homomorphism between U and R_U to determine the axis $\mathbf{c}$ of rotation and the rotation angle γ when two rotations of axes and angles respectively $(\mathbf{a}, \alpha)$ and $(\mathbf{b}, \beta)$ are performed sequentially.

Summary of classical vs. quantum postulates

Classical	Quantum
Phase space	
$(\Omega, \mathcal{F})$ measurable space	$\mathbb{H}$ separable complex Hilbert space
Composite system	
$(\Omega_1 \times \Omega_2, \mathcal{F}_1 \otimes \mathcal{F}_2)$	$\mathbb{H}_1 \otimes \mathbb{H}_2$
Real (discrete, i.e. $\mathbb{X}$ discrete) observables	
$X : \Omega \to \mathbb{X} \subseteq \mathbb{R}$	$X \in \mathfrak{B}(\mathbb{H})$ self-adjoint; $\mathbb{X} = \mathsf{spec}(X)$
States	
General	
$\rho \in \mathcal{M}_1(\Omega, \mathcal{F})$	$\rho \in \mathfrak{D}(\mathbb{H})$
Extremal	
$\rho = \delta_\omega, \omega \in \Omega$	$\rho = \vert\,\psi\,\rangle\langle\,\psi\,\vert, \psi \in \mathbb{H}, \Vert\psi\Vert = 1$
Time evolution of isolated system	
$U : \Omega \to \Omega$ measurable invertible	U unitary operator on $\mathbb{H}$
Physical measurement	
One outcome $x \in \mathbb{X}$ $\mathbb{P}(X = x) = \langle \rho, E[x] \rangle$	One eigenvalue $x \in \mathbb{X}$ $\mathbb{P}(X = x) = \langle \rho, E[x] \rangle$
State conditioned at having observed x	
$\rho_x(\cdot) = \frac{E[x]\rho E[x]}{\langle \rho, E[x] \rangle}$	$\rho_x(\cdot) = \frac{E[x]\rho E[x]}{\langle \rho, E[x] \rangle}$
Unconditional state after observation: $\rho' = \sum_{x \in \mathbb{X}} \mathbb{P}(X = x)\rho_x$	
Always: $\rho' = \rho$	**In general:** $\rho' \neq \rho$

4

First consequences of quantum formalism

> It would seem that the theory is exclusively concerned about "results of measurement", and has nothing to say about anything else. What exactly qualifies some physical systems to play the role of "measurer"? Was the wavefunction of the world waiting to jump for thousands of millions of years until a single-celled living creature appeared? Or did it have to wait a little longer, for some better qualified system . . . with a Ph.D.? If the theory is to apply to anything but highly idealised laboratory operations, are we not obliged to admit that more or less "measurement-like" processes are going on more or less all the time, more or less everywhere? Do we not have jumping then all the time?
>
> John BELL: *Against measurement* [16, p. 34].

We start this chapter by showing first, in §4.1, how the quantum formalism can be used to re-interpret results already explicable within classical physics.

We recall that the measurement postulate 2.6.5 of quantum theory is very counter-intuitive. It states that when we let a system — prepared in some state ρ — interact with a measuring apparatus designed to measure a given observable X, the outcome x of the measurement can be any eigenvalue $x \in \mathrm{spec}(X)$, these outcomes occurring randomly according to the probability $\nu_X^\rho(x)$. In other words, if we prepare an ensemble of N copies of the system in state ρ and measure X on every one of them, we get N_x times every outcome $x \in \mathrm{spec}(X)$. When $N \to \infty$, the only assertion of quantum theory is that the empirical frequency N_x/N of occurrence of the value $x \in \mathrm{spec}(X)$ tends $\nu_X^\rho(x)$ as $N \to \infty$. There are actually two predictions of quantum theory:

— every possible outcome x of X is constrained to lie in $\mathrm{spec}(X)$, independently of the state in which the measurement is performed, and

— the probability of occurrence of a given outcome x, for a measurement per-

formed within state ρ, is given by $\nu_X^\rho(x)$.

The second result that will be shown in §4.2 of this chapter — as a consequence of the formalism — is the so-called **uncertainty principle** stating that there do not exist states in which **all** dynamical variables have determinate sharp (i.e. of 0 variance) values; quantum mechanics appears as an **intrinsically and irreducibly stochastic theory**. This intrinsic randomness is exploited to construct at pre-industrial level working devices producing sequences of **true random numbers**. The principle of functioning of these devices is explained in §4.3.

In §3.10, we have introduced the the purely quantum notion of **entanglement** and in §**??**, we describe how the bi-partite entanglement can be used to explain the Orsay experiment — already described in §2.5.2 — which does not possess any classical explanation.

The conventional wisdom, known as the Copenhagen interpretation of quantum theory (incarnated in the tutelary figure of Niels Bohr), is that a "measurement does not, in general, reveal a pre-existing value of the measured property. On the contrary, the outcome of the measurement is brought into being by the act of measuring itself, a joint manifestation of the state of the probed system and the probing apparatus" [1]. This statement is not a consequence of the intrinsic stochasticity of quantum theory implied by the uncertainty principle. As a matter of fact, it is conceivable that a measurement disturbs the measured system, preventing thus the 0-variance determination of all its properties. But the question remains whether the properties of the system possess, prior to the measurement, determinate values that are revealed by the measurement process. In §**??**, we provide with another paradox, even sharper than the EPR paradox, known as Greenberg-Horne-Zeilinger (GHZ) paradox while in §**??**, we establish another "no-go" theorem excluding the possibility of existence of **hidden variables.**

We finish this chapter by establishing, in §4.8, another purely quantum notion known as **complete positivity** that governs general temporal evolution of a quantum system and conclude by §4.9 that illustrates the phenomenon of **decohrence**, i.e. the passage of the time evolution of a system from quantum into classical behaviour.

4.1 Light polarisers are not classical filters

As recalled in appendix, polarisation of light is the direction of variation of the electric field associated with it. There exist in Nature active anisotropic optical materials (like calcite) that are birefringent, i.e. their light diffraction properties depend on the polarisation of incident light. This birefringence phenomenon is exploited to construct linear polarisers. Linear polarisers are caracterised by the direction of polarisation of the emergent light. When two polarisers are sequentially traversed by light with their directions at 90 degrees, the light beam is totally absorbed. The figure 4.1 depicts a pair of commercially available polarisers with their directions crossed. The experiment we intend to analyse in this subsesction is depicted in the following figure 4.2. When nat-

1. Quoted from [108].

Figure 4.1 – Photograph of two commercially available polarisers, placed on a white surface, with their principal directions almost at 90 degrees. In the region where the two polarisers are superposed, the image appears black because all light energy is absorbed. In the regions where each polariser acts alone, the image appears grey because half of the light energy is absorbed.

ural light passes through a horizontally oriented polariser, half of the initial intensity is transmitted. When a vertical polariser is then placed in the beam, the light is totally absorbed (left part of the figure 4.2). On the contrary when three polarisers with respective orientations turned by 45 degrees each time are placed perpendicularly to the light beam, the eighth of the intensity is transmitted (right part of the figure 4.2).

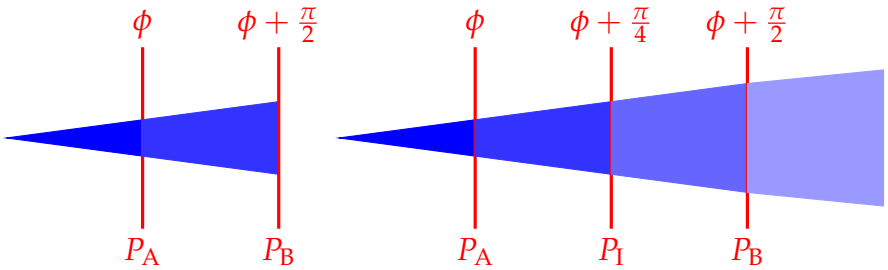


Figure 4.2 – The experimental setting with two or three polarisers and a source of non polarised light. In the left setting, after polariser P_A, oriented at an arbitrary angle ϕ, half of the intensity passes; after polariser P_B, crossed at right angle with respect to P_A, no light passes. In the right setting, after polariser P_A, oriented at angle ϕ, half of the intensity passes; after polariser P_I, oriented at 45 degrees with respect to P_1, the fourth of the initial intensity passes, and after polariser P_B, oriented at 90 degrees with respect to P_A, the eighth of the initial intensity passes.

4.1.1 Classical explanation

If we consider polarisers not as filters, the experiment has a classical explanation, we give here in a simplified form. A solution of the Maxwell equations (see appendix A) in vacuum (where charge and current densities vanish) can be given by the electric, $\boldsymbol{E}$, and magnetic vector, $\boldsymbol{B}$, fields reading respectively for $\boldsymbol{r} = (x, y, z) \in \mathbb{R}^3$,

$$\boldsymbol{E}(\boldsymbol{r}, t) = E_{\max} \boldsymbol{a}(\alpha) \sin(2\pi(z - ct)/\lambda)); \;\; \boldsymbol{B}(\boldsymbol{r}, t) = \frac{1}{c} \boldsymbol{e}_z \times \boldsymbol{E}(\boldsymbol{r}, t),$$

where $\boldsymbol{a}(\alpha) = \begin{pmatrix} \cos\alpha \\ \sin\alpha \\ 0 \end{pmatrix}$ denotes the direction of polarisation, c the speed of light, λ the wavelength, and μ_0 is a physical constant. The light intensity associated with such an electromagnetic wave is $I = \frac{\|E_{\max}\boldsymbol{a}(\alpha)\|^2}{2\mu_0 c} = CE_{\max}^2\|\boldsymbol{a}(\alpha)\|^2$.

Since polarisation has not a component on the direction of propagation of the wave, we can limit ourselves in the two dimensional plane perpendicular to the propagation axis. We can use Dirac's notation [2] to denote vectors in this plane; the unit vector in this two-dimensional plane reads $|\,\mathbf{u}_\alpha\,\rangle = \cos\alpha|\,\mathbf{e}\,\rangle_x + \sin\alpha|\,\mathbf{e}_y\,\rangle$. Since $\langle\,\mathbf{u}_\alpha\,|\,\mathbf{u}_\alpha\,\rangle = 1$, the intensity of natural light (in which all polarisations arise with the same probability) is equal to $I_0 = CE_{\max}^2$.

Now, a polariser P_A placed perpendicularly to the beam oriented according to angle β acts as a projection operator to the one dimensional subspace of $\mathbb{R}^2$ spanned by $|\,\mathbf{u}_\beta\,\rangle = \cos\beta|\,\mathbf{e}_x\,\rangle + \sin\beta|\,\mathbf{e}_y\,\rangle$. Hence, after crossing such a polariser, for every initial polarisation, α, the intensity will read

$$I_1 = CE_{\max}^2\|(|\,\mathbf{u}_\beta\,\rangle\langle\,\mathbf{u}_\beta\,|)|\,\mathbf{u}_\alpha\,\rangle\|^2 = |\langle\,\mathbf{u}_\beta\,|\,\mathbf{u}_\alpha\,\rangle|^2\langle\,\mathbf{u}_\beta\,|\,\mathbf{u}_\beta\,\rangle = CE_{\max}^2\cos^2(\alpha-\beta),$$

and averaging over all initial polarisations, the intensity of the beam crossing the first polariser reads $I_1 = CE_{\max}^2\int_0^{2\pi}\cos^2(\alpha-\beta)\frac{d\alpha}{2\pi} = \frac{1}{2}CE_{\max}^2$.

If a second polariser P_B at angle γ is placed perpendicularly to the beam after the first polariser, the emerging intensity reads

$$I_2 = CE_{\max}^2\cos^2(\beta-\gamma)\int_0^{2\pi}\cos^2(\alpha-\beta)\frac{d\alpha}{2\pi} = \frac{1}{2}CE_{\max}^2\cos^2(\beta-\gamma).$$

When $\gamma = \beta + \pi/2$, nothing emerges. Thus classical physics correctly explains the left part of the experiment described in figure 4.2.

If a third polariser P_I is placed between P_A and P_B at angle δ, the final intensity will read

$$I_2 = CE_{\max}^2\cos^2(\beta-\delta)\cos^2(\delta-\gamma)\int_0^{2\pi}\cos^2(\alpha-\beta)\frac{d\alpha}{2\pi} = \frac{1}{2}CE_{\max}^2\cos^2(\beta-\delta)\cos^2(\delta-\gamma).$$

If $\delta = \beta + \pi/4$ and $\gamma = \delta + \pi/4$, the intensity emerging from P_B is the eight of the initial intensity, in accordance with the experiment described in the right part of the figure 4.2.

4.1.2 Simplified quantum explanation

The correct quantum description of a light beam is possible only within the second quantisation formalism (that will be introduced in §16.1.2 and applied to light in appendix A). It is nevertheless instructive to provide with a simplified quantum explanation of the experiment to demonstrate the consistency of the quantum formalism.

2. Yes, Dirac's notation is useful even in standard linear algebra on Euclidean spaces!

As explained in appendix A, in its quantum mechanical description, light is composed of a tremendous number of elementary light quanta per second, called **photons**, that propagate at a constant speed reading, in the vacuum, $c = 2.99792458 \times 10^8$ m/s. For instance, the laser beam emitted by a commercial AlGaInP laser diode [3] has a power of $P = 5$ mW at a wavelength of $\lambda = 635$ nm$= 6.35 \times 10^{-7}$ m (corresponding to a colour in the orange-yellow region of the spectrum, as seen in figure A.1) has its power vehicled [4] by the flow of ca. 3.2×10^{15} photons per second. Any single photon of *natural light* has been produced by the decay of a different excited atom of the sun (or of a terrestrial incadescent lamp); it is natural then to suppose that every photon is described by a different pure state determined by the unit vector $\psi \in \mathbb{H} \cong \mathbb{C}^2$ parametrised [5] by $\psi = \cos\alpha\varepsilon_0 + \exp(i\beta)\sin\alpha\varepsilon_1$, with α, β random variables, uniformly distributed on $[0, 2\pi]$.

The action of polarisers P_A, P_I and P_B is equivalent to projective measurements of respectively $E_A := |\,\varepsilon_0\,\rangle\langle\,\varepsilon_0\,|$, $E_I = \frac{1}{2}|\,\varepsilon_0 + \varepsilon_1\,\rangle\langle\,\varepsilon_0 + \varepsilon_1\,|$, and $E_B = |\,\varepsilon_1\,\rangle\langle\,\varepsilon_1\,|$. Therefore, every polariser acts as a sharp effect on the state of every individual photon and the answer (the measurement of the effect in the state) will be either yes or no with some probability depending on the relative angle of photon and polariser's polarisations. In other words, an individual photon either passes with some probability or is absorbed with the complementary probability. The light intensity measured at the exit of the experimental setup has thus only a statistical meaning. It corresponds to the average number of photons that have been transmitted mulitplied by their power. It is then an easy matter to explain the results of the left setting. In the following table, we summarise the results concerning the right setting.

Polariser	Input ray	$\mathbb{P}$(photon passes)
P_A	$\|\,\psi_0\,\rangle = \cos(\alpha)\|\,\varepsilon_0\,\rangle + \exp(i\beta)\sin(\alpha)\|\,\varepsilon_1\,\rangle$	$\langle\,\psi_0\,|\,E_A\psi_0\,\rangle = \cos^2(\alpha)$
P_I	$\|\,\psi_A\,\rangle = \|\,\varepsilon_0\,\rangle$	$\langle\,\psi_A\,|\,E_A\psi_A\,\rangle = \frac{1}{2}$
P_B	$\|\,\psi_I\,\rangle = \frac{1}{\sqrt{2}}\|\,\varepsilon_0 + \varepsilon_1\,\rangle$	$\langle\,\psi_I\,|\,E_B\psi_I\,\rangle = \frac{1}{2}$

The overall transmission probability is $\frac{1}{4}\int_0^{2\pi}\cos^2(\alpha)\frac{d\alpha}{2\pi} = \frac{1}{8}$, explaining the experimental observation.

4.2 Heisenberg's uncertainty principle

The first and more spectacular direct consequence of the quantum mechanical formalism is the so called **Heisenberg's uncertainty principle** establishing the conceptual

3. This is small optoelectronic device that can be purchased for some 20 €. The principle of its functioning was described as early as 1953, in an unpublished manuscript of John von Neumann titled *Notes on the photon-desequilibrium-amplification scheme* that has been reproduced in Volume 5 of his collected works [151, p. 420].

4. The power of the beam is $P_{\text{beam}} = 5 \times 10^{-3}$ J/s. The energy E_{photon} carried by every individual photon at wavelength λ is $E_{\text{photon}} = 2\pi\hbar\frac{c}{\lambda}$ where c is the speed of light and $\hbar = 1.05457 \times 10^{-34}$ Js the Planck's constant. The number of photons per second crossing any plane perpendicular to the beam is then $n = \frac{P_{\text{beam}}}{E_{\text{photon}}}$. Substituting numerical values we get $n \approx 3.2 \times 10^{15}$ photons/s.

5. Recall figure 2.12.

and practical impossibility of considering systems with arbitrarily small joint randomness for certain pairs of observables. Spectral decomposition allows computation of the expectation of an operator X, in a pure state, ψ, by

$$\mathbb{E}_\psi X = \mathsf{tr}(\rho_\psi X) = \langle\, \psi \,|\, X\psi \,\rangle = \sum_{\lambda \in \mathsf{spec}(X)} \lambda |\psi_\lambda|^2$$

and when the operator X is self-adjoint, the spectrum is real and the expectation is then a real number. Following the probabilistic interpretation, denote by

$$\mathsf{Var}_\psi(X) = \mathbb{E}_\psi(X^2) - (\mathbb{E}_\psi(X))^2.$$

What makes quantum probability different from classical one, is (among other things) the impossibility of simultaneous diagonalisation of two non-commuting operators.

Theorem 4.2.1 (Heisenberg's uncertainty)**.** *Let X, Y be two bounded self-adjoint operators on a Hilbert space $\mathbb{H}$ and suppose a fixed pure state ψ is given. Then*

$$\sqrt{\mathsf{Var}_\psi(X)\mathsf{Var}_\psi(Y)} \geq \frac{|\langle\, \psi \,|\, [X,Y]\psi \,\rangle|}{2}.$$

Proof. First notice that $(i[X,Y])^* = i[X,Y]$ thus the commutator is skew-adjoint. Without loss of generality, we can assume that $\mathbb{E}_\psi X = \mathbb{E}_\psi Y = 0$ (otherwise consider $X - \mathbb{E}_\psi X$ and similarly for Y.) Now, since XY is not self-adjoint when X and Y do not commute, $\langle\, \psi \,|\, XY\psi \,\rangle = \alpha + i\beta$, with $\alpha, \beta \in \mathbb{R}$. Hence, $\langle\, \psi \,|\, [X,Y]\psi \,\rangle = 2i\beta$ and obviously

$$\begin{aligned} 0 &\leq 4\beta^2 = |\langle\, \psi \,|\, [X,Y]\psi \,\rangle|^2 \\ &\leq 4|\langle\, \psi \,|\, XY\psi \,\rangle|^2 \\ &\leq 4\langle\, \psi \,|\, X^2\psi \,\rangle\langle\, \psi \,|\, Y^2\psi \,\rangle, \end{aligned}$$

the last inequality being Cauchy-Schwarz. □

Exercise 4.2.2. Let $\rho \in \mathfrak{D}(\mathbb{H})$ be a state and $\mathbf{X} = (X_k)_{k=1,\dots,N}$ a family of centred observables (othwerwise replace X_k by $X_k - \mathbb{E}(X_k)I$). On defining the **covariance** and the **commutation** matrices, respectively denoted $C = (C_{kl})_{k,l=1,\dots,N}$ and $D = (D_{kl})_{k,l=1,\dots,N}$, where

$$C_{kl} = \mathsf{tr}(\rho \frac{1}{2}\{X_k, X_l\}), \;\; D_{kl} = \mathsf{tr}(\rho \frac{1}{2}[X_k, X_l]),$$

where $[\cdot,\cdot]$ denotes the commutator and $\{\cdot,\cdot\}$ the anticommutator, show that the matrix $M := C \pm iD$ is positive.

This is a typically quantum phenomenon without classical counterpart. In fact, given two arbitrary classical random variables X, Y on a measurable space $(\Omega, \mathcal{F})$, there exists always states (i.e. probability measures) on $(\Omega, \mathcal{F})$ such that $\mathsf{Var}(X)\mathsf{Var}(Y) = 0$ (for instance chose $\mathbb{P}(d\omega) = \delta_{\omega_0}(d\omega)$).

Remark 4.2.3. A comment is due at this point. According the quantum formalism, when an observable is measured on an individual system, it takes one of the possible values in the set of possible outcomes. The meaning of the uncertainty principle formula is a statistical one, i.e. we suppose that we dispose of a sequence of quantum systems prepared independently at a given pure state ψ. On half of those systems, we act with X^2 and on the other half, we act with Y^2 and register the experimental outcomes. When the size of the sequence tends to infinity, taking the empirical average of the outcomes of X^2 we estimate $\mathsf{Var}_\psi(X)$ and from the empirical average of the outcomes of Y^2 we estimate $\mathsf{Var}_\psi(Y)$ (recall that we have assumed that X and Y have zero mean).

Heisenberg's uncertainty relation is historically the first manifestation of the **irreducibility of quantum randomness**.

4.3 True random numbers generator

Every modern quantum cryptographic device relies on the possibility of producing sequences of truly random numbers. It can be shown that neither a classical device nor a classical algorithm (Turing machine) exist to produce true random numbers (see chapter devoted to Kolmogorov complexity in [121]), it is straightforward to produce efficiently sequences of random bits in an inexpensive way, by exploiting quantum physics. Here we present the principle of such devices.

The natural way to produce sequences of random bits is by using a polarising beam splitter (PBS). PBSs are commercially available in the form of small cubes or small plates (see figure 4.3 top left) and are made by gluing together two prisms in opposition of a transparent birefringent material (typically calcite $CaCO_3$). Birefringence means that light has different speeds inside the material depending on its polarisation. When a polarised photon enters the cube perpendicular to a face that is the vertical or the horizontal projection of the interface it is either reflected on the interface or passes through and the probability of each event depends on the polarisation. When the polarisation is at 45 degrees, theses probabilities are $1/2$.

The proper quantum mechanical treatment of the functioning of polarising beam splitter will be provided in appendix A after having developed the necessary second quantisation formalism in §16.1.2. For the time being, we give (the explanation is postponed to A) an elementary "black-box" form of the action of a PBS.

The PBS is considered as a system having two input channels (IC_1 and IC_2) and two output channels (OC_1 and OC_2) (see figure 4.3 top right). A single photon has also a polarisation that can be decomposed in its horizontal and vertical components. Thus a single photon with polarisation $p \in \{h, v\}$ is sent through the input channel $c \in \{1, 2\}$, the input state $|\,\Psi_{\text{in}}\,\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ reads

$$|\,\Psi_{\text{in}}\,\rangle = |\,pc\,\rangle, p \in \{h, v\}, c \in \{1, 2\}.$$

The action of the PBS (in the geometry of the figure 4.3 top right) results in a vector

$|\Psi_{\text{out}}\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$, reading

$$|\Psi_{\text{out}}\rangle = |p'c'\rangle, p' \in \{h, v\}, c' \in \{1, 2\},$$

where p, c, p', c' are related by a unitary transformation $|\Psi_{\text{out}}\rangle = U|\Psi_{\text{in}}\rangle$ determined by its matrix elements

$\lvert\Psi_{\text{in}}\rangle$	$\lvert\Psi_{\text{out}}\rangle$
$\lvert h1\rangle$	$-\lvert h2\rangle$
$\lvert h2\rangle$	$-\lvert h1\rangle$
$\lvert v1\rangle$	$-\lvert v1\rangle$
$\lvert v2\rangle$	$-\lvert v2\rangle$.

When the input is in a general polarisation state sent in channel 1, the input vector reads

$$|\Psi_{\text{in}}\rangle = \big(\cos(\theta)|h\rangle + \exp(i\phi)\sin(\theta)|v\rangle\big) \otimes |1\rangle$$

the output reads

$$|\Psi_{\text{out}}\rangle = \cos(\theta)|h2\rangle + \exp(i\phi)\sin(\theta)|v1\rangle.$$

The transmission probability is $\sin^2(\theta)$ and the reflection probability $\cos^2(\theta)$.

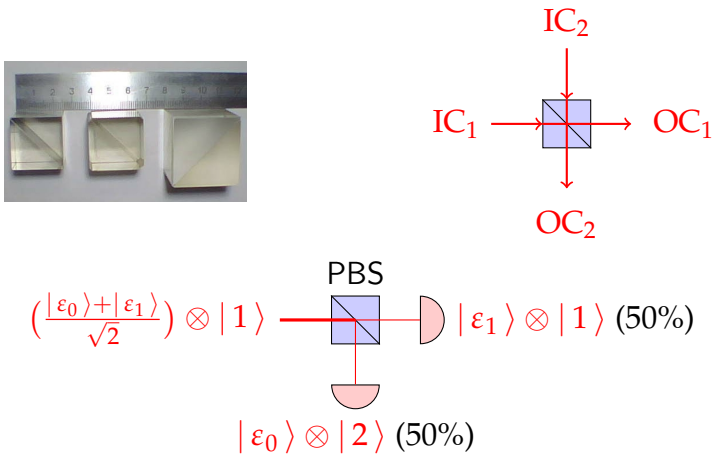


Figure 4.3 – *Top left picture:* photographs of commercially available polarising beam splitters of different sizes. The gluing of the two prisms in opposition is visible. *Top right picture:* schematic drawing of the optical circuit with the definition of input and output channels. *Bottom picture:* summary of the net effect of the PBS when the input photon is polarised at $\pi/4$. Notice that each individual photon triggers only one detector, i.e. it is either transmitted (uses the output channel 1) or reflected (uses the output channel 2) with respective probabilities $|\langle \frac{\varepsilon_0+\varepsilon_1}{\sqrt{2}}|\,\varepsilon_1\rangle|^2 = \frac{1}{2}$ and $|\langle \frac{\varepsilon_0+\varepsilon_1}{\sqrt{2}}|\,\varepsilon_0\rangle|^2 = \frac{1}{2}$.

Each individual photon incident with polarisation at 45 degrees, either is transmitted with probability $1/2$ or is reflected with probability $1/2$.

A light source is capable of producing single polarised, at 45 degrees say, photons at a constant pace. The beam is then directed on a PBS. According to the analysis made in the previous subsection, the photon passes with probability $1/2$ and is reflected with probability $1/2$. Placing photomultipliers at the output channels of the PBS, the

photons having been transmitted give 0, those having been reflected give 1. Quantum theory can only determine the probabilities of 0 and 1; there is absolutely no mean to determine a priori whether a single photon will effectively give 0 or 1.

This is the principle of functioning of commercial quantum random generators (like, for instance, the USB stick presented in figure 1.4).

4.4 The EPR paradox

As already mentioned, classical Physics relies on two properties shared by all known classical systems — and consequently —anchored in our classical intuition in perceiving and comprehending Nature, namely

locality, meaning that phenomena occurring within some finite region of space-time can be influenced by causes in some vicinity of that region (it is a consequence of finite speed of propagation of interactions), and

realism, meaning that observables of a given system have precise values, even if the system is not observed [6].

The EPR paradox was coined by Einstein, Podolsky, and Rosen to demonstrate that quantum formalism fails to be simultaneously realist **and** local; therefore — they argued — it must be incomplete.

In order to explain the EPR paradox, recall first the situation of exercise 3.12.20, where a pure state $\rho = |\Psi\rangle\langle\Psi| \in \mathfrak{D}(\mathbb{H}_1 \otimes \mathbb{H}_2)$ is considered. Both Hilbert spaces are of dimension 2 and they are equipped respectively with orthonormal bases $(\varepsilon_i)_{i=0,1}$ and $(\zeta_i)_{i=0,1}$.

1. If $|\Psi\rangle = a|\varepsilon_0\zeta_0\rangle + b|\varepsilon_1\zeta_0\rangle = |\phi\zeta_0\rangle$, where $|\phi\rangle = a|\varepsilon_0\rangle + b|\varepsilon_1\rangle$ and $|a|^2 + |b|^2 = 1$, then the vector $|\Psi\rangle$ is obviously factored and so is the pure state $\rho = |\Psi\rangle\langle\Psi| = |\phi\rangle\langle\phi| \otimes |\zeta_0\rangle\langle\zeta_0|$. The quantum marginals read then $\mathrm{tr}_{\mathbb{H}_1}(\rho) = |\zeta_0\rangle\langle\zeta_0|$ and $\mathrm{tr}_{\mathbb{H}_2}(\rho) = |\phi\rangle\langle\phi|$.
2. If $|\Psi\rangle = a|\varepsilon_0\zeta_0\rangle + b|\varepsilon_1\zeta_1\rangle$ with $|a|^2 + |b|^2 = 1$, then, if $a \notin \{0,1\}$, the vector $|\Psi\rangle$ is obviously entangled. The pure state $\rho = |\Psi\rangle\langle\Psi|$ reads

$$\begin{aligned}\rho &= |a|^2|\varepsilon_0\rangle\langle\varepsilon_0| \otimes |\zeta_0\rangle\langle\zeta_0| + |b|^2|\varepsilon_1\rangle\langle\varepsilon_1| \otimes |\zeta_1\rangle\langle\zeta_1| \\ &\quad + a\bar{b}|\varepsilon_0\rangle\langle\varepsilon_1| \otimes |\zeta_0\rangle\langle\zeta_1| + \bar{a}b|\varepsilon_1\rangle\langle\varepsilon_0| \otimes |\zeta_1\rangle\langle\zeta_0| \\ &= \begin{pmatrix} |a|^2 & 0 & 0 & a\bar{b} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \bar{a}b & 0 & 0 & |b|^2 \end{pmatrix}.\end{aligned}$$

When $a \notin \{0,1\}$, the state ρ is not a convex combination of factored states; it corresponds to an entangled state. Moreover, $\mathrm{spec}(\rho) = \{0,1\}$, the eigenvalue 1 having multiplicity 1 and the eigenvalue 0 having multiplicity 3, and since the function $t \mapsto -t\log t$ — with the convention $0\log 0$ — is well defined on the spectrum, we compute by a straightforward application of the spectral theorem

6. To mention another celebrated aphorism [107]: "Is the Moon there when nobody looks?"

that $S(\rho) = \mathrm{tr}(-\rho \log \rho) = 0$. The function S is the quantum analog of the entropy. The quantum marginals read $\rho_1 = \rho_2 = \begin{pmatrix} |a|^2 & 0 \\ 0 & |b|^2 \end{pmatrix}$ and correspond to mixed classical states and their quantum entropies read $S(\rho_1) = S(\rho_2) = H(|a|^2, 1-|a|^2)$, where H is the classical entropy of the classical probability vector $(|a|^2, 1-|a|^2)$. When $a = b = 1/\sqrt{2}$ the classical entropy equals 1 (is maximal). Thus, the joint pure quantum state has marginals which are maximally disordered.

We are now in position to formulate the **EPR paradox**. Let $\mathbb{H}_1, \mathbb{H}_2$ be as above and $\rho = |\Psi\rangle\langle\Psi|$, with $|\Psi\rangle = \frac{1}{\sqrt{2}}(|\varepsilon_0\zeta_0\rangle + |\varepsilon_1\zeta_1\rangle)$. We can think of the two components of the composite system as the two photons emerging in opposite directions in the Orsay experiment. Suppose that each photon of the pair is sent to one of two satellites very distant from one another. In each satellite an experimenter, say Alice in the first (A) and Bob in the second (B), decides either to measure the polarisation of the received photon or to do nothing. Of course, each experimenter has access only to his/her photon. So, for $x \in \{0,1\}$,

$$\mathbb{P}(\text{photon of } A \text{ has polarisation } \varepsilon_x) = \mathrm{tr}(\rho \mathcal{E}[x])$$
$$\mathbb{P}(\text{photon of } B \text{ has polarisation } \zeta_x) = \mathrm{tr}(\rho \mathcal{Z}[x])$$

where $\mathcal{E}[x] = E[x] \otimes \mathbb{I}_2$ with $E[x] = |\varepsilon_x\rangle\langle\varepsilon_x|$ and $\mathcal{Z}[x] = \mathbb{I}_1 \otimes Z[x]$ with $Z[x] = |\zeta_x\rangle\langle\zeta_x|$. Now suppose that when the photon 2 reaches B, Bob decides to do nothing, while at the moment the photon 1 reaches A, Alice asks whether its polarisation is ε_0. Obviously,

$$\mathbb{P}(\text{photon of } A \text{ has polarisation } \varepsilon_0) = \mathrm{tr}(\rho E[0] \otimes \mathbb{I}_2) = 1/2.$$

Symmetrically, if when the photon 1 reaches A she decides to do nothing while when the photon 2 reaches B, he asks whether its polarisation is ζ_0, the answer is

$$\mathbb{P}(\text{photon of } B \text{ has polarisation } \zeta_0) = \mathrm{tr}(\rho \mathbb{I}_1 \otimes Z[0]) = 1/2.$$

And these results are valid with a sequence of photons. As long as only one of the experimenters asks a question, the answer will be yes with probability $1/2$.

Suppose now that the photon 1 reached A before photon 2 reaching B and Alice decided to ask whether the polarisation is ε_0 and got the answer yes. According to the postulate of measurement, the pair of photons is now in the new state

$$\rho_0 = \frac{\mathcal{E}[0]\rho\mathcal{E}[0]}{\mathrm{tr}(\rho\mathcal{E}[0])} = |\varepsilon_0\rangle\langle\varepsilon_0| \otimes |\zeta_0\rangle\langle\zeta_0|.$$

When now the photon 2 reaches B and Bob asks whether its polarisation is ζ_0, the answer is yes with certainty! If Alice is the first to ask the question, whatever answer she gets, she knows that when Bob will ask the same question he will get the same answer! This is the **Einstein, Podolsky, and Rosen paradox (EPR)**; it is due to the fact that quantum correlations do not behave as classical ones.

We cannot refrain from reproducing here the vivid explanations (see figure 4.4) given by John Stewart Bell [19] himself on the occasion of a conference[7] he gave in 1980.

7. We got aware of this text thanks to the excellent commentary on the EPR paper made by Franck Laloë in [98].

> "The philosopher in the street, who has not suffered a course in quantum mechanics, is quite unimpressed by Einstein-Podolsky-Rosen correlations. He can point to many examples of similar correlations in everyday life. The case of Bertlman's socks is often cited. Dr. Bertlmann likes to wear two socks of different colours. Which colour he will have on a given foot on a given day is quite unpredictable. But when you see (Fig. 4.4) that the first sock is pink you can already be sure that the second sock will not be pink. Observation of the first, and experience of Bertlmann, gives immediate information about the second. There is no accounting for tastes, but apart form that there is no mystery here. And is not the EPR business just the same?"

The answer to the pholosopher's-in-the-street question is "no". The "EPR business" is definitely a different notion than that conveyed by the Dr. Bertlmann's socks paradigm (see box on page 135).

Figure 4.4 – Facsimilé from the last page of the conference of John Bell at the *Fondation Hugot*.

4.5 Hidden variables

The EPR paradox, violating simultaneous realism and locality of quantum theory, led Einstein, Podolsy, and Rosen to the conclusion that the theory was incomplete. An equivalent formulation of the lack of realism is in terms of intrinsic and irreducible randomness of quantum predictions. To understand this issue, consider a coin tossed in the air and let $(\mathbf{n}_t)_{t\in[0,T]}$ denote the (instantaneous) unit normal vector out from the "head" face. Given the initial conditions, the coin follows a trajectory described by the

equations of motion until it reaches a totally plastic surface, at instant T, where it stops. If $\mathbf{n}_T \cdot \mathbf{e}_3 > 0$, the outcome is head, if $\mathbf{n}_T \cdot \mathbf{e}_3 < 0$, it is tail. Due to the extreme sensitivity of the motion on the initial conditions, the outcome is known only at the moment it is observed. But nobody believes that the scalar product $\mathbf{n}_t \cdot \mathbf{e}_3$ has not a definite value at every instant $t \in [0, T]$. Coming to the quantum situation, a photon arriving on the optically active interface of a polarising beam splitter, is either transmitted or reflected but the formalism is "speech impaired" in predicting what an individual photon will do. The outcome is intrinsically and irreducibly random and has not a determinate value before it has been observed.

Efforts have been deployed during the second half of the 20th century to get rid of this randomness by advocating the existence of hidden variables supposedly assigning determinate values to the physical observables prior to their measurement.

4.5.1 What is a hidden-variables theory?

Let a system (classical or quantum) be described by the set $\mathbf{O}$ of observables and the set $\mathbf{S}$ of states. An observable $X \in \mathbf{O}$ can have several outcomes (in some set $\mathbb{X}$ depending on X); the probability of any individual outcome $x \in \mathbb{X}$, when the system is state $\rho \in \mathbf{S}$, is $\nu_X^\rho(x) = \langle \rho, E_X[x] \rangle$, where $E_X[x]$ is the sharp effect corresponding to the event "X takes the value x".

Suppose that there exists some additional space $\mathbf{H}$ and a $\mathbf{H}$-valued *unobserved* variable Λ, defined on some abstract space, and having distribution $\mu := \mu_\Lambda$, i.e. $\mathbb{P}(\Lambda \in \mathrm{d}\lambda) = \mu_\Lambda(\mathrm{d}\lambda)$, such that, when the information λ is used, the observable X (let it be classical or quantum) takes a determinate value x. The unobserved variable Λ is called a **hidden variable**.

Definition 4.5.1. Let $\mathbf{O}$ denote the set of observables of a physical system and $\mathbf{H}$ an additional space of hidden variables. For $\lambda \in \mathbf{H}$, hidden-variable induced **valuation** is a map $V := V_\lambda \mathbf{O} \to \mathbb{R}$. A valuation is

- **dispersion-free** if $\forall X \in \mathbf{O}, V(X^2) = V(X)^2$,
- **nomalised** if $V(I) = 1$,
- **quasi-linear** if $\forall X, Y \in \mathbf{O}$ such that $[X, Y] = 0$ and $\forall a, b \in \mathbb{R}$, we have $V(aX + bY) = aV(X) + bV(Y)$,
- **linear** if $\forall X, Y \in \mathbf{O}, \forall a, b \in \mathbb{R} : V(aX + bY) = aV(X) + bV(Y)$,

When $\mathbf{H}$ does not involve the state space $\mathbf{S}$ or other observables of the system, the valuation is called **non contextual**, otherwise it is **contextual**.

By abuse of language, a hidden-variable induced dispersion-free, (non-contextual) valuation is often simply termed hidden-variable. With this abuse, it is then meaningful to speak about a quasi-linear or a linear hidden variable.

Lemma 4.5.2. *Let V be a non contextual, dispersion-free, normalised, quasi-linear hidden-variable induced valuation on a system with set of observables $\mathbf{O}$. Then*

1. $\forall X \in \mathbf{O}, V(X) \in \mathsf{spec}(X)$, *and*

2. *for arbitrary, pairwise commuting observables $X_1, \dots, X_n$ and an arbitrary polynomial of n variables $p \in \mathbb{R}[t_1, \dots, t_n]$, we have*

$$V(p(X_1, \dots, X_n)) = p(V(X_1), \dots, V(X_n)).$$

Proof. 1. — Let $Y \in \mathbf{O}$ be an observable commuting with X. We have then

$$\begin{aligned} V((X \pm Y)^2) &= (V(X \pm Y))^2 \text{ by dispersion-freeness} \\ &= (V(X) \pm V(Y))^2 \text{ by quasi-linearity} \\ &= V(X)^2 + V(Y)^2 \pm 2V(X)V(Y). \end{aligned}$$

On the other hand,

$$\begin{aligned} V((X \pm Y)^2) &= (V(X^2 + Y^2 \pm 2XY)) \\ &= V(X^2) + V(Y^2) \pm 2V(XY) \text{ by quasi-linearity} \\ &= V(X)^2 + V(Y)^2 \pm 2V(XY) \text{ by dispersion-freeness.} \end{aligned}$$

Equating the r.h.s. of the above expressions, we get $V(XY) = V(X)V(Y)$.

— Next, we show by induction, that $\forall \ell \in \mathbb{N}, V(X^\ell) = V(X)^\ell$. Obviously, the equality holds for $\ell = 0, 1, 2$. Assume that it holds for some $\ell > 2$. Then

$$\begin{aligned} V(X^{\ell+1}) &= V(X^\ell X) = V(X^\ell)V(X) \text{ by the previous step} \\ &= V(X)^\ell V(X) \text{ by the induction hypothesis} \\ &= V(X)^{\ell+1}. \end{aligned}$$

— For $q \in \mathbb{R}[t]$ and arbitrary polynomial; then, $V(q(X)) = q(V(X))$ by the previous induction and quasilinearity. Denote by $\mathbb{X} = \mathsf{spec}(X)$ and assume now that $q(t) := \prod_{x \in \mathbb{X}}(t - x)$. Consider the equation $q(X) = 0$. It follows that

$$0 = V(q(X)) = q(V(X)).$$

Hence $V(X) \in \mathbb{X}$.

2. The claim follows from quasi-linearity.

□

4.5.2 Triviality of hidden variables for classical systems

Let $\mathbf{O}$ be the set of observables for a classical system, i.e. the set of real random variables over some probability space $(\Omega, \mathcal{F}, \rho)$. To introduce a hidden variable induced valuation on $\mathbf{O}$, it is enough to identify $\mathbf{H} = \Omega$ and define $\forall \lambda \in \mathbf{H}, V_\lambda(X) = X(\lambda) = X(\omega)$. Obviously, V is a non contextual, dispersion-free, linear valuation. On choosing the $\mathbf{H}$-valued random variable Λ distributed according to the law $\mu_\Lambda = \rho$, we get

$$\int_{\mathbf{H}} V_\lambda(X)\mu_\Lambda(\mathrm{d}\lambda) = \int_\Omega X(\omega)\rho(\mathrm{d}\omega) = \mathbb{E}X,$$

i.e. the hidden variable for a classical random variable, reproducing the statistical properties of the system, is nothing else than the choice according to the state $\rho \in \mathbf{S}$ of its realisations.

4.5.3 Quasi-linear hidden variables do exist in dimension $d = 2$

In his 1932 *Mathematische Grundlagen der Quantemechanik*, von Neumann proves that there do not exist dispersion-free states. The long lasted myth that he had also excluded the possibility of existence of determinate values for the observables prior to measurement acted as a hindrance to the quest of proving or disproving hidden variables hypothesis. But his proof [8] imposes too strong a requirement, as pointed out by Bell in [18]. As a matter of fact, von Neumann shows the following

Proposition 4.5.3. *Linear hidden variable models do not exist in dimension $d \geq 2$.*

Proof. It is enough to show the result for $d = 2$. Define

$$X = \sigma_1 = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix} \quad \text{and} \quad Y = \sigma_2 = \begin{pmatrix} & -i \\ i & \end{pmatrix}.$$

Then $\mathsf{spec}(X) = \mathsf{spec}(Y) = \{-1, 1\}$, while $\mathsf{spec}(X + Y) = \{-\sqrt{2}, \sqrt{2}\}$. Therefore, for an arbitrary valuation V, by lemma 4.5.2, we shall have $V(X) + V(Y) \in \{-2, 0, 2\}$, therefore it is impossible for linearity to hold, since $V(X + Y) \in \{-\sqrt{2}, \sqrt{2}\}$. □

But, imposing linearity of the valuation, i.e. $V(X + Y) = V(X) + V(Y)$ to hold even for non-commuting observables is very strong a requirement — as von Neumann understood himself — and cannot be imposed on physical grounds. Relaxing this statement to quasi-linear valuations, Bell [18] showed that on $\mathbb{H} = \mathbb{C}^2$, it is possible to construct a quasi-linear hidden variable model, assigning determinate values to the observables and reproducing in average the predictions of quantum theory.

Obviously, $\mathfrak{B}(\mathbb{H})$ is a complex vector space of dimension 4 on its own and the set of Pauli matrices $(\sigma_0, \sigma_1, \sigma_2, \sigma_3)$ (recall exercise 3.12.21) constitutes a basis of $\mathfrak{B}(\mathbb{H})$, i.e. any element $X \in \mathfrak{B}(\mathbb{H})$ is decomposed as

$$X := X(b_0, \mathbf{b}) = b_0\sigma_0 + \sum_{i=1}^{3} b_i\sigma_i = b_0\sigma_0 + \boldsymbol{b} \cdot \boldsymbol{\sigma}, b_0 \in \mathbb{C}, \boldsymbol{b} \in \mathbb{C}^3.$$

If $X \in \mathbf{O}$ (i.e. X is self-adjoint), then $b_0 \in \mathbb{R}$ and $\boldsymbol{b} \in \mathbb{R}^3$. Therefore, the space of self-adjoint observables is parametrised by $\mathsf{b} = (b_0, \boldsymbol{b}) \in \mathbb{R} \times \mathbb{R}^3$.

The task of a hidden variable model is to show that there exists a random variable Λ on some (unspecified space) taking values in some space $\mathbf{H}$ (we can chose for $\mathbf{H}$ real interval for instance) and a valuation map $V := V_\lambda : \mathbf{O} \to \mathbb{R}$, assigning definite values to observables, prior to their measurement, that reproduce the results of quantum formalism. We know from lemma 4.5.2, that for every $\lambda \in \mathbf{H}$, $V_\lambda \in \mathsf{spec}\, X = \{b_0 + \|\mathbf{b}\|, b_0 - \|bb\|\}$ and, if the system is in the state $\rho = |\,\varepsilon_0\,\rangle\langle\,\varepsilon_0\,|$, the quantum formalism establishes that

$$\mathbb{P}(X = x) = \langle \rho, E[x] \rangle = \mathsf{tr}(\rho E[x]) = \langle\, \varepsilon_0 \,|\, E[x]\varepsilon_0 \,\rangle, \quad \text{for } x \in \mathsf{spec}(X).$$

8. In [149, pp. 157–166] of the German edition, or [152, pp. 204–215] of the French edition, or [150, pp. 157–166] of the English edition of the *Grundlagen*.

Proposition 4.5.4. *Let Λ be a random variable uniformely distributed in $\mathbf{H} = [-1/2, 1/2]$ and define, for every $\lambda \in \mathbf{H}$, the valuation*

$$V(X) := V_\lambda(X) = b_0 + \|\mathbf{b}\| \text{sign}\left(\lambda\|\mathbf{b}\| + \frac{1}{2}|b_3|\right) \text{sign}(z(\mathbf{b})),$$

where

$$z(\mathbf{b}) = \begin{cases} b_3 & \text{if} \quad b_3 \neq 0 \\ b_1 & \text{if} \quad b_3 = 0, b_1 \neq 0 \\ b_2 & \text{if} \quad b_3 = 0, b_1 = 0, \end{cases}$$

and $\text{sign}(t) = \begin{cases} 1 & t \geq 0 \\ -1 & t < 0. \end{cases}$ *Then V is a hidden variable quasi-linear valuation reproducing the statistical predictions of quantum theory, i.e.*

$$\mathbb{E}(V_\Lambda(X)) := \int_{\mathbf{H}} V_\lambda(X)\mathbb{P}_\Lambda(d\lambda) = \langle\, \varepsilon_0 \,|\, X\varepsilon_0 \,\rangle.$$

Proof. Obviously $V_\lambda(X) \in \text{spec}\, X$. It is an easy exercise to check that the claimed form of the valuation is dispersion-free and normalised. Quasi-linearity follows from the observation that $X := X(b_0, \mathbf{b})$ and $Y := X(c_0, \mathbf{c})$ commute if, and only if, $\mathbf{b} \wedge \mathbf{c} = 0$, i.e. when $\mathbf{b}$ and $\mathbf{c}$ are collinear. Finally, due to the uniformity of distribution of Λ in $\mathbf{H}$, we compute immediately

$$\mathbb{E}(V_\Lambda(X)) = \int_{\mathbf{H}} V_\lambda(X)\mathbb{P}_\Lambda(\mathrm{d}\lambda) = b_0 + |b_3|\text{sign}(z(\mathbf{b})) = b_0 + b_3 = \langle\, \varepsilon_0 \,|\, X\varepsilon_0 \,\rangle.$$

□

4.5.4 (Bell)-Kochen-Specker theorem and contextuality

The construction carried out in §4.5.3 does not extend in dimension higher than 2. This result is known as (Bell)-Kochen-Specker theorem; it establishes that quantum theory cannot be completed by non-contextual hidden variables allowing to assign definite values to physical observables independently of which other compatible observables are jointly measured.

The original proof [95] in dimension 3 (or more) is quite involved. We present below an easy proof valid in dimension 4, given by Mermin [108]. In that case, it is easy to construct a counterexample where quasi-linearity fails. Consider the 4-dimensional system as composite system with $\mathbb{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$. Let $\mathbb{A} = \{0, 1, 2, 3\}$ and denote $A(ab) = \sigma_a \otimes \sigma_b$ for $a, b \in \mathbb{A}$. Arrange some relevant operators $A(ab)$ in the 3×3 array

A(10)	A(01)	A(11)
A(02)	A(20)	A(22)
A(12)	A(21)	A(33).

Exercise 4.5.5. 1. Show that the operators in every row are mutually commuting.

2. Show that the operators in every column are mutually commuting.
3. Show that the product of the operators appearing in the last column reads $A(11)A(22)A(33) = -I$.
4. Show that the product of the operators appearing in the first or middle column is I.
5. Show that the product of the operators appearing in each row is I.
6. If a valuation V existed, since triples of row (column) operators are mutually commuting we should have

$$\begin{aligned} 1 &= V(A(10)A(02)A(11)) = V(A(02)A(20)A(22)) = V(A(12)A(21)A(33) \\ &= V(A(10)A(02)A(12)) = V(A(01)A(20)A(21)) \\ &= -V(A(11)A(22)A(33)). \end{aligned}$$

Show that this valuation is contradictory.

During the 20th century, Bell-Kochen-Specker theorem was supposed to be only of theoretical interest. In [86] however, an experimental test of the Kochen-Specker theorem with single photons has been performed, based on a proposal of experimental feasibility made in [138].

4.6 Experimental refutation of hidden variables

Bell has established in [17] the so called Bell's inequalities[9], already presented in proposition 2.5.2. These inequalities have been generalised into the so-called **Clauser-Horne-Shimony-Holt (CHSH) inequalities** [40], given in proposition 4.6.1 below.

Proposition 4.6.1 (The Clauser-Horne-Shimony-Holt inequality)**.** *Let $\mathbb{X} = [-1, 1]$ and X_1, X_2, Y_1, Y_2 four $\mathbb{X}$-valued random variables defined on a common probability space $(\Omega, \mathcal{F}, \rho)$ and having an **arbitrary** joint distribution. Then*

$$\mathbb{E}(X_1Y_1) + \mathbb{E}(X_1Y_2) + \mathbb{E}(X_2Y_1) - \mathbb{E}(X_2Y_2)| \leq 2.$$

The proof of this proposition is quite elementary and left as an exercise. *Hint:* Introducing the random variable $Z = X_1(Y_1 + Y_2) + X_2(Y_1 - Y_2)$, remark that the sought inequality is equivalent in showing $|\mathbb{E}(Z)| \leq 2$. One can also immediately show also that supposing that the joint distribution of the four variables is reduced into an atomic one charging only the quadruples $(\pm 1, \pm 1, \pm 1, \pm 1)$ for the values of (X_1, X_2, Y_1, Y_2) we recover the four variables Bell's inequality.

The main interest of the paper [40] is not however the above, rather trivial, generalisation of the Bell's four variables inequality but rather that — based on ideas exposed in [96] — it describes an experimental protocol that could be used to experimentally definitely settle the question whether quantum mechanics admits a Kolmogorovian

9. Due to some mishandling by the editorial board of the manuscript [18], its publication occurred after [17], although it was submitted prior to the latter.

description (in terms of hidden variables) or it violates simultaneous locality and realism.

The Orsay experiment made use of these inequalities coupled with an experimental setting of unprecedented ingenuousness (see §2.5.2 and [7] for more technical details) to show that quantum theory does not admit a Kolmogorovian description; therefore, EPR is not a paradox but a genuine physical phenomenon. Nature cannot be simultaneously realistic and local!

After triggering the Calcium atom by a laser beam (recall figure 2.10), its de-excitation produces a pair of entangled photons in the state

$$|\,\Psi\,\rangle s = e^{-i\phi/2}\cos\theta|\,\varepsilon_0\zeta_1\,\rangle + e^{i\phi/2}\sin\theta|\,\varepsilon_1\zeta_0\,\rangle = \sum_{m\in\{0,1\}} \Psi_{m\overline{m}}|\,\varepsilon_m\zeta_{\overline{m}}\,\rangle \in \mathbb{H}_1\otimes\mathbb{H}_2,$$

where $\overline{m} = 1-m$. Orienting the left polariser in some angle is equivalent to performing the projective measurement $|\,L\,\rangle\langle\,L\,|\otimes I_2$, where $|\,L\,\rangle = e^{-i\gamma/2}\cos\alpha|\,\varepsilon_0\,\rangle + e^{i\gamma/2}\sin\alpha|\,\varepsilon_1\,\rangle$ and I_2 is the unit operator on $\mathbb{H}_2$. Simillarly, orienting the right polariser in some angle is equivalent to performing the projective measurement $I_1\otimes|\,R\,\rangle\langle\,R\,|$, where $|\,R\,\rangle = e^{-i\delta/2}\cos\beta|\,\zeta_0\,\rangle + e^{i\delta/2}\sin\beta|\,\zeta_1\,\rangle$ and I_2 is the unit operator on $\mathbb{H}_2$. We can now compute the probabilities appearing in the Bell's inequality by observing that *for an individual pair of photons*

$$\begin{aligned}
\mathbb{P}_{\theta,\phi}(X_\alpha = Y_\beta) &= \mathbb{P}(X_\alpha = Y_\beta = 1) + \mathbb{P}(X_\alpha = Y_\beta = 0)\\
&= \mathsf{tr}((|\,L\,\rangle\langle\,L\,|\otimes I_2)|\,\Psi\,\rangle\langle\,\Psi\,|(I_1\otimes|\,R\,\rangle\langle\,R\,|))\\
&\quad + \mathsf{tr}(((I_1 - |\,L\,\rangle\langle\,L\,|)\otimes I_2)|\,\Psi\,\rangle\langle\,\Psi\,|(I_1\otimes(I_2 - |\,R\,\rangle\langle\,R\,|)))\\
&= |\langle\,\Psi\,|\,LR\,\rangle|^2 + [1 - \sum_{j=0}|L_j|^2|\Psi_{j\bar{j}}|^2 - \sum_{j=0}|R_j|^2|\Psi_{j\bar{j}}|^2 + |\langle\,\Psi\,|\,LR\,\rangle|^2]\\
&= 2[\cos^2\theta\cos^2\alpha\sin^2\beta + \sin^2\theta\sin^2\alpha\cos^2\beta\\
&\quad + 2\cos(\phi+\gamma-\delta)\cos\theta\sin\theta\cos\alpha\sin\alpha\cos\beta\sin\beta]\\
&\quad + 1 - (\cos^2\theta\cos^2\alpha + \sin^2\theta\sin^2\alpha) - (\cos^2\theta\cos^2\beta + \sin^2\theta\sin^2\beta).
\end{aligned}$$

Now, pairs of photons are produced in a large number and since each pair are produced by the de-excitation of different Calcium atoms, there is no way to fix the angle θ in the above formula. Different pairs arrive with different angles and the only reasonable assumption is that pairs of photons are emitted with random angles θ distributed in $[0,\Pi]$ according to the uniform measure $\mathrm{d}\theta/\pi$. Computing the average over possible polarisations of the emitted photons, we get

$$\begin{aligned}
\mathsf{Prob}(X_\alpha = Y_\beta) &= \int_{[0,\pi]} \mathbb{P}_{\theta,\phi}(X_\alpha = Y_\beta)\frac{\mathrm{d}\theta}{\pi}\\
&= \cos^2\alpha\sin^2\beta + \sin^2\alpha\cos^2\beta + 1 - \frac{1}{2}(\cos^2\alpha + \sin^2\alpha) - \frac{1}{2}(\cos^2\beta + \sin^2\beta)\\
&= \cos^2\alpha\sin^2\beta + \sin^2\alpha\cos^2\beta.
\end{aligned}$$

The Orsay experiment consisted in measuring precisely the probabilities $\mathsf{Prob}(X_\alpha = Y_\beta)$ for different angles $\alpha_1,\alpha_2,\beta_1,\beta_2 \in [0,\pi]$ for the orientations of the analysing polarisers in an ingeneous experimental setting where the choice of the angle has been

made after the pair of photons were emitted from the Calcium atom. The observed results were in complete accordance with the above formula.

If the variables X_α and Y_β were Kolmogorovian random variables, they should fulfill the four-variables Bell's inequality

$$\mathsf{Prob}(X_{\alpha_1} = Y_{\beta_1}) \leq \mathsf{Prob}(X_{\alpha_1} = Y_{\beta_2}) + \mathsf{Prob}(X_{\alpha_2} = Y_{\beta_1}) + \mathsf{Prob}(X_{\alpha_2} = Y_{\beta_2}),$$

for every choice of angles $\alpha_1, \alpha_2, \beta_1, \beta_2 \in [0, \pi]$. Choosing four different angles $\alpha_1 = 0, \alpha_2 = \pi/3, \beta_1 = \pi/6$ and $\beta_2 = \pi/6$, they should verify the *impossible inequality*

$$1 \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{8}.$$

The Orsay experiment has been confirmed by a similar experiment made in in Delft with entangled electrons [82]. This realisation closed a possible loophole left by the use of photons in the Orsay setting; as a matter of fact, the use of photons cannot totally exclude the possibility that multiple photon states act as input states. This possibility is excluded when we use electrons. (Mind that photons are bosons while electrons are fermions). Therefore, EPR is not any longer a paradox but a physical phenomenon. The Nature behaves really as predicted by the quantum formalism.

It is worth stressing that the EPR phenomenon is still triggering several profound quests on the foundational aspects of quantum mechanics. If we insist on interpreting the state as containing all elements of reality about the quantum system, quantum mechanics appear as non local. If on the contrary we interpret the state as a statistical ensemble of identical systems described by a given density matrix and give to the possible outcomes only a statistical meaning, i.e. we are interested solely in the probabilities of their occurrence, there is absolutely no paradox. Similarly, the EPR phenomenon is often referred as violating the principle of relativistic causality. However, if we interpret the (entangled) density matrix of the compound system as a global property of the pair, not the juxtaposition of properties pertaining to the two (isolated) components, again, there is no violated relativistic principle since in the EPR experiment there is no super-luminal transmission of useful information between space-like separated points.

These days, most of the protocols of quantum cryptography, somewhere in their make, use entanglement. Information transmission protocols and teleportation rely also upon entanglement. Finally, entanglement is an important resource for quantum computing. Beyond its usefulness in applications, entanglement is important for the theoretical foundations of quantum mechanics.

4.7 The Greenberg, Horne, and Zeilinger (GHZ) paradox

This paradox, introduced in [72], is intending to provide with an impossibility result sharper than Bell's inequalities. As a matter of fact, contrary to Bell's inequality where the probability of occurrence of an event is bounded from other probabilities,

here, the probability of a certain event is shown to be 1, leading to a maximal violation of classical prediction.

This statement and the proof of this paradox is quite straightforward; for this reason, we state it as an exercise.

Exercise 4.7.1. 1. Let $X_a, X_b, X_c, Y_a, Y_b, Y_c$ be six classical $\{-1,1\}$-valued random variables, defined on the same probability space $(\Omega, \mathcal{F}, \mathbb{P})$. Their law $\mathbb{P}$ is **arbitrary**, i.e. the variables can be independent or not, symmetric or not, degenerate or not. Denote by W_0, W_1, W_2, W_3 the random variables

$$W_0 := X_a X_b X_c; W_1 := X_a Y_b Y_c; W_2 := Y_a X_b Y_c \text{ and } W_3 := Y_a Y_b X_c,$$

also definided on $(\Omega, \mathcal{F}, \mathbb{P})$ and taking values also in $\{-1,1\}$. Show that

$$\mathbb{P}(W_0 = 1, W_1 = -1, W_2 = -1, W_3 = -1) = 0.$$

2. Henceforth, $\mathcal{H} = \mathbb{C}^2$ and

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

are the **Pauli matrices** in the canonical basis $\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$. Show that $\mathsf{spec}(\sigma_1) = \mathsf{spec}(\sigma_2) = \mathsf{spec}(\sigma_3) = \{-1,1\}$.
3. Denote by $|+\rangle$ et $|-\rangle$ the eigenvectors of σ_3 associated respectively with the eigenvalues $+1$ and -1. We have thus $\sigma_3|s\rangle = s|s\rangle$ for $s \in \mathbb{S} := \{+,-\}$; otherwise stated: $|+\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $|-\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Compute, $\sigma_1|s\rangle$ and $\sigma_2|s\rangle$ for $s \in \mathbb{S}$.
4. Let $|\Psi\rangle = \frac{1}{\sqrt{2}}(|++\!+\rangle + |---\rangle) \in \mathbb{H} := \mathcal{H}^{\otimes 3}$. Show that $|\Psi\rangle$ is an eigenvector for the operators W_i, $i = 0, \ldots, 3$, acting on $\mathbb{H}$, where

$$W_0 := \sigma_1 \otimes \sigma_1 \otimes \sigma_1$$
$$W_1 := \sigma_1 \otimes \sigma_2 \otimes \sigma_2$$
$$W_2 := \sigma_2 \otimes \sigma_1 \otimes \sigma_2$$
$$W_3 := \sigma_2 \otimes \sigma_2 \otimes \sigma_1.$$

5. What we can conclude on the probabilities $\mathbb{P}_\Psi(W_i = 1)$, for $i = 0, \ldots, 3$, and for the state of the system after each question has been asked?
6. Show that $\sigma_1\sigma_2 = -\sigma_2\sigma_1$.
7. For A, B, C, and D operators acting on $\mathcal{H}$, show that $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$.
8. Comment why the results obtained so far can be characterised as paradoxical if they are interpreted classically. (Recall that $\sigma_1^2 = \sigma_2^2 = I$).

4.8 Complete positivity, Stinespring theorem, Kraus operators

It has been postulated in §2.6 that isolated quantum systems evolve unitarily, i.e. quantum states evolve as $\rho \mapsto \rho' := U\rho U^*$, where U is a unitary operator while unfil-

tered measurement acts as a transformation on quantum states of the form $\rho \mapsto \rho' := \sum_{x\in\mathbb{X}} E[x]\rho E[x]$, where $(E[x])_x$ is a partition of unity on a space $\mathbb{X}$. In other words, an arbitary **transformation of a quantum systems** is encoded into an affine map

$$\mathfrak{D}(\mathbb{H}) \ni \rho \mapsto \rho' := \Phi(\rho) \in \mathfrak{D}(\mathbb{H}).$$

The map Φ can be extended by linearity to the whole space $\Phi : \mathfrak{B}(\mathbb{H}) \to \mathfrak{B}(\mathbb{H})$; the map is reversible for unitary evolution but not for measurements.

There are several questions that can be asked about transformations acting on states of quantum systems to be physically acceptable.

1. States are trace class operators of unit trace, hence a **state transformation** must be trace preserving. However, this requirement can be relaxed by requiring merely preservation of the trace class property, not imposing the normalisation of the state. Such more general transformations are called **quantum operations** and constitute a convex set whose extremal elements are the aforementioned state transformations.
2. States are represented by positive operators. To be mathematically consistent, any map $\Phi : \mathfrak{B}(\mathbb{H}) \to \mathfrak{B}(\mathbb{H})$ must — at least — preserve positivity, i.e. $\Phi(\rho)$ must remain positive for any $\rho \in \mathfrak{D}(\mathbb{H})$. However, this requirement proves insufficient to prevent inconsistencies on composite systems because of the phenomenon of **entanglement**. In case the quantum operation is unitary — the state transformation is then a unitary evolution — or the initial state is separable, this requirement is enough and leads to physically acceptable operations (see exercise 4.8.2 below). But this requirement of positivity must be strengthened into **complete positivity** (see defintion 4.8.1 below) in case of non unitary operations on entangled states.

Definition 4.8.1. Let $\mathbb{H}$ be an arbitrary Hilbert space and $n \in \mathbb{N}$. Consider the quantum system described by the finite-dimensional extension of the Hilbert space into $\mathbb{H} \otimes \mathbb{C}^n$, where the Hilbert space $\mathbb{C}^n$ carries the degrees of freedom of an inert ancillary system. A linear transformation $\Phi : \mathfrak{D}(\mathbb{H}) \to \mathfrak{D}(\mathbb{H})$ is **n-positive** if the transformation

$$\Phi \otimes \mathsf{id}_n : \mathfrak{D}(\mathbb{H} \otimes \mathbb{C}^n) \to \mathfrak{D}(\mathbb{H} \otimes \mathbb{C}^n),$$

where id_n is the identity map on $\mathbb{C}^n$. The transformation is **completely positive** if it is n-positive for every $n \in \mathbb{N}$.

Exercise 4.8.2. Let $\Phi : \mathbb{C}^n \to \mathbb{C}^n$ be a linear map. Show that if Φ

1. stems from a unitary evolution, i.e. $\Phi(X) = UXU^*$, or
2. is (the extension to $\mathfrak{M}_p = \mathfrak{B}(\mathbb{C}^p)$ of) a positive evolution of a separable state $\rho \in \mathfrak{D}(\mathbb{C}^p \otimes \mathbb{C}^p)$,

then Φ is completely positive.

Complete positivity is a purely quantum phenomenon, i.e. occurs solely in the case of non-commutative algebras [10] and stems from entanglement. Although its mathematical description is quite well established, its profound physical significance is still

10. It is shown in [142, theorem 4] that positive transformations on commutative algebras, i.e. on Markov operators acting on classical random variables, are always completely positive.

paritally understood. Its mathematical description enters the more general framework of **dilations**. Loosely speaking a dilation is the fact that a complicated transformation acting on a state space can be equivalently described by an embedding of the space into a larger one followed by a simpler transformation acting on the larger state space, followed by a restriction to the initial space. The archetypical example of dilation is given by the Stinespring's theorem. In finite dimension [11] it takes the following form given in theorem 4.8.3.

For arbitrary $q \in \mathbb{N}$, denote by $\mathfrak{M}_q = \mathfrak{B}(\mathbb{C}^q)$.

Theorem 4.8.3. *[Stinespring's theorem in finite dimension]. A linear map $\Phi : \mathfrak{M}_m \to \mathfrak{M}_n$ is completely positive if there exist an integer $p \in \mathbb{N}$, a unital $*$-homomorphism $\alpha : \mathfrak{M}_m \to \mathfrak{M}_p$ and a linear map $V : \mathfrak{M}_n \to \mathfrak{M}_p$ such that*

$$\Phi(X) = V^* \alpha(X) V, \quad \textit{for all} \quad X \in \mathfrak{M}_m.$$

Corollary 4.8.4. *A linear map $\Phi : \mathfrak{B}_1(\mathbb{H}) \to \mathfrak{B}_1(\mathbb{H})$ is completely positive if, and only if, there exist a (finite or infinite) sequence of bounded operators $(V_i)_{i\in I}$ satisfying $\sum_{i\in I} V_i^* V_i = \mathbb{I}_{\mathbb{H}}$ such that*

$$\Phi(X) = \sum_i V_i^* X V_i, \quad \textit{for all} \quad X \in \mathfrak{B}_1(\mathbb{H}).$$

The operators (V_i) are called **Kraus operators**. In finite dimension, the family I can be chosen so that $\mathrm{card} I \leq (\dim \mathbb{H})^2$.

For the finite dimensional case, complete positivity is totally characterised (see [89] and [38]) by elementary means. See also [81] for a more recent text.

Theorem 4.8.5. *Choi [38, theorems 1 and 2]: Let $\mathfrak{M}_m = \mathfrak{B}(\mathbb{C}^m)$ and $\mathfrak{M}_n = \mathfrak{B}(\mathbb{C}^n)$, for $m, n \in \mathbb{N}$. For a linear map $\Phi : \mathfrak{M}_m \to \mathfrak{A}_n$ the following statements are equivalent:*

1. *Φ is completely positive.*
2. *Φ is m-positive.*
3. *The Choi's matrix of Φ, defined by*

$$M_\Phi := \begin{pmatrix} \Phi(E_{11}) & \dots & \Phi(E_{1m}) \\ \vdots & \dots & \vdots \\ \Phi(E_{m1}) & \dots & \Phi(E_{mm}) \end{pmatrix} = \sum_{j,k=1}^{m} \Phi(E_{jk}) \otimes E_{jk},$$

   where $E_{jk} = |\,\varepsilon_j\,\rangle\langle\,\varepsilon_k\,|$ for an arbitrary orthonormal basis $(\varepsilon_j)_{j=1,\dots,m}$ of $\mathbb{C}^m$, is positive.
4. *Φ has the form $\Phi(X) = \sum_{i\in I} V_i^* X V_i$ for all $X \in \mathfrak{M}_m$, where $(V_i)_{i\in I}$ are $m \times n$ matrices.*

11. Stinespring's theorem can be formulated in the much more general framework of (infinite dimensional) C^*-algebras [142]. In this general framework, the theorem reads:
Theorem: *Let $\mathfrak{A}$ be a unital C^*-algebra, $\mathbb{H}$ a Hilbert space, and Φ a linear function from $\mathfrak{A}$ to $\mathfrak{B}(\mathbb{H})$. The following statements are equivalent:*
— *Φ is completely positive.*
— *There is a Hilbert space $\mathbb{F}$, a bounded linear transformation $V : \mathbb{H} \to \mathbb{F}$, and a $*$-representation α of $\mathfrak{A}$ into $\mathfrak{B}(\mathbb{F})$, such that*

$$\Phi(X) = V^* \alpha(X) V, \quad \textit{for all} \quad X \in \mathfrak{A}.$$

Proof. See exercise 4.8.6 below. □

Exercise 4.8.6 (Proof of the theorem 4.8.5)**.** Let $(\varepsilon_k)_{k=1,\dots,m}$ be an arbitrary orthonormal basis of $\mathbb{C}^m$.

1. Let $Y = \sum_{j,k=1}^m |\, \varepsilon_j\varepsilon_j \,\rangle\langle\, \varepsilon_k\varepsilon_k \,| \in \mathfrak{M}_m \otimes \mathfrak{M}_m$. Show that Y is positive.
2. Show that $(\Phi \otimes \mathrm{id}_m)(Y) = M_\Phi$. If Φ is m-positive conclude that from statement 2 of the theorem follows statement 3.
3. Assume that M_Φ is positive and let $(\psi_l)_{l=1,\dots,p}$, with $\psi_l \in \mathbb{C}^n \otimes \mathbb{C}^m$ and $1 \leq p \leq nm$ be the family of eigenvectors of M_Φ corresponding to its non-vanishing eigenvalues. Argue that they form an orthogonal (not necessarily normalised) system allowing to write $M_\Phi = \sum_{l=1}^p |\, \psi_l \,\rangle\langle\, \psi_l \,|$.
4. Remark that $\mathbb{C}^n \otimes \mathbb{C}^m$ can be considered as a direct sum $\mathbb{C}^n \otimes \mathbb{C}^m = \oplus_{k=1}^m \mathbb{H}_k$, where $\mathbb{H}_k \simeq \mathbb{C}^n$ for all $k = 1, \dots, m$, and denote by P_k the orthoprojection $P_k : \mathbb{C}^n \otimes \mathbb{C}^m \to \mathbb{H}_k$. Show that $\Phi(E_{jk}) = P_j M_\Phi P_k$.
5. For every $l = 1, \dots, p$ and $j = 1, \dots, m$, define the operator $V_l : \mathbb{C}^m \to \mathbb{C}^n$ by its action on basis vectors:
$$V_l |\, \varepsilon_j \,\rangle := P_j |\, \psi_l \,\rangle.$$
6. Show that $\Phi(E_{jk}) = \sum_{l=1}^p V_l E_{jk} V_l^*$ and conclude that $\Phi(X) = \sum_{l=1}^p V_l X V_l^*$, for all $X \in \mathfrak{M}_m$.
7. Use Stinespring's theorem to complete the proof of the theorem 4.8.5.

A natural question that can be asked is whether the above definition of complete positivity encompasses non-trivial cases, i.e. whether there are positive transformations that fail to be completely positive. The answer is of course yes as is shown in the following exercice.

Exercise 4.8.7 (A positive transformation that fails to be 2-positive)**.** Suppose that $\mathbb{H} \simeq \mathbb{C}^2$ and X a positive operator acting on $\mathfrak{M}_2 = \mathfrak{B}_1(\mathbb{C}^2)$. Let $\Phi(X) = X^t$ be transposition. Show that Φ is positive without being 2-positive (hence failing to be completely positive).

One can construct several other simple examples of positive transformations that fail to be 2-positive (see [142] or [5] for instance). The question arises subsequently whether this is always the case. The answer is no: for every $n \geq 2$, there are $(n-1)$-positive transformations $\Phi : \mathfrak{M}_n \to \mathfrak{M}_n$ that fail to be n-positive (see [38, theorem 1]).

Exercise 4.8.8 (Choi-Jamiołkowksi isomorphism)**.** Let $\Phi : \mathfrak{M}_m \to \mathfrak{M}_n$ as in theorem 4.8.5 and $Y = \sum_{j,k=1}^m |\, \varepsilon_j\varepsilon_j \,\rangle\langle\, \varepsilon_k\varepsilon_k \,| \in \mathfrak{M}_m \otimes \mathfrak{M}_m$, for an orthonormal basis $(\varepsilon_j)_{j=1,\dots,m}$ of $\mathbb{C}^m$ as in exercise 4.8.6.

1. Compute $\mathrm{tr}(Y)$ and conclude that $\rho = \frac{1}{m}\sum_{j,k=1}^m |\, \varepsilon_j\varepsilon_j \,\rangle\langle\, \varepsilon_k\varepsilon_k \,|$ is a state in $\mathfrak{D}(\mathbb{C}^m \otimes \mathbb{C}^m)$.
2. Show that the state ρ is pure.
3. Define $J[\Phi] := \Phi \otimes \mathrm{id}_m$. Show that Φ is completely positive if, and only if, $J[\Phi](\rho)$ is positive.
4. Argue that $J[\Phi](\rho)$ is an isomorphism (the **Choi-Jamiołkowski isomorphism**) between the space of completely positive linear maps from $\mathfrak{M}_m \to \mathfrak{M}_n$ and the space of positive maps on $\mathfrak{M}_m \otimes \mathfrak{M}_n$.

Note that the previous isomorphism allows to check complete positivity of Φ solely by checking whether the map $J[\Phi]$ applied on a given pure state ρ is positive.

4.9 Decoherence and quantum to classical transition

4.9.1 Measurement and effects revisited

Recall briefly the measurement postulate in the finite dimensional case, i.e. suppose for simplicity that the system is described by finite-dimensional Hilbert space. We are given a sharp observable $X \in \mathbf{O}_s(\mathbb{H})$, admitting a non-degenerated spectral decomposition $X = \sum_{x\in\mathbb{X}} xE[x]$, where $\mathbb{X} = \mathsf{spec}\, X$, $E[x] = |\,\zeta[x]\,\rangle\langle\,\zeta[\,|$, and $\zeta[x]$ is the normalised eigenvector of X associated with the eigenvalue x. The set of eigenvectors forms an orthonormal basis of $\mathbb{H}$ and $(E[x])_{x\in\mathbb{X}}$ is a decomposition of unity into a sum of orthogonal orthoprojections. This kind of decomposition is termed in the literature **projection-valued measure** (also known by its acronym **PVM**).

When the system is prepared in state $\rho \in \mathfrak{D}(\mathbb{H})$ and we measure *once* the observable X, the experimental outcome is one of the possible eigenvalues $x \in \mathbb{X}$. The quantum formalism is unable to predict *which eigenvalue* will occur. It can on the contrary predict that when we repeat the experiment on an ensemble of equally prepared systems in state ρ, the probability of each outcome x is given by the — so called **Born rule** —

$$p_x = \nu_X^\rho(x) = \mathsf{tr}(\rho E[x]) = \mathsf{tr}(E[x]\rho E[x]) = \mathsf{tr}(\rho E[x]^2).$$

The formalism predicts also that once the outcome x has been observed, the conditional a posteriori state of the system becomes

$$\rho_x = \frac{1}{p_x} E[x]\rho E[x].$$

In particular, the projective measurement transforms pure states into pure states.

In case we don't filter the results but mix the output systems with the corresponding probabilities, the so obtained statistical ensemble will correspond to the state $\rho' = \sum_{x\in\mathbb{X}} E[x]\rho E[x]$.

What is important in the expression for p_x above is that $(p_x)_{x\in\mathbb{X}}$ is a probabiity vector, i.e. $p_x \geq 0$ and $\sum_{x\in\mathbb{X}} p_x = 1$. Focusing on the rightmost form of the expression of p_x, we see that this imposes that $E[x]^2 \geq 0$ and $\sum_{x\in\mathbb{X}} E[x]^2 = I$. Therefore, we can relax the orthoprojective orthogonality of the effects $E[x]$, and consider a family of positive operators $(F[x])_{x\in\mathbb{X}}$ — indexed by some finite set $\mathbb{X}$ — verifying $\sum_{x\in\mathbb{X}} F[x] = I$, i.e. a positive-operator valued measure or unsharp effect. The measure corresponding to F is termed in the literature **positive operator-valued measure** (also known by its acronym **POVM**).

Since $F[x] \geq 0$, the operator $F[x]^{1/2}$ is well defined. Using polar decomposition, we can define the detection operators $M[x] = U[x]\sqrt{F[x]}$ and write

$$p_x = \mathsf{tr}(\rho F[x]) = \mathsf{tr}(M^*[x]\rho M[x]).$$

In the same vein, we can define the conditional state after the unsharp outcome x has been observed by

$$\rho_x = \frac{1}{p_x} M^*[x]\rho M[x],$$

and the unfiltered one by

$$\rho' = \Phi(\rho) := \sum_{x\in\mathbb{X}} M^*[x]\rho M[x],$$

with $\sum_{x\in\mathbb{X}} M^*[x]M[x] = I$.

Using the Stinespring theorem 4.8.3, we have shown in the previous section, that any map of the form $\Phi(\rho) = \sum_{x\in\mathbb{X}} M^*[x]\rho M[x]$, with $\sum_{x\in\mathbb{X}} M^*[x]M[x] = I$, is completely positive. We have justified there the necessity of considering complete positivity as a requirement to preserve positivity of states in case the system is coupled to an unobserved environment. We have also established, in §2.7.1, the necessity to consider unsharp effects. A natural question to ask is whether an unsharp effect (POVM) can be sharpened by considering it as a PVM on a larger space. The answer is yes as shown in the following

Theorem 4.9.1 (Naimark theorem)**.** *Let F be a finite* POVM *on $\mathbb{F}$, i.e. there exists a set $\mathbb{X}$, with $\mathsf{card}(\mathbb{X}) < \infty$, and $F : \mathbb{X} \to \mathfrak{B}_+(\mathbb{F})$, such that $\sum_{x\in\mathbb{X}} F(x) = 1$. Then, there exist*

— *a Hilbert space $\mathbb{G}$,*
— *a unit vector $\psi \in \mathbb{G}$ (and, correspondingly, the pure state $\rho = |\,\psi\,\rangle\langle\,\psi\,|$),*
— *a unitary operator $U := \mathbb{F}\otimes\mathbb{G} \to \mathbb{F}\otimes\mathbb{G}$,*
— *a* PVM *E on $\mathbb{G}$ indexed by $\mathbb{X}$,*

such that we can express the unsharp effect F as

$$F[x] = \mathsf{tr}_{\mathbb{G}}\big((I_{\mathbb{F}}\otimes\rho)U^*(I_{\mathbb{F}}\otimes E[x])U\big).$$

Proof. Let $\mathbb{G}$ be a Hilbert space with $\dim\mathbb{G} = \mathsf{card}\mathbb{X}$ and $(\zeta[x])_{x\in\mathbb{X}}$ an arbitrary orthonormal basis of $\mathbb{G}$. Denote by $M[x]$ the detection operator associated with the unsharp effect $F[X]$, i.e. $M[x]^*M[x] = F[x]$. Fix ψ an arbitrary unit vector of $\mathbb{G}$ and define for every $\phi \in \mathbb{F}$:

$$U|\,\phi\psi\,\rangle := \sum_{x\in\mathbb{X}} (M[x]\otimes I_{\mathbb{G}})|\,\phi\zeta[x]\,\rangle.$$

The above form for U, defines the operator on the subspace $\mathbb{F}\otimes\mathbb{C}\psi$ and, in any case, U depends on the choice of the arbitrary vector ψ, although we do not write explicitly U_ψ. Computing

$$\begin{aligned}\langle\,\phi'\psi\,|\,U^*U\phi\psi\,\rangle &= \sum_{x,x'\in\mathbb{X}} \langle\,\phi'\zeta[x']\,|\,(M[x']^*\otimes I_{\mathbb{G}})(M[x]\otimes I_{\mathbb{G}})\phi\zeta[x]\,\rangle\\ &= \sum_{x\in\mathbb{X}} \langle\,\phi'\,|\,M[x]^*M[x]\phi\,\rangle = \langle\,\phi'\,|\,\phi\,\rangle = \langle\,\phi'\psi\,|\,\phi\psi\,\rangle,\end{aligned}$$

establishes the unitarity of U on $\mathbb{F}\otimes\mathbb{C}\psi$. The operator U can be extended to a unitary on the whole space, by letting U to be the identity operator on $\mathbb{F}\otimes(\mathbb{C}\psi)^\perp$.

Now, since $U|\,\phi\psi\,\rangle := \sum_{x'\in\mathbb{X}}(M[x']|\,\phi\,\rangle)\otimes|\,\zeta[x']\,\rangle$, we have that $\langle\,\phi'\zeta[x]\,|\,U\phi\psi\,\rangle = \langle\,\phi'\,|\,M[x]\phi\,\rangle$. Hence

$$\begin{aligned}|\,M_x\phi\,\rangle\otimes|\,\zeta[x]\,\rangle &= \sum_{x'\in\mathbb{X}}(I_{\mathbb{F}}\otimes E[x])|\,M[x']\phi\,\rangle\otimes|\,\zeta[x']\,\rangle\\ &= (I_{\mathbb{F}}\otimes E[x])U|\,\phi\psi\,\rangle.\end{aligned}$$

It remains to show that $F[x]$ can be expressed as a partial trace. Compute

$$\begin{aligned}\langle\,\phi'\,|\,F[x]\phi\,\rangle &= \langle\,\phi'\,|\,M[x]^*M[x]\phi\,\rangle = \langle\,M[x]\phi'\,|\,M[x]\phi\,\rangle\\ &= \langle\,(M[x]\phi')\psi\,|\,(I_{\mathbb{F}}\otimes E[x])U\phi\psi\,\rangle\\ &= \langle\,U\phi'\psi\,|\,(I_{\mathbb{F}}\otimes E[x])U\phi\psi\,\rangle\\ &= \langle\,\phi'\psi\,|\,U^*(I_{\mathbb{F}}\otimes E[x])U\phi\psi\,\rangle\\ &= \langle\,\phi'\,|\,\mathrm{tr}_{\mathbb{G}}\big((I_{\mathbb{F}}\otimes\rho)U^*(I_{\mathbb{F}}\otimes E[x])U\big)\phi\,\rangle.\end{aligned}$$

□

4.9.2 A first look on decoherence

Let $\mathbb{H}$ be a finite dimensional Hilbert space and H a self-adjoint operator on $\mathbb{H}$. It is immediate that $U(t) = \exp(itH)$ is unitary for all $t\in\mathbb{R}$. Moreover, $U(0) = I$, $U(t+s) = U(t)U(s) = U(s)U(t)$, and $U(t)^* = U(-t)$. Therefore, $(U(t))_{t\in\mathbb{R}}$ is an Abelian group. Conversely, if $(U(t))_{t\in\mathbb{R}}$ is a unitary Abelian group, there exists a self-adjoint operator H, such that $U(t) = \exp(itH)$. The operator H is the generator of the group, called the **Hamiltonian** of the system, and physically is interpreted as the total energy of the system. The unitarity of the time evolution is equivalent to the conservation of energy.

We have seen that an isolated system evolves according to a unitary operator U, i.e. its time evolution is implemented by a family $(U(t))_{t\in\mathbb{R}}$ of unitaries, so that if at time 0 the system is in the pure state defined by the unit vector ψ, at time t it will be in a pure state defined by the unit vector $\psi(t) = \exp(itH)\psi$. Nevertheless, we cannot expect that a realistic physical system can remain isolated in the long run; an interaction — may be small — with the environment must be taken into account.

We consider a very simple model, introduced in [158] and studied again in [129], to illustrate how this interaction spoils the quantum character of the system by turning its state from a full-fledged quantum density operator into a diagonal operator interpreted as a classical probability. The system is a two-dimensional toy-model — described by the phase space $\mathbb{F} = \mathbb{C}^2$ — coupled with a $2N$-dimensional environment, for some large N — described by the phase space $\mathbb{G} = (\mathbb{C}^2)^{\otimes N}$. It is only the composite $2(N+1)$-dimensional system, described by $\mathbb{F}\otimes\mathbb{G}$, that is assumed to be isolated, while the small system interacts with the environment through a toy Hamiltonian H. To be more specific, assume that every copy of $\mathbb{C}^2$ is endowed with an orthonormal basis $(\zeta_0^k,\zeta_1^k)_{k=0,\dots,N}$. The Hamiltonian $H\in\mathfrak{B}(\mathbb{F}\otimes\mathbb{G})$ is assumed to be of the form $H = \sum_{k=1}^N R_k$ where

$$R_k = c_k\big(|\,\zeta_0^0\,\rangle\langle\,\zeta_0^0\,| - |\,\zeta_1^0\,\rangle\langle\,\zeta_1^0\,|\big)\otimes I^1\otimes\cdots\otimes I^{k-1}\otimes\big(|\,\zeta_0^k\,\rangle\langle\,\zeta_0^k\,| - |\,\zeta_1^k\,\rangle\langle\,\zeta_1^k\,|\big)\otimes I^{k+1}\otimes\cdots\otimes I^N,$$

where c_k is a real parameter, the strength of the interaction. Remark that the family of operators $(R_k)_{k=1,\dots,N}$ are mutually commuting, so that they can be diagonalised simultaneously and give rise to a unitary evolution group totally factored $U(t) = \exp(itH) = \prod_{k=1}^{N} \exp(itR_k)$. Notice moreover that $(|\,\zeta^0_{k_0}, \zeta^1_{k_1} \cdots \zeta^N_{k_N}\,\rangle)_{k_0,k_1,\dots,k_N\in\{0,1\}}$ is an eigenbasis of R_k for all k, of H and of $U(t)$. Therefore, starting at time 0 from the pure state described by the vector

$$|\,\Psi\,\rangle = (a|\,\zeta^0_0\,\rangle + b|\,\zeta^0_1\,\rangle) \otimes_{k=1}^{N} (a_k|\,\zeta^k_0\,\rangle + b_k|\,\zeta^k_1\,\rangle),$$

the total evolution transforms it into the entangled vector

$$|\,\Psi(t)\,\rangle := U(t)|\,\Psi\,\rangle = a|\,z^0_0\,\rangle|\,\Phi_0(t)\,\rangle + b|\,z^0_1\,\rangle|\,\Phi_1(t)\,\rangle,$$

where

$$|\,\Phi_0(t)\,\rangle = |\,\Phi_1(-t)\,\rangle = \otimes_{k=1}^{N}(a_k \exp(itc_k)|\,\zeta^k_0\,\rangle + b_k \exp(-itc_k)|\,\zeta^k_1\,\rangle).$$

Due to the entanglement of the time evolved vector, the quantum marginal at time t reads

$$\begin{aligned}\rho(t) := \rho_N(t) &= \mathrm{tr}_{\mathrm{G}}(|\,\Psi(t)\,\rangle\langle\,\Psi(t)\,|) \\ &= \begin{pmatrix} |a|^2 & z(t)ab^* \\ z(t)^*a^*b & |b|^2 \end{pmatrix}\end{aligned}$$

where

$$z(t) := z_N(t) = |\,\Phi_0(t)\,\rangle\langle\,\Phi_1(t)\,| = \prod_{k=1}^{N}(|a_k|^2 \exp(ic_kt) + |b_k|^2 \exp(-ic_kt)).$$

From the last expression follows that

$$|z(t)|^2 = \prod_{k=1}^{N}\left(1 - 4|a_k|^2|b_k|^2 \sin^2(c_kt)\right);$$

(mind that the constraint $|a_k|^2 + |b_k|^2 = 1$ guarantees that $4|a_k|^2|b_k|^2 \leq 1$). At time 0, we have $z_N(t) = 1$ and we conclude that the density operator is a full fledged quantum pure state. If for each k either a_k or b_k is equal to 1, then $|z(t)|^2$ remains equal to 1 and the coherence is preserved. However, if $0 < |a_k| < 1$ for infinitely many indices when $N \to \infty$, then $\lim_{N\to\infty} z(t) = 0$ and the quantum marginal $\rho(t)$, for $t \neq 0$ and $N \to \infty$, tends to

$$\rho_c(t) = \begin{pmatrix} |a|^2 & 0 \\ 0 & |b|^2 \end{pmatrix}$$

which is isomorphic to a classical probability on the set $\{0, 1\}$. And this will inexorably occur because it is not expected to be able to control perfectly the state of the environment with the precision required to keep the coherence. This phenomenon is termed **decoherence**. It causes the gradual disappearance of quantum phenomena leading to a transition from quantum behaviour to classical. It is the main impediment for the implementation of large quantum computers.

Quite remarkably, while the phenomenon of decoherence was known since the early days of quantum mechanics, in 1996, in an ingeneous experiment [31], the installment of a progressive decoherence phenomenon was observed for a two-dimensional system corresponding to a two-level atom.

Entanglement is different from classical correlations

The example of "Berltmann's socks" is intended to constantly remind us that the EPR paradox cannot be described classically, as one naïvely could think. Of course, we can create classical correlations between Alice's and Bob's states. But compare the following situations.

Classical: An experimenter on earth, say Eve, tosses a coin and prepares two envelops both of them containing a postal card with 0 if the coin showed heads or both containing a postal card with 1 if the coin showed tails. Eve sends one envelope to Alice and one envelop to Bob. Whatever value Alice obtains, she knows that Bob will obtain the same. The outcome A and B obtain has been pre-determined by Eve who tossed a coin on earth to decide which digit to inscribe on the cards sent to A and B. The joint probability vector of Alice's and Bob's cards is given by $\kappa = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$ with marginals $\kappa_A = (1/2, 1/2)$ and $\kappa_B = (1/2, 1/2)$ and κ induces non trivial correlations because $\kappa \neq \kappa_A \otimes \kappa_B = \begin{pmatrix} 1/4 & 1/4 \\ 1/4 & 1/4 \end{pmatrix}$, i.e. is not a product state. **But EPR paradox is not describing that setting!**

Quantum: Eve prepares on earth an entangled unit vector $\Psi = \frac{1}{2}(\varepsilon_0 \otimes \zeta_0 + \varepsilon_1 \otimes \zeta_1)$ and a system in the pure entangled state $\rho = |\Psi\rangle\langle\Psi|$ (think, for instance, of a pair of photons in the entangled pure state). She sends one photon to Alice and the other to Bob. The quantum marginals are $\rho_A = \mathrm{tr}_{\mathbb{H}_2}\rho = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix} = \mathrm{tr}_{\mathbb{H}_1}\rho = \rho_B$, i.e. quantum marginals are isomorphic to the classical probability measures κ_A and κ_B defined above. But before Alice or Bob measure the polarisation, the vector Ψ (determining the state) is still in a superposition. It is only after the one of them measures 0 that the state will be collapsed onto the eigenspace associated with the eigenvalue 0. If Alice measures first and then Bob, whatever Alice gets she is certain that Bob will get the same. The situation is as if Alice and Bob each received a coin of an entangled pair of "quantum coins". If one of them tosses the coin, whatever she/he gets, the other will obtain the same. But before measuring, both Alice and Bob have still the potentiality of getting heads or tails, i.e. the outcome of their experiment has not been decided by the outcome of a coin previously tossed on earth. This is precisely the reason for which the quantum mechanical prediction sounds like a paradox.

Part II

Quantum mechanics in finite dimensional spaces and its applications

5 Information

In present days, one of the major applications of quantum mechanics concerns storage, retrieval, protection, processing, and transmission of information encoded in digital form. In this chapter, we start defining the notion of classical **information** — introduced by Shannon in [135] — and present shortly its connection with the notion of thermodynamic **entropy**, introduced by Boltzmann in [28] to explain irreversibility; the **Landauer's principle** is then stated on a very simple system illustrating the connection of information retrieval with thermodynamic irreversibility. We introduce then the notion of classical and quantum **register** as a general mathematical model of physical systems allowing the storage of information. We then generalise the definition of information to the quantum case following [1] [149]. We proceed finally with the general notion of **channel** as a versatile model for the transmission or the processing of information.

5.1 Classical information and entropy

Let X be a random variable defined on $(\Omega, \mathcal{F})$ and taking values in the finite set $\mathbb{X}$, with $n = \mathsf{card}\mathbb{X}$. Let $\mathsf{PV}_n = \{\mathbf{p} \in \mathbb{R}_+^{\mathbb{X}} : \sum_{x\in\mathbb{X}} p_x = 1\}$. To each element $\mathbf{p} \in \mathsf{PV}_n$ corresponds a probability measure $\nu_X^{\mathbf{p}}$ defined by $\nu_X^{\mathbf{p}}(x) = p_x$, for $x \in \mathbb{X}$. Suppose first that $\mathsf{supp}\,\mathbf{p} = \mathbb{X}$, i.e. all elements of $\mathbb{X}$ can occur with positive probability. Therefore, before the outcome of X is observed, we are perplex about the possible outcome. After having observed the outcome however, the *a posteriori* probability, conditioned on the observed value, becomes a Dirac mass on that value and there is not any residual perplexity. For instance, suppose that $\mathbb{X} = \{0, 1\}$ and X models a fair coin. Before

1. Also available in its English translation as a poor quality typewritten and mimeographed text [150], or in its French translation in the nicely printed book [152].

the coin is tossed, our perplexity on the outcome is maximal (100%). After the coin is tossed and its upper face revealed to us, our perplexity is reduced to 0. The main result of Shannon can be viewed as

— a quantifying of the perplexity associated with a given probability vector, and
— defining the information as the reduction of perplexity when the outcome is revealed.

Some reasonable requirements on the perplexity of X taking values in some finite set $\mathbb{X}$, with cardinality n (or more precisely its law $\nu_X^{\mathbf{p}}$) are given below:

— Suppose that all $p_x, x \in \mathbb{X}$ but one are 0 and $p_y = 1$, for some y. Then $\nu_X^{\mathbf{p}}(y) = 1$ and there is no perplexity about the possible outcome of X;
— Suppose on the contrary that $p_x = 1/n, x \in \mathbb{X}$. Our perplexity is maximal and this perplexity increases with n.
— If S is to be interpreted as a perplexity associated with a probability vector $\mathbf{p} \in \mathsf{PV}_n$, on denoting $\mathsf{PV} = \cup_{n\in\mathbb{N}}\mathsf{PV}_n$, the first statement implies that $S(1,0,0,\ldots,0) = 0$ while $S(1/n,\ldots,1/n)$ is an increasing function of n.
— The function S must be invariant under permutations of its arguments i.e.

$$S(p_{\sigma(1)},\ldots,p_{\sigma(n)}) = S(p_1,\ldots,p_n)$$

for all the permutations $\sigma \in S_n$.
— If we split the possible outcome values into two sets, the function S must verify the *grouping property*, i.e.

$$\begin{aligned} S(p_1,\ldots,p_n;p_{n+1},\ldots,p_N) &= S(q_A,q_B) \\ &\quad + q_A S(\frac{p_1}{q_A},\ldots,\frac{p_n}{q_A}) \\ &\quad + q_B S(\frac{p_{n+1}}{q_B},\ldots,\frac{p_N}{q_B}), \end{aligned}$$

where $q_A = p_1 + \ldots + p_n$ and $q_B = p_{n+1} + \ldots + p_N$.
— Finally, we require $S(p_1,\ldots,p_n;0,\ldots,0) = S(p_1,\ldots,p_n)$.

Theorem 5.1.1. *The only function $S : PV \to \mathbb{R}_+$ satisfying the above requirements and the technical condition that $S((p,1-p))$ is a continuous function of $p \in [0,1]$ is the function defined by*

$$PV \ni (p_1,\ldots,p_n) \mapsto S(p_1,\ldots,p_n) = -k\sum_{i=1}^{n} p_i \log p_i,$$

*where k is an arbitrary non-negative constant and the convention $0\log 0 = 0$ is used. The function S is called the **(classical) entropy** of the probability vector $\mathbf{p}$.*

Proof: See [120]. □

Remark 5.1.2. The basis chosen for the logarithm in the expression of S is irrelevant as it can be absorbed into the constant k. When $k = 1$ and the logarithm is in basis 2, the units of S are bits, when $k = 1.380649 \times 10^{-23}$ J/K and the natural logarithm is used, the entropy is measured in J/K. In the former case, we speak about Shannon's entropy; in the latter, about Boltzmann's entropy.

Example 5.1.3. Let $\mathbb{X} = \{0,1\}$ and $\mathbf{p} = (1/2,1/2)$. Then $S(\mathbf{p}) = 1$ bit. In other words, the perplexity (≡ entropy) associated with a fair coin is $S_{\text{initial}} = 1$ bit. If the value

of the outcome $x \in \mathbb{X}$ is revealed, the probability conditional on the event that the coin showed face x becomes a Dirac mass on x, corresponding to an entropy $S_{\text{final}} = 0$ bit. Therefore, the information obtained from the "measurement" of the outcome is $S_{\text{initial}} - S_{\text{final}} = 1$ bit.

We summarise below what we learn from the previous example:
— The physical system "fair coin" can store 1 bit of information.
— An unfair coin with $\mathbf{p} = (\lambda, 1-\lambda)$, with $\lambda \in [0,1] \setminus \{1/2\}$, can store $-\lambda \log_2(\lambda) - (1-\lambda)\log_2(1-\lambda) < 1$ bit of information.
— As an extreme case, when $\lambda \in \{0,1\}$, i.e. the coin is totally biased (or what is equivalent $\mathsf{card}\mathbb{X} = 1$), the system cannot serve as an information storage since it can hold 0 bits of information.
— As a consequence only a system with outcomes in some finite set $\mathbb{X}$ with $\mathsf{card}\mathbb{X} > 1$ (more precisely with a set of outcomes $\mathbb{X}$ sufficiently large so that probability vectors satisfying $\mathsf{card}\,\mathsf{supp}\,\mathbf{p} > 1$ can hold on it) can serve as a storage device. Moreover, the information content of the system is $S(\mathbf{p})$ bits; it is precisely the amount of information we get when the outcome is revealed to us.

5.2 Entropy, irreversibility, and the Landauer's principle

Entropy has been introduced by Clausius [41] (see [42] for a more easily accessible source) to study the Carnot's cycle. Later on, Boltzmann in [28] introduced a microscopic version of the entropy to explain the observed macroscopic irreversibility of physical systems described by microscopically reversible transformations. It is remarkable that Boltzmann had obtained the formula of theorem 5.1.1 half a century before Shannon (see figure 5.1).

Entropy is closely related to irreversibility since the second principle of thermodynamics, in the microscopic version formulated by Carathéodory [34], states that entropy
— of an **isolated** system is a non decreasing function of time; for such systems energy is preserved and they spontaneously evolve towards thermodynamic equilibrium, i.e. maximum entropy states;
— remains constant **only** for reversible isolated evolutions.
The remark 5.2.1 and the exercise 5.2.2 below clarify this statement.

We have postulated that the evolution of isolated systems (both classical and quantum) is reversible. This postulate intuitively means that there is not a physically realisable experiment allowing to distinguish between a movie showing a system evolving forwards in time or the system evolving backwards.

Remark 5.2.1. An evolution of a classical physical system with set of states $\mathbf{S}$ is a stochastic kernel acting (to the left) on states ($\equiv$ probabilities) and transforming them into new probabilities. Let S be the entropy function defined on the finite setting (i.e. in the situation $\mathsf{card}\mathbb{X} < \infty$) in theorem 5.1.1 In this setting, stochastic kernels are stochastic matrices; they correspond to reversible evolutions if the kernel is a deterministic

[Gleich. 35] § 6. Math. Bedeutung der Grösse H. 41

andere Permutation möglich. Viel wahrscheinlicher schon wäre der Fall, dass die Hälfte der Moleküle eine bestimmte, bestimmt gerichtete, die andere Hälfte eine andere, wieder für alle gleiche und gleichgerichtete Geschwindigkeit hätten. Dann wäre die Hälfte der Geschwindigkeitspunkte in einer, die andere Hälfte in einer zweiten Zelle; es wäre also:

$$Z = \frac{n!}{\left(\frac{n}{2}\right)!\left(\frac{n}{2}\right)!} \text{ u. s. w.}$$

Da nun die Anzahl der Moleküle eine überaus grosse ist, so sind $n_1\,\omega$, $n_2\,\omega$ u. s. w. ebenfalls als sehr grosse Zahlen zu betrachten.

Wir wollen die Annäherungsformel:

$$p! = \sqrt{2\,p\,\pi}\left(\frac{p}{e}\right)^p$$

benützen, wobei e die Basis der natürlichen Logarithmen und p eine beliebige grosse Zahl ist.[1])

Bezeichnen wir daher wieder mit l den natürlichen Logarithmus, so folgt:

$$l[(n_1\,\omega)!] = (n_1\,\omega + \tfrac{1}{2})\,l\,n_1 + n_1\,\omega\,(l\,\omega - 1) + \tfrac{1}{2}(l\,\omega + l\,2\,\pi).$$

Vernachlässigt man hier $\frac{1}{2}$ gegen die sehr grosse Zahl $n_1\,\omega$ und bildet den analogen Ausdruck für $(n_2\,\omega)!$, $(n_3\,\omega)!$ u. s. f., so ergibt sich:

$$l\,Z = -\,\omega\,(n_1\,l\,n_1 + n_2\,l\,n_2 \ldots) + C,$$

wobei

$$C = l(n!) - n\,(l\,\omega - 1) - \frac{\zeta}{2}\,(l\,\omega + l\,2\,\pi)$$

für alle Geschwindigkeitsvertheilungen denselben Werth hat, also als Constante zu betrachten ist. Denn wir fragen ja bloss nach der relativen Wahrscheinlichkeit der Eintheilung der verschiedenen Geschwindigkeitspunkte unserer Moleküle in unsere Zellen ω, wobei selbstverständlich die Zelleneintheilung, daher auch die Grösse einer Zelle ω, die Anzahl der Zellen ζ und die Gesammtzahl n der Moleküle und deren gesammte lebendige Kraft als unveränderlich gegeben betrachtet werden müssen. Die wahrscheinlichste Eintheilung der Geschwindig-

[1]) Siehe Schlömilch, Comp. der höh. Analysis. Bd. 1. S. 437. 3. Aufl.

Figure 5.1 – Facsimilé of the page 41 of Boltzmann's book *Vorlesungen über Gastheorie* [28], where the mathematical definition of the entropy function, identical to the definition of theorem 5.1.1 has been obtained. In the original book of Boltzmann, the natural logarithm is denoted by l. This book has been translated into French in [29].

invertible matrix, i.e. corresponds to a permutation on $\mathbb{X}$. The invariance of S on permutations is built-in in its definition.

Exercise 5.2.2. Let K be a bistochastic matrix on $\mathbb{X}$, i.e. K has non-negative elements whose every row and every column sum up to one.

1. Show that if K is irreducible, then the Markov evolution determined by K admits a uniform invariant probability.
2. Show that $S(\mathbf{p}K) \geq S(\mathbf{p})$.
3. Examine under which circumstances the above inequality is an equality.

For a system undergoing an irreversible transformation the entropy increases; however the system can be considered as part of a larger isolated composite system (A and environment), undergoing globally a reversible transformation. In that case the total entropy (of the system A and of the environment) remains constant but since the entropy of A must increase, the entropy of the environment must decrease [2] hence the missing information decreases. In other words, when the system A undergoes an irreversible transformation, the environment gains information.

This leads to the Landauer's principle: *When a computer erases a single bit of information, the environment gains at least* $k \ln 2$ *units of information, where* $k > 0$ *is a constant.*

5.3 Registers

5.4 Channels

2. Notice that this assertion is not in contradiction with the second principle of thermodynamics because the environment is not isolated.

6

Cryptology

Cryptology, grouping cryptography and cryptanalysis, is an old preoccupation of mankind because information is, as a matter of fact, a valuable resource. Nowadays classical technology allows secure ciphering of information that cannot be deciphered in real time. However, the cryptologic protocols used nowadays are all based on the **unproven conjecture** that factoring large integers is a hard computational task. Should this conjecture be proved false, and an efficient polynomial factorisation algorithm be discovered, the security of our communication networks could become vulnerable. But even without any technological breakthrough, the ciphered messages we exchange over public channels (internet, commutated telephone network, SMS, etc.) can be deciphered by spending 8–10 months of computing time; hence our information exchange is already vulnerable for transporting information that remains important 10 months after its transmission.

Quantum information acquired an unprecedented impetus when Peter Shor [136] proved that on a quantum computer, factoring can be solved in polynomial (in the number of its digits) time. Nowadays, the initial dust — created by the enthusiasm of the feasibility of a universal quantum computer — has somehow settled down; as a counterpart, we have now a much more realistic approach to the subject.

Quantum communication can use the existing technology to securely cipher information. It is therefore economically and strategically important to master the issues of advanced cryptography and to invent new cryptologic methods.

6.1 An old idea: the Vernam's code

In 1917, Gilbert Vernam proposed [147] the following ciphering scheme.[1] Let $\mathbb{A}$ be a finite alphabet, identified with the set $\{0, \ldots, |\mathbb{A}| - 1\}$ and m a message of length N over the alphabet $\mathbb{A}$, i.e. a word $m \in \mathbb{A}^N$. The Vernam's ciphering algorithm uses a ciphering key of same length as m, i.e. a word $k \in \mathbb{A}^N$ and performs character-wise addition as explained in the following

Algorithm 6.1.1. *VernamsCiphering*

Require: *Original message $m \in \mathbb{A}^N$ and* UNIFRANDOMGENERATOR($\mathbb{A}^N$).
Ensure: *Ciphered message $c \in \mathbb{A}^N$.*
  choose *randomly ciphering key $k \in \mathbb{A}^N$;*
  $i \leftarrow 1$;
  repeat
    add character-wise $c_i = m_i + k_i \mod |\mathbb{A}|$;
    $i \leftarrow i + 1$;
  until $i > N$.

The recipient of the ciphered message c, knowing the ciphering key k, performs the following

Algorithm 6.1.2. *VernamsDeciphering*

Require: *Ciphered message $c \in \mathbb{A}^N$ and ciphering key $k \in \mathbb{A}^N$.*
Ensure: *Original message $m \in \mathbb{A}^N$.*
  $i \leftarrow 1$;
  repeat
    subtract character-wise $m_i = c_i - k_i \mod |\mathbb{A}|$;
    $i \leftarrow i + 1$;
  until $i > N$.

As far as the ciphering key is used only once, the key word has the same length as the message (i.e. N), and N is sufficiently large, the Vernam's algorithm is proved [134] to be perfectly secure. The main problem of the algorithm is how to securely communicate the key k?

6.2 The classical cryptologic scheme RSA

Theorem 6.2.1. *(Fermat's little theorem) Let p be a prime. Then*

1. *any integer a satisfies $a^p = a \mod p$,*
2. *any integer a, not divisible by p, satisfies $a^{p-1} = 1 \mod p$.*

Definition 6.2.2. The *Euler's function* $\phi : \mathbb{N} \to \mathbb{N}$ is defined by

$$\phi(n) = \mathsf{card}\{0 < a < n : \gcd(a, n) = 1\}, n \in \mathbb{N}.$$

1. Appeared as a first patent US Patent 1310719 issued on 22 July 1919, and further improved in a series of patents: US Patent 1416765, US Patent 1584749, and US Patent 1613686.

In particular, if p is prime, then $\phi(p) = p - 1$.

Theorem 6.2.3. *(Euler's) If* $\gcd(a, m) = 1$, *then* $a^{\phi(m)} = 1 \mod m$.

Proposition 6.2.4. *Let m be an integer, strictly bigger than 1, without square factors, and r a multiple of $\phi(m)$. Then*

— $a^r = 1 \mod m$, *for all integers a relatively prime with respect to m, and*
— $a^{r+1} = a \mod m$ *for all integers.*

The proofs of all the previous results are straightforward but outside the scope of the present course; they can be found in [46, pp. 50–60].

The RSA protocols, named after its inventors Rivest, Shamir, and Adleman [125], involves two legal parties: Alice and Bob, and an eavesdropper, Eve. Bob produces by the classical key distribution algorithm a private key d and a public key π. Alice uses the public key of Bob to cipher the message and Bob uses his private key to decipher it. Eve, even if she intercepts the ciphered message, cannot decipher it in real time.

Algorithm 6.2.5. *ClassicalKeyDistribution*

Require: *Two primes p and q.*
Ensure: *Public, π, and private, d, keys of Bob.*
$n \leftarrow pq$ *(hence* $\phi(n) = (p-1)(q-1)$*);*
choose *any* $e < n$, *such that* $\gcd(e, \phi(n)) = 1$;
$d \leftarrow e^{-1} \mod \phi(n)$;
$\pi \leftarrow (e, n)$.

Bob publishes his public key π on his internet page. Alice uses π to cipher the message m using the following

Algorithm 6.2.6. *Ciphering*

Require: *Public key $\pi = (e, n)$ and message $m \in \mathbb{N}$, with $m < n$.*
Ensure: *Ciphered text $c \in \mathbb{N}$.*
$c \leftarrow m^e \mod n$.

Alice transmits the ciphered text c through a vulnerable public channel to Bob. He uses his private key to decipher by using the following

Algorithm 6.2.7. *Deciphering*

Require: *Private key d and ciphered message $c \in \mathbb{N}$.*
Ensure: *Deciphered text $\mu \in \mathbb{N}$.*
$\mu \leftarrow c^d \mod n$.

Theorem 6.2.8. $\mu = m$

Proof:

$$\begin{aligned} c^d &= m^{ed} \mod n \\ ed &= 1 + k\phi(n), \text{ for some } k \in \mathbb{N} \\ m^{ed} &= m^{1+k\phi(n)}, \end{aligned}$$

and since $n = pq$ has no square factors, by using proposition 6.2.4, we get $m^{1+k\phi(n)} \bmod n = m \bmod n$. □

If Eve intercepts the message, to compute d she must know $\phi(n)$, hence the factoring of n into primes. Security of the protocol is based on the conjecture that it is algorithmically hard to factor n. If we denote by $N = \log n$, then it is worth noticing that when the RSA protocol has been introduced, the best known algorithm of factor n run in $\exp(N)$ time. The best[2] known algorithm nowadays [100] runs in $\exp(N^{1/3}(\log N)^{2/3})$ time. This algorithmic improvement, combined with the increasing in the computational capabilities of computers, allows the factoring of a 1000 digits number in ca. 8 months instead of a time exceeding the age of the universe at the moment the algorithm has been proposed. Until May 2007, the RSA company ran an international contest offering several hundreds thousand dollars to whoever could factor multi-digit numbers they provided on line. When the contest stopped the company gave the official reasons explained in RSA factoring challenge.

6.3 Quantum key distribution

6.3.1 The non cloning theorem

We start by stating a basic fact in quantum mechanics that guarantees the inviolability of most cryptologic protocols.

Theorem 6.3.1 (Non-cloning theorem). *Let $|\phi\rangle$ and $|\psi\rangle$ be two rays in $\mathbb{H}$ such that $\langle\phi|\psi\rangle \neq 0$ and $|\phi\rangle \neq \exp(i\theta)|\psi\rangle$. Then there does not exist any quantum device allowing duplication of ϕ and ψ.*

Proof: Suppose that such a device exists. Then, for some $n \geq 1$, there exists a unitary $U : \mathbb{H}^{\otimes(n+1)} \to \mathbb{H}^{\otimes(n+1)}$ and some ancillary ray $|\alpha_1 \cdots \alpha_n\rangle \in \mathbb{H}^{\otimes n}$ such that we get

$$\begin{aligned} |\phi\phi\beta_1 \cdots \beta_{n-1}\rangle &= U|\phi\alpha_1 \cdots \alpha_n\rangle \\ |\psi\psi\gamma_1 \cdots \gamma_{n-1}\rangle &= U|\psi\alpha_1 \cdots \alpha_n\rangle. \end{aligned}$$

Then

$$\begin{aligned} \langle\psi|\phi\rangle &= \langle\psi\alpha_1 \cdots \alpha_n|U^*U|\phi\alpha_1 \cdots \alpha_n\rangle \\ &= \langle\psi|\phi\rangle^2 \prod_{i=1}^{n-1} \langle\gamma_i|\beta_i\rangle. \end{aligned}$$

Since $\langle\phi|\psi\rangle \neq 0$ we get $\langle\psi|\phi\rangle \prod_{i=1}^{n-1} \langle\gamma_i|\beta_i\rangle = 1$ and since $|\phi\rangle \neq \exp(i\theta)|\psi\rangle$, it follows that $0 < |\langle\psi|\phi\rangle| < 1$. Subsequently, $\prod_{i=1}^{n-1} |\langle\gamma_i|\beta_i\rangle| > 1$ but this is impossible since for every i, $|\langle\gamma_i|\beta_i\rangle| \leq 1$. □

2. See also [102] for an updated state of the art.

6.3.2 The BB84 protocol

This protocol, due to Bennett and Brassard [20], relies on the random use of of two non-orthogonal bases for encoding a secret quantum key. Its security stems from the impossibility — thanks to the theorem 6.3.1 — for an unauthorised intruder to tap the communication line in order to copy the quantum code without being detected.

Alice and Bob communicate through a quantum and a classical public channels; they agree publicly to use two different orthonormal bases of $\mathbb{H} = \mathbb{C}^2$ (describing the photon polarisation):

$$\begin{aligned} \mathbb{B}^+ &= \{\varepsilon_0^+ = |\,0\,\rangle, \varepsilon_1^+ = |\,1\,\rangle\} \\ \mathbb{B}^\times &= \{\varepsilon_0^\times = \frac{|\,0\,\rangle - |\,1\,\rangle}{\sqrt{2}}, \varepsilon_1^\times = \frac{|\,0\,\rangle + |\,1\,\rangle}{\sqrt{2}}\}. \end{aligned}$$

The first element of each basis is associated with the bit 0, the second with the bit 1. Moreover Alice and Bob agree on some integer $n = (4+\delta)N$ with some $\delta > 0$, where N is the length of the key they wish to exchange securely; N will be also the length of their key. Alice finally needs an apparatus implementing the function $T : \{0,1\}^2 \to \mathbb{H}$ defined by

$$T(x,y) = \begin{cases} \varepsilon_0^+ & \text{if } (x,y) = (0,0) \\ \varepsilon_1^+ & \text{if } (x,y) = (0,1) \\ \varepsilon_0^\times & \text{if } (x,y) = (1,0) \\ \varepsilon_1^\times & \text{if } (x,y) = (1,1). \end{cases}$$

Therefore, the bit x determines which bit to encode into the qubit; the bit y which basis to use in order to do so.

Algorithm 6.3.2. *AlicesKeyGeneration*

Require: UNIFRANDOMGENERATOR($\{0,1\}$), T, n.
Ensure: *Two strings of n random bits* $\mathbf{a}, \mathbf{b} \in \{0,1\}^n$ *and a sequence of n qubits* $(|\,\psi_i\,\rangle)_{i=1,\dots,n}$.

```
generate randomly a_1, ..., a_n;
a ← (a_1, ..., a_n) ∈ {0,1}^n;
generate randomly b_1, ..., b_n;
b ← (b_1, ..., b_n) ∈ {0,1}^n;
i ← 1;
repeat
    |ψ_i⟩ ← T(a_i, b_i);
    transmit photon in pure state ρ_i = |ψ_i⟩⟨ψ_i| to Bob via public quantum channel;
    i ← i + 1;
until i > n.
```

On reception of the ith qubit, Bob performs a measurement of the projection operator $B_1^\sharp = |\,\varepsilon_1^\sharp\,\rangle\langle\,\varepsilon_1^\sharp\,|$, where $\sharp \in \{+,\times\}$, i.e. asks whether the encoded bit is 1 by acting with the projector $B_1^\sharp$ on $|\,\psi_1\,\rangle$; he gets an answer 0 or 1 and the probability of getting 1 is $\langle\,\psi_i\,|\,B_1\psi\,\rangle$.

Algorithm 6.3.3. *BobsKeyGeneration*

Require: UNIFRANDOMGENERATOR($\{0,1\}$), n, *sequence* $|\psi_i\rangle$ *for* $i = 1,\dots,n$, $P^\sharp$ *for* $\sharp \in \{+,\times\}$.
Ensure: *Two strings of* n *bits* $\mathbf{a}', \mathbf{b}' \in \{0,1\}^n$.
  generate *randomly* $b'_1,\dots,b'_n$;
  $\mathbf{b}' \leftarrow (b'_1,\dots,b'_n) \in \{0,1\}^n$:
  $i \leftarrow 1$;
  repeat
    if $b'_i = 0$ ***then***
      ask whether B_1^+ *takes value 1;*
    else
      ask whether $B_1^\times$ *takes value 1;*
    end if
    if *photomultiplier (PM) is triggered* ***then***
      $a'_i \leftarrow 1$;
    else
      $a'_i \leftarrow 0$;
    end if
    $i \leftarrow i+1$;
  until $i > n$.
  $\boldsymbol{a}' \leftarrow (a'_1,\dots,a'_n) \in \{0,1\}^n$;
  transmit *string* $\mathbf{b}' \in \{0,1\}^n$ *to Alice via public classical channel.*

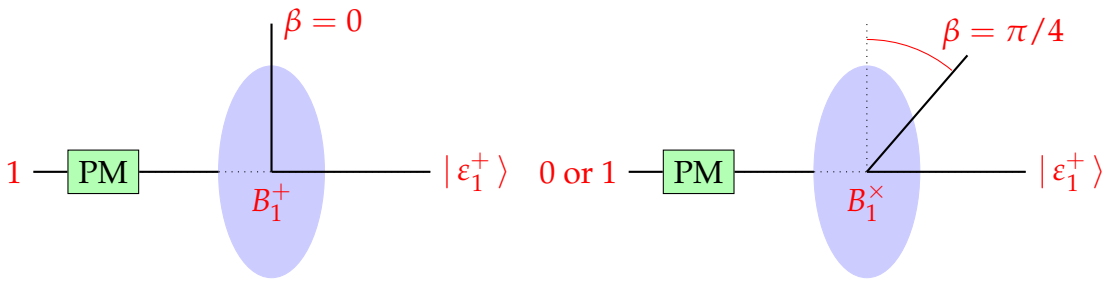


Figure 6.1 – Schematic experimental setting of Bob's generation algorithm instantiated with input $|\varepsilon_1^+\rangle$. When $b' = 0$ is tossed, Bob decides to ask the question B_1^+ in state $|\varepsilon_1^+\rangle$ (left picture); if $b' = 1$, he asks the question $B_1^\times$ in state $|\varepsilon_1^+\rangle$ (right picture). The answer in the first case is "yes" with probability 1, it is "yes" with probability 1/2 and "no" with probability 1/2 in the second case.

When Alice receives the string $\mathbf{b}'$, she performs the conciliation algorithm described below.

Algorithm 6.3.4. *Conciliation*

Require: *Strings* $\mathbf{b}, \mathbf{b}' \in \{0,1\}$.
Ensure: *Sequence* $(k_1, \ldots, k_L)$ *with some* $L \leq n$ *of positions of coinciding bits.*

```
c ← b ⊕ b′;
i ← 1;
k ← 1;
repeat
    k ← min{j : k ≤ j ≤ n such that c_j = 0};
    if k ≤ n then
        k_i ← k;
        i ← i + 1;
    end if
until k > n.
L ← i − 1;
transmit (k_1, ..., k_L) to Bob via public classical channel.
```

Theorem 6.3.5. *If there is no eavesdropping on the quantum channel then*

$$\mathbb{P}((a'_{k_1}, \ldots, a'_{k_L}) = (a_{k_1}, \ldots, a_{k_L})) = 1.$$

Proof: Since $[B_0^\sharp, B_1^\sharp] = 0$, the two operators are simultaneously diagonalised in base $\mathbb{B}^\sharp$. Compute $\langle \psi_i \,|\, B_x^+ \psi_i \rangle$ and $\langle \psi_i \,|\, B_x^\times \psi_i \rangle$ for all different possible choices of $|\, \psi_i \,\rangle \in \mathbb{B}^+ \cup \mathbb{B}^\times$ and for $x = 0, 1$.

a_i	b_i	ψ_i	b'_i	$\langle \psi_i \,\vert\, B_1^+ \psi_i \rangle$	$\langle \psi_i \,\vert\, B_0^* \psi_i \rangle$	a'_i	b'_i	$\langle \psi_i \,\vert\, B_1^\times \psi_i \rangle$	$\langle \psi_i \,\vert\, B_0^\times \psi_i \rangle$	a'_i
0	0	ε_0^+	0	0	1	0	1	1/2	1/2	0 or 1
1	0	ε_1^+	0	1	0	1	1	1/2	1/2	0 or 1
0	1	$\varepsilon_0^\times$	0	1/2	1/2	0 or 1	1	0	1	0
1	1	$\varepsilon_1^\times$	0	1/2	1/2	0 or 1	1	1	0	1

We observe that for those i's such that $b'_i = b_i$ we have $\mathbb{P}(a'_i = a_i) = 1$. Hence on deciding to consider only the substrings of $\mathbf{a}$ and $\mathbf{a}'$ defined on the locations where $\mathbf{b}$ and $\mathbf{b}'$ coincide, we have the certainty of sharing the same substrings, although $\mathbf{a}$ and $\mathbf{a}'$ have never been exchanged. □

Lemma 6.3.6. *If there is no eavesdropping, for* N *large enough,* L *is of the order* $2N$.

Proof: Elementary use of the law of large numbers. □

If Eve is eavesdropping, since she cannot copy quantum states (no-cloning theorem), she can measure with the same procedure as Bob and in order for the leakage not to be apparent, she re-emits a sequence of qubits $|\, \tilde{\psi}_i \,\rangle$ to Bob. Now again L is of the order $2N$ but since Eve's choice of the $\mathbf{b}$'s is independent of the choices of Alice and Bob, the string $\mathbf{a}'$ computed by Bob will coincide with Alice's string $\mathbf{a}$ at only $L/2 \simeq N$ positions.

Hence to securely communicate, Alice and Bob have to go through the eavesdropping detection procedure and conciliation.

Bob randomly chooses half of the bits of the substring $(a'_{k_1}, \ldots, a'_{k_L})$, i.e. $(a'_{r_1}, \ldots, a'_{r_{L/2}})$ with $r_i \in \{k_1, \ldots, k_L\}$ and $r_i \neq r_j$ for $i \neq j$, and sends the randomly chosen positions

$(r_1, \dots, r_{L/2})$ and the corresponding bit values $(a'_{r_1}, \dots, a'_{r_{L/2}})$ to Alice. If $(a'_{k_1}, \dots, a'_{k_{L/2}}) = (a_{k_1}, \dots, a_{k_{L/2}})$ (conciliation) then Alice announces this fact to Bob and they use the complementary substring of $(a'_{k_1}, \dots, a'_{k_L})$ (of length $L/2 \simeq N$) as their key to cipher with Vernam's algorithm. Else, they restart BB84 protocol.

Notice that Alice and Bob never exchanged the ultimate substring of N bits they use as key.

6.4 Other cryptologic protocols

6.4.1 Six-state protocol

6.4.2 B92

[21]

6.4.3 Ekert protocol

Ekert, A. K. Quantum cryptography based on Bell's theorem [56]

6.5 Eavesdropping strategy for individual attacks

In §6.3.2, the detection of intrusion is made in quite a rudimentary way. In particular, we have supposed that Eve is sufficiently greedy to be uncovered quite easily. Here we present some subtler intrusion methods.

Start by fixing (or recalling) the notation.

Notation 6.5.1. There are three parties: Alice, Bob (the legal partners) and Eve (the eavesdropper).

- Pure states of each party are associated with different Hilbert spaces, $\mathbb{H}_A, \mathbb{H}_B$, and $\mathbb{H}_E$ respectively.
- If $x \in \{0,1\}$ designs a bit, then $\overline{x} = 1 - x$ is the conjugate bit of x.
- If $\sharp \in \{+, \times\}$ designs the index of the used basis, then $\flat$ denotes the conjugate of $\sharp$ basis, i.e. if $\sharp = +$ then $\flat = \times$ and vice versa.
- $(B_x^\sharp)_{x\in\{0,1\}}$ is the sharp resolution of the identity in $\mathbb{H}_B$

$$\sum_{x\in\{0,1\}} B_x^\sharp = I_{\mathbb{H}_B}$$

into orthogonal orthoprojectors $B_0^\sharp = |\,\varepsilon_0^\sharp\,\rangle\langle\,\varepsilon_0^\sharp\,|$ and $B_1^\sharp = |\,\varepsilon_1^\sharp\,\rangle\langle\,\varepsilon_1^\sharp\,|$.

— For Γ a finite indexing set, $(E[\gamma])_{\gamma\in\Gamma}$ denotes fuzzy (non-projective) resolution of $I_{\mathbb{H}_E}$ into unsharp effects $E[\gamma] \geq 0$, i.e. $\sum_{\gamma\in\Gamma} E[\gamma] = I_{\mathbb{H}_E}$.
— Alice sends qubits $|\,\psi\,\rangle \in \{|\,\varepsilon_0^+\,\rangle, |\,\varepsilon_1^+\,\rangle, |\,\varepsilon_0^\times\,\rangle, |\,\varepsilon_1^\times\,\rangle\} = \mathbb{B}^+ \cup \mathbb{B}^\times$ according to its key generation algorithm. Any element of $\mathbb{B}^\sharp$ can be decomposed into elements of $\mathbb{B}^\flat$ by

$$|\,\varepsilon_x^\sharp\,\rangle = \frac{|\,\varepsilon_0^\flat\,\rangle + (-)^x |\,\varepsilon_1^\flat\,\rangle}{\sqrt{2}}, x \in \{0,1\}, \sharp \in \{+,\times\}, \flat \text{ conjugate of } \sharp.$$

We summarise below the possible actions that can be taken by the intruder:
— The pure states produced initially by Alice are unit vectors $|\,\psi\,\rangle = |\,\varepsilon_t^\sharp\,\rangle \in \mathbb{H}_A$. Once they are sent over the quantum channel, Alice has no access on them any longer. When these vectors are received by their (legal or illegal) recipient, he or she can on them in various manners. For instance, if Bob receives such a vector, he can act on it by operators of his own space $\mathbb{H}_B$, although we still write $|\,\psi\,\rangle \in \mathbb{H}_A$.
— Eve cannot copy $|\,\psi\,\rangle \in \mathbb{H}_A$ but can
  — couple every $|\,\varepsilon_x^\sharp\,\rangle \in \mathbb{H}_A$ with a state $|\,\phi\,\rangle \in \mathbb{H}_E$ of her own to produce $|\,\varepsilon_x^\sharp\,\rangle \otimes |\,\phi\,\rangle \in \mathbb{H}_A \otimes \mathbb{H}_E$,
  — let the vector $|\,\varepsilon_x^\sharp\,\rangle \in \mathbb{H}_A$ evolve unitarily for a while to get $|\,\Phi_x^\sharp\,\rangle = U|\,\varepsilon_x^\sharp\,\rangle$, where U is an appropriate unitary operator acting on $\mathbb{H}_A \otimes \mathbb{H}_E$,
  — perform partial unsharp measurements $I_{\mathbb{H}_A} \otimes E[\gamma]$ on $|\,\Phi_x^\sharp\,\rangle$ and send first part to Bob. (Notice that unsharp measurements can be thought as sharp measurements on some bigger Hilbert space).

To grasp the *rationale* of the estimate we are doing just now, suppose for the moment being that the unitary evolution U — that always preserves pure states — preserves also the tensor product structure, i.e. the evolved states remain tensor product states:

$$U|\,\varepsilon_x^\sharp \phi\,\rangle = |\,\zeta_x^\sharp \phi_x^\sharp\,\rangle,$$
$$U|\,\varepsilon_{\overline{x}}^\flat \phi\,\rangle = |\,\zeta_{\overline{x}}^\flat \phi_{\overline{x}}^\flat\,\rangle.$$

Now

$$\frac{1}{2} = \langle\,\varepsilon_{\overline{x}}^\flat\,|\,\varepsilon_x^\sharp\,\rangle = \langle\,\zeta_x^\sharp\,|\,\zeta_{\overline{x}}^\flat\,\rangle\langle\,\phi_x^\sharp\,|\,\phi_{\overline{x}}^\flat\,\rangle$$

and if $\langle\,\varepsilon_{\overline{x}}^\flat\,|\,\varepsilon_x^\sharp\,\rangle = \langle\,\zeta_x^\sharp\,|\,\zeta_{\overline{x}}^\flat\,\rangle$, i.e. the Alice's (Bob's) parts of the state are not altered, then $\langle\,\phi_x^\sharp\,|\,\phi_{\overline{x}}^\flat\,\rangle = 1$. The last equality means that $|\,\phi_x^\sharp\,\rangle$ and $|\,\phi_{\overline{x}}^\flat\,\rangle$ cannot be discriminated and Eve can get no information from her observations. To well discriminate these states, the quantity $|\langle\,\phi_x^\sharp\,|\,\phi_{\overline{x}}^\flat\,\rangle|$ must be minimised, hence $|\langle\,\zeta_x^\sharp\,|\,\zeta_{\overline{x}}^\flat\,\rangle|$ maximised, i.e. maximally disturbed. This Idea survives even when U does not preserve tensor products as explained in the sequel.

Let now proceed with the general case. Suppose that Alice has sent a bit x encoded in the basis $\sharp$, i.e. has sent a photon in state $|\,\varepsilon_x^\sharp\,\rangle\langle\,\varepsilon_x^\sharp\,|$. Eve entangles the unit vector $|\,\varepsilon_x^\sharp\,\rangle$ with $|\,\phi\,\rangle$ and let the product state unitarily evolve for a while; after that she gets

the pure state $|\,\Phi_x^\sharp\,\rangle\langle\,\Phi_x^\sharp\,|$, where $|\,\Phi_x^\sharp\,\rangle = U|\,\varepsilon_x^\sharp\phi\,\rangle$, and measures $I\otimes E[\gamma]$ to get

$$\begin{aligned}Q_{x\gamma}^\sharp &= \mathbb{P}(\text{Eve } \textbf{unsharply} \text{ observes } \gamma|\text{Alice has sent } x \text{ encoded in basis } \sharp)\\ &= \mathsf{tr}(|\,\Phi_x^\sharp\,\rangle\langle\,\Phi_x^\sharp\,|I\otimes E[\gamma])\\ &= \langle\,\Phi_x^\sharp\,|\,(I_A\otimes E[\gamma])\Phi_x^\sharp\,\rangle\\ &= \langle\,\varepsilon_x^\sharp\phi\,|\,U^*(I_A\otimes E[\gamma])U\varepsilon_x^\sharp\phi\,\rangle.\end{aligned}$$

Henceforth, to alleviate notation, we write $Q_{x\gamma}$ instead of $Q_{x\gamma}^\sharp$. Notice that $Q_{x\gamma}$ is a Markovian kernel that can be thought as a classical communication channel (see [120]) between the classical state spaces $\{0,1\}$ and Γ. Hence, if we know

$$p_x = \mathbb{P}(\text{Alice sends bit } x)$$

we can compute the joint probability

$$\kappa(x,\gamma) = \mathbb{P}(\text{Alice sends bit } x \text{ and Eve measures } \gamma) = p_x Q_{x\gamma},$$

and the marginal on the output states

$$q_\gamma = \sum_{x\in\{0,1\}} p_x Q_{x\gamma} = \mathbb{P}(\text{Eve measures } \gamma).$$

Now, we are in position to compute the reversed Markov kernel

$$\hat{Q}_{\gamma x} = \frac{\kappa(x,\gamma)}{q_\gamma} = \frac{p_x Q_{x\gamma}}{q_\gamma} = \mathbb{P}(\text{Eve guesses that Alice has emitted } x|\text{Eve measures } \gamma),$$

from the output states Γ, i.e. Eve's measurements, to input bits $\{0,1\}$, i.e. Alice's signals. This quantity has a very important meaning; it gives the probability that Eve assigns to input values x given that she has measured γ. It follows that

$$G_\gamma = |\hat{Q}_{\gamma x} - \hat{Q}_{\gamma\bar{x}}|$$

is a quantifier of Eve's **information gain** incurred by her indirect measurement $E[\gamma]$; its expectation $\mathbb{E}G = \sum_{\gamma\in\Gamma} q_\gamma|\hat{Q}_{\gamma x} - \hat{Q}_{\gamma\bar{x}}|$ is her average information gain.

Lemma 6.5.2. *If Alice encodes in $\sharp$ basis and $p_0 = p_1 = 1/2$, the following bound holds:*

$$q_\gamma G_\gamma = q_\gamma|\hat{Q}_{\gamma x} - \hat{Q}_{\gamma\bar{x}}| \le \|Z_{00}^{\flat\gamma}\|\|Z_{10}^{\flat\gamma}\| + \|Z_{01}^{\flat\gamma}\|\|Z_{11}^{\flat\gamma}\|,$$

where $Z_{xy}^{\flat\gamma} := B^\flat[y]\otimes\sqrt{E[\gamma]}\Phi_x^\flat$, $x,y\in\{0,1\}$.

Proof. Compute under the hypotheses of the lemma:

$$\begin{aligned}q_\gamma G_\gamma = q_\gamma|\hat{Q}_{\gamma x} - \hat{Q}_{\gamma\bar{x}}| &= |p_x Q_{x\gamma} - p_{\bar{x}} Q_{\bar{x}\gamma}| \overset{\mathbf{p}=(\frac12,\frac12)}{=} \frac12|Q_{x\gamma} - Q_{\bar{x}\gamma}|\\ &= \frac12\left|\langle\,\Phi_0^\sharp\,|\,(I\otimes E[\gamma])\Phi_0^\sharp\,\rangle - \langle\,\Phi_1^\sharp\,|\,(I\otimes E[\gamma])\Phi_1^\sharp\,\rangle\right|\\ &= \frac14\left|\langle\,\Phi_0^\flat + \Phi_1^\flat\,|\,(I\otimes E[\gamma])(\Phi_0^\flat + \Phi_1^\flat)\,\rangle - \langle\,\Phi_0^\flat - \Phi_1^\flat\,|\,(I\otimes E[\gamma])(\Phi_0^\flat - \Phi_1^\flat\,\rangle)\right|\\ &= \left|\mathsf{Re}\,\langle\,\Phi_0^\flat\,|\,I\otimes E[\gamma]\Phi_1^\flat\,\rangle\right|.\end{aligned}$$

Recall now that $B^\flat[0] + B^\flat[1]$ is a resolution of I_B into sharps effects. We can pursue the previous computations to get:

$$\begin{aligned} q_\gamma G_\gamma &= |\operatorname{Re}(\langle \Phi_0^\flat \,|\, (B^\flat[0] \otimes E[\gamma])|\, \Phi_1^\flat \rangle) + \operatorname{Re}(\langle \Phi_0^\flat \,|\, (B^\flat[1] \otimes E[\gamma])|\, \Phi_1^\flat \rangle)| \\ &= |\operatorname{Re}\langle Z_{00}^{\flat\gamma} \,|\, Z_{10}^{\flat\gamma} \rangle + \operatorname{Re}\langle Z_{01}^{\flat\gamma} \,|\, Z_{11}^{\flat\gamma} \rangle| \\ &\leq |\langle Z_{00}^{\flat\gamma} \,|\, Z_{10}^{\flat\gamma} \rangle| + |\langle Z_{01}^{\flat\gamma} \,|\, Z_{11}^{\flat\gamma} \rangle| \\ &\leq \|Z_{00}^{\flat\gamma}\|\|Z_{10}^{\flat\gamma}\| + \|Z_{01}^{\flat\gamma}\|\|Z_{11}^{\flat\gamma}\|. \end{aligned}$$

□

Now,

$$\begin{aligned} \|Z_{xy}^{\flat\gamma}\|^2 &= \langle \Phi_x^\flat \,|\, B[y]^\flat \otimes E[\gamma]\Phi_x^\flat \rangle \\ &= \mathbb{P}(\text{Bob measures } y, \text{Eve measures } \gamma | \text{Alice sends } x) \\ &= \mathbb{P}(\text{Bob measures } y | \text{Eve measures } \gamma, \text{Alice sends } x) Q_{x\gamma}. \end{aligned}$$

Introduce the quantity

$$D_{x\gamma}^\flat = \mathbb{P}(\text{Bob measure erroneous value } \overline{x} | \text{Eve measures } \gamma \text{ and Alice has sent } x),$$

interpreted as the **distortion** occurring in Bob's measure in the conjugate basis of the basis of Alice (erroneous determination of the bit) given that Alice has sent x and Eve has measured γ.

Lemma 6.5.3. *Assuming that Alice encodes in ♯ basis, that* $\mathbf{p} = (1/2, 1/2)$*, and with* $D_{x\gamma}^\flat$ *as above,*

$$q_\gamma G\gamma \leq \sqrt{Q_{0\gamma}^\flat Q_{1\gamma}^\flat} \left(\sqrt{D_{0\gamma}^\flat (1 - D_{1\gamma}^\flat)} + \sqrt{D_{1\gamma}^\flat (1 - D_{0\gamma}^\flat)} \right).$$

Proof. Write

$$\begin{aligned} \|Z_{xy}^{\flat\gamma}\|^2 &= \langle \Phi_x^\flat \,|\, (B^\flat[y] \otimes E[\gamma])\Phi_x^\flat \rangle \\ &= \mathbb{P}(\text{Bob measures } y, \text{Eve measures } \gamma | \text{Alice sent } x) \\ &= \mathbb{P}(\text{Bob measures } y | \text{Eve measures } \gamma, \text{Alice sent } x) \mathbb{P}(\text{Eve measures } \gamma | \text{Alice sent } x). \end{aligned}$$

Since $B^\flat[0] + B^\flat[1] = I$, it follows that

$$\begin{aligned} \|Z_{00}^{\flat\gamma}\|\|^2 &= Q_{0\gamma}(1 - D_{0\gamma}^\flat) \\ \|Z_{10}^{\flat\gamma}\|\|^2 &= Q_{1\gamma} D_{1\gamma}^\flat \\ \|Z_{01}^{\flat\gamma}\|\|^2 &= Q_{0\gamma} D_{0\gamma}^\flat \\ \|Z_{11}^{\flat\gamma}\|\|^2 &= Q_{1\gamma}(1 - D_{1\gamma}^\flat). \end{aligned}$$

□

Theorem 6.5.4. *Assuming that Alice encodes in ♯ basis,* $\mathbf{p} = (1/2, 1/2)$*, and* $D_{0\gamma}^\flat = D_{0\gamma}^\flat = d_\gamma$*, then* $\mathbb{E}G \leq 2\sqrt{\mathbb{E}d(1 - \mathbb{E}d)}$.

Proof. Recalling that $\sqrt{ab} \leq \frac{1}{2}(a+b)$, for a and b non negative numbers, we get

$$\sqrt{Q_{0\gamma}Q_{1\gamma}} \leq \frac{1}{2}(Q_{0\gamma}+Q_{1\gamma}) \overset{\mathbf{p}=(1/2,1/2)}{=} q_\gamma.$$

Replacing in the inequality established in lemma 6.5.3, we get

$$G_\gamma \leq \sqrt{D^\flat_{0\gamma}(1-D^\flat_{1\gamma})}+\sqrt{D^\flat_{1\gamma}(1-D^\flat_{0\gamma})} \overset{D^\flat_{0\gamma}=D^\flat_{0\gamma}=d_\gamma}{=} 2\sqrt{d_\gamma(1-d_\gamma)}.$$

Using the concavity of the function $f(t)=\sqrt{t(1-t)}$ for $t\in[0,1]$ and Jensen's inequality, we get

$$\mathbb{E}G = \sum_{\gamma\in\Gamma} q_\gamma G_\gamma \leq 2\sum_{\gamma\in\Gamma} q_\gamma f(d_\gamma) \leq 2f\left(\sum_{\gamma\in\Gamma} q_\gamma d_\gamma\right) = 2f(\mathbb{E}d).$$

□

Remark 6.5.5. The figure 6.2 depicts, for every value of mean distortion, the upper bound of the average information gain. Since the function ϕ has infinite slope at 0, the obtained bound does not prevent Eve from getting a significant information gain (10% say) inducing only a negligible distortion into Bob's conjugate basis measurements. The following theorem 6.5.6 shows that this is only due to the fact that the bound in theorem 6.5.4 is not very sharp and can be substantially improved.

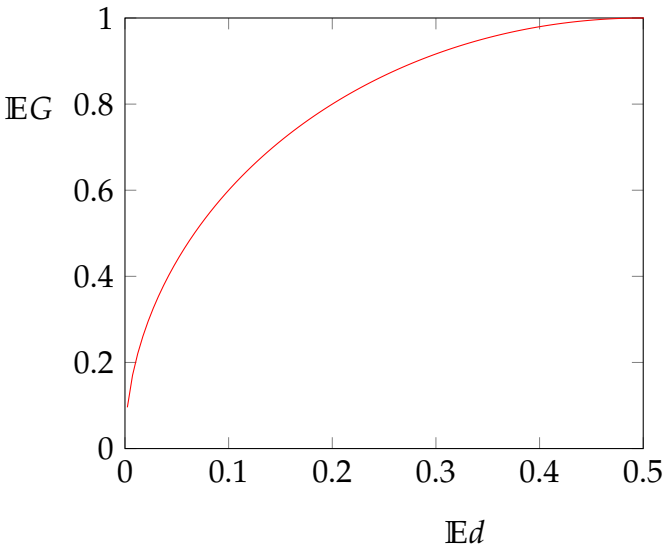


Figure 6.2 – Naive bound $\mathbb{E}G \leq 2\sqrt{\mathbb{E}d(1-\mathbb{E}d)}$.

Recall that the entropy of a probability vector $\mathbf{r}$ on a finite set $\mathbb{X}$ is defined by

$$H(\mathbf{r}) = -\sum_{x\in\mathbb{X}} r_x \log r_x$$

and that the mutual information between the probability vectors $\mathbf{r}$ and $\mathbf{s}$ on the finite sets $\mathbb{X}$ and $\mathbb{Y}$ obtained as marginal probabilities of a joint probability described by the probability vector $\mathbf{w}$ on $\mathbb{X}\times\mathbb{Y}$ is defined by

$$I(\mathbf{r}:\mathbf{s}) = H(\mathbf{r})+H(\mathbf{s})-H(\mathbf{w}).$$

Instead of computing a bound on the raw gain of information, it is more natural to seek a bound on the joint information $I(\mathbf{q} : \mathbf{p})$ between Eve's outcomes $\gamma \in \Gamma$ occurring with probability determined by the probability vector $\mathbf{q} = (q_\gamma)_{\gamma\in\Gamma}$, under the condition that Alice has used the $\mathbf{p} = (1/2, 1/2)$ probability vector to decide which bit to send. This approach yields an improved bound as established in theorem **??** and depicted in figure **??**.

Theorem 6.5.6. *Assuming that Alice encodes in ♯ basis,* $\mathbf{p} = (1/2, 1/2)$*, and* $D^\flat_{0\gamma} = D^\flat_{0\gamma} = d_\gamma$*, then*

$$I(\mathbf{q} : \mathbf{p}) \leq \frac{1}{2} g\left(2\sqrt{\mathbb{E}d(1-\mathbb{E}d)}\right)$$

where $g(z) := (1+z)\log(1+z) + (1-z)\log(1-z)$*, for* $z \in [-1, 1]$.

Proof. Since $\kappa_{t\gamma} = p_t Q_{t\gamma} = q_\gamma \hat{Q}_{\gamma t}$ denotes the joint probability on $\{0, 1\} \times \Gamma$, we compute

$$\begin{aligned} H(\kappa) &= -\sum_{t,\gamma} \kappa_{t\gamma} \log \kappa_{t\gamma} \\ &= -\sum_{t,\gamma} q_\gamma \hat{Q}_{\gamma t} (\log q_\gamma + \log \hat{Q}_{\gamma t}) \\ &= H(q) - \sum_\gamma q_\gamma \sum_t \hat{Q}_{\gamma t} \log \hat{Q}_{\gamma t}. \end{aligned}$$

Since $\hat{Q}_{\gamma 0} + \hat{Q}_{\gamma 1} = 1$, on introducing the parametre $r_\gamma = \hat{Q}_{\gamma 1} - \hat{Q}_{\gamma 1} = \pm G_\gamma \in [-1, 1]$, we can re-express

$$\hat{Q}_{\gamma 0} = \frac{1 + r_\gamma}{2}; \hat{Q}_{\gamma 1} = \frac{1 - r_\gamma}{2}.$$

Expressing now

$$\begin{aligned} I(q : p) &= H(q) + H(p) - H(\kappa) \\ &= H(p) + H(q) - H(q) + \sum_\gamma q_\gamma \sum_t \hat{Q}_{\gamma t} \log \hat{Q}_{\gamma t} \\ &\overset{p=(\frac{1}{2},\frac{1}{2})}{=} \log 2 + \frac{1}{2} \sum_\gamma q_\gamma \left[(1 + r_\gamma) \log \frac{1 + r_\gamma}{2} + (1 - r_\gamma) \log \frac{1 - r_\gamma}{2} \right] \\ &= \frac{1}{2} \sum_\gamma q_\gamma g(r_\gamma). \end{aligned}$$

Observe that g is an even function on $[-1, 1]$, satisfying $g'(z) = \log \frac{1+z}{1-z} > 0$ on $[0, 1[$. Hence g is increasing on $[0, 1[$. Using the bound $G_\gamma \leq 2\sqrt{d_\gamma(1 - d_\gamma)}$ — established in the course of the proof of theorem 6.5.4, — we conclude that $I(\mathbf{q} : \mathbf{p}) = \frac{1}{2}\sum_\gamma q_\gamma g(G_g)$ and because $r_\gamma = \pm G_\gamma$,

$$I(\mathbf{q} : \mathbf{p}) \leq \frac{1}{2} \sum_{\gamma\in\Gamma} q_\gamma g(2\sqrt{d_\gamma(1 - d_\gamma)}).$$

Now the function $h : t \mapsto h(t) := g(2f(t))$ is concave on $[0, 1]$. Jensen's inequality is then used to bound

$$I(\mathbf{q} : \mathbf{p}) = \frac{1}{2} \sum_\gamma q_\gamma g(G_g) \leq \frac{1}{2} h(\mathbb{E}d).$$

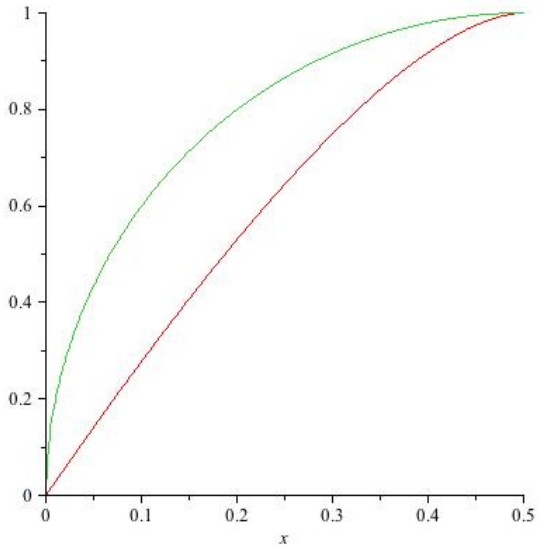


Figure 6.3 – The horizontal axis represents $\mathbb{E}d$; the vertical axis for green curve represents $\mathbb{E}G$ and for the red curve $I(\mathbf{q}:\mathbf{p})$. The curve representing the mutual information $I(\mathbf{q}:\mathbf{p})$ has a finite slope 2 at 0. Therefore, it is impossible to have a substantial gain in the mutual information without a proportional average distortion on Bob's bits.

□

6.5.1 Other issues

Random numbers

ompléter. True random number generation.

Authentication

10, 113] Must be treated after quantum computing.

7

Turing machines, algorithms, computing, and complexity classes

All computers, from Babbage's analytical machine (1833) to the latest model of supercomputer, are based on the same principles. A **universal computer** uses some **input** (a sequence of bits) and a **programme** (a sequence of instructions) to produce an **output** (another sequence of bits.) Universal computers are modelled by **Turing machines.** Never forget however that, in spite of the term "machine" entering its name, a Turing machine is an abstract theoretical scheme that can be laid on paper and help us understanding the flow of elementary logical operations we must carry in order to compute something, but left alone can never compute anything.

Their technological interest is concentrated in the observation made by Turing that a function is **effectively calculable** if its values can be found by some purely mechanical process. We may take "purely mechanical process" literally to mean one which could be carried out by a machine. But we had to wait until the first ENIAC was **physically constructed** to obtain the first output of numbers.

Their theoretical interest is summarised into the **Church-Turing thesis**, tating that every effectively calculable function is a computable function (see defintion 7.2.1 below).

7.1 Deterministic Turing machines

There are several variants of deterministic Turing machines; all of them are equivalent in the sense that a problem solvable by one variant is also solvable by any other variant within essentially the same amount of time (see below, definition **??** and section

7.3.) A Turing machine is a model of computation; it is to be thought as a finite state machine disposing of an infinite scratch space (an external tape [1].) The tape consists of a semi-infinite or infinite sequence of squares, each of which can hold a single symbol. A tape-head can read a symbol from the tape, write a symbol on the tape, and move one square in either direction (for semi-infinite tape, the head cannot cross the origin.) More precisely, a Turing machine is defined as follows.

Definition 7.1.1. A **deterministic Turing machine** is a quadruple $(\mathbb{A}, \mathbb{S}, u, s_0)$ where

1. $\mathbb{A}$ is a finite set, the **alphabet**, containing a particular symbol called the **blank symbol** and denoted by $\sharp$; the alphabet deprived from its blank symbol, denoted $\mathbb{A}_b = \mathbb{A} \setminus \{\sharp\}$, is assumed non-empty,
2. $\mathbb{S}$ is a finite non-empty set, the **states** of the machine, partitioned into the set $\mathbb{S}_i$ of intermediate states and the set $\mathbb{S}_f$ of final states,
3. $D = \{L, R\} \equiv \{-1, 1\}$ is the **displacement set**,
4. $u : \mathbb{A} \times \mathbb{S} \to \mathbb{A} \times \mathbb{S} \times D$ is the **transition function**, and
5. $s_0 \in \mathbb{S}_i$ the **initial state** of the machine.

The set of deterministic Turing machines is denoted by DTM.

The machine is presented an input, i.e. a finite sequence of contiguous non-blank symbols, and either it stops by producing an output, i.e. another finite sequence of symbols, else the programme does never halt.

Example 7.1.2. (A very simple Turing machine) Let $M \in \mathsf{DTM}$ with $\mathbb{A} = \{0, 1, \sharp\}$, $\mathbb{S} = \mathbb{S}_i \cup \mathbb{S}_f$ where $\mathbb{S}_i = \{\mathsf{go}\}$, $\mathbb{S}_f = \{\mathsf{halt}\}$, and transition function $u(a, s) = (a', s', d)$ defined by the following table:

a	s	a'	s'	d
0	go	0	go	L
1	go	1	go	L
$\sharp$	go	$\sharp$	halt	R

If the programme, described by this Turing machine, starts with the head over any non-blank symbol of the input string, it ends with the head over the leftmost non-blank symbol while the string of symbols remains unchanged.

Other equivalent variants of the deterministic Turing machine may have displacement sets with a 0 (do not move) displacement, have their alphabet $\mathbb{A}$ partitioned into external and internal alphabet, etc. The distinction into internal and external alphabet is particularly useful in the case of semi-infinite tape, an internal character $*$, identified as "first symbol", can be used to prevent the head from going outside the tape. It is enough to define $u(*, \mathsf{go}) = (*, \mathsf{go}, R)$.

Notation 7.1.3. If W is a finite set, we denote by $W^* = \cup_{n \in \mathbb{Z}_+} W^n$ and $W^\infty = \partial W = W^{\mathbb{Z}_+}$. Notice that $\mathbb{Z}_+ = \{0, 1, 2, \ldots\} \neq \mathbb{N} = \{1, 2, \ldots\}$ and that $W^0 = \{\emptyset\}$. Elements of W^* are called **words** of finite length over the alphabet W. For every $w \in W^*$, there exists $n \in \mathbb{Z}_+$ such that $w \in W^n$; we denote then by $|W| = n$ the **length** of the word w.

1. Mind that during Turing's times no computer was physically available. The external tape was invented by Alan Turing — who was fascinated by typewriters — as an external storage device.

For every $\alpha \in \mathbb{A}_b^*$, we denote by $\overline{\alpha} \in \mathbb{A}^\infty$ the completion of the word α by blanks, namely $\overline{\alpha} = (\alpha_1, \ldots, \alpha_{|\alpha|}, \sharp, \sharp, \sharp, \ldots)$.

Considering the example 7.1.2, we can, without loss of generality, always assume that the machine starts at the first symbol of the input string $\alpha = \alpha \in \mathbb{A}_b^*$. Starting from $(\alpha, s_0, h_0 = 1)$, successive applications of the transition function U induce a dynamical system on $\mathbb{X} = \mathbb{A}^* \times \mathbb{S} \times \mathbb{Z}$. A configuration is an instantaneous description of the word written on the tape, the internal state of the machine, and the position of the head, i.e. an element of $\mathbb{X}$.

Let $\tau_\alpha = \inf\{n \geq 1 : s_n \in \mathbb{S}_f\}$. The programme starting from initial configuration $(\alpha, s_0, h_0 = 1)$ stops running if $\tau_\alpha < \infty$, it never halts when $\tau_\alpha = \infty$. While $1 \leq n < \tau_\alpha$, the sequence $(\alpha^{(n)}, s_n, h_n)_{n \leq \tau_\alpha}$ is defined by updates of single characters; if, for $0 \leq n < \tau_\alpha$, we have $u(\alpha_{h_n}^{(n)}, s_n) = (a', s', d)$, then $(\alpha^{(n+1)}, s_{n+1}, h_{n+1})$, is defined by

$$\begin{aligned} s_{n+1} &= s' \\ h_{n+1} &= h_n + d \\ \alpha^{(n+1)} &= (\alpha_1^{(n)}, \ldots, \alpha_{h_n-1}^{(n)}, a', \alpha_{h_n+1}^{(n)}, \ldots, \alpha_{|\alpha^{(n)}|}^{(n)}). \end{aligned}$$

If the machine halts at some finite instant, the output is obtained by reading the tape from left to right until the first blank character. The sequence of words $(\alpha^{(n)})_n$ is called a **computational path** or **computational history** starting from α.

7.2 Computable functions and decidable predicates

Every $M \in \mathsf{DTM}$ computes a particular partial function $\phi_M : \mathbb{A}_b^* \to \mathbb{A}_b^*$. Since the value of $\phi_M(\alpha)$ remains undetermined when the programme M does not halt, the function ϕ_M is termed partial because in general $\mathsf{Dom}(\phi_M) \subset \mathbb{A}_b^*$.

Definition 7.2.1. A partial function $f : \mathbb{A}_b^* \to \mathbb{A}_b^*$ is called **computable** if there exists a $M \in \mathsf{DTM}$ such that $\phi_M = f$. In that case, f is said to be computed by the programme M.

Exercise 7.2.2. Show that there exist non-computable functions.

Definition 7.2.3. A **predicate**, P, is a function taking Boolean values 0 or 1. A **language**, L, over an alphabet $\mathbb{A}$ is a subset of $\mathbb{A}_b^*$.

Thus, for predicates P with $\mathsf{Dom}(P) = \mathbb{A}_b^*$, the set $\{\alpha \in \mathbb{A}_b^* : P(\alpha)\}$ is a language. Hence predicates are in bijection with languages.

Definition 7.2.4. A predicate $P : \mathbb{A}_b^* \to \{0, 1\}$ is **decidable**, if the function P is computable.

Let P be a predicate and L the corresponding language. The predicate is decidable if there exists a $M \in \mathsf{DTM}$ such that for every word α, the programme halts after a finite number of steps and

— if $\alpha \in L$, then the machine halts returning 1, and
— if $\alpha \notin L$, then the machine halts returning 0.

Definition 7.2.5. Let $M \in \mathsf{DTM}$ and $s_M, t_M : \mathbb{Z}_+ \to \mathbb{R}_+$ be given functions. If for every $\alpha \in \mathbb{A}_b^*$, the machine stops after having visited at most $s_M(|\alpha|)$ cells, we say that it works in **computational space** s_M. We say that it works in **computational time** t_M if $\tau_\alpha \leq t_M(|\alpha|)$.

7.3 Complexity classes

Computability of a function does not mean effective computability since the computing algorithm can require too much time or space. We say that $r : \mathbb{N} \to \mathbb{R}_+$ is of **polynomial growth** if there exist constants $c, C > 0$ such that $r(n) \leq Cn^c$, for large n. We write symbolically $r(n) = \mathsf{poly}(n)$.

Definition 7.3.1. The **complexity class** P consists of all languages L whose predicates P are **decidable in polynomial time**, i.e. for every L in the class, there exists a machine $M \in \mathsf{DTM}$ such that $\phi_M = P$ and $t_M(|\alpha|) = \mathsf{poly}(|\alpha|)$ for all $\alpha \in \mathbb{A}^*$.

Similarly, we can define the class PSPACE of languages whose predicates are **decidable in polynomial space**. functions computable in polynomial space.

Other complexity classes will be determined in the subsequent sections. Obviously P $\subseteq$ PSPACE.

Conjecture 7.3.2. P $\neq$ PSPACE.

7.4 Non-deterministic Turing machines and the NP class

Definition 7.4.1. A **non-deterministic Turing machine** is a quadruplet $(\mathbb{A}, \mathbb{S}, \mathbf{u}, s_0)$ where $\mathbb{A}$, $\mathbb{S}$ and s_0 are as in definition 7.1.1; $\mathbf{u}$ is now a multivalued function, i.e. there are r different branches $u_i, i = 1, \ldots, r$ and $u_i : \mathbb{A} \times \mathbb{S} \to \mathbb{A} \times \mathbb{S} \times D$. For every pair $(a, s) \in \mathbb{A} \times \mathbb{S}$ there are different possible outputs $(a_i', \sigma_i', d_i)_{i=1,\ldots,r}$, the choice of a particular branch can be done in a non-deterministic way at each moment. All such choices are legal actions. The set of non-deterministic Turing machines is denoted by NTM.

A computational path for a $M \in \mathsf{NTM}$ is determined by a choice of one legal transition at every step. Different steps are possible for the same input. Notice that NTM do not serve as models of practical devices but rather as logical tools for the formulation of problems rather than their solution.

Definition 7.4.2. A language L (or its predicate P) belongs to the NP class if there exists a $M \in \mathsf{NTM}$ such that
— if $\alpha \in L$ (i.e. $P(\alpha) = 1$) for some $\alpha \in \mathbb{A}^*$, then there exists a computational path with $\tau_\alpha \leq \mathsf{poly}(|\alpha|)$ returning 1,

— if $\alpha \notin L$ (i.e. $P(\alpha) = 0$) for some $\alpha \in \mathbb{A}^*$, then there exists no computational path with this property.

It is elementary to show that P $\subseteq$ NP. Clay Institute offers you [2] USD 1 000 000 if you solve the following

Exercise 7.4.3. Is it true that P = NP?

7.5 Probabilistic Turing machine and the BPP class

Definition 7.5.1. Let $\tilde{\mathbb{R}}$ be the set of real numbers computable by a deterministic Turing machine within accuracy 2^{-n} in $\mathrm{poly}(n)$ time. A **probabilistic Turing machine** is a quintuple $(\mathbb{A}, \mathbb{S}, \mathbf{u}, \mathbf{p}, s_0)$ where $\mathbb{A}$, $\mathbb{S}$, $\mathbf{u}$, and s_0 are as in definition 7.4.1 while $\mathbf{p} = (p_1, \ldots, p_r) \in \tilde{\mathbb{R}}_+$, with $\sum_{i=1}^{r} p_i = 1$ is a probability vector on the set of branches of $\mathbf{u}$. All branches correspond to legal actions; at each step, the branch i is chosen with probability p_i, independently of previous choices. The set of probabilistic Turing machine is denoted by PTM.

Each $\alpha \in \mathbb{A}^*$ generates a family of computational paths. The local probability structure on the transition functions induces a natural probability structure on the computational path space. The evolution of the machine is a Markov process with the state space $\mathbb{A}_b^* \times \mathbb{S} \times \mathbb{Z}$ and stochastic evolution kernel determined by the local probability vector $\mathbf{p}$. Hence, any input gives a set of possible outputs each of them being assigned a probability of occurrence. A machine in PTM is also called a **Monte Carlo algorithm**.

Definition 7.5.2. Let $\varepsilon \in]0, 1/2[$. A predicate P (hence a language L) belongs to the BPP class if there exists a $M \in$ BPP such that for any $\alpha \in \mathbb{A}^*$, $\tau_\alpha \leq \mathrm{poly}(|\alpha|)$ and
— if $\alpha \in L$, then $\mathbb{P}(P(\alpha) = 1) \geq 1 - \varepsilon$, and
— if $\alpha \notin L$, then $\mathbb{P}(P(\alpha) = 1) \leq \varepsilon$.

Exercise 7.5.3. Show that the definition of the class does not depend on the choice of ε provided it lies in $]0, 1/2[$.

7.6 Boolean functions and circuits

On the basis of the Church-Turing thesis, a classical computer or classical algorithm is a Turing machine. If we forget the internal functioning of the machine and its internal states, a classical computer can be thought as a "black-box" transforming some input from $\mathbb{A}^m$ into outputs from $\mathbb{A}^n$, for appropriate integers m and n.

To compute a function on a computer, a real-valued function on reals for the sake of definiteness, means to
— model this function by some discretised approximation,

2. http://www.claymath.org/millennium/

— express the computation as a sequence of computable functions,
— physically implement the elementary Turing machines corresponding to the aforementioned computable functions.

Notation 7.6.1. For $d \in \mathbb{N}$ and $\mathbb{Z}_d = \{0, \dots, d-1\}$, we denote by $x = \langle\, x_{n_1} \cdots x_0 \,\rangle_d$ the mapping defined by

$$\mathbb{Z}_d^n \ni (x_0, \dots, x_n) \mapsto x = \langle\, x_n \cdots x_0 \,\rangle_d = \sum_{k=0}^{n-1} x_k d^k \in \mathbb{Z}_{d^n}.$$

Since conversely for every $x \in \mathbb{Z}_{d^n}$ the sequence $(x_0, \dots, x_n) \in \mathbb{Z}_d^n$ is uniquely determined, we identify x with the sequence of its digits. For $d = 2$ we omit the basis subscript and we write simply $\langle\, \cdot \,\rangle$

If rest of this subsection, the symbol $\mathbb{A}$ will stand for $\mathbb{A} = \mathbb{Z}_2 = \{0, 1\}$.

Definition 7.6.2. Let $f : \mathbb{A}^m \to \mathbb{A}^n$ be a Boolean function of m entries and n outputs. Let $\mathbf{B}$ be a fixed set of Boolean functions of different arities. We call **Boolean circuit** of f in terms of the basis $\mathbf{B}$ a representation of f in terms of functions from $\mathbf{B}$.

Example 7.6.3. The list of all possible unary ($d = 1$) and binary ($d = 2$) Boolean functions with one output $f : \mathbb{A}^d \to \mathbb{A}$.

1. For $d = 1$ there are 4 different functions:

x	**0**	$\mathbb{1}$	NOT	**1**
0	0	0	1	1
1	0	1	0	1

2. For $d = 2$ there are 16 different functions:

x_1	x_0	**0**	AND		x_1		x_0	XOR	OR	NOR	NXOR	$\overline{x}_0$		$\overline{x}_1$		NAND	**1**
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Example 7.6.4. (Addition with carry of 2 binary 2-digit numbers.) Let $x = \langle\, x_1 x_0 \,\rangle$ and $y = \langle\, y_1 y_0 \,\rangle$. We wish to express $z = x + y = \langle\, z_2 z_1 z_0 \,\rangle$ in terms of Boolean functions in $\mathbf{B} = \{\text{XOR}, \text{AND}\} = \{\oplus, \wedge\}$. The truth table is given in table 7.1. We verify immediately that:

$$\begin{aligned} z_0 &= x_0 \oplus y_0 \\ z_1 &= (x_0 \wedge y_0) \oplus (x_1 \oplus y_1) \\ z_2 &= (x_1 \wedge y_1) \oplus [(x_1 \oplus y_1) \wedge (x_0 \wedge y_0)] \end{aligned}$$

Consequently, the Boolean circuit is depicted in figure **??**.

A basis $\mathbf{B}$ is **complete** if any Boolean function f can be constructed as a circuit with Boolean functions from $\mathbf{B}$.

x_1	x_0	y_1	y_0	z_2	z_1	z_0
0	0	0	0	0	0	0
0	1	0	0	0	0	1
1	0	0	0	0	1	0
1	1	0	0	0	1	1
0	0	0	1	0	0	1
0	1	0	1	0	1	0
1	0	0	1	0	1	1
1	1	0	1	1	0	0
0	0	1	0	0	1	0
0	1	1	0	0	1	1
1	0	1	0	1	0	0
1	1	1	0	1	0	1
0	0	1	1	0	1	1
0	1	1	1	1	0	0
1	0	1	1	1	0	1
1	1	1	1	1	1	0

Table 7.1 – The truth table of the Boolean function $\mathbb{A}^4 \to \mathbb{A}^3$ implementing the addition with carry of two binary 2-digit numbers.

Basis of Boolean functions vs. logical gates

Every **physically realised** computer uses a particular complete basis **B**. The corresponding set of realised Boolean functions in **B** are called **logical gates**. In other terms, logical gates are the physical electronic circuits having the appropriate number of input electrodes and one output electrode. Bit values 0 or 1 correspond to physical voltages staying below a certain threshold voltage or exceeding it. Arbitrary Boolean functions are computed by physically connecting inputs and outputs so that the resulting circuit implements the sought Boolean function.

The "miracle" of nowadays classical computer technology is that we can totally forget the physical substratum of logical gates and think of them as abstract Boolean functions.

Example 7.6.5. $\{\text{NOT}, \text{OR}, \text{AND}\}$ is a complete but redundant basis; $\{\text{NOT}, \text{OR}\}$, $\{\text{NOT}, \text{AND}\}$, and $\{\text{AND}, \text{XOR}\}$ are complete minimal bases.

Definition 7.6.6. The minimal number of gates from **B** needed to compute f, denoted by $c_B(f)$, is **circuit complexity** of f in **B**.

The function implementing the addition with carry of table 7.1 over the basis $\mathbf{B} = \{\text{AND}, \text{XOR}\}$, has circuit complexity 7.

Any DTM can be implemented by circuits.

Classical computers are based on gates {XOR, AND} for example. It is easily shown that these gates are irreversible. Therefore it is intuitively clear why classical computers can produce information. What is much less intuitively clear is how quantum processes can produce information since they are reversible (unitary).

In 1973, BENNETT predicted that it is possible to construct reversible universal gates. In 1982, FREDKIN exemplifies such a reversible gate. **Fredkin's gate** is a 3 inputs - 3 outputs gate, whose truth tableau is given in table **??**. This gate produces

Input			Output		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	0	1
1	0	0	1	0	0
1	0	1	0	1	1
1	1	0	1	1	0
1	1	1	1	1	1

Table 7.2 – The truth table of Fredkin's gate. We remark that $c' = c$ and if $c = 0$ then ($a' = a$ and $b' = b$) else ($a' = b$ and $b' = a$.)

both AND (since inputs $0, x, y$ return outputs $x \wedge y, \overline{x} \wedge y, x$) and NOT gates (since inputs $1, 0, x$ return outputs $\overline{x}, x, x$.) The gates AND and NOT forming a complete basis for Boolean circuits, the universality of Freidkin's gate is established.

In 1980, BENIOFF describes how to use quantum mechanics to implement a Turing machine, in 1982, FEYNMAN proves that there does not exist a Turing machine (either deterministic or probabilistic) on which quantum phenomena can be efficiently simulated; only a quantum Turing machine could do so. Finally, in 1985, DEUTSCH constructs (on paper) a universal quantum Turing machine.

7.7 Quantum Turing machines

Definition 7.7.1. et $\tilde{\mathbb{C}}$ be the set of complex numbers whose real and imaginary part can be computed by a deterministic algorithm with precision 2^{-n} within $\mathrm{poly}(n)$ time. A **pre-quantum Turing machine** is a quadruple $(\mathbb{A}, \mathbb{S}, c, s_0)$, where $\mathbb{A}, \mathbb{S}, s_0$ are as for a deterministic machine and $c : (\mathbb{A} \times \mathbb{S})^2 \times D \to \tilde{C}$, where D is the displacement set.

Any configuration x of the machine is represented by a triple $x = (a, s, h) \in \mathbb{A}^* \times \mathbb{S} \times \mathbb{Z} = \mathbb{X}$. The quantum configuration space $\mathbb{H}$ is decomposed into $\mathbb{H}_T \otimes \mathbb{H}_S \otimes \mathbb{H}_H$, where the indices $T, \mathbb{S}, H$ stand respectively for tape, internal states, and head. The space $\mathbb{H}$ is spanned by the orthonormal system $(|\,\psi\,\rangle)_{\psi\in\mathbb{X}} = (|\,ash\,\rangle)_{a\in\mathbb{A}^*, s\in\mathbb{S}, h\in\mathbb{Z}}$.

Define now onservables having $(|\,a\,\rangle)_{a\in\mathbb{A}^*}$, $(|\,s\,\rangle)_{s\in\mathbb{S}}$, and $(|\,h\,\rangle)_{h\in\mathbb{Z}}$ as respective eigenvectors. To do so, identify the sets $\mathbb{A}$ with $\{0, \ldots, |\mathbb{A}| - 1\}$ and $\mathbb{S}$ with $\{0, \ldots, |\mathbb{S}| -$

1}. Denoty by $\hat{T}$, $\hat{\mathbb{S}}$, and $\hat{H}$ the self-adjoint operators describing these observables, i.e.

$$\begin{aligned}\hat{\mathbb{S}} &= \sum_{s=0}^{|\mathbb{S}|-1} s|\,s\,\rangle\langle\,s\,| \\ \hat{H} &= \sum_{h\in\mathbb{Z}} h|\,h\,\rangle\langle\,h\,| \\ \hat{T} &= \otimes_{i\in\mathbb{Z}}\hat{T}_i \text{ where } \hat{T}_i = \sum_{a=0}^{|\mathbb{A}|-1} a|\,a\,\rangle\langle\,a\,|.\end{aligned}$$

Due to the linearity of quantum flows, it is enough to describe the flow on the basis vectors $\psi = |\,\alpha, s, h\,\rangle; a \in \mathbb{A}^{\mathbb{Z}}, s \in \mathbb{S}, h \in \mathbb{Z}$. The machine is prepared at some initial pure state $\psi = |\,\alpha, s, h\,\rangle$, with α a string of contiguous non blank symbols and we assume that the time is discretised:

$$|\,\psi_n\,\rangle = U^n|\,\psi\,\rangle.$$

Suppose that the displacement set D reads $\{-1, 0, 1\}$. Then for $\psi = |\,\alpha, s, h\,\rangle$ and $\psi' = |\,\alpha', s', h'\,\rangle$

$$\begin{aligned}U_{\psi,\psi'} &= \langle\,\alpha', s', h'\,|\,U\alpha, s, h\,\rangle \\ &= [\delta_{h',h+1}c(\alpha_h, s, \alpha'_h, s', 1) \\ &\quad +\delta_{h',h}c(\alpha_h, s, \alpha'_h, s', 0) \\ &\quad +\delta_{h',h-1}c(\alpha_h, s, \alpha'_h, s', -1)]\prod_{j\in\mathbb{Z}\setminus\{h\}}\delta_{\alpha_j,\alpha'_j}.\end{aligned}$$

Definition 7.7.2. pre-quantum Turing machine is called a **quantum Turing machine** if the function c is such that the operator U is unitary.

Exercise 7.7.3. Find the necessary and sufficient conditions on the function c so that U is unitary.

To halt the machine, we can not perform intermediate measurements of the composite state because quantum mechanical measurement perturbs the system. To proceed, suppose that $\mathbb{S}_f = \{\mathsf{halt}\} \equiv \{0\}$ and introduce a **halting flag** operator $\hat{F} = |\,0\,\rangle\langle\,0\,|$. Once the state s is set to 0, the function c is such that U does not any longer change either the state s or the result of the computation.

A **predicate** is a projection operator $P_\alpha = |\,\alpha\,\rangle\langle\,\alpha\,|$. Let the machine evolve for some time n: it is at the state $|\,\psi_n\,\rangle = U^n|\,\psi\,\rangle$. Perform the measurement $\langle\,\psi_n\,|\,P_\alpha \otimes \hat{F} \otimes I\psi_n\,\rangle = p \in [0, 1]$.

Definition 7.7.4. A language L belongs to the BQP complexity class if there is a machine $M \in \mathsf{QTM}$ such that
— if $\alpha \in L$, then the machine accepts with probability $p > 2/3$,
— if $\alpha \notin L$, then the machine rejects with probability $p > 2/3$,
within a running time $\mathsf{poly}(|\alpha|)$.

Theorem 7.7.5. P $\subseteq$ BPP $\subseteq$ BQP $\subseteq$ PSPACE.

8

Elements of quantum computing

We arrived at the point where an answer must be given to the question "what is a quantum computer?" One could possibly say that a quantum computer is one whose operation governed by quantum mechanics. But classical law is subsumed under quantum law. Hence classical computers operate already under quantum mechanical laws. Nevertheless, your laptop is not a quantum computer.

If we admit that the Church-Turing thesis extends to quantum system, a **universal quantum computer** should be a quantum Turing machine. Recalling the definitions 7.7.1 and 7.7.2 given in the last chapter, a quantum computer is a physical system whose operation exploits certain very special transformations — quantum unitary transformations — of internal states to perform all intermediate computations more efficiently than a classical computer. At the final stage, some irreversible operation — measurement — is performed on the system. It should be stressed however that this definition, although largely advocated by computer scientists, is quite restrictive. The present [1] technology allows to solve rather elementary instances of potentially difficult problems. For example, a quantum computer can factor 21 (see [106]), not very an algorithmically outstanding achievement indeed. The hope is that technology will evolve quite rapidly to allow factoring much larger composite integers, a problem that could be solved in polynomial time on a general quantum computer, should there exist a sufficiently powerful enough one.

A looser definition of a quantum computer/algorithm departs from the category of universal quantum computers to encompass special purpose machines. These machines exploit quantum phenomena (without classical counterpart, like quantum tunneling) to propose much faster simulation algorithms for solving optimisation problems. The commercially available computer bearing the brand name D-WAVE falls into this category.

1. End of 2017.

In this chapter, we stick however to the notion of universal quantum computer and examine the possible quantum logical gates that must be composed to produce algorithmically sensible results.

8.1 Data representation on quantum computer

In the sequel, $\mathbb{B}$ denotes the set $\{0,1\}$ with cardinality 2; elements of $\mathbb{B}$ will be denoted $a, b, x \in \mathbb{B}$ and called **bits**. Elements of $\mathbb{B}^n$ are n-bit strings; they are meant to denote $b_1 \cdots b_n$ or $b_0 \cdots b_{n-1}$ or written in reverse order $b_n \cdots b_1$ or $b_{n-1} \cdots b_0$, with $b_i \in \mathbb{B}$. The indexing set and the order will be specified on each occurrence.

The quantum analog of the two-element set $\mathbb{B}$ is the Hilbert space $\mathbb{H} = \mathbb{C}^2$ of dimension 2. Rays $|\psi\rangle \in \mathbb{H}$, with $\|\psi\| = 1$, are called **qubits** and are associated with pure states $\rho = |\psi\rangle\langle\psi|$. Similarly, arrays of n bits are denoted by $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{B}^n$; arrays of n qubits by $|\psi\rangle = |\psi_1 \cdots \psi_n\rangle \in \mathbb{H}^{\otimes n}$. The **canonical basis** [2] of $\mathbb{H}$ is written in Dirac's notation $(|\varepsilon_0\rangle, |\varepsilon_1\rangle)$, where $|\varepsilon_0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ and $|\varepsilon_1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$. Therefore $|\varepsilon_0\rangle$ and $|\varepsilon_1\rangle$ correspond to qubits. Since an arbitrary unit vector $|\psi\rangle \in \mathbb{H}$ can be decomposed in the canonical basis, any qubit can be written as the linear superposition of basis qubits: $|\psi\rangle = \sum_{i=0}^{1} \psi_i |\varepsilon_i\rangle$.

The quantum analog of n-bit strings are tensor products of n qubits, denoted as $|\Psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle = |\psi_1 \cdots \psi_n\rangle$. All types of conventions regarding the indexing set or the order of the indices in force for classical n-bit strings explained above, will be in force here, i.e. $|\Psi\rangle$ is meant to denote $|\psi_1 \cdots \psi_n\rangle$ or $|\psi_0 \cdots \psi_{n-1}\rangle$ or $|\psi_n \cdots \psi_1\rangle$ or $|\psi_{n-1} \cdots \psi_0\rangle$. The indexing set and the order will be specified on each occurrence.

Some care must be paid to the notational issues since a systematic notation can greatly simplify expressions.

Notation 8.1.1. **Digits and strings:** If $\mathbb{D}$ is a finite alphabet of cardinality D, then $\mathbb{D}$ will be identified with $\mathbb{D} = \{0, \ldots, D-1\}$; elements of $\mathbb{D}$ are called digits (in base D). For $n \in \mathbb{N}_>$, the set $\mathbb{D}^n$ denotes the set of strings of length n out of the alphabet $\mathbb{D}$. $\mathbb{D}^0$ contains the empty string (of zero length) and we denote $\mathbb{D}^* = \cup_{n\in\mathbb{N}}\mathbb{D}^n$ and $\mathbb{D}^+ = \cup_{n\in\mathbb{N}_>}\mathbb{D}^n$. The special case of the set of cardinality $D = 2$ is denoted $\mathbb{B}$ and its elements are called **bits**.

Numerical values and binary representations: Various conventions can be used to display an n-bit string:

$$\mathbf{b} = b_{n-1} \cdots b_0, \mathbf{b} = b_n \cdots b_1, \mathbf{b} = b_0 \cdots b_{n_1}, \mathbf{b} = b_1 \cdots b_n.$$

For every $n \in \mathbb{N}_>$ there are two natural mappings

$$\mathbb{B}^n \ni \mathbf{b} \mapsto \mathsf{num}(\mathbf{b}) \in \{0, \ldots, 2^n - 1\} \text{ and } \{0, \ldots, 2^n - 1\} \ni k \mapsto \mathsf{rep}(k) \in \mathbb{N}^n,$$

2. Note that in the quantum computer science community, the canonical basis is often called the **computational basis**; we don't find necessary to depart from the term canonical basis used by mathematicians.

defined by

$$\mathbf{b} = b_{n-1}\cdots b_0 \mapsto \mathsf{num}(\mathbf{b}) = \sum_{k=0}^{n-1} b_k 2^k$$

$$l \mapsto \mathsf{rep}(l) = l_{n-1}\cdots l_0, \text{ s.t. } \sum_{k=0}^{n-1} l_k 2^k = l.$$

Often, $\mathsf{num}(b_{n-1}\cdots b_0)$ will be denoted $\langle b_{n-1}\cdots b_0\rangle$. When the reverse order $\mathbf{b} = b_1\cdots b_n$ is used to represent the string, then $L = \mathsf{num}(\mathbf{b}) = \sum_{k=1}^{n} b_k 2^{n-k}$ and $\frac{L}{2^n} = \langle 0.b_1\ldots b_n\rangle$.

Tensor products of qubits: It will prove convenient to simplify further Dirac's notation by writing $|\,0\,\rangle$ and $|\,1\,\rangle$ instead of $|\,\varepsilon_0\,\rangle$ and $|\,\varepsilon_1\,\rangle$, i.e. use the indices of the basis to label the unit vectors[3]. Accordingly, the notation of the standard basis $(|\,\varepsilon_{b_{n-1}}\cdots\varepsilon_{b_0}\,\rangle)_{\mathbf{b}\in\mathbb{B}^n}$ of $\mathbb{H}^{\otimes n}$ will be simplified into $(|\,b_{n-1}\cdots b_0\,\rangle)_{\mathbf{b}\in\mathbb{B}^n}$. Letting $x = \langle b_{n-1}\cdots b_0\rangle = \sum_{m=0}^{n-1} b_m 2^m \in \{0,\ldots,2^n-1\}$; we can now index the standard basis of $\mathbb{H}^{\otimes n}$ by $(|\,x\,\rangle)_{x\in\{0,\ldots,2^n-1\}}$. Hence, we can decompose

$$\mathbb{H}^{\otimes n} \ni |\,\Psi\,\rangle = \sum_{x=0}^{2^n-1} \Psi_x |\,x\,\rangle.$$

8.2 Classical and quantum gates and circuits

A **classical circuit** implements a Boolean mapping $f : \mathbb{B}^n \to \mathbb{B}^n$ by using elementary gates of small arities[4], chosen from a family G of gates. A **quantum circuit** implements a unitary mapping $U : \mathbb{H}^{\otimes n} \to \mathbb{H}^{\otimes n}$ by using unitary elementary gates of small arities[5], chosen from a family G.

Definition 8.2.1. et $U : \mathbb{H}^{\otimes n} \to \mathbb{H}^{\otimes n}$ for some n and G be a fixed family of unitary operators of different arities. A **quantum circuit** over G is a product of operators from G acting on appropriate qubit entries.

It is usually assumed that G is closed under inversion.

Definition 8.2.2. Let $V : \mathbb{H}^{\otimes n} \to \mathbb{H}^{\otimes n}$ be a unitary operator. This operator is said to be **realised** by a unitary operator $W : \mathbb{H}^{\otimes N} \to \mathbb{H}^{\otimes N}$, with $N \geq n$ entries, acting on n qubits and $N-n$ ancillary qubits, if for all $|\,\xi\,\rangle \in \mathbb{H}^{\otimes n}$,

$$W(|\,\xi\,\rangle \otimes |\,0^{N-n}\,\rangle) = (V|\,\xi\,\rangle) \otimes |\,0^{N-n}\,\rangle.$$

Ancillary qubits correspond to some memory in a fixed initial state we borrow for intermediate computations that is returned into the same state. Returning ancillary

3. Beware of the fact that although $|\,\varepsilon_0+\varepsilon_1\,\rangle$ represents a perfectly legal — although not normalised —vector of $\mathbb{H}$, the notation $|\,0+1\,\rangle$ is meaningless!
4. usually acting on $\mathcal{O}(1)$ bits.
5. usually acting on $\mathcal{O}(1)$ qubits.

qubits into the same state can be relaxed. What cannot be relaxed is that ancilla must not be entangled with the n qubits (it must remain in tensor form); otherwise the anicllary subsystem could not be forgotten.

Quantum circuits are supposed to be more general than classical circuits. However, arbitrary Boolean circuits cannot be considered as classical counterparts of quantum ones because the classical analogue of a unitary operator on $\mathbb{H}^{\otimes n}$ is an invertible map on $\mathbb{B}^n$, i.e. a permutation $\pi \in S_{2^n}$. Since to any n-bit array $\xi = (\xi_1 \cdots \xi_n) \in \mathbb{B}^n$ corresponds a basis vector $|\,\xi\,\rangle = |\,\xi_1 \cdots \xi_n\,\rangle \in \mathbb{H}^{\otimes n}$, to every permutation $\pi \in S_{2^n}$ naturally corresponds a unitary operator $\hat{\pi}$, defined by

$$\hat{\pi}|\,\xi\,\rangle = |\,\pi(\xi)\,\rangle,$$

with $\hat{\pi}^* = \hat{\pi}^{-1} = \widehat{\pi^{-1}}$. Hence we can define:

Definition 8.2.3. Let $G \subseteq S_{2^n}$. A **reversible circuit** over G is a sequence of permutations from G.

An arbitrary Boolean function $F : \mathbb{B}^m \to \mathbb{B}^n$ can be extended to a function $F_\oplus : \mathbb{B}^{m+n} \to \mathbb{B}^{m+n}$, defined by

$$F_\oplus(x, y) = (x, y \oplus F(x)),$$

where the symbol $\oplus$ in the right hand side stands for the bit-wise addition modulo 2. It is easily checked that $F_\oplus$ is a permutation. Moreover $F_\oplus(x, 0) = (x, F(x))$.

Notice that 2-bit permutation gates do not suffice the realise all functions of the form $F_\oplus$. On the contrary $G = \{\text{NOT}, \Lambda\}$ with $\Lambda : \mathbb{B}^3 \to \mathbb{B}^3$ the **Toffoli gate**, defined by $\Lambda(x, y, z) = (x, y, z \oplus (x \wedge y))$, is a basis.

8.3 Approximate realisation

There are uncountably many unitary operators $U : \mathbb{H}^{\otimes n} \to \mathbb{H}^{\otimes n}$. Hence if a quantum computer is to be constructed, the notion of exact realisation of a unitary operator must be weakened to an approximate realisation. The same **rationale** prevails also in classical computing, instead of all real functions (uncountably many), only Boolean functions are implemented.

Lemma 8.3.1. *An arbitrary unitary operator $U : \mathbb{C}^m \to \mathbb{C}^m$ can be represented as a product $V = \prod_{i=1}^{m(m-1)/2} V^{(i)}$ of matrices of the form*

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \begin{pmatrix} a & b \\ c & d \end{pmatrix} & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{U}(2).$$

Moreover, the sequence of matrices appearing in the product can be explicitly constructed in a running time $\mathcal{O}(m^3)\,poly(\log(1/\delta))$ *where* $\delta = \|U - V\|$.

Proof: An exercise if one recalls that for all $c_1, c_2 \in \mathbb{C}$, there exists a unitary operator $W \in \mathbf{U}(2)$ such that

$$W \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} \sqrt{|c_1|^2 + |c_2|^2} \\ 0 \end{pmatrix}.$$

□

Basic properties of the operator norm are recalled below:

$$\begin{aligned} \|XY\| &\leq \|X\|\|Y\| \\ \|X\| &= \|X\| \\ \|U\| &= 1 \\ \|X \otimes Y\| &= \|X\|\|Y\|, \end{aligned}$$

where X and Y are arbitrary operators and U is a unitary.

Definition 8.3.2. A unitary operator U' **approximates** a unitary operator U within δ if $\|U - U'\| \leq \delta$.

Lemma 8.3.3. *If a unitary* U' *approximates a unitary* U *within* δ*, then* U'^{-1} *approximates* U^{-1} *within* δ.

Proof: Since $U'^{-1}(U' - U)U^{-1} = U^{-1} - U'^{-1}$, it follows that $\|U^{-1} - U'^{-1}\| \leq \|U' - U\| \leq \delta$. □

Lemma 8.3.4. *If unitary operators* $(U'_k)_{k=1,\ldots,L}$ *approximate unitary operators* $(U_k)_{k=1,\ldots,L}$ *within* δ_k*, then* $U' = U'_L \cdots U'_1$ *approximates* $U = U_L \cdots U_1$ *within* $\sum_{k=1}^{L} \delta_k$.

Proof: $\|U'_2U'_1 - U_2U_1\| \leq \|U'_2(U'_1 - U_1) + (U'_2 - U_2)U_1\| \leq \delta_1 + \delta_2$. □

Definition 8.3.5. A unitary operator $U : \mathbb{H}^{\otimes n} \to \mathbb{H}^{\otimes n}$ **is approximated** by a unitary operator $U : \mathbb{H}^{\otimes N} \to \mathbb{H}^{\otimes N}$, with $N \geq n$, within δ if for all $|\,\xi\,\rangle \in \mathbb{H}^{\otimes n}$

$$\|U'(|\,\xi\,\rangle \otimes |\,0^{N-n}\,\rangle) - U|\,\xi\,\rangle \otimes |\,0^{N-n}\,\rangle\| \leq \delta\|\xi\|.$$

Definition 8.3.6. For every unitary operator $U : \mathbb{H}^{\otimes n} \to \mathbb{H}^{\otimes n}$ there exists a unitary operator $C(U) : \mathbb{H} \otimes \mathbb{H}^{\otimes n} \to \mathbb{H} \otimes \mathbb{H}^{\otimes n}$, called the **controlled-U operator**, defined for all $|\,\xi\,\rangle \in \mathbb{H}^{\otimes n}$ by

$$C(U)|\,\varepsilon\,\rangle \otimes |\,\xi\,\rangle = \begin{cases} |\,\varepsilon\,\rangle \otimes |\,\xi\,\rangle & \text{if } \varepsilon = 0 \\ |\,\varepsilon\,\rangle \otimes U|\,\xi\,\rangle & \text{if } \varepsilon = 1 \end{cases}$$

Similarly, multiply controlled-U $C^k(U) : \mathbb{H}^{\otimes k} \otimes \mathbb{H}^{\otimes n} \to \mathbb{H}^{\otimes n} \otimes \mathbb{H}^{\otimes n}$, is defined by

$$C^k(U)|\,\varepsilon_1 \cdots \varepsilon_k\,\rangle \otimes |\,\xi\,\rangle = \begin{cases} |\,\varepsilon_1 \cdots \varepsilon_k\,\rangle \otimes |\,\xi\,\rangle & \text{if } \varepsilon_1 \cdots \varepsilon_k = 0 \\ |\,\varepsilon_1 \cdots \varepsilon_k\,\rangle \otimes U|\,\xi\,\rangle & \text{if } \varepsilon_1 \cdots \varepsilon_k = 1 \end{cases}$$

Example 8.3.7. Let $\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ be the unitary operator corresponding to the classical NOT gate. Then $C^2(\sigma_1) = \hat{\Lambda}$, where Λ is the Toffoli gate.

Definition 8.3.8. The set

$$G = \{H, K, K^{-1}, C(\sigma_1), C^2(\sigma_1)\},$$

with $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ (Hadamard gate) and $K = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, is the (complete) **basis of standard gates**.

Theorem 8.3.9. *Any unitary operator $U : \mathbb{H}^{\otimes n} \to \mathbb{H}^{\otimes n}$ can be approximated within δ by a poly$(\log(1/\delta))$-size circuit over the basis of standard gates using ancillary qubits. There is a poly(n)-time algorithm describing the construction of the approximating circuit.*

Proof: A simple fact, once you have solved the exercise 8.3.10 □

Exercise 8.3.10. Let $\sigma_{0,\ldots,3}$ be the 3 Pauli matrices augmented by the identity matrix, H the Hadamard gate, and $\Phi(\phi) = \begin{pmatrix} 1 & 0 \\ 0 & \exp(2i\phi) \end{pmatrix}$.

1. Show that if $A \in \mathcal{M}_2(\mathbb{C})$ with $A^2 = \mathbb{1}$ and $\phi \in \mathbb{R}$, then
$$\exp(i\phi A) = \cos\phi\sigma_0 + i\sin\phi A.$$
2. Let $R_j(\theta) = \exp(-i\frac{\theta}{2}\sigma_j)$, for $j = 1, 2, 3$ and $R_{\hat{n}}(\theta) = \exp(-i\frac{\theta}{2}\hat{n}\cdot\vec{\sigma})$, where $\hat{n} = (N_1, n_2, n_3)$ with $n_1^2 + n_2^2 + n_3^2 = 1$ and $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$. Express $R_j(\theta)$ and $R_{\hat{n}}(\theta)$ on the basis $\sigma_0, \ldots, \sigma_3$.
3. Show that $H = \exp(i\phi)R_1(\alpha)R_3(\beta)$, for some ϕ, α, β to be determined.
4. If $|\,\xi\,\rangle \in \mathbb{C}^2$ is a ray represented by a vector of the Bloch sphere $\mathbb{S}^2 = \{x \in \mathbb{R}^3 : \|x\|_2 = 1\}$, show that
$$R_{\hat{n}}(\theta)|\,\xi\,\rangle = |\,T_{\hat{n}}(\theta)x\,\rangle$$
where $T_{\hat{n}}(\theta)x$ is the rotation of x around $\hat{n}$ by an angle θ.
5. Show that every $U \in \mathbf{U}(2)$ can be written as
$$U = \exp(i\alpha)R_{\hat{n}}(\theta)$$
for some $\alpha, \theta \in \mathbb{R}$.
6. Show that every $U \in \mathbf{U}(2)$ can be written as
$$U = \exp(i\alpha)R_3(\beta)R_2(\gamma)R_3(\delta)$$
for some $\alpha, \beta, \gamma, \delta \in \mathbb{R}$.
7. Suppose that $\hat{m}$ and $\hat{n}$ are two not parallel vectors of $\mathbb{S}^2$. Show that every $U \in \mathbf{U}(2)$ can be written as
$$U = \exp(i\alpha)R_{\hat{n}}(\beta_1)R_{\hat{m}}(\gamma_1)R_{\hat{n}}(\beta_2)R_{\hat{m}}(\gamma_2)\cdots.$$
8. Establish identities
$$\begin{aligned} H\sigma_1 H &= \sigma_3 \\ H\sigma_2 H &= -\sigma_2 \\ H\sigma_3 H &= \sigma_1 \\ H\Phi(\frac{\pi}{8})H &= \exp(i\alpha)R_1(\frac{\pi}{4}) \end{aligned}$$
for some α.

8.4 Examples of quantum gates

8.4.1 The Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

$$H|\, b\,\rangle = \frac{1}{\sqrt{2}}((-1)^b|\, b\,\rangle + |\, 1-b\,\rangle), b \in \mathbb{B}.$$

$$H^{\otimes 3}|\, 000\,\rangle = \frac{1}{\sqrt{8}} \sum_{x=0}^{7} |\, x\,\rangle.$$

More generally, if $x = \langle x_{n-1} \cdots x_0 \rangle$, with $x_i \in \mathbb{B}$, we have

$$H^{\otimes n}|\, x\,\rangle = \sum_{y=0}^{2^n-1} (-1)^{x\cdot y}|\, y\,\rangle,$$

where $x \cdot y = \sum_{i=0}^{n-1} x_i y_i$.

8.4.2 The phase gate

$$\Phi(\phi) = \begin{pmatrix} 1 & 0 \\ 0 & \exp(2i\phi) \end{pmatrix}.$$

$$\Phi(\phi)|\, b\,\rangle = \exp(2ib\phi)|\, b\,\rangle$$

$$\Phi(\frac{\pi}{4} + \frac{\phi}{2}) H \Phi(\theta) H|\, 0\,\rangle = \cos\theta|\, 0\,\rangle + \exp(i\phi)\sin\theta|\, 1\,\rangle.$$

Note that the gate K appearing in the basis of standard gates reads $K = \Phi(\pi/4)$.

8.4.3 Controlled-NOT gate

$$C(\sigma_1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

For any $x \in \mathbb{B}$, $C(\sigma_1)|\, x0\,\rangle = |\, xx\,\rangle$, but for arbitrary $|\, \psi\,\rangle = \alpha|\, 0\,\rangle + \beta|\, 1\,\rangle$,

$$C(\sigma_1)|\, \psi 0\,\rangle = \alpha|\, 00\,\rangle + \beta|\, 11\,\rangle \neq |\, \psi\psi\,\rangle.$$

8.4.4 Controlled-phase gate

$$C(\Phi(\phi)) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \exp(2i\phi) \end{pmatrix}.$$

For $x, y \in \mathbb{B}$,

$$C(\Phi(\phi))|\, xy \,\rangle = \exp(2i\phi xy)|\, xy \,\rangle.$$

8.4.5 The quantum Toffoli gate

For all $x, y, z \in \mathbb{B}$,

$$C^2(\sigma_3)|\, xyz \,\rangle = |\, x, y, (x \wedge y) \oplus z \,\rangle.$$

Suppose that $f : \mathbb{B}^m \to \mathbb{B}^n$ is a Boolean function, implemented by the unitary operator $U_f : \mathbb{H}^{\otimes(n+m)} \to \mathbb{H}^{\otimes(n+m)}$. If $|\, \psi \,\rangle = \frac{1}{2^{m/2}} \sum_{b_1,\ldots,b_m \in \mathbb{B}} |\, b_1, \ldots, b_m \,\rangle$ then

$$U_f|\, \psi \,\rangle \otimes |\, 0^n \,\rangle = \frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} |\, x, f(x) \,\rangle.$$

Hence computing **simultaneously** all values of f over its domain of definition requires the same computational effort as computing the value over a singleton of the domain. This remark is a manifestation of the **massive parallelism** of quantum computers and explains the tremendous gain in their computational power compared to classical ones.

9

Error correcting codes, classical and quantum

10

The Shor's factoring algorithm

The factoring algorithm, presented by Peter Shor at the International Congress of Mathematicians held in Zürich in 1994 — nowadays known as Shor's algorithm — is an algorithm allowing the solve the integer factorisation problem of a large integer n into prime components in a polynomial time in the number of digits $N = \log n$.

The algorithm can be split into 4 subroutines that present an interest *per se*:
— quantum Fourier transform,
— phase estimation,
— order determination,
— factoring.

10.1 Quantum Fourier transform (QFT)

The quantum Fourier transform can be seen as a generalisation of the discrete Fourier transform (DFT).

Definition 10.1.1. (DFT and QFT.) Let N be given integer (interpreted as time instants) and suppose that $x : \mathbb{R} \to \mathbb{C}$ is a signal. Sample this signal at instants $\{0, \dots, N-1\}$ i.e. consider the vector $\mathbf{x} = (x_0, \dots, x_{N-1}) \in \mathbb{C}^N$.

— We define the **discrete Fourier transform** to be the mapping

$$\mathbb{C}^N \ni \mathbf{x} = (x_0, \dots, x_{N-1}) \mapsto \mathcal{F}(\mathbf{x}) := \tilde{\mathbf{x}} = (\tilde{x}_0, \dots, \tilde{x}_{N-1}) \in \mathbb{C}^N,$$

where $\tilde{x}_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp(2\pi i k \frac{j}{N}) x_k$, for $j \in \{0, \dots, N-1\}$.

— By analogy, the **quantum Fourier transform** is the mapping on $\mathbb{H}_N = \mathbb{C}^N$ de-

fined by

$$\mathbb{H}_N = \mathbb{C}^N \ni |\, j \,\rangle \mapsto \mathcal{F}|\, j \,\rangle := |\, \widetilde{j} \,\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp(2\pi i k \frac{j}{N}) |\, k \,\rangle \in \mathbb{H}_N.$$

We use the simplified Dirac's notation $|\, i \,\rangle$ to denote the unit vector $|\, e_i \,\rangle$ of the canonical basis $(|\, e_i \,\rangle)_{i=0,\ldots,N-1} \in \mathbb{H}_N$.

Lemma 10.1.2. *The operator $\mathcal{F}$ defined in 10.1.1 is unitary*

Proof. We compute straightforwardly

$$\begin{aligned} \langle\, j' \,|\, \mathcal{F}^* \mathcal{F} j \,\rangle &= \frac{1}{N} \sum_{k,l=0}^{N-1} \exp(-2\pi i l \frac{j'}{N}) \exp(2\pi i k \frac{j}{N}) \langle\, l \,|\, k \,\rangle \\ &= \frac{1}{N} \sum_{k}^{N-1} \exp(-2\pi i k \frac{j-j'}{N}) = \delta_{j,j'}. \end{aligned}$$

□

Denote by $z := z_N = \exp(\frac{2\pi i}{N})$. The Fourier operator $\mathcal{F}$ acts linearly on vectors of $\mathbb{H}_N$, hence it is totally determined through its matrix elements

$$\mathcal{F}_{kl} := \langle\, k \,|\, \mathcal{F} l \,\rangle = \frac{1}{\sqrt{N}} z^{kl}.$$

Now,

$$\begin{aligned} \mathcal{F}^*_{kl} &:= \langle\, k \,|\, \mathcal{F}^* l \,\rangle = \langle\, \mathcal{F} k \,|\, l \,\rangle \\ &= \overline{\langle\, l \,|\, \mathcal{F} k \,\rangle} = \overline{\mathcal{F}_{lk}} = \frac{1}{\sqrt{N}} \bar{z}^{kl}. \end{aligned}$$

It is instructive to determine the action of $\mathcal{F}$ on the canonical basis in the case $N = 2$. In this situation, $|\, \widetilde{l} \,\rangle = \mathcal{F}|\, l \,\rangle = \frac{1}{\sqrt{2}} \sum_{k=0}^{1} z^{kl} |\, k \,\rangle$. Hence

$$\widetilde{|\, 0 \,\rangle} = \frac{|\, 0 \,\rangle + |\, 1 \,\rangle}{\sqrt{2}}; \quad \widetilde{|\, 1 \,\rangle} = \frac{|\, 0 \,\rangle - |\, 1 \,\rangle}{\sqrt{2}},$$

since $z_2 = \exp(\pi i) = -1$. Therefore, the Fourier transform in this case corresponds to the passage from the canonical basis to the conjugate one.

Suppose now that, for some real parameter t, we form the unit norm vector $|\, \psi_t \,\rangle = \frac{1}{N} \sum_{k=0}^{N-1} \exp(ikt) |\, k \,\rangle$ depending on t. Now this vector can also be decomposed into any other basis, for instance the conjugate basis $(|\, \widetilde{l} \,\rangle)_{l=0,\ldots,N-1}$. The squared moduli of the corresponding Fourier coefficients, namely $|\langle\, \widetilde{l} \,|\, \psi_t \rangle|^2$, are interpreted as the probability, π_t, that the pure state corresponding to the vector $|\, \psi_t \,\rangle$ is in the pure state corresponding to the vector $|\, \widetilde{l} \,\rangle$. The usefulness of the quantum Fourier transforms stems from the fact that this probability is sharply peaked around very few values of l; these values depend on t. Therefore, we have an efficient algorithm to determine the phase t.

Notation 10.1.3. In the sequel $N = 2^n$, $\mathcal{H} = \mathbb{C}^2$, and $\mathbb{H} = \otimes_{k=0}^{n-1}\mathcal{H}$. Basis vectors $|\, j \,\rangle \in \mathbb{H}$ are indexed by integers $j = 0, \ldots, 2^n - 1$ and we identify

$$\{0, \ldots, 2^n - 1\} \ni j \mapsto \mathbf{j} = \mathsf{seq}(j) = j_1 \cdots j_n \in \mathbb{B}^n.$$

With this notation

$$j = j_1 2^{n-1} + \ldots + j_n 2^0 = 2^n(\frac{j_1}{2^1} + \ldots + \frac{j_n}{2^n}) = 2^n \langle 0.j_1 \cdots j_n \rangle_2 = \langle j_1 \cdots j_n \rangle_2 = \langle \mathbf{j} \rangle_2.$$

Consequently,

$$\begin{aligned}
|\, j \,\rangle = |\, j_1 \cdots j_n \,\rangle &\overset{\mathcal{F}}{\mapsto} \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} \exp(2\pi i j \frac{k}{2^n}) |\, k \,\rangle \\
&= \frac{1}{2^{n/2}} \sum_{(k_1 \cdots k_n) \in \mathbb{B}^n} \exp(2\pi i j \langle 0.k_1 \cdots k_n \rangle_2) |\, k_1 \cdots k_n \,\rangle \\
&= \frac{1}{2^{n/2}} [|\, 0 \,\rangle + \exp(2\pi i j/2) |\, 1 \,\rangle] \otimes \cdots \otimes [|\, 0 \,\rangle + \exp(2\pi i j/2^n) |\, 1 \,\rangle] \\
&= \frac{1}{2^{n/2}} [|\, 0 \,\rangle + \exp(2\pi i \langle 0.j_n \rangle) |\, 1 \,\rangle] \otimes \cdots \otimes [|\, 0 \,\rangle + \exp(2\pi i \langle 0.j_1 \cdots j_n \rangle) |\, 1 \,\rangle] .
\end{aligned}$$

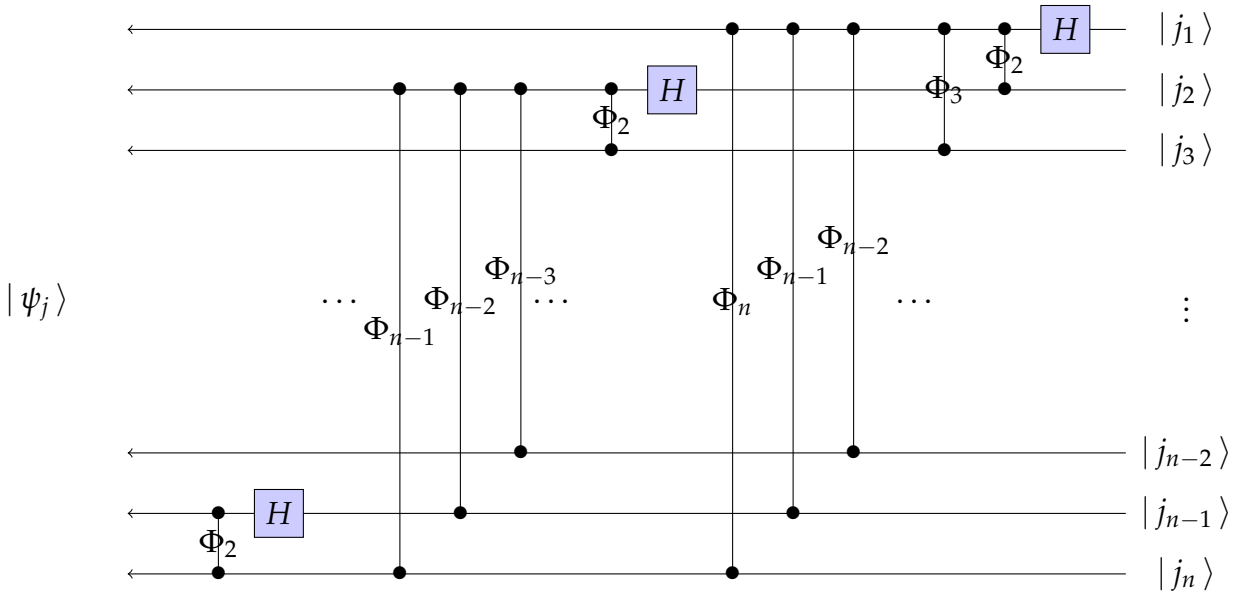


Figure 10.1 – Circuit implementing the quantum Fourier transform. The input is on the right and the output on the left.

Exercise 10.1.4. Denote, for $k = 1, \ldots, n$, by $\Phi_k = C(\Phi(\pi/2^k))$ the controlled phase gates and by H the Hadamard gates (see 8.4.4 and 8.4.1).

1. Show that the circuit depicted in figure 10.1 implements the quantum Fourier transform defined in 10.1.1, i.e. $|\, \psi_j \,\rangle = \mathcal{F} |\, j \,\rangle$.
2. Determine the circuit implementing the adjoint of $\mathcal{F}$.

10.2 Phase estimation

Definition 10.2.1. Let $U : \mathbb{H}^{\otimes n} \to \mathbb{H}^{\otimes n}$ be a unitary operator and suppose that $|\, u \,\rangle \in \mathbb{H}^{\otimes n}$ is a known (i.e. determined elsewhere) eigenvector of U. The **phase estimation problem** consists in determining $\phi_u \in [0,1]$ such that the corresponding eigenvalue of U is $\exp(2\pi i \phi_u)$, i.e. determine $\phi_u \in [0,1]$ verifying

$$U|\, u \,\rangle = \exp(2\pi i \phi_u)|\, u \,\rangle.$$

The purpose of this section is to give an algorithm allowing to estimate ϕ_u with an arbitrary precision. The resources needed for this algorithm are "black-box" gates implementing powers of the form U^{2^j} for $j = 0, \ldots, t-1$, and t some positive integer and of a quantum register containing the eigenvector $|\, u \,\rangle$. Once, the circuits for the gates U^{2^j} are available, it is immediate to construct circuits implementing their controlled version $C(U^{2^j})$.

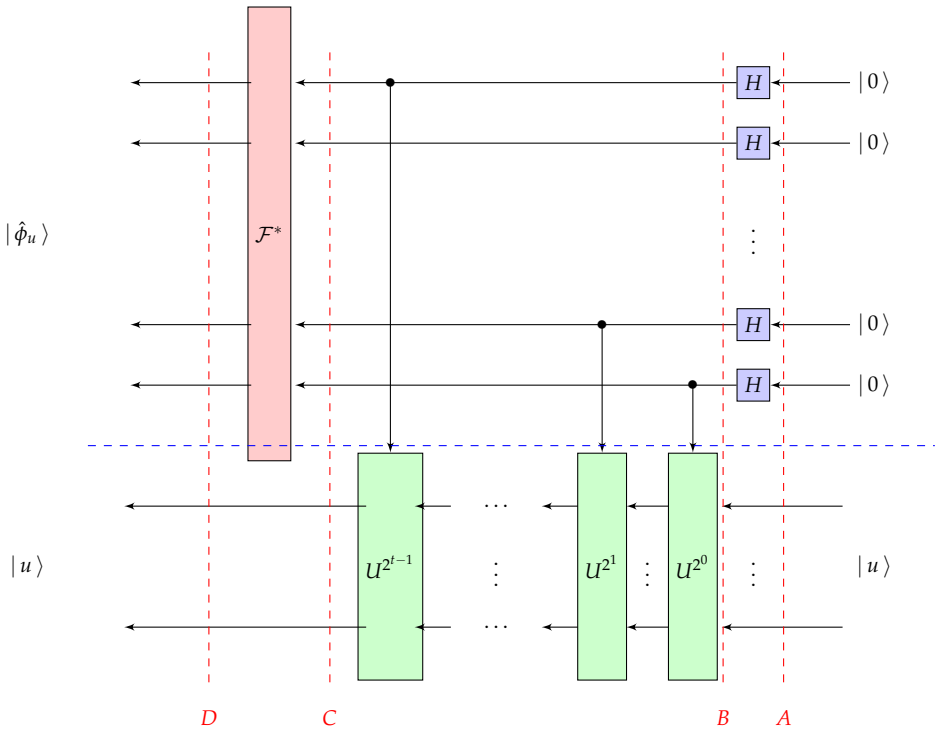


Figure 10.2 – Circuit allowing to determine a vector $|\,\hat{\phi}_u\,\rangle \in \mathbb{H}^{\otimes t}$ encoding a good rational approximation of the phase ϕ_u. The input of the circuit is composed from two registers, a t-qubit register $|\,0\cdots 0\,\rangle \in \mathbb{H}^{\otimes t}$ tensored with a n-qubit register $|\,u\,\rangle \in \mathbb{H}^{\otimes n}$. The red block marked $\mathcal{F}^*$ is the reverse — i.e. read from left to right — of the circuit depicted in figure 10.1. The green blocks are controlled gates $C(U^{2^j})$ (the bullets denoting the corresponding control qubits) and the blue bolcks depict Hadamard gates.

Theorem 10.2.2. *Consider the circuit depicted in figure 10.3. For every $\varepsilon \in (0,1)$, there exists an integer $p := p(\varepsilon) > 0$ such that, for $t = n + p$, and $\Delta = \{m \in \{0, \ldots, 2^t - 1\} : |\frac{m}{2^t} - \phi_u| \leq \frac{1}{2^n}\}$, then*

$$\mathbb{P}_{\mathcal{F}^* \psi_D}(\Delta) \geq 1 - \varepsilon.$$

Proof. We read the figure from right to left; consider the vector $|\,\Psi\,\rangle \in \mathbb{H}^{\otimes t} \otimes \mathbb{H}^{\otimes n}$ at the four instants materialised by the vertical dotted lines denoted A – D. It turns out that at all these moments, the vector $|\,\Psi\,\rangle$ can be split into two **mutually unentangled** registers $|\,\psi\,\rangle \otimes |\,u\,\rangle \in \mathbb{H}^{\otimes t} \otimes \mathbb{H}^{\otimes n}$. Thus

$$
\begin{aligned}
|\,\Psi_A\,\rangle &= |\,\psi_A\,\rangle \otimes |\,u\,\rangle = |\,\underbrace{0\cdots 0}_{t \text{ times}}\rangle \otimes |\,u\,\rangle \\
|\,\Psi_B\,\rangle &= |\,\psi_B\,\rangle \otimes |\,u\,\rangle = \frac{1}{2^{t/2}} \sum_{(k_1,\ldots,k_n)\in\mathbb{B}^n} |\,k_1\cdots k_n\,\rangle \otimes |\,u\,\rangle \\
|\,\Psi_C\,\rangle &= |\,\psi_C\,\rangle \otimes |\,u\,\rangle = \frac{1}{2^{t/2}} \Big[|\,0\,\rangle + \exp(2\pi i 2^{t-1}\phi_u |\,1\,\rangle\Big] \otimes \cdots \otimes \Big[|\,0\,\rangle + \exp(2\pi i 2^0 \phi_u |\,1\,\rangle\Big] \otimes |\,u\,\rangle \\
&= \frac{1}{2^{t/2}} \sum_{k_0,\ldots,k_{t-1}\in\mathbb{B}} \exp\left(2\pi i \phi_u \langle k_{t-1}\cdots k_0\rangle\right) |\,k_{t-1}\cdots k_0\,\rangle \otimes |\,u\,\rangle \\
&= \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} \exp(2\pi i \phi_u k) |\,k\,\rangle \otimes |\,u\,\rangle.
\end{aligned}
$$

Since the vector $|\,\Psi_C\,\rangle = |\,\psi_C\,\rangle \otimes |\,u\,\rangle$ is disentangled between its $\mathbb{H}^{\otimes t}$ and $\mathbb{H}^{\otimes n}$ components, we can examine the action of the inverse quantum Fourier transform on its first component. Define $|\,\hat{\phi}_u\,\rangle := |\,\psi_D\,\rangle = \mathcal{F}^*|\,\psi_C\,\rangle$ and let $L := L(\phi_u, t) = \lfloor 2^t \phi_u \rfloor$ and $0 \le \delta := \delta(\phi_u, t) = \phi_u - \frac{L}{2^t} < 1$. We have then

$$
\begin{aligned}
|\,\hat{\phi}_u\,\rangle &= \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} \exp(2\pi i \phi_u k) \mathcal{F}^* |\,k\,\rangle \\
&= \frac{1}{2^t} \sum_{k=0}^{2^t-1} \exp(2\pi i \phi_u k) \sum_{l=0}^{2^t-1} \exp(-2\pi i k \frac{l}{2^t}) |\,l\,\rangle \\
&= \frac{1}{2^t} \sum_{k,l=0}^{2^t-1} \exp(2\pi i \phi_u k) \exp(-2\pi i k \frac{l+L}{2^t}) |\,L+l \mod 2^t\,\rangle \\
&= \sum_{l=-2^{t-1}}^{2^{t-1}-1} \underbrace{\sum_{k=0}^{2^t-1} \left[\frac{1}{2^t} \exp\left(-2\pi i(\delta - \frac{l}{2^t})\right)^k\right]}_{\alpha_l} |\,L+l \mod 2^t\,\rangle.
\end{aligned}
$$

Now, for $l \in \{0,\ldots,2^t-1\}$, we can compute explicitely

$$
\alpha_l = \begin{cases} \mathbb{1}_{\{0\}}(l) & \text{if } \delta = 0, \\ \frac{1}{2^t} \frac{\exp\left(-\pi i(2^t\delta - l)\right)}{\exp\left(-\pi i(\delta - \frac{l}{2^t})\right)} \frac{\sin\left(\pi(2^t\delta - l)\right)}{\sin\left(\pi(\delta - \frac{l}{2^t})\right)} & \text{if } 0 < \delta < 1. \end{cases}
$$

If ϕ_u is exactly expressible as the dyadic rational $\frac{L}{2^t}$, i.e. $\delta = 0$, then obviously $|\,\hat{\phi}_u\,\rangle = |\,L\,\rangle$ and the theorem holds with $\varepsilon = 0$ and $\Delta = \{L\}$. In the other cases, it turns out that $|\alpha_l|^2$ is sharply peaked around 0 (see figure 10.3 for an example). The end of the proof consists in finding the smallest Δ so that $\mathbb{P}_{\tilde{\phi}_u}(\Delta^c) < \varepsilon$. First remark that for $-\frac{\pi}{2} < \theta < \frac{\pi}{2}$ we have $|\sin(\theta)| \ge \frac{2|\theta|}{\pi}$. Therefore, by writing

$$
|\alpha_l| = \frac{1}{2^t} \frac{\left|\sin\left(\pi(2^t\delta - l)\right)\right|}{\left|\sin\left(\pi(\delta - \frac{l}{2^t})\right)\right|} \le \frac{1}{2^t} \frac{1}{\left|\sin\left(\pi(\delta - \frac{l}{2^t})\right)\right|},
$$

we conclude that $|\alpha_l|^2 \leq \frac{1}{4|l|^2}$. Suppose now that $\Delta_M = \{L - M \mod 2^t, \ldots, L + M \mod 2^t\}$ for some integer $M \leq 2^{t-1}$ and consider the effect $E[\Delta_M] = \sum_{m\in\Delta_M} |\, m \,\rangle\langle\, m \,|$. Then

$$\begin{aligned}
\mathbb{P}_{\tilde{\phi}_u}(\Delta_M) &= \sum_{m\in\Delta_M} \langle\, \tilde{\phi}_u \,|\, m \,\rangle\langle\, m \,|\, \tilde{\phi}_u \,\rangle \\
&= \sum_{m\in\Delta_M} \sum_{l,l'=-2^{t-1}}^{2^{t-1}-1} \overline{\alpha_l}\alpha_{l'} \langle\, L + l \mod 2^t \,|\, m \,\rangle\langle\, m \,|\, L + l' \mod 2^t \,\rangle \\
&= \sum_{m\in\Delta_M} |\alpha_{m-L \mod 2^t}|^2 = \sum_{m=-M}^{M} |\alpha_m|^2.
\end{aligned}$$

We must now optimise M so that $\frac{M}{2^t} = \mathcal{O}(\frac{1}{2^n})$ and $\mathbb{P}_{\tilde{\phi}_u}(\Delta_M^c) < \varepsilon$. We estimate

$$\mathbb{P}_{\tilde{\phi}_u}(\Delta_M^c) \leq 2 \sum_{m=M}^{2^{t-1}-1} |\alpha_l|^2 \leq \sum_{m=M}^{2^{t-1}-1} \frac{1}{2m^2} \leq \frac{1}{2M} \leq \varepsilon,$$

and

$$\max\{|\frac{m + L \mod 2^t}{2^t} - \phi_u|, m \in \Delta_M\} = \frac{M}{2^t} \leq \frac{1}{2^n}.$$

The choice $p = \lceil -\log_2 \varepsilon \rceil + 1$ and $t = n + p$ establishes the conclusion of the theorem. □

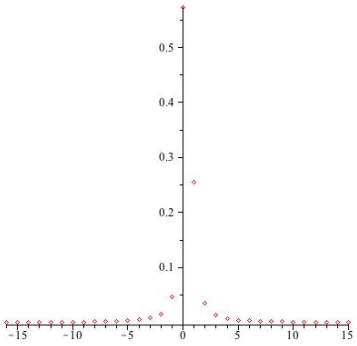


Figure 10.3 – Example values of $|\alpha_l|^2$ for $l \in \{-16, \ldots, 15\}$ for the case $t = 10$ and $\delta = 0.2$. Only the values near 0 are depicted since the values in the range $\{-512, \ldots, 511\} \setminus \{L - 16, \ldots, 15\}$ are so small that are represented by points lying beneath the threshold of graphical discrimination from 0.

We can summarise the results obtained so far, in the algorithm 10.2.3.

Algorithm 10.2.3. *Phase estimation*

Require: *Black boxes* $C(U^{2^j})$,
eigenvector $|\, u \,\rangle$ *of* U,
precision threshold ε,
$t = n + \lceil \log(2 + \frac{1}{2\varepsilon}) \rceil$ *qubits initialised at* $|\, 0 \,\rangle$.
Ensure: *Estimation of* ϕ_u *precise up to* t *bits.*

Initialise $|\,0\,\rangle^{\otimes t} \otimes |\,u\,\rangle$.
Apply operators as in regions $A - C$ *of figure 10.3 .*
Apply $\mathcal{F}^*$ *on the t first qubits register to get* $|\,\tilde{\phi}_u\,\rangle$.
Mesure the t-qubit register to obtain estimation of $\tilde{\phi}_u$

10.3 Order finding

10.3.1 The order finding problem

Definition 10.3.1. Let x, N be fixed integers strictly larger than 1 with $\mathrm{pgcd}(x, N) = 1$. We define the **order** of x in N by

$$\mathrm{ord}(x, N) = \inf\{r > 0 : x^r = 1 \mod N\}.$$

It is conjectured that the problem of order finding is an algorithmically hard problem. As a matter of fact, if $L = \lceil \log N \rceil$, we don't know any classical algorithm solving this problem in polynomial (in L) time. For an L-bit string $\mathbf{y} = y_1 \dots y_L \in \mathbb{B}^L$, denote by $y = \langle \mathbf{y} \rangle \in \{0, \dots, 2^L - 1\}$. These integers serve as an indexing set for the canonical basis and $|\,y\,\rangle = |\,y_1 \dots y_L\,\rangle \in \mathbb{H}^{\otimes L}$, with $\mathbb{H} = \mathbb{C}^2$.

Definition 10.3.2. For x and N as in definition 10.3.1, $L = \lceil \log N \rceil$, and $|\,y\,\rangle \in \mathbb{H}^{\otimes L}$, define the unitary operator

$$U|\,y\,\rangle = \begin{cases} |\,xy \mod N\,\rangle & \text{if } 0 \le y \le N-1, \\ |\,y\,\rangle & \text{if } N \le y \le 2^L - 1. \end{cases}$$

Lemma 10.3.3. *Let* $r := \mathrm{ord}(x, N) \le N$. *For* $s = 0, \dots, r-1$, *and*

$$|\,u_s\,\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp(-2\pi i k \frac{s}{r}) |\,x^k \mod N\,\rangle,$$

we have

1. *that the vector* $|\,u_s\,\rangle$ *is an eigenvector of* U*:*

$$U|\,u_s\,\rangle = \exp(2\pi i \frac{s}{r}) |\,u_s\,\rangle;$$

2. *that the vector* $|\,1\,\rangle$ *is a linear combination of eigenvectors:*

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\,u_s\,\rangle = |\,1\,\rangle.$$

Proof. 1. We compute plainly

$$\begin{aligned} U|\,u_s\,\rangle &= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp(-2\pi iks/r)|\,x^{k+1} \mod N\,\rangle \\ &= \frac{1}{\sqrt{r}}\sum_{k=1}^{r}\exp(-2\pi i(k-1)s/r)|\,x^{k} \mod N\,\rangle \\ &= \frac{1}{r}\exp(2\pi is/r)\left(\sum_{k=1}^{r-1}\exp(-2\pi iks/r)|\,x^{k} \mod N\,\rangle + |\,x^{r} \mod N\,\rangle\right) \\ &= \exp(2\pi is/r)|\,u_s\,\rangle. \end{aligned}$$

2. Since $\sum_{s=0}^{r-1}\exp(-2\pi isk/r) = r\delta_{k,0}$, we compute

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|\,u_s\,\rangle = \frac{1}{r}\exp(-2\pi isk/r)|\,x^{k} \mod N\,\rangle = |\,1\,\rangle.$$

□

Remark 10.3.4. The lemma 10.3.3 establishes that for every s, the construction of the vector $|\,u_s\,\rangle$ supposes previous knowledge of r. Item 2 of this lemma is of the utmost importance for the feasibility of the algorithm because it suggests that instead of initialising the algorithm with $|\,u_s\,\rangle$ it is enough to initialise with $|\,1\,\rangle$ and the result will be a linear combination of actions of U.

10.3.2 Classical continued fraction expansion

If we are able to determine the ratio s/r for different values of s, we shall be able to estimate r and the problem of order finding will be solved. This estimation problem is solved by the classical algorithm of continued fraction expansion. Let recall briefly what is the continued fraction expansion.

We associate with every $\alpha \in \mathbb{R}_+$ a (finite or infinite) sequence of $(a_0; a_1, a_2, \cdots)$ such that α can be decomposed into the **continued fraction expansion** (CFE)

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}.$$

The terms $a_1, a_2, \ldots$ appearing in this expansion are in $\mathbb{N}_>$, the term a_0 — corresponding to $\lfloor\alpha\rfloor$ — can take also the value 0. We write $\alpha = [a_0; a_1, a_2, a_3, \ldots]$ to denote the previous expansion.

— If $\alpha \in \mathbb{Q}_+$, there exists a $M > 0$ such that the sequence defining the CFE of α is finite, i.e. $\alpha = [a_0; a_1 \ldots, a_M]$.
— If $\alpha \in (\mathbb{R}_+ \setminus \mathbb{Q})$, its CFE is given by an infinite sequence $\alpha = [a_0; a_1, a_2, a_3, \ldots]$, with $a_i > 0$ for all $i \geq 1$.

If α is represented by an infinite expansion $\alpha = [a_0; a_1, a_2, \ldots]$, then its truncated (at order m) expansion $[a_0; a_1 \ldots, a_m]$ is a rational approximation of α. As a matter of fact,

$$[a_0; a_1 \ldots, a_m] = \frac{p_m(\alpha)}{q_m(\alpha)},$$

where $p_m := p_m(\alpha)$ and $q_m := q_m(\alpha)$ are integers defined by the recursive relations:

$$p_m = a_m p_{m-1} + p_{m-2} \text{ and } q_m = a_m q_{m-1} + q_{m-2}, m \geq 1,$$

and $p_0 = a_0$, $q_0 = 1$, $p_{-1} = 1$, and $q_{-1} = 0$. The sequence of ratios $\frac{p_m(\alpha)}{q_m(\alpha)}$ are called **principal convergent** of α.

Lemma 10.3.5. *(See [99, chapter 1]). Denote by $\alpha_m = [a_0; a_1 \ldots, a_m] = p_m/q_m$ the sequence of principal convergents.*

1. $\alpha_0 \leq \alpha_{2m} \leq \alpha_{2m+2} \leq \ldots \alpha \leq \ldots \leq \alpha_{2m+1} \leq \alpha_{2m-1} \leq \ldots \alpha_1$ *and* $\lim_{m\to\infty} := \lim_{m\to\infty} \frac{p_m(\alpha)}{q_m(\alpha)} = \alpha$.
2. *Let $\frac{p}{q}$ be an irreducible fraction with $q > 0$. If*

$$|\alpha - \frac{p}{q}| \leq \frac{1}{2q^2}$$

then there exists an M such that $\frac{p}{q} = \alpha_M$, i.e. the sequence of principal convergents verifies $|\alpha - \frac{p_m}{q_m}| \leq \frac{1}{2q_m^2}$ for all $m \in \mathbb{N}_>$.

The classical algorithm 10.3.6 summarises the construction of the (truncated) CFE.

Algorithm 10.3.6. *Continued fraction expansion (CFE)*

Require: *real $\alpha > 0$, integer $M > 0$.*
Ensure: *$a_0, \ldots, a_M$ with $a_i > 0$ pour $1 \leq i \leq M$.*

Initialise $m \leftarrow 0$.
repeat
  $a_m \leftarrow \lfloor \alpha \rfloor$.
  $\beta \leftarrow \{\alpha\}$ *(It is recalled that* $\{\alpha\} := \alpha - \lfloor \alpha \rfloor$*).*
  $m \leftarrow m + 1$.
  if $\beta \neq 0$ ***then***
    $\alpha \leftarrow \frac{1}{\beta}$
  else
    $\alpha \leftarrow 0$
  end if
until $m > M$.

10.3.3 Order finding algorithm

The order finding algorithm — summarised in 10.3.8 below — is *in fine* a phase estimation algorithm for a particular unitary operator $U = U_{x,N}$, for x and N fixed positive coprime integers (i.e. $\gcd(x, N) = 1$). Denote by $L = \log_2 N\rceil$ the number of bits required to represent N and set $t = 2L + 1$.

Proposition 10.3.7. *Let x, N, and L as above.*

1. *Consider the circuit depicted in figure 10.3 instanciated with $U := U_{x,N}$ and initialised with $|\,0\,\rangle \otimes |\,u_s\,\rangle \in \mathbb{H}^{\otimes t} \otimes \mathbb{H}^{\otimes n}$. Measuring in the state of the first register $|\,\psi_D\,\rangle = |\,\widetilde{s/r}\,\rangle$ provides with an approximation θ of the phase s/r.*
2. *Applying the CFE algorithm on this approximation determines the order r with large probability.*
3. *If the second register of the initialisation vector is set at $|\,1\,\rangle \in \mathbb{H}^{\otimes n}$, the vector $|\,\Psi_D\,\rangle$ reads $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\,\widetilde{s/r}\,\rangle \otimes |\,u_s\,\rangle$.*

Proof. 1. When the circuit is initialised with $|\,0\,\rangle \otimes |\,u_s\,\rangle \in \mathbb{H}^{\otimes t} \otimes \mathbb{H}^{\otimes n}$, the registers at position C read

$$|\,\Psi_C\,\rangle = \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} \exp\left(2\pi i \frac{s}{r} k\right) |\,k\,\rangle \otimes |\,u_s\,\rangle.$$

We conclude by theorem 10.2.2 that

$$|\,\Psi_D\,\rangle = (\mathcal{F}^* \otimes I)|\,\Psi_C\,\rangle = |\,\widetilde{s/r}\,\rangle \otimes |\,u_s\,\rangle$$

and measuring in that vector yields s/r with large probability.

2. Since θ is an $2L+1$-bit approximation of s/r, it follows that $|\theta - r/s| \leq 2^{-2L-1} \leq 1/2r^2$ because $r \leq N\, 2^L$. Hence, by lemma **??**, the approximation ϕ is the continued fraction expansion of s/r. Therefore, the continued fraction expansion yields numbers r' and s' without common factors verifying $s'/r' = s/r$. The number r' is a good candidate for $\mathrm{ord}(x, N)$. It is effectively the order if $x^{r'} = 1 \mod N$. And this happens with high probability.
3. The result follows by linearity since $|\,1\,\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\,u_s\,\rangle$.

□

The proposition 10.3.7 guarantees that the algorithm 10.3.8 solves the order finding problem.

Algorithm 10.3.8. *Order finding algorithm (OFA)*

Require: *Integer N with L bits,*
x comprime with N,
precision threshold ε,
$t = L + \lceil -\log_2 \varepsilon\rceil$ qubits initialised at $|\,0\,\rangle$,
L qubits initialised at $|\,1\,\rangle$,
implementation of unitary $U_{N,x} : \mathbb{H}^{\otimes t} \otimes \mathbb{H}^{\otimes L} \to \mathbb{H}^{\otimes t} \otimes \mathbb{H}^{\otimes L}$,
CFE algorithm.

Ensure: $\mathsf{ord}(x, N)$ *with probability* $1 - \varepsilon$ *within* $\mathcal{O}(L^3)$ *steps.*

Act as in figure 10.3 to get state $|\,\psi_D\,\rangle$.
Measure in state $|\,\psi_D\,\rangle$ *to get L-bit approximation* θ *of the phase.*
$\mathbf{a} := [a_0; a_1, \ldots, a_n] \leftarrow \mathit{CFE}(\theta)$.
$\frac{s}{r} \leftarrow \frac{p_n(\mathbf{a})}{q_n(\mathbf{a})}$.
if $x^r \mod N = 1$ ***then***
  return r
else
  The algorithm fails.
end if

Let us examine when the algorithm can fail:

— A first possibility is that the algorithm produces an false estimate of the phase s/r. This can occur with probability less than ε at the expense of a size $\lceil -\log_2 \varepsilon \rceil$ of the circuit.

— A second possibility is that s and r have a common factor. In that case, the ratio returned by the OFA is an irreducible fraction s'/r' equal to s/r. In that case, the value r' determined by the algorithm is not the true order but only a factor of it.

Suppose that we run the algorithm 10.3.8 twice and let s'_1, r'_1 and s'_2, r'_2 be the values determined by each run. Provided that s'_1 and s'_2 have no common factor, the true value r can be determined by taking $r = \mathrm{lcm}(r'_1, r'_2)$. Proposition 10.3.9 minorises the probability to obtain the correct answer r.

Proposition 10.3.9.

$$\mathbb{P}(r \textit{ is the correct order }) \geq \frac{1}{4}.$$

Proof. For two positive integers x and y denote by $x|y$ the fact that x divides y. The probability that s' and s' have no common factor is given by

$$\mathbb{P}(s' \text{ and } s'' \text{ have a common factor }) = 1 - \sum_{p \in \text{ primes}} \mathbb{P}(p|s'_1)\mathbb{P}(p|s'_2).$$

Now, if p divides s'_1 then it must also divide the value s. To majorise $\mathbb{P}(p|s'_1)$ it is enough to majorise $\mathbb{P}(p|s_1)$ where s_1 is chosen uniformly at random in $\{0, \ldots, r-1\}$. In that case $\mathbb{P}(p|s_1) = \mathbb{P}(s \in \{p, 2p, \ldots, kp\})$ with $kp < r$; therefore $\mathbb{P}(s \in \{p, 2p, \ldots, kp\}) \leq \frac{1}{p}$. Hence

$$1 - \sum_{p \in \text{ primes}} \mathbb{P}(p|s'_1)\mathbb{P}(p|s'_2) \geq 1 - \sum_{p \in \text{ primes}} \frac{1}{p^2} \geq 1 - \sum_{p \geq 2} \frac{1}{p^2} \geq \frac{1}{4}.$$

□

Exercise 10.3.10. Show that the lower bound $1/4$ in the above proposition can be arbitrarily improved at the expense of several independent repetitions of the procedure.

10.4 Shor's factoring algorithm

Shor's algorithm exploits the algorithmic efficacy of the quantum order finding algorithm to solve the factoring problem within polynomial time.

The algorithm relies on lemmata 10.4.1 and 10.4.2.

Lemma 10.4.1. *Let N be a composite number representable within L bits. Suppose that x is a non-trivial solution to $x^2 = 1 \mod N$ for $x \in \{1, \ldots, N\}$ (i.e. neither $x = 1 \mod N$ nor $x = N-1 \mod N = -1 \mod N$ hold). Then at least one of $\gcd(x-1, N)$ and $\gcd(x+1, N)$ is a non-trivial factor of N (computable within $\mathcal{O}(L^3)$ steps).*

Proof. Since $x^2 = 1 \mod N$ it follows that N divides $x^2 - 1 = (x-1)(x+1)$; hence N must have a common factor with one of the terms $x-1$ or $x+1$. However, $1 < x < N-1$ by assumption. Therefore, N cannot be a common factor of either $x-1$ or $x+1$. Then at least one of $\gcd(x-1, N)$ and $\gcd(x+1, N)$ is a non-trivial factor of N. Euclid's algorithm determines the gcd in $\mathcal{O}(L^3)$ operations. □

Lemma 10.4.2. *Let $N = p_1^{n_1} \ldots p_m^{n_m}$ be the prime factoring of an odd composite integer N and x a random integer, uniformely chosen in $\{1, \ldots, N-1\}$ under the condition of being coprime with N, and $r = \mathsf{ord}(x, N)$. Then*

$$\mathbb{P}(r \text{ is even and } x^{r/2} \neq -1 \mod N) \geq 1 - \frac{1}{2^m}.$$

Proof. See [110, §A4.3] for instance. □

Shor's factoring algorithm is summarised in 10.4.3. Its efficiency is estimated by the number of gates required for modular exponentiation and order finding. Those tasks can be achieved by using a total of $\mathcal{O}(L^3)$ gates and this resource requirement determines also the time complexity of the algorithm.

Algorithm 10.4.3. *Shor's factoring algorithm*

Require: *Composite integer N with L bits,*
OFA.
Ensure: *A non-trivial factor of N with probability $\mathcal{O}(1)$ within $\mathcal{O}(L^3)$ steps.*

if *N is even* ***then***
  return 2. End.
end if
if *$N = a^b$ for integers $a \geq 1$ and $b \geq 2$* ***then***
  return a. End.
end if
Randomly choose $x \in \{1, \ldots, N-1\}$
if *$f = \gcd(x, N) > 1$* ***then***
  return f. End.
end if

Use OFA to find $r = \mathrm{ord}(x, N)$
if *r is even and* $x^{r/2} \neq -1 \mod N$ ***then***
  $f_1 = \gcd(x^{r/2} - 1, N)$ *and* $f_2 = \gcd(x^{r/2} + 1, N)$
end if
if f_1 *is a factor* ***then***
  return f_1. *End.*
end if
if f_2 *is a factor* ***then***
  return f_2. *End.*
else
  the algorithm fails. End.
end if

10.5 Scalability requirements to implement Shor's algorithm

Section to be re-written

The naïve resource scaling $\mathcal{O}(L^3)$ quoted in the previous section presupposes a flawless functioning of quantum gates. However, this is only an idealisation of the physical process. Error correction codes are needed in all steps to control the analog quantum gates.

To factor an L-bit integer N with full fledged — i.e. including error corrections — Shor's algorithm, we need (see [15]):
— $5L + 1$ qubits,
— $72L^3$ quantum gates.
A simple numerical application:

$L = 4$**:** 21 qubits, 4608 gates,

$L = 100$**:** 501 qubits, 7.2×10^7 gates,

$L = 4096$**:** 20481 qubits, 4.95×10^{12} gates.

Shor's algorithm: — $15 = 3 \times 5$ ($k = 4$). Factored by using 7 qubits.
— $21 = 3 \times 7$ ($k = 5$). Factored by using 10 qubits [106].

Optimisation: — $143 = 11 \times 13$ (with 4 qubits) and $56153 = 233 \times 241$ (with 4 qubits) [156].
— Foreseen — not yet implemented — factoring of $291311 = 523 \times 557$ with 6 qubits [44].

Part III

Quantum mechanics in infinite dimensional spaces

11

Algebras of operators

11.1 Introduction and motivation

Let $\mathbb{V} = \mathbb{C}^n$, with $n \in \mathbb{N}$. Elementary linear algebra establishes that the set of linear mappings $\mathfrak{L}(\mathbb{V}) = \{T : \mathbb{V} \to \mathbb{V} : T \text{ linear }\}$ is a $\mathbb{C}$-vector space of (complex) dimension n^2, isomorphic to $\mathbf{M}_n(\mathbb{C})$, the space of $n \times n$ matrices with complex coefficients. Moreover, if $S, T \in \mathfrak{L}(\mathbb{V})$, the maps S and T can be composed, their composition $T \circ S$ being represented by the corresponding matrix product. Thus, on the vector space $\mathfrak{L}(\mathbb{V})$, is defined an internal multiplication

$$\mathfrak{L}(\mathbb{V}) \times \mathfrak{L}(\mathbb{V}) \ni (T, S) \mapsto T \circ S \in \mathfrak{L}(\mathbb{V})$$

turning this vector space into **an algebra**.

When the underlying vector space $\mathbb{V}$ is of infinite dimension, caution must be paid on defining linear maps. In general, linear mappings $T : \mathbb{V} \to \mathbb{V}$, called **(linear) operators**, are defined only on some proper subset of $\mathbb{V}$ denoted $\mathsf{Dom}(T)$ and called the **domain** [1] of T. When $\mathbb{V}$ is a normed space, there is a natural way to define a norm on $\mathfrak{L}(\mathbb{V})$. We denote by $\mathfrak{B}(\mathbb{V})$ the vector space of **bounded linear operators** on $\mathbb{V}$, i.e. linear maps $T : \mathbb{V} \to \mathbb{V}$ such that $\|T\| < \infty$ (equivalently, verifying $\mathsf{Dom}(T) = \mathbb{V}$.) When $\mathbb{H}$ is a Hilbert space, bounded linear operators on $\mathbb{H}$, whose set is denoted by $\mathfrak{B}(\mathbb{H})$, with operator norm $\|T\| = \sup\{\|Tx\|, x \in \mathbb{H}, \|x\| \leq 1\}$, share the properties of linear operators defined on more algebraic setting. Sometimes it is more efficient to work with explicit representations of operators in $\mathfrak{B}(\mathbb{H})$ (that play the rôle of matrices in the infinite dimensional setting) and some others with abstract algebraic setting.

Since all operators encountered in quantum mechanics are linear, we drop henceforth the adjective linear.

1. The set $\mathsf{Dom}(T)$ is generally a vector subspace of $\mathbb{V}$ which is not necessarily topologically closed.

11.2 Algebra of operators

Definition 11.2.1. An **algebra** is a set $\mathfrak{A}$ endowed with three operations:

1. a **scalar multiplication** $\mathbb{C} \times \mathfrak{A} \ni (\lambda, a) \mapsto \lambda a \in \mathfrak{A}$,
2. a **vector addition** $\mathfrak{A} \times \mathfrak{A} \ni (a, b) \mapsto a + b \in \mathfrak{A}$, and
3. a **vector multiplication** $\mathfrak{A} \times \mathfrak{A} \ni (a, b) \mapsto ab \in \mathfrak{A}$,

such that $\mathfrak{A}$ is a vector space with respect to scalar multiplication and vector addition and a ring (not necessarily commutative) with respect to vector addition and vector multiplication. Moreover, $\lambda(ab) = (\lambda a)b = a(\lambda b)$ for all $\lambda \in \mathbb{C}$ and all $a, b \in \mathfrak{A}$. The algebra is called **commutative** if $ab = ba$, for all $a, b \in \mathfrak{A}$; it is called **unital** if there exists (a necessarily unique) element $e \in \mathfrak{A}$ (often also written $\mathbb{1}$ or $\mathbb{1}_{\mathfrak{A}}$) such that $ae = ea = a$ for all $a \in \mathfrak{A}$;

A linear map from an algebra $\mathfrak{A}_1$ to an algebra $\mathfrak{A}_2$ is a **homomorphism** if it is a ring homomorphism for the underlying rings, it is an **isomorphism** if it is a bijective homomorphism.

Definition 11.2.2. An **involution** on an algebra $\mathfrak{A}$ is a map $\mathfrak{A} \ni a \mapsto a^* \in \mathfrak{A}$ that verifies

1. $(\lambda a + \mu b)^* = \overline{\lambda} a^* + \overline{\mu} b^*$,
2. $(ab)^* = b^* a^*$, and
3. $(a^*)^* = a$.

Involution is also called **adjoint operation** and a^* the **adjoint** of a. An involutive algebra is termed a $*$**-algebra**.

An element $a \in \mathfrak{A}$ is said **normal** if $aa^* = a^*a$, an **isometry** if $a^*a = \mathbb{1}$, **unitary** if both a and a^* are isometries, **self-adjoint or Hermitean** if $a = a^*$. On denoting $h : \mathfrak{A}_1 \to \mathfrak{A}_2$ a homomorphism between two $*$-algebras, we call it a $*$**-homomorphism** if it preserves adjoints, i.e. $h(a^*) = h(a)^*$.

A **normed** (respectively **Banach**) algebra $\mathfrak{A}$ is an algebra equipped with a norm map $\|\cdot\| : \mathfrak{A} \to \mathbb{R}_+$ that is a normed (respectively Banach) vector space for the norm and verifies $\|ab\| \leq \|a\|\|b\|$ for all $a, b \in \mathfrak{A}$. $\mathfrak{A}$ is **normed** (respectively **Banach**) $*$**-algebra** if it has an involution verifying $\|a^*\| = \|a\|$ for all $a \in \mathfrak{A}$.

Theorem 11.2.3. *Let $T : \mathbb{H}_1 \to \mathbb{H}_2$ be a linear map between two Hilbert spaces $\mathbb{H}_1$ and $\mathbb{H}_2$. Then the following are equivalent:*

1. $\|T\| = \sup\{\|Tf\|_{\mathbb{H}_2}, f \in \mathbb{H}_1, \|f\|_{\mathbb{H}_1} \leq 1\} < \infty$,
2. *T is continuous,*
3. *T is continuous at one point of $\mathbb{H}_1$.*

Proof: Analogous to the proof of the theorem **??** for linear functional. (Please complete the proof!) □

Notation 11.2.4. We denote by $\mathfrak{B}(\mathbb{H}_1, \mathbb{H}_2)$ the algebra of bounded operators with respect to the aforementioned norm:

$$\mathfrak{B}(\mathbb{H}_1, \mathbb{H}_2) = \{T \in \mathfrak{L}(\mathbb{H}_1, \mathbb{H}_2) : \|T\| < \infty\}.$$

When $\mathbb{H}_1 = \mathbb{H}_2 = \mathbb{H}$, we write simply $\mathfrak{B}(\mathbb{H})$.

Proposition 11.2.5. *Let $\mathbb{H}_1$ and $\mathbb{H}_2$ be two Hilbert spaces and $T \in \mathfrak{B}(\mathbb{H}_1, \mathbb{H}_2)$. Then, there exists a unique bounded operator $T^* : \mathbb{H}_2 \to \mathbb{H}_1$ such that*

$$\langle\, T^* g \,|\, f \,\rangle = \langle\, g \,|\, Tf \,\rangle \text{ for all } f \in \mathbb{H}_1, g \in \mathbb{H}_2.$$

Proof: For each $g \in \mathbb{H}_2$, the map $\mathbb{H}_1 \ni f \mapsto \langle\, g \,|\, Tf \,\rangle_{\mathbb{H}_2} \in \mathbb{C}$ is a continuous (why?) linear form. By Riesz-Fréchet theorem **??**, there exists a unique $h \in \mathbb{H}_1$ such that $\langle\, h \,|\, f \,\rangle_{\mathbb{H}_1} = \langle\, g \,|\, Tf \,\rangle_{\mathbb{H}_2}$, for all $f \in \mathbb{H}_1$. Let $T^* : \mathbb{H}_2 \to \mathbb{H}_1$ be defined by the assignment $T^* g = h$; it is obviously linear and easily checked to be bounded (exercise!) □

Proposition 11.2.6. *For all $T \in \mathfrak{B}(\mathbb{H}_1, \mathbb{H}_2)$,*

1. $\|T^*\| = \|T\|$,
2. $\|T^* T\| = \|T\|^2$.

Proof:

1. By Cauchy-Schwarz inequality, for all $f \in \mathbb{H}_2$, $g \in \mathbb{H}_1$,

$$\begin{aligned} |\langle\, f \,|\, Tg \,\rangle_{\mathbb{H}_2}| &\leq \|f\|_{\mathbb{H}_2} \|Tg\|_{\mathbb{H}_2} \\ &\leq \|T\|_{\mathfrak{B}(\mathbb{H}_1, \mathbb{H}_2)} \|g\|_{\mathbb{H}_1} \|f\|_{\mathbb{H}_2} \end{aligned}$$

   so that

$$\|T\| \geq \sup\{|\langle\, f \,|\, Tg \,\rangle| : \|g\| \leq 1, \|f\| \leq 1\}.$$

   Conversely, we may assume that $\|T\| \neq 0$, and therefore choose some $\varepsilon \in]0, \|T\|/2[$. Choose now $g \in \mathbb{H}_1$ with $\|g\| \leq 1$, such that $\|Tg\| \geq \|T\| - \varepsilon$ and $f = \frac{Tg}{\|Tg\|} \in \mathbb{H}_2$, $\|f\| = 1$. For this particular choice of f and g:

$$|\langle\, f \,|\, Tg \,\rangle_{\mathbb{H}_2}| \geq \|Tg\| \geq \|T\| - \varepsilon.$$

   Hence,

$$\sup\{|\langle\, f \,|\, Tg \,\rangle| : \|g\| \leq 1, \|f\| \leq 1\} \geq \|T\| - \varepsilon.$$

   Since ε is arbitrary, we get $\|T\| = \sup\{|\langle\, f \,|\, Tg \,\rangle_{\mathbb{H}_2}| : g \in \mathbb{H}_1, f \in \mathbb{H}_2, \|g\| \leq 1, \|f\| \leq 1\}$. As $\langle\, f \,|\, Tg \,\rangle = \langle\, T^* f \,|\, g \,\rangle$ for all f and g, we get $\|T^*\| = \|T\|$

2. $\mathfrak{B}(\mathbb{H}_1, \mathbb{H}_2)$ being a normed algebra, $\|T^* T\| \leq \|T^*\| \|T\| = \|T\|^2$. Conversely,

$$\begin{aligned} \|T\|^2 &\leq \sup\{|Tf\| : f \in \mathbb{H}_1, \|f\| \leq 1\} \\ &= \sup\{|\langle\, Tf \,|\, Tf \,\rangle| : f \in \mathbb{H}_1, \|f\| \leq 1\} \\ &= \sup\{|\langle\, f \,|\, T^* Tf \,\rangle| : f \in \mathbb{H}_1, \|f\| \leq 1\} \\ &\leq \|T^* T\|. \end{aligned}$$

□

Definition 11.2.7. A C^***-algebra** $\mathfrak{A}$ is an involutive Banach algebra verifying additionally

$$\|a^*a\| = \|a\|^2, \text{ for all } a \in \mathfrak{A}.$$

Example 11.2.8. Let $\mathbb{X}$ be a compact Hausdorff[2] space and

$$\mathfrak{A} = \{f : \mathbb{X} \to \mathbb{C} \mid f \text{ continuous}\} \equiv C(\mathbb{X}).$$

Define

1. $\mathbb{C} \times \mathfrak{A} \ni (\lambda, f) \mapsto \lambda f \in \mathfrak{A}$ by $(\lambda f)(x) = \lambda f(x), \forall x \in \mathbb{X}$,
2. $\mathfrak{A} \times \mathfrak{A} \ni (f, g) \mapsto f + g \in \mathfrak{A}$ by $(f + g)(x) = f(x) + g(x), \forall x \in \mathbb{X}$,
3. $\mathfrak{A} \times \mathfrak{A} \ni (f, g) \mapsto fg \in \mathfrak{A}$ by $(fg)(x) = f(x)g(x), \forall x \in \mathbb{X}$,
4. $\mathfrak{A} \ni f \mapsto f^* \in \mathfrak{A}$ by $f^*(x) = \overline{f(x)}, \forall x \in \mathbb{X}$,

Then $\mathfrak{A}$ is a unital (specify the unit!) C^*-algebra for the norm $\|f\| = \sup_{x\in\mathbb{X}} |f(x)|$. (Prove it!) The algebra $\mathfrak{A}$ is moreover commutative.

Example 11.2.9. Let $\mathbb{H}_1$ and $\mathbb{H}_2$ be two Hilbert spaces. Then $\mathfrak{B}(\mathbb{H}_1, \mathbb{H}_2)$ is a unital C^*-algebra. In general, this algebra is not commutative.

This example has also a converse, given in theorem 11.5.2, below.

Example 11.2.10. Let $\mathbb{X}$ be a compact Hausdorff space. Then

$$\mathfrak{A} = C(\mathbb{X}) := \{f : \mathbb{X} \to \mathbb{C}, \text{ continuous}\}$$

equipped with the uniform norm and pointwise multiplication is a unital Banach commutative algebra; further equipped with an involution defined by complex conjugation, becomes a B^*-algebra.

Example 11.2.11. $\mathfrak{A} = \ell^1(\mathbb{Z})$, with à compléter.

Example 11.2.12. $\mathfrak{A} = L^1(\mathbb{R})$, with à compléter.

The previous example must not induce the reader to erroneously conclude that non-unital algebras have natural approximate identities since à compléter.

11.3 Convergence of sequences of operators

11.4 Classes of operators in $\mathfrak{B}(\mathbb{H})$

We shall see that any C^*-algebra can be faithfully represented on some Hilbert space $\mathbb{H}$; the different classes of abstract elements of the algebra, introduced in the previous section, have a counterpart in the context of this representation. But additionally, $\mathfrak{B}(\mathbb{H})$ is a very special C^*-algebra because is closed for the weak operator topology

2. Recall that a topological space is called Hausdorff when every two distinct of its points possess disjoint neighbourhoods.

(defined in §11.3). This fact endows $\mathfrak{B}(\mathbb{H})$ with a very rich family of projections allowing to generate [3] back the unital C^*-algebra $\mathfrak{B}(\mathbb{H})$.

11.4.1 Self-adjoint and positive operators

Definition 11.4.1. An operator $T \in \mathfrak{B}(\mathbb{H})$ is called **self-adjoint or Hermitean** [4] if $T = T^*$. The set of Hermitean operators on $\mathbb{H}$ is denoted by $\mathfrak{B}_h(\mathbb{H})$.

Exercise 11.4.2. The operator $T \in \mathfrak{B}(\mathbb{H})$ is self-adjoint if and only if $\langle f \mid Tf \rangle \in \mathbb{R}$ for all $f \in \mathbb{H}$. (Hint: use the polarisation equality **??**.)

Exercise 11.4.3. If $T \in \mathfrak{B}(\mathbb{H})$ is self-adjoint then $\|T\| = \sup\{\langle f \mid Tf \rangle, f \in \mathbb{H}, \|f\| \leq 1\}$.

Definition 11.4.4. An operator $T \in \mathfrak{B}(\mathbb{H})$ is called **positive** if $\langle f \mid Tf \rangle \geq 0$ for all $f \in \mathbb{H}$. Such an operator is necessarily self-adjoint. We denote by $\mathfrak{B}_+(\mathbb{H})$ the set of positive operators.

Exercise 11.4.5. Show that $T \in \mathfrak{B}_+(\mathbb{H})$ if and only if there exists $S \in \mathfrak{B}(\mathbb{H})$ such that $T = S^*S$.

11.4.2 Projections

Definition 11.4.6. Let $P, P_1, P2 \in \mathfrak{B}(\mathbb{H})$.

1. P is a **projection** if $P^2 = P$.
2. P is an **orthoprojection** if is a projection satisfying further $P^* = P$.
3. Two orthoprojections $P_1, P_2 \in \mathfrak{B}(\mathbb{H})$ are **orthogonal**, denoted $P_1 \perp P_2$ of their images are orthogonal subspaces of $\mathbb{H}$ (equivalently $P_1P_2 = 0$).

Projections are necessarily positive (why?). The set of orhoprojections is denoted by $\mathfrak{P}(\mathbb{H})$. All projections considered henceforth will be orthoprojections.

Exercise 11.4.7. (A very important one!) Let (P_n) be a sequence of orthoprojections. We have already shown that there is a bijection between $\mathfrak{P}(\mathbb{H})$ and the set of closed subspaces of $\mathbb{H}$ and orthoprojections, given by $\mathfrak{P}(\mathbb{H}) \ni P \mapsto P(\mathbb{H}) \subset \mathbb{H}$, with $P(\mathbb{H})$ closed.

1. Show that that $\mathfrak{P}(\mathbb{H})$ is partially ordered, i.e. $P_1 \leq P_2$ if $P_1(\mathbb{H})$ subspace of $P_2(\mathbb{H})$ (equivalently $P_1P_2 = P_1$.)
2. For general orthoprojections P_1 and P_2, is P_1P_2 an orthoprojection?
3. Show that P_1 and P_2 have a least upper bound.
4. Is $Q = P_1 + \ldots + P_n$ an orthoprojection?
5. Is $Q = P_2 - P_1$ an orthoprojection?

3. In some general unital C^*-algebras there are only two trivial projections 0 and 1. Therefore the situation arising in $\mathfrak{B}(\mathbb{H})$ is far from being a general property of C^*-algebras.

4. Strictly speaking, the term Hermitean is more general; it applies also to unbounded operators and it means self-adjoint on a dense domain. The two terms coincide for bounded operators.

6. Show that a monotone sequence of orthoprojections converges strongly towards an orthoprojection.

11.4.3 Unitary operators

Definition 11.4.8. An operator $U \in \mathfrak{B}(\mathbb{H})$ is **unitary** if $U^*U = UU^* = \mathbb{1}$. The set of unitary operators is denoted by $\mathfrak{U}(\mathbb{H}) = \{U \in \mathfrak{B}(\mathbb{H}) : U^*U = UU^* = \mathbb{1}\}$ (it is in fact a group; for $\mathbb{H} = \mathbb{C}^n$ it is the Lie group denoted by $U(n)$.)

11.4.4 Isometries and partial isometries

Definition 11.4.9. An operator $T \in \mathfrak{B}(\mathbb{H}_1, \mathbb{H}_2)$ is an **isometry** if $T^*T = \mathbb{1}$ (or equivalently $\|Tf\| = \|f\|$, for all $f \in \mathbb{H}_1$.)

Exercise 11.4.10. Let $\mathbb{H} = \ell^2(\mathbb{N})$ and for $x = (x_1, x_2, x_3, \ldots) \in \mathbb{H}$, define the left and right shifts by

$$Lx = (x_2, x_3, \ldots) \in \mathbb{H},$$

and

$$Rx = (0, x_1, x_2, x_3, \ldots) \in \mathbb{H}.$$

1. Show that $R^* = L$.
2. Show that R is an isometry.
3. Determine $\mathsf{Ran}R$.

This exercise demonstrates that, in infinite dimensional spaces, isometries are not necessarily surjective.

Theorem 11.4.11. *For $T \in \mathfrak{B}(\mathbb{H}_1, \mathbb{H}_2)$, the five following conditions are equivalent:*

1. $(T^*T)^2 = T^*T$,
2. $(TT^*)^2 = TT^*$,
3. $TT^*T = T$,
4. $T^*TT^* = T^*$,
5. *there exist closed subspaces $E_1 \subseteq \mathbb{H}_1$ and $E_2 \subseteq \mathbb{H}_2$ such that $T = I \circ S \circ P$ where $P : \mathbb{H}_1 \to E_1$ is a projection, $S : E_1 \to E_2$ an isometry, and $I : E_2 \to \mathbb{H}_2$ the inclusion map.*

*If one (hence all) condition holds then T^*T is the projection $\mathbb{H}_1 \to E_1$ and TT^* is the projection $\mathbb{H}_2 \to E_2$. In this situation T is called a **partial isometry** with initial space E_1, initial projection T^*T, final space E_2, and final projection TT^*.*

Proof. Exercise! (See [4] or [128].) □

Exercise 11.4.12. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space and $T : \Omega \to \Omega$ a measure preserving transformation i.e. $\mathbb{P}(T^{-1}B) = \mathbb{P}(B)$ for all $B \in \mathcal{F}$. On the Hilbert space $\mathbb{H} = L^2(\Omega, \mathcal{F}, \mathbb{P})$ define $U : \mathbb{H} \to \mathbb{H}$ by $Uf(\omega) = f(T^{-1}\omega)$.

1. Show that U is a partial isometry.
2. Under which condition is U surjective (hence unitary)?

11.4.5 Normal operators

Definition 11.4.13. An operator $T \in \mathfrak{B}(\mathbb{H})$ is **normal** if $T^*T = TT^*$ (or equivalently if $\|T^*f\| = \|Tf\|$ for all $f \in \mathbb{H}$.)

Exercise 11.4.14. A vector $f \in \mathbb{H} \setminus \{0\}$ is called an **eigenvector** corresponding to an **eigenvalue** λ of an operator $T \in \mathfrak{B}(\mathbb{H})$ if $Tf = \lambda f$ for some $\lambda \in \mathbb{C}$. Show that if T is normal and f_1, f_2 are eigenvectors corresponding to different eigenvalues then $f_1 \perp f_2$. (The proof goes as for the finite dimensional case.)

Exercise 11.4.15. Let M be the multiplication operator on $L^2[0,1]$ defined by $Mf(t) = tf(t), t \in [0,1]$. Show that

1. M is self-adjoint (hence normal),
2. M has no eigenvectors.

Exercise 11.4.16. Choose some $z \in \mathbb{C}$ with $|z| < 1$ and consider $\zeta \in \ell^2(\mathbb{N})$ given by $\zeta = (1, z, z^2, z^3, \ldots)$. Let L and R be the left and right shifts defined in exercise 11.4.10.

1. Show that R is not normal,
2. compute $R^*\zeta$,
3. conclude that R^* has uncountably many eigenvalues.

11.5 States on algebras, GNS construction, representations

Paragraphe incomplet.

Definition 11.5.1. Let $\mathfrak{A}$ be an involutive Banach algebra. A **representation** on a Hilbert space $\mathbb{H}$ of $\mathfrak{A}$ is a $*$-homomorphism of $\mathfrak{A}$ into $\mathfrak{B}(\mathbb{H})$, i.e. a linear map $\pi : \mathfrak{A} \to \mathfrak{B}(\mathbb{H})$ such that

1. $\pi(ab) = \pi(a)\pi(b), \forall a, b \in \mathfrak{A}$,
2. $\pi(a^*) = \pi(a)^*, \forall a \in \mathfrak{A}$,

The space $\mathbb{H}$ is called the **representation space**. We write $(\pi, \mathbb{H})$, or $\mathbb{H}_\pi$ if necessary. Two representations $(\pi_1, \mathbb{H}_1)$ and $(\pi_2, \mathbb{H}_2)$ are said to be **unitarily equivalent** if there exists an isometry $U : \mathbb{H}_1 \to \mathbb{H}_2$ such that for all $a \in \mathfrak{A}$, it holds $U\pi_1(a)U^* = \pi_2(a)$. If moreover for every non zero element of $\mathfrak{A}$, $\pi(a) \neq 0$, then the representation is called **faithful**.

Theorem 11.5.2 (Gel'fand-Naïmark). *If $\mathfrak{A}$ is an arbitrary C^*-algebra, there exists a Hilbert space $\mathbb{H}$ and a linear mapping $\pi : \mathfrak{A} \to \mathfrak{B}(\mathbb{H})$ that is a faithful representation of $\mathfrak{A}$.*

Proof: It can be found in [92, theorem 4.5.6, page 281]. □

12

Spectral theory in Banach algebras

12.1 Motivation

In linear algebra one often encounters systems of linear equations of the type

$$Tf = g \tag{12.1}$$

with $f, g \in \mathbb{C}^n$ and $T = (t_{i,j})_{i,j=1,\dots,n}$ a $n \times n$ matrix with complex coefficients. Elementary linear algebra establishes that this system of equations has **solutions** provided that the map $f \mapsto Tf$ is surjective and the solution is unique provided that this map is injective. Thus the system has a unique solution for each $g \in \mathbb{C}^n$ provided that the map is bijective, or equivalently the matrix T is invertible. This happens precisely when $\det T \neq 0$. However, this criterion of invertibility is of limited practical use even for the elementary (finite-dimensional) case because det is too complicated an object to be efficiently computed for large n. For infinite dimensional cases, this criterion becomes totally useless since there is no infinite dimensional analogue of det that discriminates between invertible and non-invertible operators T (see exercise 12.1.1 below!)

Another general issue connected with the system (12.1) is that of **eigenvalues**. For every $\lambda \in \mathbb{C}$, denote by $V_\lambda = \{f \in \mathbb{C}^n : Tf = \lambda f\}$. For most choices of λ, the subspace V_λ is the trivial subspace $\{0\}$; this subspace is not trivial only when $T - \lambda\mathbb{1}$ is not injective (i.e. $\ker(T - \lambda\mathbb{1}) \neq \{0\}$.) On defining the **spectrum** of T by

$$\operatorname{spec}(T) = \{\lambda \in \mathbb{C} : T - \lambda\mathbb{1} \text{ is not invertible } \},$$

one easily shows that $\operatorname{spec}(T) \neq \emptyset$ and $\operatorname{card}\operatorname{spec}(T) \leq n$ (why?) Not always the family $(V_\lambda)_{\lambda \in \operatorname{spec}(T)}$ spans the whole space $\mathbb{C}^n$. When it does, on decomposing $g = g^{(1)} + \dots + g^{(k)}$ where $g^{(j)} \in V_{\lambda_j}$ and $\operatorname{spec}(T) = \{\lambda_1, \dots, \lambda_k\}$, the solution of (12.1) is given by

$$f = \frac{g^{(1)}}{\lambda_1} + \dots + \frac{g^{(k)}}{\lambda_k}.$$

(Notice that $\lambda_i \neq 0$, for all $i = 1, \ldots, k$; why?) When the family $(V_\lambda)_{\lambda \in \mathsf{spec}(T)}$ does not span $\mathbb{C}^n$, the problem is more involved but the rôle of the spectrum remains fundamental.

A final issue involving the spectrum of T is the **functional calculus** associated with T. If $p \in \mathbb{R}[t]$, this polynomial can be naturally extended on $\mathfrak{B}(\mathbb{H})$. In fact, if $p(t) = a_n t^n + \ldots a_0$ is the expression of the polynomial p; the expression $p(T) = a_n T^n + \ldots a_0 \mathbb{1}$ is well defined for all $T \in \mathfrak{B}(\mathbb{H})$. Moreover, if $T \in \mathfrak{B}_h(\mathbb{H})$ then $p(T) \in \mathfrak{B}_h(\mathbb{H})$. Suppose now that $T \in \mathfrak{B}_h(\mathbb{H})$, $m = \inf_{\|f\|=1} \langle f \,|\, Tf \rangle$, $M = \sup_{\|f\|=1} \langle f \,|\, Tf \rangle$, and $p(t) \geq 0$ for all $t \in [m, M]$; then $p(T) \in \mathfrak{B}_+(\mathbb{H})$. Now every $f \in C[m, M]$ can be uniformly approximated by polynomials, i.e. there is a sequence $(p_l)_{l \in \mathbb{N}}$, with $p_l \in \mathbb{R}[t]$ such that for all $\varepsilon > 0$, there exists $n_0 \in \mathbb{N}$ such that for $l \geq n_0$, $\max_{t \in [m,M]} |f(t) - p_l(t)| < \varepsilon$. It is natural then to define $f(T) = \lim_l p_l(T)$. However, the computations involved in the right hand side of this equation can be very complicated. Suppose henceforth that $\mathbb{H} = \mathbb{C}^n$ and T is a Hermitean $n \times n$ matrix that is diagonalisable, i.e. $T = UDU^*$ with $D = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$ and U unitary. Then $p_l(T) = U p_l(D) U^*$ and letting $l \to \infty$ we get $f(T) = U f(D) U^*$. Thus, if T is diagonalisable, the computation of $f(T)$ is equivalent to the knowledge of $f(t)$ for $t \in \mathsf{spec}(T)$. For the infinite dimensional case, the problem is more involved but again the spectrum remains fundamental.

The rest of this chapter, based on [4], is devoted to the appropriate generalisation of the spectrum for infinite dimensional operators.

Exercise 12.1.1. (Infinite-dimensional determinant) Let $\mathbb{H} = \ell^2(\mathbb{N})$ and $(t_n)_{n \in \mathbb{N}}$ be a fixed numerical sequence. Suppose that there exist constants $K_1, K_2 > 0$ such that $0 < K_1 \leq t_n \leq K_2 < \infty$ for all $n \in \mathbb{N}$. For every $x \in \ell^2(\mathbb{N})$ define $(Tx)_n = t_n x_n, n \in \mathbb{N}$.

1. Show that $T \in \mathfrak{B}(\mathbb{H})$.
2. Exhibit a bounded operator S on $\mathbb{H}$ such that $ST = TS = \mathbb{1}$.
3. Assume henceforth that $(t_n)_{n \in \mathbb{N}}$ is a monotone sequence. Let $\Delta_n(T) = t_1 \cdots t_n$. Show that $\Delta_n(T)$ converges to a non-zero limit $\Delta(T)$ if and only if $\sum_n (1 - t_n) < \infty$.
4. Any plausible generalisation, δ, of det in the infinite dimensional setting should verify $\delta(\mathbb{1}) = 1$, $\delta(AB) = \delta(A)\delta(B)$, and if T is diagonal $\delta(T) = \Delta(T)$. Choosing $t_n = \frac{n}{n+1}$, for $n \in \mathbb{N}$, conclude that although T is diagonal and invertible, nevetheless has $\delta(T) = 0$.

12.2 The spectrum of an operator acting on a Banach space

Let $\mathbb{V}$ be a $\mathbb{C}$-Banach space. Denote by $\mathfrak{B}(\mathbb{V})$ the set of bounded operators $T : \mathbb{V} \to \mathbb{V}$. This space is itself a unital Banach algebra for the induced operator norm.

Exercise 12.2.1. If $\mathbb{X}$ and $\mathbb{Y}$ are metric spaces and $d_{\mathbb{X}}$ and $d_{\mathbb{Y}}$ denote their respective metrics

1. verify that

$$d_p((x_1,y_1),(x_2,y_2)) = (d_{\mathbb{X}}(x_1,x_2)^p + d_{\mathbb{Y}}(y_1,y_2)^p)^{1/p},$$

with $p \in [1,\infty[$ and

$$d_\infty((x_1,y_1),(x_2,y_2)) = \max(d_{\mathbb{X}}(x_1,x_2), d_{\mathbb{Y}}(y_1,y_2))$$

are metrics on $\mathbb{X}\times\mathbb{Y}$; (the corresponding metric space $(\mathbb{X}\times\mathbb{Y}, d_p)$, $p\in[1,\infty]$ is denoted [1] $\mathbb{X}\oplus\mathbb{Y}$)

2. show that the sequence $(x_n,y_n)_n$ in $\mathbb{X}\times\mathbb{Y}$ converges to a point $(\xi,\psi)\in\mathbb{X}\times\mathbb{Y}$ with respect to any of the metrics d_p if and only if $d_{\mathbb{X}}(x_n,\xi)\to 0$ and $d_{\mathbb{Y}}(y_n,\psi)\to 0$.

Exercise 12.2.2. Let $\mathbb{X}$ and $\mathbb{Y}$ be metric spaces and $f:\mathbb{X}\to\mathbb{Y}$ be a continuous map. We denote by

$$\Gamma(f) = \{(x,f(x)) : x\in\mathbb{X}\}$$

the graph of f. Show that $\Gamma(f)$ is closed (i.e. if $(x_n)_n$ is a sequence in $\mathbb{X}$ and if there exists $(x,y)\in\mathbb{X}\times\mathbb{Y}$ such that $x_n\to x$ and $f(x_n)\to y$, then necessarily $y=f(x)$.)

Exercise 12.2.3. (The closed graph theorem) Suppose $\mathbb{X}$ and $\mathbb{Y}$ are Banach spaces and $T:\mathbb{X}\to\mathbb{Y}$ a linear map having closed graph. Show that T is continuous.

Theorem 12.2.4. *For every $T\in\mathfrak{B}(\mathbb{V})$, the following are equivalent:*

1. *for every $y\in\mathbb{V}$ there is a unique $x\in\mathbb{V}$ such that $Tx=y$,*
2. *there is an operator $S\in\mathfrak{B}(\mathbb{V})$ such that $ST=TS=\mathbb{1}$.*

Proof: Only the part $1\Rightarrow 2$ is not trivial to show. Condition 1 implies that T is invertible; call S its inverse. The only thing to show is the boundedness of S. As a subset of $\mathbb{V}\oplus\mathbb{V}$, the graph of S is related to the graph of T. In fact

$$\Gamma(S) = \{(y,Sy) : y\in\mathbb{V}\} = \{(Tx,x), x\in\mathbb{V}\}.$$

Now T is bounded, hence continuous, so that that the set $\{(Tx,x), x\in\mathbb{V}\}$ is closed (see exercise 12.2.2.) Thus the graph of S is closed, and by the closed graph theorem (see exercise 12.2.3), S is continuous hence bounded. □

Definition 12.2.5. Let $T\in\mathfrak{B}(\mathbb{V})$ where $\mathbb{V}$ is a Banach space.

1. T is called **invertible** if there exists an operator $S\in\mathfrak{B}(\mathbb{V})$ such that $ST=TS=\mathbb{1}$.
2. The **spectrum** of T, denoted by $\mathsf{spec}(T)$, is defined by

$$\mathsf{spec}(T) = \{\lambda\in\mathbb{C} : T-\lambda\mathbb{1} \text{ is not invertible}\}.$$

3. The **resolvent set** of T, denoted by $\mathsf{Res}(T)$, is defined by

$$\mathsf{Res}(T) = \mathbb{C}\setminus\mathsf{spec}(T).$$

1. more precisely $\mathbb{X}\oplus_{\ell^p}\mathbb{Y}$.

Notice that in finite dimension, invertibility of an operator R reduces essentially to injectivity of R since surjectivity of R can be trivially verified if we reduce the space V into $\mathsf{Ran}(R)$. In infinite dimension, several things can go wrong: of course injectivity may fail as in finite dimension; but a new phenomenon can appear when $\mathsf{Ran}(R)$ is not closed: in this latter case, $\mathsf{Ran}(R)$ can further be dense in V or fail to be dense in V. All these situations may occur and correspond to different types of sub-spectra.

Definition 12.2.6. Let $T \in \mathfrak{B}(\mathbb{V})$ where $\mathbb{V}$ is a Banach space.

1. The **point spectrum** of T is defined by
$$\mathsf{spec}_p(T) = \{\lambda \in \mathbb{C} : T - \lambda\mathbb{1} \text{ is not injective}\}.$$
Every $\lambda \in \mathsf{spec}_p(T)$ is called an **eigenvalue** of T.
2. The **continuous spectrum**, $\mathsf{spec}_c(T)$, of T is defined as the set of complex values λ such that $T - \lambda\mathbb{1}$ is injective but not surjective and $\mathsf{Ran}(T - \lambda\mathbb{1})$ is dense in $\mathbb{V}$.
3. The **residual spectrum**, $\mathsf{spec}_r(T)$, of T is defined as the complex values λ such that $T - \lambda\mathbb{1}$ is injective but not surjective and $\mathsf{Ran}(T - \lambda\mathbb{1})$ is not dense in $\mathbb{V}$.

Example 12.2.7. Let $\mathbb{V}$ be a finite dimensional Banach space and $T : \mathbb{V} \to \mathbb{V}$ a linear transformation (hence bounded.) Since $\dim \ker(T - \lambda\mathbb{1}) + \dim \mathsf{Ran}(T - \lambda\mathbb{1}) = \dim \mathbb{V}$, it follows that $T - \lambda\mathbb{1}$ is injective if and only if $\mathsf{Ran}(T - \lambda\mathbb{1}) = \mathbb{V}$. Therefore $\mathsf{spec}_r(T) = \emptyset$. Further, if $T - \lambda\mathbb{1}$ is injective, then it has an inverse on $\mathbb{V}$. Since any linear transformation of a finite dimensional space is continuous, it follows that $(T - \lambda\mathbb{1})^{-1}$ is continuous, hence $\mathsf{spec}_c(T) = \emptyset$. Therefore, in finite dimension we always have $\mathsf{spec}(T) = \mathsf{spec}_p(T)$.

Exercise 12.2.8. Let $\mathbb{V} = \ell^2(\mathbb{N})$ and consider the right shift, R, on $\mathbb{V}$.

1. Show that $R - \lambda\mathbb{1}$ is injective for all $\lambda \in \mathbb{C}$. Conclude that $\mathsf{spec}_p(R) = \emptyset$.
2. Show that for $|\lambda| > 1$, $\mathsf{Ran}(R - \lambda\mathbb{1}) = \mathbb{V}$. Conclude that all $\lambda \in \mathbb{C}$ with $|\lambda| > 1$ belong to $\mathsf{Res}(R)$.
3. For $|\lambda| < 1$, show that $\mathsf{Ran}(R - \lambda\mathbb{1})$ is orthogonal to the vector $\Lambda = (1, \lambda, \lambda^2, \ldots)$. Show that for $|\lambda| < 1$, $\mathsf{Ran}(R - \lambda\mathbb{1}) = \{y \in \mathbb{V} : y \perp \Lambda\}$. Conclude that all $\lambda \in \mathbb{C}$ with $|\lambda| < 1$ belong to $\mathsf{spec}_r(R)$.
4. The case $|\lambda| = 1$ is the most difficult. Try to show that $\mathsf{Ran}(R - \lambda\mathbb{1})$ is dense in $\mathbb{V}$ so that the unit circle coincides with $\mathsf{spec}_c(R)$.

12.3 The spectrum of an element of a Banach algebra

In the previous section we studied spectra of bounded operators acting on Banach spaces. They form a Banach algebra with unit. Spectral theory can be established also abstractly on Banach algebras. Before stating spectral properties, it is instructive to give some more examples.

Example 12.3.1. Let $C_c(\mathbb{R})$ be the set of continuous functions on $\mathbb{R}$ which vanish outside a bounded interval; it is a normed vector space (with respect to the L^1 norm for

instance; its completion is the Banach space $L^1(\mathbb{R}, \lambda)$, where λ stands for the Lebesgue measure.) A product can be defined by the convolution

$$f \star g(x) = \int_{\mathbb{R}} f(y)g(x-y)\lambda(dy)$$

turning this space into a commutative Banach algebra. This algebra is not unital (this can be seen by solving the equation $f \star f = f$ in L^1), but it has an approximate unit (i.e. a sequence $(f_n)_n$ of integrable functions with $\|f_n\| = 1$ for all n and such that for all $g \in L^1(\mathbb{R})$, $\|g \star f_n - g\| \to 0$. (Give an explicit example of such an approximate unit!)

Example 12.3.2. The algebra $\mathbf{M}_n(\mathbb{C})$ is a unital non-commutative algebra. There are many norms that turn it into a finite-dimensional Banach algebra, for instance:

1. $\|A\| = \sum_{i,j=1}^n |a_{i,j}|$
2. $\|A\| = \sup_{\|x\|\leq 1} \frac{\|Ax\|}{\|x\|}$.

Definition 12.3.3. Let $\mathfrak{A}$ be a unital Banach algebra. (We can always assume that $\|\mathbb{1}\| = 1$, may be after re-norming the elements of $\mathfrak{A}$.) An element $a \in \mathfrak{A}$ is called **invertible** if there is an element $b \in \mathfrak{A}$ such that $ab = ba = \mathbb{1}$. The set of all invertible elements of $\mathfrak{A}$ is denoted by $\mathsf{GL}(\mathfrak{A})$ and called the **general linear group of invertible elements** of $\mathfrak{A}$.

Theorem 12.3.4. *Let $\mathfrak{A}$ be a unital Banach algebra. If $a \in \mathfrak{A}$ and $\|a\| < 1$ then $\mathbb{1} - a$ is invertible and*

$$(\mathbb{1} - a)^{-1} = \sum_{n=0}^{\infty} a^n.$$

Moreover,

$$\|(\mathbb{1} - a)^{-1}\| \leq \frac{1}{1 - \|a\|}$$

and

$$\|\mathbb{1} - (\mathbb{1} - a)^{-1}\| \leq \frac{\|a\|}{1 - \|a\|}.$$

Proof: Since $\|a^n\| \leq \|a\|^n$ for all n, we can define $b \in \mathfrak{A}$ as the sum of the absolutely convergent series $b = \sum_{n=0}^{\infty} a^n$. Moreover, $b(\mathbb{1} - a) = (\mathbb{1} - a)b = \lim_{N\to\infty} \sum_{n=0}^N b^n = \lim_{N\to\infty}(\mathbb{1} - b^{N+1}) = \mathbb{1}$. Hence $\mathbb{1} - a$ is invertible and $(\mathbb{1} - a)^{-1} = b$. The first majorisation holds because $\|b\| \leq \sum_{n=0}^{\infty} \|a\|^n = \frac{1}{1-\|a\|}$. The second one follows from remarking that $\mathbb{1} - b = -\sum_{n=1}^{\infty} a^n = -ab$, hence $\|\mathbb{1} - b\| \leq \|a\|\|b\|$. □

Exercise 12.3.5.

1. Prove that $\mathsf{GL}(\mathfrak{A})$ is an open set in $\mathfrak{A}$ and that the mapping $a \mapsto a^{-1}$ is continuous on $\mathsf{GL}(\mathfrak{A})$.
2. Justify the term "general linear group" of invertible elements, i.e. show that $\mathsf{GL}(\mathfrak{A})$ is a topological group in the relative norm topology.

Definition 12.3.6. Let $\mathfrak{A}$ be a unital Banach algebra. For every $a \in \mathfrak{A}$, the **spectrum** of a is the set

$$\mathsf{spec}(a) = \{\lambda \in \mathbb{C} : a - \lambda\mathbb{1} \notin \mathsf{GL}(\mathfrak{A})\}.$$

In the rest of this section, $\mathfrak{A}$ will be a unital algebra and we shall write $a - \lambda$ instead of $a - \lambda\mathbb{1}$.

Proposition 12.3.7. *For every $a \in \mathfrak{A}$, the set* $\mathsf{spec}(a)$ *is a closed subset of the disk* $\{\lambda \in \mathbb{C} : |\lambda| \leq \|a\|\}$.

Proof: Consider the resolvent set

$$\mathsf{Res}(a) = \{\lambda \in \mathbb{C} : a - \lambda \in \mathsf{GL}(A)\} = \mathbb{C} \setminus \mathsf{spec}(a).$$

Since the set $\mathsf{GL}(\mathfrak{A})$ is open (see exercise 12.3.5) and the map $\mathbb{C} \ni \lambda \mapsto a - \lambda \in \mathfrak{A}$ continuous, the set $\mathsf{Res}(a)$ is open hence the set $\mathsf{spec}(a)$ is closed. Moreover, if $|\lambda| > \|a\|$, on writing $a - \lambda = (-\lambda)[1 - a/\lambda]$ and remarking that $\|a/\lambda\| < 1$, we conclude that $a - \lambda \in \mathsf{GL}(\mathfrak{A})$. □

Theorem 12.3.8. *For every $a \in \mathfrak{A}$, the set* $\mathsf{spec}(a)$ *is non-empty.*

Proof: Fix some $\lambda_0 \in \mathsf{Res}(a)$. Since $\mathsf{Res}(a)$ is open, there is a small neighbourhood $\mathcal{V}_{\geq}$ of λ_0 contained in $\mathsf{Res}(a)$. The $\mathfrak{A}$-valued function $\lambda \mapsto (a - \lambda)^{-1}$ is well defined for all $\lambda \in \mathcal{V}_{\geq}$. Moreover, for $\lambda, \lambda_0 \in \mathsf{Res}(a)$,

$$\begin{aligned}(a-\lambda)^{-1} - (a-\lambda_0)^{-1} &= (a-\lambda)^{-1}[(a-\lambda_0) - (a-\lambda)](a-\lambda_0)^{-1} \\ &= (\lambda - \lambda_0)(a-\lambda)^{-1}(a-\lambda_0)^{-1}.\end{aligned}$$

Thus

$$\lim_{\lambda \to \lambda_0} \frac{1}{\lambda - \lambda_0}[(a-\lambda) - (a-\lambda_0)] = (a-\lambda_0)^{-2}.$$

Assume now that $\mathsf{spec}(a) = \emptyset$ and choose an arbitrary bounded linear functional $\phi : \mathfrak{A} \to \mathbb{C}$. Then, the scalar function $f : \mathbb{C} \to \mathbb{C}$ defined by $\lambda \mapsto f(\lambda) = \phi((a-\lambda)^{-1})$ is defined on the whole $\mathbb{C}$. By linearity, the function f has everywhere a complex derivative, satisfying $f'(\lambda) = \phi((a-\lambda)^{-2})$. Thus f is an entire function. Notice moreover that f is bounded and for $|\lambda| > \|a\|$, by theorem 12.3.4,

$$\begin{aligned}\|(a-\lambda)^{-1}\| &= \frac{\|(1-a/\lambda)^{-1}\|}{|\lambda|} \\ &\leq \frac{1}{|\lambda|(1 - \|a\|/|\lambda|)} \\ &= \frac{1}{|\lambda| - \|a\|}.\end{aligned}$$

Thus $\lim_{\lambda\to\infty} f(\lambda) = 0$ and since this function is bounded and entire, by Liouville's theorem (see [**?**] for instance), it is constant, hence $f(\lambda) = 0$ for all $\lambda \in \mathbb{C}$ and every linear functional ϕ. The Hahn-Banach theorem implies then that $(a-\lambda)^{-1} = 0$ for all $\lambda \in \mathbb{C}$. But this is absurd because $(a-\lambda)$ is invertible and $\mathbb{1} \neq 0$ in $\mathfrak{A}$. □

Definition 12.3.9. For every $a \in \mathfrak{A}$, the **spectral radius** of a is defined by $r(a) = \sup\{|\lambda| : \lambda \in \mathsf{spec}(a)\}$.

Exercise 12.3.10.

1. Let $p \in \mathbb{R}[t]$ and $a \in \mathfrak{A}$. Show that $p(\mathsf{spec}(a)) \subseteq \mathsf{spec}(p(a))$. (Hint: if $\lambda \in \mathsf{spec}(a)$, the map $\lambda' \mapsto p(\lambda') - p(\lambda)$ is a polynomial vanishing at $\lambda' = \lambda$. Conclude that $p(a) - p(\lambda)$ cannot be invertible.)
2. For every $a \in \mathfrak{A}$ show that $r(a) = \lim_{n\to\infty} \|a^n\|^{1/n}$.

12.4 Relation between diagonalisability and the spectrum

Motivated again by elementary linear algebra, we recall that a self-adjoint $n \times n$ matrix T can be diagonalised, i.e. it is possible to find a diagonal matrix $D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$ and a unitary matrix U such that $T = UDU^*$; we have then $\mathrm{spec}(T) = \{d_1, \ldots, d_n\}$. We shall generalise this result to infinite dimensional spaces.

An orthonormal basis for $\mathbb{H}$ is a sequence $\mathcal{E} = (e_1, e_2, \ldots)$ of mutually orthogonal unit vectors of $\mathbb{H}$ such that [2] $\overline{\mathrm{span}}\mathcal{E} = \mathbb{H}$. On fixing such a basis, we define a unitary operator $U : \ell^2(\mathbb{N}) \to \mathbb{H}$ by

$$Uf = \sum_{i \in \mathbb{N}} f_i e_i$$

for $f = (f_1, f_2, \ldots)$. Specifying a particular orthonormal basis in $\mathbb{H}$ is equivalent to specifying a particular unitary operator U. Suppose now that $T \in \mathfrak{B}(\mathbb{H})$ is a normal operator and admits the basis vectors of $\mathcal{E}$ as eigenvectors, i.e. $Te_k = t_k r_k$, $t_k \in \mathbb{C}$, $k \in \mathbb{N}$. Then $t = (t_k)_k \in \ell^\infty(\mathbb{N})$ and $U^*TU = M$ where M is the multiplication operator defined by $(Mf)_k = (U^*TUf)_k = (U^{-1}TUf)_k = (U^{-1}T\sum_i f_i e_i)_k = f_k t_k$. Thus an operator T on $\mathbb{H}$ is diagonalisable in a given basis $\mathcal{E}$ if the unitary operator associated with $\mathcal{E}$ implements an equivalence between T and a multiplication operator M acting on $\ell^2(\mathbb{N})$. This notion is still inadequate since it involves only normal operators with pure point spectrum; it can nevertheless be appropriately generalised.

Definition 12.4.1. An operator T acting on a Hilbert space $\mathbb{H}$ is said **diagonalisable** if there exist a (necessarily separable) σ-finite measure space $(\Omega, \mathcal{F}, \mu)$, a function $m \in L^\infty(\Omega, \mathcal{F}, \mu)$, and a unitary operator $U : L^2(\Omega, \mathcal{F}, \mu) \to \mathbb{H}$ such that

$$UM_m = TU$$

where M_m denotes the multiplication operator by m, defined by $M_m f(\omega) = m(\omega) f(\omega)$, for all $\omega \in \Omega$ and all $f \in L^2(\Omega, \mathcal{F}, \mu)$

Example 12.4.2. Let $\mathbb{H} = L^2([0,1])$ and $T : \mathbb{H} \to \mathbb{H}$ defined by $Tf(t) = tf(t)$, for $t \in [0,1]$ and $f \in \mathbb{H}$. This operator is diagonalisable since it is already a multiplication operator.

Notice that a diagonalisable operator is always normal because the multiplication operator is normal. The following theorem asserts the converse.

Theorem 12.4.3. *Every normal operator acting on a Hilbert space is diagonalisable.*

Proof: Long but without any particular difficulty; it can be found in [4], pp. 52–55. □

Le reste du chapitre doit être re-écrit.

2. Recall that $\mathbb{H}$ is always considered separable.

12.5 Spectral measures and functional calculus

Recall the example 2.3.3. In the non-commutative setting, the analogue of a bounded, real-valued, measurable function is a bounded Hermitean operator on $\mathbb{H}$. Idempotence, characterising indicators in the commutative case, is verified by projections belonging to $\mathfrak{P}(\mathbb{H})$. Hence, we are seeking approximations of bounded Hermitean operators by complex finite combinations of projections. Now we can turn into precise definitions.

Definition 12.5.1. Let $(\mathbb{X}, \mathcal{F})$ be a measurable space and $\mathbb{H}$ a Hilbert space. A function $P : \mathcal{F} \to \mathfrak{P}(\mathbb{H})$ is called a **spectral measure** on $(\mathbb{X}, \mathcal{F})$ if

1. $P(\mathbb{X}) = \mathbb{1}$,
2. if $(F_n)_{n\in\mathbb{N}}$ is a sequence of disjoint elements in $\mathcal{F}$, then
$$P(\sqcup_{n\in\mathbb{N}} F_n) = \sum_{n\in\mathbb{N}} P(F_n).$$

Example 12.5.2. Let $(\mathbb{X}, \mathcal{F}, \mu)$ be a probability space and $\mathbb{H} = L^2(\mathbb{X}, \mathcal{F}, \mu)$. Then the mapping $\mathcal{F} \ni F \mapsto P(F) \in \mathfrak{P}(\mathbb{H})$, defined by $P(F)f = \mathbb{1}_F f$ for all $f \in \mathbb{H}$, is a spectral measure.

Exercise 12.5.3. If P is a spectral measure on $(\mathbb{X}, \mathcal{F})$, then $P(\emptyset) = 0$ and P is finitely disjointly additive.

Theorem 12.5.4. *Let $(\mathbb{X}, \mathcal{F})$ be a measurable space and $\mathbb{H}$ a Hilbert space. If P is a finitely disjointly additive function $\mathcal{F} \to \mathfrak{P}(\mathbb{H})$ such that $P(\mathbb{X}) = \mathbb{1}$ then (for $F, G \in \mathcal{F}$)*

1. *P is monotone: $F \subseteq G \Rightarrow P(F) \leq P(G)$,*
2. *P is subtractive: $F \subseteq G \Rightarrow P(G \setminus F) = P(G) - P(F)$,*
3. *P is modular: $P(F \cup G) + P(F \cap G) = P(F) + P(G)$,*
4. *P is multiplicative: $P(F \cap G) = P(F)P(G)$.*

Proof. 1. The statement is immediate by noticing that $F \subseteq G \Rightarrow G = F \sqcup (G \setminus F)$.

2. The same remark holds.

3. Since $F \cup G = (F \setminus G) \sqcup (F \cap G) \sqcup (G \setminus F)$ we have:
$$\begin{aligned} P(F \cup G) + P(F \cap G) &= [P(F \setminus G) + P(F \cap G)] + [P(G \setminus F) + P(G \cap F)] \\ &= P(F) + P(G). \end{aligned}$$

4. By 1.
$$P(F \cap G) \leq P(F) \leq P(F \cup G). \qquad (*)$$
Multiplying the first inequality of (*) by $P(F \cap G)$, we get $P(F \cap G) \leq P(F)P(F \cap G)$ and since $P(F) \leq \mathbb{1}$, the right hand side of the latter inequality is bounded further by $P(F \cap G)$. Hence $P(F)P(F \cap G) = P(F \cap G)$. Similarly, multiplying the second inequality of (*) by $P(F)$ and since again $P(F \cup G) \leq \mathbb{1}$, we get $P(F)P(F \cup G) = P(F)$. Adding the thus obtained equalities, we get:
$$P(F)[P(F \cup G) + P(F \cap G)] = P(F \cap G) + P(F)$$
and we conclude by modularity.

□

Exercise 12.5.5. Show that for all $F, G \in \mathcal{F}$,

1. $P(F)$ is an orthoprojection, and
2. we have $[P(F), P(G)] = 0$.

Theorem 12.5.6. *Let $(\mathbb{X}, \mathcal{X})$ be a measurable space and $\mathbb{H}$ a Hilbert space. A map $P : \mathcal{F} \to \mathfrak{P}(\mathbb{H})$ is a spectral measure if and only if*

1. *$P(\mathbb{X}) = \mathbb{1}$, and*
2. *for all $f, g \in \mathbb{H}$, the set function $\mu_{f,g} : \mathcal{F} \to \mathbb{C}$, defined by*

$$\mu_{f,g}(F) = \langle f \,|\, P(F)g \rangle, F \in \mathcal{F},$$

is countably additive.

Proof. ($\Rightarrow$): If P is a spectral measure, then statements 1 and 2 hold trivially.
($\Leftarrow$): Suppose, conversely, that 1 and 2 hold. If $F \cap G = \emptyset$ then $\langle f \,|\, P(F \cup G)g \rangle = \langle f \,|\, P(F)g \rangle + \langle f \,|\, P(G)g \rangle = \langle f \,|\, [P(F) + P(G)]g \rangle$, hence P is finitely additive (hence multiplicative). Let now $(F_n)_n$ be a sequence of disjoint sets in $\mathcal{F}$. Multiplicativity of P implies $(P(F_n))_n$ is a sequence of orthogonal projections and hence $(P(F_n)g)_n$ a sequence of orthogonal vectors for any $g \in \mathbb{H}$. Let $F = \cup_n F_n$. Hence, for all $f, g \in \mathbb{H}$, we have: $\langle f \,|\, P(F)g \rangle = \langle f \,|\, \sum_n P(F_n)g \rangle$, due to the countable additivity property of $\mu_{f,g}$. We are tempted to conclude that $P(F) = \sum_n P(F_n)$. Yet, it may happen that $\sum_n P(F_n)$ does not make any sense because weak convergence does not imply convergence in the operator norm. However, $\sum_n \|P(F_n)g\|^2 = \sum_n \langle g \,|\, P(F_n)g \rangle = \langle g \,|\, P(F)g \rangle = \|P(F)g\|^2$. It follows that the sequence $(P(f_n)g)_n$ is summable. If we write $\sum_n P(f_n)g = Tg$, it defines a bounded operator T coinciding with $P(F)$.

□

Notation 12.5.7. Let $(\mathbb{X}, \mathcal{F})$ be a measurable space and $F : \mathbb{X} \to \mathbb{C}$. We denote by $\|F\| \equiv \sup\{|F(x)| : x \in \mathbb{X}\}$, and $\mathfrak{B}(\mathbb{X}) = \{F : \mathbb{X} \to \mathbb{C} \mid \text{measurable}, \ \|F\| < \infty\}$.

Henceforth, the Hilbert space $\mathbb{H}$ will be fixed and $\mathfrak{B}(\mathbb{H})$ (respectively $\mathfrak{P}(\mathbb{H})$) will denote as usual the set of bounded operators (respectively projections) on $\mathbb{H}$.

Theorem 12.5.8. *Let $(\mathbb{X}, \mathcal{F})$ be a measurable space and $\mathbb{H}$ a Hilbert space. If P is a spectral measure on $(\mathbb{X}, \mathcal{F})$ and $F \in \mathfrak{B}(\mathbb{X})$, then there exists a unique operator $T_F \in \mathfrak{B}(\mathbb{H})$ such that*

$$\langle f \,|\, T_F g \rangle = \int_{\mathbb{X}} F(x) \langle f \,|\, P(dx)g \rangle,$$

for all $f, g \in \mathbb{H}$. We write $T_F = \int_{\mathbb{X}} F(x)P(dx)$.

Proof: The boundedness of F implies that the right hand side of the integral gives rise to a well-defined sesquilinear functional $\phi(f, g) = \int_{\mathbb{X}} F(x) \langle f \,|\, P(dx)g \rangle$, for $f, g \in \mathbb{H}$. Moreover, $|\phi(f, f)| \leq \int_{\mathbb{X}} |F(x)| \|P(dx)f\|^2 \leq \|F\| \|f\|^2$, hence the functional ϕ is bounded. Existence and uniqueness of T_F follows from the Riesz-Fréchet theorem. □

Theorem 12.5.9 (Spectral decomposition theorem). *If $T \in \mathfrak{B}_h(\mathbb{H})$ then there exists a spectral measure on $(\mathbb{C}, \mathcal{B}(\mathbb{C}))$, supported by $\mathsf{spec}(T) \subseteq \mathbb{R}$, such that*

$$T = \int_{\mathsf{spec}(T)} \lambda P(d\lambda).$$

Proof. Let $p \in \mathbb{R}[t]$ and $f, g \in \mathbb{H}$ be two arbitrary vectors. Denote by $L_{f,g}(p) = \langle f \,|\, p(T)g \rangle$. Then $|L_{f,g}(p)| \leq \|p(T)\|\|f\|\|g\|$ and since $p(T) \in \mathfrak{B}(\mathbb{H})$ we have also $\|p(T)\| = \sup\{|p(\lambda)| : \lambda \in \mathsf{spec}(T)\}$ (exercise!). Since $\mathsf{spec}(T)$ is a bounded set, $\|p(T)\| < \infty$ for all $p \in \mathbb{R}[t]$. Hence the linear functional $L_{f,g}$ is a bounded linear functional on $\mathbb{R}[t]$. By Riesz-Fréchet theorem, there exists consequently a unique complex measure $\mu_{f,g}$, supported by $\mathsf{spec}(T)$, such that

$$L_{f,g}(p) \equiv \langle f \,|\, p(T)g \rangle = \int_{\mathsf{spec}(T)} p(\lambda)\mu_{f,g}(d\lambda),$$

for all $p \in \mathbb{R}[t]$, verifying $|\mu_{f,g}(B)| \leq \|f\|\|g\|$, for all $B \in \mathcal{B}(\mathbb{C})$. Using the uniqueness of $\mu_{f,g}$, it is immediate to show that for every $B \in \mathcal{B}(\mathbb{C})$, $S_B(f,g) = \mu_{f,g}(B)$ is a sesquilinear form. Now, $|S_B(f,g)| = |\mu_{f,g}(B)| \leq \|f\|\|g\|$, for all B. Hence the sesquilinear form is bounded; therefore, there exists an operator $P(B) \in \mathfrak{B}_h(\mathbb{H})$ such that $S_B(f,g) = \langle f \,|\, P(B)g \rangle$ for all $f, g \in \mathbb{H}$. Recall that neither $\mu_{f,g}$, nor S_B, nor P depend on the initially chosen polynomial p. Choosing $p_0(\lambda) = 1$, we get $\int_{\mathsf{spec}(T)} \langle f \,|\, P(d\lambda)g \rangle = \langle f \,|\, P(\mathsf{spec}(T))g \rangle = \langle f \,|\, g \rangle$ and choosing $p_1(\lambda) = \lambda$, we get $\int_{\mathsf{spec}(T)} \langle f \,|\, \lambda P(d\lambda)g \rangle = \langle f \,|\, Tg \rangle$, for all $f, g \in \mathbb{H}$. To complete the proof, it remains to show that P is a projection-valued measure. It is enough to show the multiplicativity property. For any fixed pair $f, g \in \mathbb{H}$ and any fixed real polynomial q, introduce the auxiliary complex measure $\nu(B) = \int_B q(\lambda)\langle f \,|\, P(d\lambda)g \rangle$, with $B \in \mathcal{B}(\mathbb{C})$. For every real polynomial p, we have

$$\begin{aligned}
\int p(\lambda)\nu(d\lambda) &= \int p(\lambda)q(\lambda)\langle f \,|\, P(d\lambda)g \rangle \\
&= \langle f \,|\, p(T)q(T)g \rangle \\
&= \langle q(T)f \,|\, p(T)g \rangle \ \text{(recall that } [p(T), q(T)] = 0) \\
&= \int p(\lambda)\langle q(T)f \,|\, P(d\lambda)g \rangle.
\end{aligned}$$

Therefore,

$$\begin{aligned}
\nu(B) &= \int q(\lambda)\mathbb{1}_B(\lambda)\langle f \,|\, P(d\lambda)g \rangle \\
&= \langle q(T)f \,|\, P(B)g \rangle \\
&= \langle f \,|\, q(T)P(B)g \rangle \\
&= \int q(\lambda)\langle f \,|\, P(d\lambda)P(B)g \rangle.
\end{aligned}$$

Since q is arbitrary,

$$\begin{aligned}
\langle f \,|\, P(B \cap C)g \rangle &= \int_C \langle f \,|\, P(d\lambda)P(B)g \rangle \\
&= \langle f \,|\, P(B)P(C)g \rangle,
\end{aligned}$$

and since $f, g \in \mathbb{H}$ are arbitrary, we get $P(B \cap C) = P(B)P(C)$. □

Theorem 12.5.10. *If T is a normal operator in $\mathfrak{B}(\mathbb{H})$, then there exists a necessarily unique complex spectral measure on $(\mathbb{C}, \mathcal{B}(\mathbb{C}))$, supported by $\mathsf{spec}(T)$, such that*

$$T = \int_{\mathsf{spec}(T)} \lambda P(d\lambda).$$

Proof: Exercise! (Hint: $T = T_1 + iT_2$ with $T_1, T_2 \in \mathfrak{B}_h(\mathbb{H})$.) □

12.6 Some basic notions on unbounded operators

The operators arising in quantum mechanics are very often unbounded.

Definition 12.6.1. Let $\mathbb{H}$ be a Hilbert space. An **operator** on $\mathbb{H}$, possibly unbounded, is a pair $(\mathsf{Dom}(T), T)$ where $\mathsf{Dom}(T) \subseteq \mathbb{H}$ is a linear manifold and $T : \mathsf{Dom}(T) \to \mathbb{H}$ is a linear map. The set of operators on $\mathbb{H}$ is denoted $\mathfrak{L}(\mathbb{H})$.

The **graph** of an operator $T \in \mathfrak{L}(\mathbb{H})$ is the linear sub-manifold of $\mathbb{H} \oplus \mathbb{H}$ of the form

$$\Gamma(T) = \{((f, Tf) \in \mathbb{H} \times \mathbb{H} : f \in \mathsf{Dom}(T)\}.$$

The operator T is **closed** if $\Gamma(T)$ is closed. The operator T is **closable** if there exists $\hat{T} \in \mathfrak{L}(\mathbb{H})$ such that $\Gamma(\hat{T}) = \overline{\Gamma(T)}$ in $\mathbb{H} \oplus \mathbb{H}$. Such an operator is unique and is called the **closure** of T. An operator T is said **densely defined** if $\overline{\mathsf{Dom}(T)} = \mathbb{H}$.

If $T_1, T_2 \in \mathfrak{L}(\mathbb{H})$ with $\mathsf{Dom}(T_1) \subseteq \mathsf{Dom}(T_2)$ and $T_1 f = T_2 f$ for all $f \in \mathsf{Dom}(T_1)$, then T_2 is called an **extension** of T_1 and T_1 the **restriction** of T_2 on $\mathsf{Dom}(T_1)$; we write $T_1 \subseteq T_2$. If T is bounded on its domain and $\overline{\mathsf{Dom}(T)} = \mathbb{H}$, then T can be extended by continuity on the whole space.

The definitions of null space and range are also modified for unbounded operators:

$$\begin{aligned} \mathsf{ker}(T) &= \{f \in \mathsf{Dom}(T) : Tf = 0\} \\ \mathsf{Ran}(T) &= \{Tf \in \mathbb{H} : f \in \mathsf{Dom}(T)\}. \end{aligned}$$

The operator T is **invertible** if $\mathsf{ker}(T) = \{0\}$ and its inverse, T^{-1} is the operator defined on $\mathsf{Dom}(T^{-1}) = \mathsf{Ran}(T)$ by $T^{-1}(Tf) = f$ for all $f \in \mathsf{Dom}(T)$.

If $T_1, T_2 \in \mathfrak{L}(\mathbb{H})$, then $T_1 + T_2$ is defined on $\mathsf{Dom}(T_1 + T_2) = \mathsf{Dom}(T_1) \cap \mathsf{Dom}(T_2)$ by $(T_1 + T_2)f = T_1 f + T_2 f$. Similarly, the product $T_1 T_2$ is defined on $\mathsf{Dom}(T_1 T_2) = \{f \in \mathsf{Dom}(T_2) : T_2 \in \mathsf{Dom}(T_1)\}$ by $(T_1 T_2)f = T_2(T_1 f)$.

Definition 12.6.2. Suppose that T is densely defined. Then T is the **adjoint operator** with $\mathsf{Dom}(T^*) = \{g \in \mathbb{H} : \sup |\langle g \,|\, Tf \rangle| < \infty, f \in \mathsf{Dom}(T), \|f\| = 1\}$; since $\overline{\mathsf{Dom}(T)} = \mathbb{H}$, by Riesz theorem, there exists a unique $g^* \in \mathbb{H}$ such that $\langle g^* \,|\, f \rangle = \langle g \,|\, Tf \rangle$ for all $f \in \mathsf{Dom}(T)$. We define then $T^* g = g^*$.

Example 12.6.3. (The position operator) Let $(\Omega, \mathcal{F}, \mu)$ be any separable, σ-finite measure space, $\mathbb{H} = L^2(\Omega, \mathcal{F}, \mu; \mathbb{C})$, and $f \in \mathbb{H}$ measurable. Let $T \in \mathfrak{L}(\mathbb{H})$ be the operator

defined by $\mathrm{Dom}(T) = \{g \in \mathbb{H} : \int (1+|f|^2)|g|^2 d\mu < \infty\}$ and $Tg(\omega) = f(\omega)g(\omega)$ for $g \in \mathrm{Dom}(T)$ and $\omega \in \Omega$. Then T is closed, densely defined, with $\mathrm{Dom}(T^*) = \mathrm{Dom}(T)$ and $T^*g(\omega) = \overline{f}(\omega)g(\omega)$. When $\Omega = \mathbb{R}$, $\mathcal{F} = \mathcal{B}(\mathbb{R})$, and μ is the Lebesque measure, we say that T is the **position operator** (usually denoted by q); it is obviously self-adjoint.

Example 12.6.4. (The momentum operator) Let $\mathbb{H} = L^2(\mathbb{R})$. A function $u : \mathbb{R} \to \mathbb{R}$ is called **absolutely continuous**, (a.c.) if there exists a function $v : \mathbb{R} \to \mathbb{R}$ such that

$$u(b) - u(a) = \int_a^b v(x)dx, \quad \text{for all } \ a < b.$$

In such a case, we write $u' = v$, u' is called the derivative of u. The function v is determined almost everywhere. Define now $T \in \mathfrak{L}(\mathbb{H})$ on

$$\mathrm{Dom}(T) = \{f \in \mathbb{H} : f \text{ a.c.}, \int (|f|^2 + |f'|^2)dx < \infty\}$$

by $Tf = f'$. Then T is a closed, densely defined operator with $T^* = -iT$. The operator $-iT$ (usually denoted by p) is called the **momentum operator**.

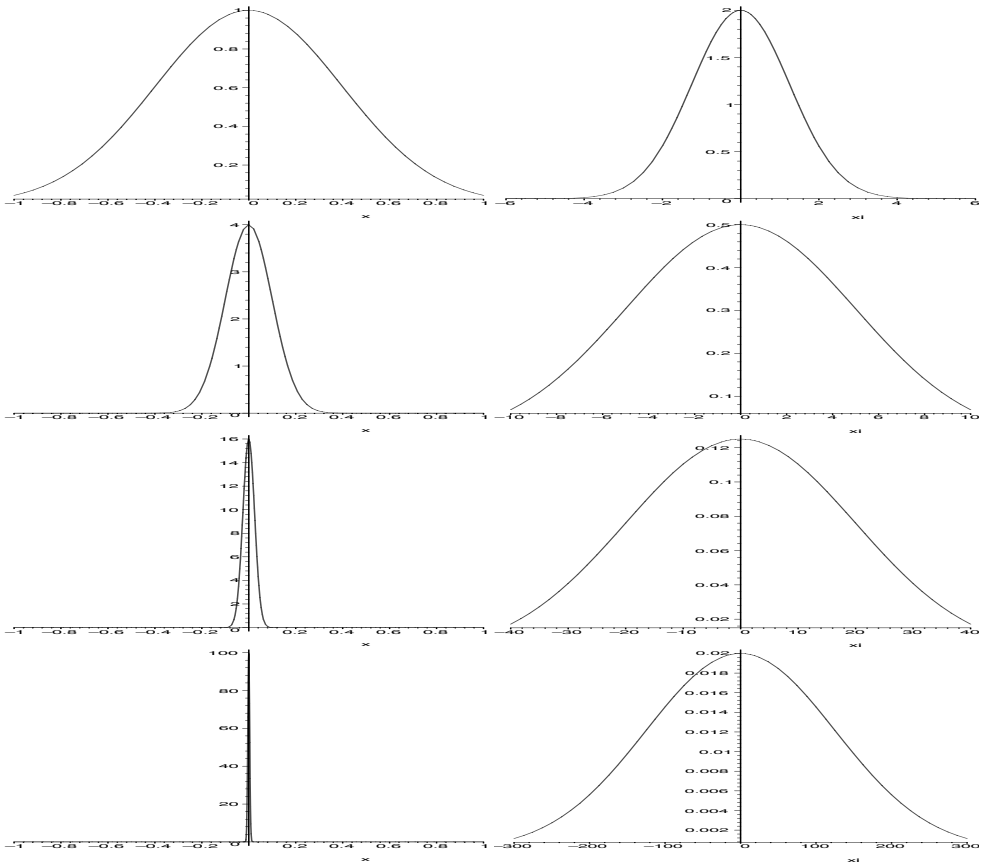
Exercise 12.6.5. Let q be the position operator, p the momentum operator. Show that $[q, p] \subseteq i\mathbb{1}$.

Exercise 12.6.6. (Heisenberg's uncertainty principle) Denote by $\mathbf{S}(\mathbb{R})$ the so called Schwartz [3] space of indefinitely differentiable functions of rapid decrease [4] If $f \in \mathbf{S}(\mathbb{R})$, denote by $\hat{f}$ its Fourier transform $\hat{f}(\xi) = \int_{\mathbb{R}} f(x)\exp(-i\xi x)dx$. Let $p : \mathbf{S}(\mathbb{R}) \to \mathbf{S}(\mathbb{R})$ be defined by $pf = -if'$ and $q : \mathbf{S}(\mathbb{R}) \to \mathbf{S}(\mathbb{R})$ by $qf(x) = xf(x)$, for all $x \in \mathbb{R}$.

1. Show that $[q, p] = i\mathbb{1}$.
2. If $\langle \cdot \,|\, \cdot \rangle$ denotes the L^2 scalar product on $\mathbf{S}(\mathbb{R})$, show that
$$|\langle f \,|\, f \rangle| \leq 2\|pf\|_2\|qf\|_2.$$
3. Conclude that for any $f \in \mathbf{S}(\mathbb{R})$,
$$\|f\|_2 \leq 4\pi\|xf\|_{L^2(\mathbb{R})}\|\xi\hat{f}\|_{L^2(\hat{\mathbb{R}})}.$$
4. Below are depicted the graphs of pairs $|f(x)|^2$ and $|\hat{f}(\xi)|^2$, chosen among a class of Gaussian functions, for different values of some parameter. How do you interpret these results?

3. Named after Laurent Schwartz 1915–2004, French mathematician; has been awarded the Fields Medal in 1950 for his work on the theory of distributions conceived to give a precise meaning to the Dirac's "delta function" and its derivatives. The (class of tempered) distributions are constructed as topological duals of $\mathbf{S}(\mathbb{R})$.

4. $\mathbf{S}(\mathbb{R}) = \{f \in C^\infty(\mathbb{R}) : \forall n \in \mathbb{N}, \forall \alpha \geq 0, \exists K_{\alpha,n} < \infty, \text{ s.t. } \sup_{x\in\mathbb{R}} |x^\alpha f^{(n)}(x)| \leq K_{\alpha,n}\}$. Typical examples of such functions are functions of the form $f(x) = x^\beta \exp(-x^2)$, for some $\beta > 0$.


x
xi
x
xi
x
xi
x
xi

13

Propositional calculus and quantum formalism based on quantum logic

Phenomenology is an essential step in constructing physical theories. Phenomenological results are of the following type: if a physical system is subject to conditions $A, B, C, \ldots$, then the effects $X, Y, Z, \ldots$ are observed. We further introduced yes-no experiments consisting in measuring questions in given states. However, there may exist questions that depend on other questions and hold independently of the state in which they are measured. More precisely, suppose for instance that Q_A denotes the question: "does the physical particle lie in A, for some $A \in \mathcal{B}(\mathbb{R}^3)$?" Let now $B \supseteq A$ be another Borel set in $\mathbb{R}^3$. Whenever Q_A is true (i.e. for every state for which Q_A is true) Q_B is necessarily true. This remark defines a natural order relation in the set of questions. Considering questions on given physical system more abstractly, as a logical propositions, it is interesting to study first the abstract properties of a partially ordered set of propositions. This abstract setting allows the statement of the basic axioms for classical or quantum systems on an equal footing.

13.1 Lattice of propositions

Let Λ be a set of propositions and for any two propositions a and b, denote by $a \leq b$ the implication "whenever a is true, it follows that b is true"

Definition 13.1.1. The pair $(\Lambda, \leq)$ is a **partially ordered set (poset)** if the relation $\leq$ is a partial order (i.e. a reflexive, transitive, and antisymmetric binary operation). For $a, b \in \Lambda$, we say that u is a **least upper bound** if

1. $a \leq u$ and $b \leq u$,
2. if $a \leq v$ and $b \leq v$ for some $v \in \Lambda$, then $u \leq v$.

If a least upper bound of two elements a and b exists, then it is unique and denoted by $\sup(a,b) \in \Lambda$,

Definition 13.1.2. A **lattice** is a set Λ with two binary operations, denoted respectively by $\vee$ ('join') and $\wedge$ ('meet'), and two constants $\mathbf{0} \in \Lambda$ and $\mathbf{1} \in \Lambda$, satisfying, for all $a, b, c \in \Lambda$ the following properties:

1. idempotence: $a \wedge a = a = a \vee a$,
2. commutativity: $a \wedge b = b \wedge a$ and $a \vee b = v \vee a$,
3. associativity: $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ and $a \vee (b \vee c) = (a \vee b) \vee c$,
4. identity: $a \wedge \mathbf{1} = a$ and $a \vee \mathbf{0} = a$,
5. absorption: $a \wedge (a \vee b) = a = a \vee (a \wedge b)$.

Theorem 13.1.3. *Let $(\Lambda, \leq)$ be a poset. Suppose that*

1. *Λ has a least element $\mathbf{0}$ and a greatest element $\mathbf{1}$, i.e. for all $a \in \Lambda$, we have $\mathbf{0} \leq a \leq \mathbf{1}$,*
2. *any two elements $a, b \in \Lambda$ have a least upper bound in Λ, denoted by $a \vee b$, and a greatest lower bound in Λ, denoted by $a \wedge b$. Then $(\Lambda, \wedge, \vee, \mathbf{0}, \mathbf{1})$ is a lattice.*

Conversely, if $(\Lambda, \wedge, \vee, \mathbf{0}, \mathbf{1})$ is a lattice, then, on defining $a \leq b$ whenever $a \wedge b = a$, the pair $(\Lambda, \leq)$ is a poset verifying properties 1 and 2 of definition 13.1.1

Proof: : Exercise! □

Definition 13.1.4. A lattice $(\Lambda, \wedge, \vee, \mathbf{0}, \mathbf{1})$ is called **distributive** if it verifies, for all $a, b, c \in \Lambda$,

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c),$$

and

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

Remark 13.1.5. A finite lattice (or finite poset) can be represented by its **Hasse diagram** in the plane. The points of the lattice are represented by points in the plane arranged so that if $a \leq b$ then the representative of b lies higher in the plane than the representative of a. We join the representatives of a and b by a segment when b covers a, i.e. when $a \leq b$ but there is no $c \in \Lambda$ such that $a < c < b$.

Example 13.1.6. Let S be a finite set and $\mathcal{P}(S)$ the collection of its subsets. Then $(\mathcal{P}(S), \subseteq)$ is a poset, equivalent to the lattice $(\mathcal{P}(S), \cap, \cup, \emptyset, S)$, called the **lattice of subsets** of S. This lattice is distributive. For the particular choice $S = \{1, 2, 3\}$ its Hasse diagram is depicted in figure 13.1.

Exercise 13.1.7. Let $\mathbb{V} = \mathbb{R}^2$ (viewed as a $\mathbb{R}$-vector space) and E_1, E_2, E_3 be three distinct one-dimensional subspaces of $\mathbb{V}$. Denote by $\leq$ the order relation "be a vector subspace of". Show that there is a finite set S of vector subspaces of $\mathbb{V}$ containing E_1, E_2, and E_3 such that $(S, \leq)$ is a lattice. Is this lattice distributive?

In any lattice Λ, a **complement** of $a \in \Lambda$ is an element $a' \in \Lambda$ such that $a \wedge a' = \mathbf{0}$ and $a \vee a' = \mathbf{1}$. Complements may fail to exist and they may be not unique. However, in a distributive lattice, any element has at most one complement.

Definition 13.1.8. A **Boolean algebra** is a complemented distributive lattice (i.e. a distributive lattice in which any element has a — necessarily unique — complement.)

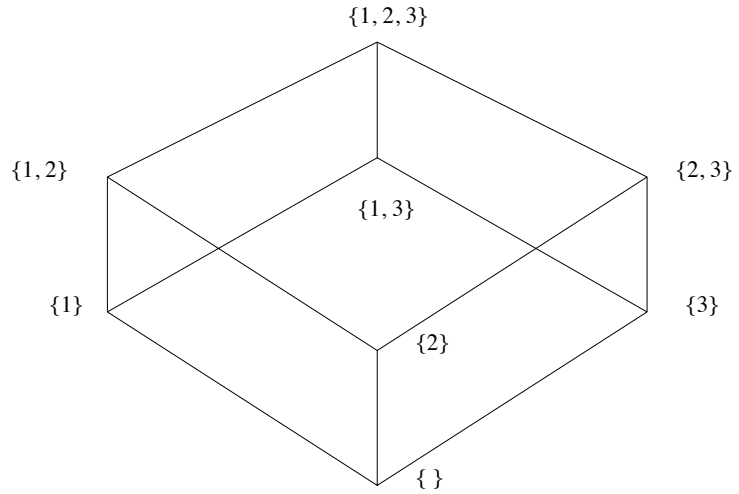


Figure 13.1 – The Hasse diagram of the lattice of subsets of the set $\{1, 2, 3\}$.

When the lattice Λ is infinite, one can consider infinite subsets $F \subseteq \Lambda$. When both $\wedge_{a\in F} a$ and $\vee_{a\in F} a$ exist (in Λ) for any countable subset F, the lattice is called **σ-complete**. A Boolean σ-algebra is a Boolean algebra that is σ-complete.

Definition 13.1.9. A lattice Λ is called **modular** if it satisfies the modularity condition:

$$a \leq c \Rightarrow \forall b \in \Lambda, a \vee (b \wedge c) = (a \vee b) \wedge c.$$

If Λ is a modular and complemented lattice then, for every complement a' of a, the modularity condition reads

$$a \leq b \Rightarrow b = a \vee (a' \wedge b).$$

If the complement of a is an orthocomplement, then the complemented modular lattice is called **orthomodular**.

Example 13.1.10. The **Dilworth lattice**, whose Hasse diagram is depicted in figure 13.2, is a complemented modular but not distributive.

Exercise 13.1.11. Show that a Boolean algebra is always modular.

Definition 13.1.12. An **atom** in a lattice is a minimal non-zero element, i.e. $a \in \Lambda$ is an atom if $a \neq \mathbf{0}$ and if $x < a$ for some $x \in \Lambda$ then $x = \mathbf{0}$. A lattice is **atomic** if every point is the join of a finite number of atoms.

Definition 13.1.13. A **homomorphism** from a complemented lattice Λ_1 into a complemented lattice Λ_2 is a map $h : \Lambda_1 \to \Lambda_2$ such that

1. $h(\mathbf{0}_1) = \mathbf{0}_2$ and $h(\mathbf{1}_1) = \mathbf{1}_2$,
2. $h(a') = h(a)'$ for all $a \in \Lambda_1$,
3. $h(a \vee b) = h(a) \vee h(b)$ and $h(a \wedge b) = h(a) \wedge h(b)$, for all $a, b \in \Lambda_1$

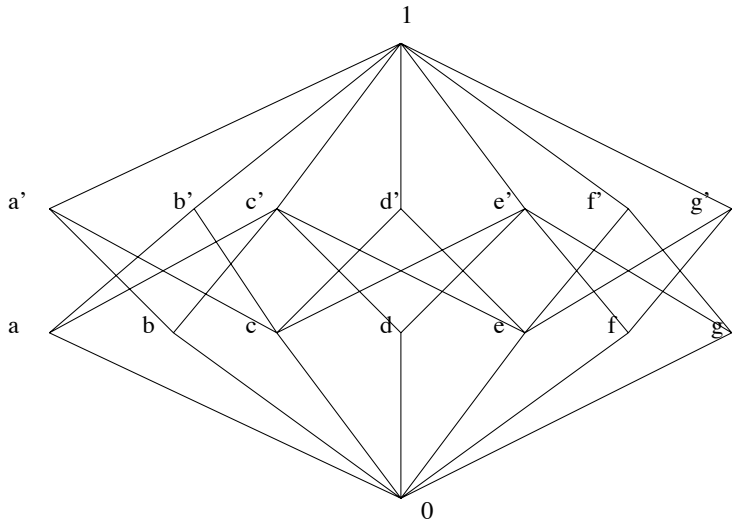


Figure 13.2 – The Hasse diagram of the Dilworth lattice.

An **isomorphism** is a lattice homomorphism that is bijective. If the condition 3 above holds also for countable joins and meets, h is called a σ-homomorphism. If $\Lambda_1 = \Lambda_2$ a lattice isomorphism is called **lattice automorphism**.

Theorem 13.1.14. *Let Λ be a Boolean σ-algebra. Then there exist an abstract set $\mathbb{X}$, a σ-algebra, $\mathcal{X}$, of subsets of $\mathbb{X}$ and a σ-homomorphism $h : \mathcal{X} \to \Lambda$.*

Proof: It is first given in [103] and later reproduced in [146]. □

This theorem serves to extend the notion of measurability, defined for maps between measurable spaces, to maps defined on abstract Boolean σ-algebras. Recall that if $\mathbb{X}$ is an arbitrary set of points equipped with a Boolean σ-algebra of subsets $\mathcal{X}$, and $\mathbb{Y}$ a complete separable metric space equipped with its Borel σ-algebra $\mathcal{B}(\mathbb{Y})$, a map $f : \mathbb{X} \to \mathbb{Y}$ is called **measurable** if for all $B \in \mathcal{B}(\mathbb{Y})$, $f^{-1}(B) \in \mathcal{X}$.

Definition 13.1.15. Let Λ be an abstract Boolean σ-algebra and $(\mathbb{Y}, \mathcal{B}(\mathbb{Y}))$ a complete separable metric space equipped with its Borel σ-algebra. A **$\mathbb{Y}$-valued classical observable** associated with Λ is a σ-homomorphism $h : \mathcal{B}(\mathbb{Y}) \to \Lambda$. If $\mathbb{Y} = \mathbb{R}$, the observable is called real-valued.

The careful reader will have certainly remarked that the previous definition is compatible with axiom 2.3.20. As a matter of fact, with every real random variable X on an abstract measurable space $(\Omega, \mathcal{F})$ is associated a family of propositions $Q_B^X = \mathbb{1}_{\{X \in B\}}$, for $B \in \mathcal{B}(\mathbb{R})$. The aforementioned σ-homomorphism $h : \mathcal{B}(\mathbb{R}) \to \mathcal{F}$, stemming from $X(\cdot)$ through the spectral measure $K_X(\cdot, B)$, is given by

$$h(B) = \{\omega \in \Omega : Q_B^X(\omega) = 1\} = X^{-1}(B) \in \mathcal{F}.$$

Notice that this does not hold for quantum systems where some more general notion is needed.

13.2 Classical, fuzzy, and quantum logics; observables and states on logics

13.2.1 Logics

Definition 13.2.1. Let $(\Lambda, \leq)$ be a poset (hence a lattice). By an **orthocomplementation** on Λ is meant a mapping $\perp: \Lambda \ni a \mapsto a^{\perp} \in \Lambda$, satisfying for $a, b \in \Lambda$:

1. $\perp$ is injective,
2. $a \leq b \Rightarrow b^{\perp} \leq a^{\perp}$,
3. $(a^{\perp})^{\perp} = a$,
4. $a \wedge a^{\perp} = \mathbf{0}$.

A lattice with an orthocomplementation operation is called **orthocomplemented**.

We remark that from condition 2 it follows that $\mathbf{0}^{\perp} = \mathbf{1}$ and $\mathbf{1}^{\perp} = \mathbf{0}$. From condition 3 it follows that $\perp$ is also surjective. Finally, conditions 1, 2, and 3 imply that $a \vee a^{\perp} = \mathbf{1}$.

Definition 13.2.2. An orthocomplemented σ-complete lattice, Λ, is said to be a **logic**.

Remark 13.2.3. Let $a_1 \leq a_2$ be arbitrary propositions. Modularity condition reads $\forall c : a_1 \vee (c \wedge a_2) = (a_1 \vee c) \wedge a_2$; applying this condition for $c = a_1^{\perp}$, we get $a_1 \vee (a_1^{\perp} \wedge a_2) = (a_1 \vee a_1^{\perp}) \wedge a_2 = a_2$. Therefore, we have shown that if $a_1 \leq a_2$, then there exists a $b := a_1^{\perp} \wedge a_2 \leq a_1^{\perp}$ such that $a_1 \vee b = a_2$.

The element $a^{\perp}$ is called the **orthogonal complement** of a in Λ. If $a \leq b^{\perp}$ and $b \leq a^{\perp}$, then a and b are said **orthogonal** and we write $a \perp b$.

Exercise 13.2.4. Assume that $(\Lambda, \leq)$ is a poset (hence a lattice) that is orthocomplemented. Let $a, b \in \Lambda$ be such that $a < b$. Denote by

$$\Lambda[a, b] = \{c \in \Lambda : a \leq c \leq b\}.$$

Show that

1. $\Lambda[\mathbf{0}, b]$ becomes a lattice in which countable joins and meets exist and whose zero element is $\mathbf{0}$ and unit element is b,
2. if we define, for $x \in \Lambda[\mathbf{0}, b]$, $x' = x^{\perp} \wedge b$, then the operation $' : \Lambda[\mathbf{0}, b] \to \Lambda[\mathbf{0}, b]$ is an orthocomplementation,
3. conclude that $\Lambda[\mathbf{0}, b]$ is a logic.

Example 13.2.5. Any Boolean σ-algebra is a logic provided we define, for any element a, its orthocomplement to be its complement a'. Boolean σ-algebras are called **classical logics**.

Example 13.2.6. Let $\mathbb{H}$ be a $\mathbb{C}$-Hilbert space. Let Λ be the collection of all Hilbert subspaces of $\mathbb{H}$. If $\leq$ is meant to denote "be a Hilbert subspace of" and $\perp$ the orthogonal complementation in the Hilbert space sense, then Λ is a logic, called **standard quantum logic**.

Postulate 13.2.7. *In any physical system (classical or quantum), the set of all experimentally verifiable propositions is a logic (classical or standard quantum).*

13.2.2 Observables associated with a logic

Suppose that Λ is the logic of verifiable propositions of a physical system and let X be any real physical quantity relative to this system. Denoting $x(B)$ the proposition "the numerical results of the observation of X lie in B", it is natural and harmless to consider that $B \in \mathcal{B}(\mathbb{R})$; obviously then, x is a mapping $x : \mathcal{B}(\mathbb{R}) \to \Lambda$. We regard to physical quantities X and X' as identical whenever the corresponding maps $x, x' : \mathcal{B}(\mathbb{R}) \to \Lambda$ are the same. If $f : \mathbb{R} \to \mathbb{R}$ is a Borel function, we mean by $X' = f \circ X$ a physical quantity taking value $f(r)$ whenever X takes value r. The corresponding map is given by $\mathcal{B}(\mathbb{R}) \ni B : x' \mapsto x'(B) = x(f^{-1}(B)) \in \Lambda$. Hence we are led naturally to the following

Definition 13.2.8. Let Λ be a logic. A real **observable** associated with Λ is a mapping $x : \mathcal{B}(\mathbb{R}) \to \Lambda$ verifying:

1. $x(\emptyset) = \mathbf{0}$ and $x(\mathbb{R}) = \mathbf{1}$,
2. if $B_1, B_2 \in \mathcal{B}(\mathbb{R})$ with $B_1 \cap B_2 = \emptyset$ then $x(B_1) \perp x(B_2)$,
3. if $(B_n)_{n\in\mathbb{N}}$ is a sequence of mutually disjoint Borel sets, then $x(\cup_{n\in\mathbb{N}} B_n) = \vee_{n\in\mathbb{N}} x(B_n)$.

We write $\mathcal{O}(\Lambda)$ for the set of all real observables associated with Λ.

Exercise 13.2.9. Let Λ be a logic and $x \in \mathcal{O}(\Lambda)$. Show that for any sequence of Borel sets $(B_n)_{n\in\mathbb{N}}$ we have

$$x(\cup_{n\in\mathbb{N}} B_n) = \vee_{n\in\mathbb{N}} x(B_n)$$

and

$$x(\cap_{n\in\mathbb{N}} B_n) = \wedge_{n\in\mathbb{N}} x(B_n).$$

Definition 13.2.10. Let Λ be a logic and $\mathcal{O}(\Lambda)$ the set of its associated observables. A real number λ is called a **strict value** of an observable $x \in \mathcal{O}(\Lambda)$, if $x(\{\lambda\}) \neq \mathbf{0}$. The observable $x \in \mathcal{O}(\Lambda)$ is called **discrete** if there exists a countable set $C = \{c_1, c_2, \ldots\}$ such that $x(C) = \mathbf{1}$; it is called **constant** if there exists $c \in \mathbb{R}$ such that $x(\{c\}) = \mathbf{1}$. It is called **bounded** if there exists a compact Borel set K such that $x(K) = \mathbf{1}$.

Definition 13.2.11. We call **spectrum** of $x \in \mathcal{O}(\Lambda)$ the closed set defined by

$$\mathsf{spec}(x) = \cap_{C \text{ closed } : x(C)=\mathbf{1}} C.$$

The numbers $\lambda \in \mathsf{spec}(x)$ are called **spectral values** of x.

Any strict value is a spectral value; the converse is not necessarily true.

Exercise 13.2.12. Show that $\lambda \in \mathsf{spec}(x)$ if and only if any open set U containing λ verifies $x(U) \neq \mathbf{0}$.

If $(a_n)_{n\in\mathbb{N}}$ is a partition of unity, i.e. a family of mutually orthogonal propositions in Λ such that $\vee_{n\in\mathbb{N}} a_n = \mathbf{1}$, there exists a unique discrete observable admitting as spectral values a given discrete subset $\{c_1, c_2, \ldots\}$ of the reals. In fact, it is enough to define for all $n \in \mathbb{N}$, $x(\{c_n\}) = a_n$ and for any $B \in \mathcal{B}(\mathbb{R})$, $x(B) = \vee_{n:c_n\in B} a_n$. Notice however that discrete observables do not exhaust all the physics of quantum mechanics; important physical phenomena involve continuous observables.

13.2.3 States on a logic

We have seen that to every classical system is attached a measurable space $(\Omega, \mathcal{F})$ (its phase space); observables are random variables and states are probability measures that may degenerate to Dirac masses on particular points of the phase space. This description is incompatible with the experimental observation for quantum systems. For the latter, the Heisenberg's uncertainty principle stipulates that no matter how carefully the system is prepared, there always exist observables whose values are distributed according to some non-trivial probability distribution.

Definition 13.2.13. Let Λ be a logic and $\mathcal{O}(\Lambda)$ its set of associated observables. A **state function** is a mapping $\rho : \mathcal{O}(\Lambda) \ni x \mapsto \rho_x \in \mathcal{M}_1^+(\mathbb{R}, \mathcal{B}(\mathbb{R}))$.

For every Borel function $f : \mathbb{R} \to \mathbb{R}$, for every observable x, and every Borel set B on the line, we have:

$$\rho_{f\circ x}(B) = \rho_x(f^{-1}(B)).$$

Denoting by o the zero observable and 0 the zero of $\mathbb{R}$, we have that $\rho_o = \delta_0$. In fact, suppose that $f : \mathbb{R} \to \mathbb{R}$ is the identically zero map. Then $f \circ o = o$ and

$$f^{-1}(B) = \begin{cases} \mathbb{R} & \text{if } 0 \in B \\ \emptyset & \text{otherwise.} \end{cases}$$

Hence, if $0 \in B$, then $\rho_o(B) = \rho_{f\circ o}(B) = \rho_o(f^{-1}(B)) = 1$, because ρ_o is a probability on $\mathbb{R}$; if $0 \notin B$ then similarly $\rho_o(B) = 0$. Therefore, in all circumstances, $\rho_o(B) = \delta_0(B)$.

If $x \in \mathcal{O}(\Lambda)$ is any observable and $B \in \mathcal{B}(\mathbb{R})$ is such that $x(B) = \mathbf{0} \in \Lambda$, then $\rho_x(B) = 0$. In fact, for this B, we have $\mathbb{1}_B \circ x = o$ and $\rho_x(B) = \rho_o(\{1\}) = \delta_0(\{1\}) = 0$. This implies that if x is discrete, the measure ρ_x is supported by the set of the strict values of x.

Definition 13.2.14. An observable $q \in \mathcal{O}(\Lambda)$ is a **question** if $q(\{0,1\}) = \mathbf{1}$. A question is the necessarily discrete. If $q(\{1\}) = a \in \Lambda$, then q is the only question such that $q(\{1\}) = a$; we call it **question associated with the proposition** a and denote by q_a if necessary.

Definition 13.2.15. Let Λ be a logic. A function $p : \Lambda \to [0,1]$ satisfying

1. $p(\mathbf{0}) = 0$ and $p(\mathbf{1}) = 1$,

2. if $(a_n)_{n\in\mathbb{N}}$ is a sequence of mutually orthogonal propositions of Λ, and $a = \vee_{n\in\mathbb{N}} a_n$, then $p(a) = \sum_{n\in\mathbb{N}} p(a_n)$

is called **state (or probability measure) on the logic** Λ. The set of states on Λ is denoted by $\mathcal{S}(\Lambda)$.

The concept of probability measure on a logic coincides with a classical probability measure when the logic is a Boolean σ-algebra. For non distributive logics however, the associated probability measures are genuine generalisations of the classical probabilities. For standard quantum logics, the associated states are called quantum probabilities.

Theorem 13.2.16. *Let $p \in \mathcal{S}(\Lambda)$, where Λ is a logic.*

1. *On defining a map $\rho^p : \mathcal{O}(\Lambda) \to \mathcal{M}_1^+(\mathbb{R}, \mathcal{B}(\mathbb{R}))$, by the formula: for every $x \in \mathcal{O}(\Lambda)$ and for every $B \in \mathcal{B}(\mathbb{R})$, $\rho^p_x(B) = p(x(B))$, then ρ^p is a state function.*
2. *Conversely, if ρ is an arbitrary state function, then there exists a unique probability measure $p \in \mathcal{S}(\Lambda)$ such that for every $x \in \mathcal{O}(\Lambda)$ and for every $B \in \mathcal{B}(\mathbb{R})$, $\rho_x(B) = p(x(B))$.*

Proof. 1. The map $\rho^p_x : \mathcal{B}(\mathbb{R}) \to [0,1]$ is certainly a σ-additive, non-negative map. Moreover, $\rho^p_x(\mathbb{R}) = p(\mathbf{1}) = 1$, hence it is a probability. If $f : \mathbb{R} \to \mathbb{R}$ is a Borel function,

$$\rho^p_{f\circ x}(B) = p(f \circ x(B)) = p(x(f^{-1}(B))) = \rho^p_x((f^{-1}(B)).$$

Hence ρ^p is a state function.

2. Let ρ be a state function. If $a \in \Lambda$ and $q_a \in \mathcal{O}(\Lambda)$ the question associated with proposition a, then ρ_{q_a} is a probability measure on $\mathcal{B}(\mathbb{R})$. Since q_a is a question, $\rho_{q_a}(\{0,1\}) = 1$. Define $p(a) = \rho_{q_a}(\{1\})$. Obviously, for all $a \in \Lambda$, $p(a)$ is well defined and is taking values in $[0,1]$. It remains to show that p is a probability measure on Λ, that is to say verify σ-additivity and normalisation. For $\mathbf{0} \in \Lambda$, $q_0(\{1\}) = \mathbf{0}$. Hence $\rho_{q_0}(\{1\}) = 0 = p(\mathbf{0})$. Similarly, we show that $= p(\mathbf{1}) = 1$. This shows normalisation.
Let $(a_n)_{n\in\mathbb{N}}$ be a sequence of mutually orthogonal elements of Λ, and denote by $a = \vee_{n\in\mathbb{N}} a_n$. Let $x \in \mathcal{O}(\Lambda)$ be the discrete observable defined by $x(\{0\}) = a^\perp$ and $x(\{n\}) = a_n$, for $n = 1, 2, \ldots$. Then, $\mathbb{1}_{\{n\}} \circ x(\{1\}) = x(\{n\}) = a_n$. Hence $q_{a_n} = \mathbb{1}_{\{n\}} \circ x$ and $p(a_n) = \rho_x(\{n\})$. Since ρ_x is a probability measure, $\sum_n p(a_n) = \rho_x(\{1,2,3,\ldots\}) = \rho_x(\mathbb{N})$. Similarly, $\mathbb{1}_{\mathbb{N}} \circ x = q_a$ because $\mathbb{1}_{\mathbb{N}} \circ x(\{1\}) = x(\mathbb{N}) = \vee_{n\in\mathbb{N}} x(\{n\}) = \vee_{n\in\mathbb{N}} a_n = a$. Hence, finally, $p(a) = \sum_n p(a_n)$ establishing thus σ-additivity of p. Finally, for $x \in \mathcal{O}(\Lambda)$ and $B \in \mathcal{B}(\mathbb{R})$,

$$\rho_x(B) = \rho_{\mathbb{1}_B\circ x}(\{1\}) = \rho_{q_{x(B)}}(\{1\}) = p(x(B)).$$

□

If $p \in \mathcal{S}(\Lambda)$ and $x \in \mathcal{O}(\Lambda)$, the map $\mathcal{B}(\mathbb{R}) \ni B \mapsto p(x(B)) \in [0,1]$ defines a probability measure on $\mathcal{B}(\mathbb{R})$. It is called the **probability distribution** induced on the

space of its values by the observable x when the system is in state p and is denoted ρ_x^p. The **expected value** of x in state p is

$$\mathbb{E}_p(x) = \int_{\mathbb{R}} t\rho_x^p(dt)$$

and for a Borel function $f : \mathbb{R} \to \mathbb{R}$, we have

$$\mathbb{E}_p(f \circ x) = \int_{\mathbb{R}} f(t)\rho_x^p(dt)$$

(provided the above integrals exist.) If $\mathbb{E}_p(x^2) < \infty$, the **variance** of x in p is $\mathsf{Var}_p(x) = \mathbb{E}_p(x^2) - (\mathbb{E}_p(x))^2$.

Postulate 13.2.17. *The phase space of a physical system described by the logic Λ. States of the system are given by $\mathcal{S}(\Lambda)$.*

Postulate 13.2.18. *Observables of a physical system described by the logic Λ are $\mathcal{O}(\Lambda)$.*

Postulate 13.2.19. *Measuring whether the values of a physical observable $x \in \mathcal{O}(\Lambda)$ lie in $B \in \mathcal{B}(\mathbb{R})$ when the system is prepared in state $p \in \mathcal{S}(\Lambda)$ means determining $\rho_x^p(B)$.*

13.3 Pure states, superposition principle, convex decomposition

Proposition 13.3.1. *Let $\mathcal{S}(\Lambda)$ be the set of states on the logic Λ. Let $(p_n)_{n\in\mathbb{N}}$ be a sequence in $\mathcal{S}(\Lambda)$ and $(c_n)_{n\in\mathbb{N}}$ a sequence in $\mathbb{R}_+$ such that $\sum_{n\in\mathbb{N}} c_n = 1$. Then $p = \sum_{n\in\mathbb{N}} c_n p_n$, defined by $p(a) = \sum_{n\in\mathbb{N}} c_n p_n(a)$ for all $a \in \Lambda$, is a state.*

Proof: Exercise! □

Corollary 13.3.2. *For any logic Λ, the set $\mathcal{S}(\Lambda)$ is convex.*

Remark 13.3.3. Notice that if $p = \sum_{n\in\mathbb{N}} c_n p_n$ as above, for every $x \in \mathcal{O}(\Lambda)$, we have that $\rho_x^p = \sum_{n\in\mathbb{N}} c_n \rho_x^{p_n}$. In fact, for all $B \in \mathcal{B}(\mathbb{R})$,

$$\rho_x^p(B) = p(x(B)) = \sum_{n\in\mathbb{N}} c_n p_n(x(B)) = \sum_{n\in\mathbb{N}} c_n \rho_x^{p_n}(B).$$

This decomposition has the following interpretation: the sequence $(c_n)_{n\in\mathbb{N}}$ defines a classical probability on $\mathbb{N}$ meaning that in the sum defining p, each p_n is chosen with probability c_n. Therefore, for each integrable observable $x \in \mathcal{O}(\Lambda)$, the expectation $\mathbb{E}_p(x) = \sum_{n\in\mathbb{N}} c_n \mathbb{E}_{p_n}(x)$ consists in two averages: a classical average on the choice of p_n and a (may be) quantum average $\mathbb{E}_{p_n}(x)$.

Exercise 13.3.4. Give a plausible definition of the notion of **integrable observable** used in the previous remark and then prove the claimed equality: $\mathbb{E}_p(x) = \sum_{n\in\mathbb{N}} c_n \mathbb{E}_{p_n}(x)$

Definition 13.3.5. A state $p \in \mathcal{S}(\Lambda)$ is said to be **pure** if the equation $p = cp_1 + (1 - c)p_2$, for $p_1, p_2 \in \mathcal{S}(\Lambda)$ and $c \in [0, 1]$ implies $p = p_1 = p_2$. We write $\mathcal{S}_p(\Lambda)$ for the set of pure states of Λ. Obviously $\mathcal{S}_p(\Lambda) = \mathsf{Extr}\,\mathcal{S}(\Lambda)$.

Definition 13.3.6. Let $\mathcal{D} \subseteq \mathcal{S}(\Lambda)$ and $p_0 \in \mathcal{S}(\Lambda)$. We say that p_0 is a **superposition of states in** $\mathcal{D}$ if for $a \in \Lambda$,

$$\forall p \in \mathcal{D}, p(a) = 0 \Rightarrow p_0(a) = 0.$$

It is an exercise to show that the state $p = \sum_{n\in\mathbb{N}} c_n p_n$ defined in the proposition **??** is a superposition of states in $\mathcal{D} = \{p_1, p_2, \ldots\}$. In the case Λ is a Boolean σ-algebra, the next theorem 13.3.7 shows that this is in fact the only kind of possible superposition. This implies, in particular, the **unicity** of the decomposition of a classical state into extremal (pure) states. If Λ is a standard quantum logic, unicity of the decomposition does not hold any longer!

Theorem 13.3.7. *Let Λ be a Boolean σ-algebra of subsets of a space $\mathbb{X}$. Suppose that*

1. *Λ is separable*[1],
2. *for all $a \in \mathbb{X}$, $\{a\} \in \Lambda$.*

For any $a \in \mathbb{X}$ and any $A \subseteq \mathbb{X}$, let δ_a be the state defined by

$$\delta_a(A) = \begin{cases} 1 & \text{if } a \in A \\ 0 & \text{otherwise.} \end{cases}$$

Then, $(\delta_a)_{a\in\mathbb{X}}$ is precisely the set of all pure states in Λ. If $\mathcal{D} \subseteq \mathcal{S}_p(\Lambda)$ and $p_0 \in \mathcal{S}_p(\Lambda)$, then p_0 is a superposition of states in $\mathcal{D}$ if and only if $p_0 \in \mathcal{D}$.

Proof: Denote $\{A_1, A_2, \ldots\}$ a denumerable collection of subsets of $\mathbb{X}$ generating Λ. Purity of δ_a is trivially verified. Suppose that p is a pure state. If for some $A_0 \in \Lambda$ we have $0 < p_0(A) < 1$, then, on putting for $A \in \Lambda$

$$p_1(A) = \frac{1}{p(A_0)} p(A \cup A_0) \qquad (*)$$

and

$$p_2(A) = \frac{1}{1 - p(A_0)} p(A \cap A_0^c), \qquad (**)$$

we get $p(A) = p(A_0)p_1(A) + (1 - p(A_0))p_2(A)$. Yet, applying (*) and (**) to A_0, we get $p_1(A_0) = 1$ and $p_2(A_0) = 0$, hence $p_1 \neq p_2$. This is in contradiction with the assumed purity of p. Therefore, we conclude that for all $A \in \Lambda$, we have $p(A) \in \{0, 1\}$. Replacing A_n by A_n^c if necessary, we can assume without loss of generality that $p(A_n) = 1$ for all the sets of the collection generating Λ. Let $B = \cap_n A_n$. Then $p(B) = 1$ and consequently B cannot be empty. Now B cannot contain more than one point either. In fact, the collection of all sets $C \in \Lambda$ such that either $B \subseteq C$ or $B \cap C = \emptyset$ is a σ-algebra containing all the sets A_n, $n \in \mathbb{N}$. Hence, it coincides with Λ. As singletons are members of Λ, the set B must be a singleton, i.e. $B = \{a\}$ for some $a \in \mathbb{X}$. Put then $p = \delta_a$. Finally, let p_0 be a superposition of states in $\mathcal{D}$ (all its elements are pure states). If $p_0 = \delta_{a_0}$ but $p_0 \notin \mathcal{D}$, then $p(\{a_0\}) = 0$ for all $p \in \mathcal{D}$ but $p_0(\{a_0\}) \neq 0$, a contradiction. □

1. i.e. there is a countable collection of subsets $A_n \subseteq \mathbb{X}$, $n \in \mathbb{N}$, generating Λ by complementation, intersections, and unions.

13.4 Simultaneous observability

In quantum systems, the Heisenberg's uncertainty principle, already shown in chapter 2, there are observables that cannot be simultaneously observed with arbitrary precision.

Definition 13.4.1. Let $a, b \in \Lambda$. Propositions a and b are said to be **simultaneously verifiable**, denoted by $a \leftrightarrow b$, if there exists elements $a_1, b_1, c \in \Lambda$ such that

1. a_1, b_1, c are mutually orthogonal and,
2. $a = a_1 \vee c$ and $b = b_1 \vee c$ hold.

Observables $x, y \in \mathcal{O}(\Lambda)$ are **simultaneously observable** if for all $B \in \mathcal{B}(\mathbb{R})$, $x(B) \leftrightarrow y(B)$. For $A, B \subseteq \Lambda$, we write $A \leftrightarrow B$ if for all $a \in A$ and all $b \in B$ we have $a \leftrightarrow b$.

Lemma 13.4.2. *Let $a, b \in \Lambda$. The following are equivalent:*

1. $a \leftrightarrow b$,
2. $a \wedge (a \wedge b)^{\perp} \perp b$,
3. $b \wedge (a \wedge b)^{\perp} \perp a$,
4. *there exist $x \in \mathcal{O}(\Lambda)$ and $A, B \in \mathcal{B}(\mathbb{R})$ such that $x(A) = a$ and $x(B) = b$,*
5. *there exists a Boolean sub-algebra of Λ containing a and b.*

Proof:

$1 \Rightarrow 2$:

$$\begin{aligned} a \leftrightarrow b &\Leftrightarrow a = a_1 \vee c \text{ and } b = b_1 \vee c \\ &\Rightarrow c \leq a \text{ and } c \leq b \\ &\Rightarrow c \leq a \wedge b. \end{aligned}$$

From the definition 13.2.2 (logic), it follows that there exists $d \in \Lambda$ such that $c \perp d$ and $c \vee d = a \wedge b$.
Now $d \leq c \vee d = a \wedge b \leq a$ and $d \leq c^{\perp}$ (since $d \perp d$.) Hence, $d \leq a \wedge c^{\perp} = a_1$ (see remark immediately following the definition 13.2.2.) Similarly, $d \leq b_1 \Rightarrow d \leq b_1 \wedge q_1 = \mathbf{0}$. Therefore $d = \mathbf{0}$ and consequently $c = a \wedge b$. It follows $a_1 = a \wedge (a \wedge b)^{\perp}$. Yet, $a_1 \perp c$ and $a_1 \perp b_1$ so that $a_1 \perp (b_1 \perp c) = b$. Summarising, $a \wedge (a \wedge b)^{\perp} \perp b$.

$1 \Rightarrow 3$: By symmetry.

$2 \Rightarrow 1$: Since $a \wedge (a \wedge b)^{\perp} \perp b$, on writing $a_1 = a \wedge (a \wedge b)^{\perp}$, $b_1 = b \wedge (a \wedge b)^{\perp}$, and $c = a \wedge b$, we find $a = a_1 \vee c$ and $b = b_1 \vee c$. Since $a_1 \perp b$, it follows that $a_1 \perp b_1$ and $a_1 \perp c$, while, by definition, $c \perp b_1$ which proves the implication.
Henceforth, the equivalence $1 \Leftrightarrow 2 \Leftrightarrow 3$ is established.

$1 \Rightarrow 4$: If $a = a_1 \vee c$, $b = b_1 \vee c$ and a_1, b_1, c mutually orthogonal, write $d = a_1 \vee b_1 \vee c$ and define x to be the discrete observable such that $x(\{0\}) = a_1$, $x(\{1\}) = b_1$, $x(\{2\}) = c$, and $x(\{3\}) = d$. Then $x(\{0,2\}) = a$ and $x(\{1,2\}) = b$.

$4 \Rightarrow 5$: $x(A \cap (A \cap B)^c) = a \wedge (a \wedge b)^{\perp}$ and $x(B \cap (A \cap B)^c) = b \wedge (a \wedge b)^{\perp}$. On writing $a_1 = a \wedge (a \wedge b)^{\perp}$, $a_2 = a \wedge b$, $a_3 = b \wedge (a \wedge b)^{\perp}$, and $a_4 = (a \vee b)^{\perp}$, we see that $(a_i)_{i=1,\ldots,4}$ are mutually orthogonal and $a_1 \vee a_2 \vee a_3 \vee a_4 = \mathbf{1}$. If

$$\mathcal{A} = \{a_{i_1} \vee \ldots \vee a_{i_k} : k \leq 4; 1 \leq i_1 \leq \ldots \leq i_k \leq 4\},$$

it is easily verified that $\mathcal{A}$ is Boolean sub-algebra of Λ. Since $a, b \in \mathcal{A}$, this proves the implication.

5 $\Rightarrow$ 2: Let $\mathcal{A}$ be a Boolean sub-algebra of Λ containing a and b. Now, $[a \wedge (a \wedge b)^\perp] \wedge b = \mathbf{0}$. As $a, b, a \wedge (a \wedge b)^\perp, b^\perp \in \mathcal{A}$, it follows that

$$\begin{aligned} a \wedge (a \wedge b)^\perp &= [(a \wedge (a \wedge b)^\perp) \wedge b] \\ &\quad \vee [(a \wedge (a \wedge b)^\perp) \wedge b^\perp] \\ &= [(a \wedge (a \wedge b)^\perp) \wedge b^\perp] \\ &\leq b^\perp. \end{aligned}$$

Therefore $a \wedge (a \wedge b)^\perp \perp b$.

□

The significance of this lemma is that if two propositions are simultaneously verifiable, we can operate on them as if they were classical.

Theorem 13.4.3. *Let Λ be any logic and $(x_\lambda)_{\lambda \in D}$ a family of observables. Suppose that $x_\lambda \leftrightarrow x_{\lambda'}$ for all $\lambda, \lambda' \in D$. Then there exist a space $\mathbb{X}$, a σ-algebra $\mathcal{X}$ of subsets of $\mathbb{X}$, a family of measurable functions $g_\lambda : \mathbb{X} \to \mathbb{R}$, $\lambda \in D$, and a σ-homomorphism $\tau : \mathcal{X} \to \Lambda$ such that $\tau(g_l^{-1}(B)) = x_\lambda(B)$ for all $\lambda \in D$ and all $b \in \mathcal{B}(\mathbb{R})$. Suppose further that either Λ is separable or D is countable. Then, for all $\lambda \in D$, there exist a $x \in \mathcal{O}(\Lambda)$ and a measurable function $f_\lambda : \mathbb{R} \to \mathbb{R}$ such that $x_\lambda = f_\lambda \circ x$.*

The proof of this theorem is omitted. Notice that it allows to construct functions of several observables that are simultaneously observable. This latter result is also stated without proof.

Theorem 13.4.4. *Let Λ be any logic and $(x_1, \ldots, x_n)$ a family of observables that are simultaneously observable. Then there exists a σ-homomorphism $\tau : \mathcal{B}(\mathbb{R}^n) \to \Lambda$ such that for all $B \in \mathcal{B}(\mathbb{R})$ and all $i = 1, \ldots, n$,*

$$x_i(B) = \tau(\pi_i^{-1}(B)), \qquad (*)$$

where $\pi_i : \mathbb{R}^n \to \mathbb{R}$ is the projection $\pi(t_1, \ldots, t_n) = t_i$, $i = 1, \ldots, n$. If g is a Borel function on $\mathbb{R}^n$, then $g \circ (x_1, \ldots, x_n)(B) = \tau(g^{-1}(B))$ is an observable. If $g_1, \ldots, g_k$ are real valued Borel functions on $\mathbb{R}^n$ and $y_i = g_i \circ (x_1, \ldots, x_n)$, then $y_1, \ldots, y_k$ are simultaneously observable and for any real valued Borel function h on $\mathbb{R}^k$, we have $h \circ (y_1, \ldots, y_k) = h(g_1, \ldots, g_k) \circ (x_1, \ldots, x_n)$ where, for $\mathbf{t} = (t_1, \ldots, t_n)$, $h(g_1, \ldots, g_k)(\mathbf{t}) = h(g_1(\mathbf{t}), \ldots, g_k(\mathbf{t}))$.

An immediate consequence of this theorem is that if p is a probability measure on Λ, then $\rho^p_{x_1,\ldots,x_n}(B) = p(\tau(B))$, for $B \in \mathcal{B}(\mathbb{R}^n)$, is the **joint probability distribution** of $(x_1, \ldots, x_n)$ in state p.

13.5 Automorphisms and symmetries

Let Λ be a logic. The set $\mathrm{Aut}(\Lambda)$, of automorphisms of Λ, acquires as usual a group structure; they induce naturally automorphisms on $\mathcal{S}(\Lambda)$, called **convex automorphisms**.

Let, in fact, $\alpha \in \mathsf{Aut}(\Lambda)$ and $p \in \mathcal{S}(\Lambda)$. If we define $\tilde{\alpha}$ to be the induced action of α on p, by $\tilde{\alpha}(p)(a) = p(\alpha^{-1}(a))$, for all $a \in \Lambda$, then $\tilde{\alpha}$ is a convex automorphism of $\mathcal{S}(\Lambda)$.

Definition 13.5.1. A map $\beta : \mathcal{S}(\Lambda) \to \mathcal{S}(\Lambda)$ is a **convex automorphisms** if

1. β is bijective and
2. if $(c_n)_{n\in\mathbb{N}}$ is a sequence of non-negative reals such that $\sum_{n\in\mathbb{N}} c_n = 1$ and $(p_n)_{n\in\mathbb{N}}$ is a sequence of states in $\mathcal{S}(\Lambda)$, then

$$\beta(\sum_{n\in\mathbb{N}} c_n p_n) = \sum_{n\in\mathbb{N}} c_n \beta(p_n).$$

The set of convex automorphisms of $\mathcal{S}(\Lambda)$ is denoted $\mathsf{Aut}(\mathcal{S}(\Lambda))$.

Lemma 13.5.2. *Let $\alpha \in \mathsf{Aut}(\Lambda)$. Then the induced automorphism $\tilde{\alpha}$ on $\mathcal{S}(\Lambda)$ is convex.*

Proof: Bijectivity of $\tilde{\alpha}$ follows immediately from the bijectivity of α. If $p = \sum_{n\in\mathbb{N}} c_n p_n \in \mathcal{S}(\Lambda)$ (with the notation of definition 13.5.1), then $\tilde{\alpha}(p)(a) = p(\alpha^{-1}(a)) = \sum_{n\in\mathbb{N}} c_n p_n(\alpha^{-1}(a)) = \sum_{n\in\mathbb{N}} c_n \tilde{\alpha}(p_n)(a)$ for all $a \in \Lambda$. □

Remark 13.5.3. It is obvious that convex automorphisms map pure states of $\mathcal{S}_p(\Lambda)$ into pure states.

Dynamics, i.e. time evolution of a system described by a logic Λ can be defined in the following manner. For each $t \in \mathbb{R}$, there exists a unique map $D(t) : \mathcal{S}(\Lambda) \to \mathcal{S}(\Lambda)$ having the following interpretation: if $p \in \mathcal{S}(\Lambda)$ is the state of the system at time t_0, then $D(t)(p)$ will represent the state of the system at time $t + t_0$.

Definition 13.5.4. Let G be a locally compact topological group. By a **representation** of G into $\mathsf{Aut}(\mathcal{S}(\Lambda))$, we mean a map $\pi : G \to \mathsf{Aut}(\mathcal{S}(\Lambda))$ such that

1. $\pi(g_1 g_2) = \pi(g_1)\pi(g_2)$ for all $g_1, g_2 \in G$,
2. for each $a \in \Lambda$ and each $p \in \mathcal{S}(\Lambda)$, the mapping $g \mapsto \pi(g)(p)(a)$ is $\mathcal{B}(G)$-measurable.

Postulate 13.5.5. *Time evolution of an isolated physical system described by a logic Λ, is implemented by a map $\mathbb{R} \ni t \mapsto D(t) \in \mathsf{Aut}(\mathcal{S}(\Lambda))$. This map provides a representation of the Abelian group $(\mathbb{R}, +)$ into $\mathsf{Aut}(\mathcal{S}(\Lambda))$. More generally, any physical symmetry, implemented by the action of a locally compact topological group G, induces a representation into $\mathsf{Aut}(\mathcal{S}(\Lambda))$.*

Here is an interpretation and/or justification of this axiom. If $p = \sum_{n\in\mathbb{N}} c_n p_n$ represents the initial state of the system, we can realise this state as follows. First chose an integer $n \in \mathbb{N}$ with probability c_n and prepare the system at state p_n. Let the system evolve under the dynamics. Then at time t it will be at state $p'_n = D(t)(p_n)$ with probability c_n. Assuming now that $D(t)$ is a convex automorphism means that $D(t)(p) = \sum_{n\in\mathbb{N}} c_n D(t)(p_n)$, i.e. at time t, the system is in state $p'_n = D(t)(p_n)$ with probability c_n, exactly the result we obtained with the first procedure.

To further exploit the notions of logic, states, observables, and convex automorphisms, we must specialise the physical system.

14

Standard quantum logics

We recall that a standard quantum logic Λ was defined in chapter 12 to be the set of Hilbert subspaces of $\mathbb{C}$-Hilbert space $\mathbb{H}$. For every Hilbert subspace $M \in \Lambda$, we denote by P_M the orthogonal projection to M. If $x \in \mathcal{O}(\Lambda)$, then $B \mapsto P_{x(B)}$, for $B \in \mathcal{B}(\mathbb{R})$, is a projection-valued measure on $\mathcal{B}(\mathbb{R})$. Conversely, for every projection-valued measure P on $\mathcal{B}(\mathbb{R})$, there exists an observable $x \in \mathcal{O}(\Lambda)$ such that $P(B) = P_{x(B)}$, for all $B \in \mathcal{B}(\mathbb{R})$. We identify henceforth Hilbert subspaces with the orthogonal projectors mapping the whole space on them (recall exercise 11.4.7.)

14.1 Observables

Lemma 14.1.1. *Let $M_1, M_2 \in \Lambda$. Then propositions associated with M_1 and M_2 are simultaneously verifiable if and only if $[P_{M_1}, P_{M_2}] = 0$.*

Proof:

— ($\Rightarrow$): Propositions M_1 and M_2 are simultaneously verifiable if there exist mutually orthogonal elements $N_1, N_2, N \in \Lambda$ such that $M_i = N_i \vee N$, for $i = 1, 2$. Then $P_{M_i} = P_{N_i} + P_N$ and the commutativity of the projectors follows immediately.

— ($\Leftarrow$): If $[P_{M_1}, P_{M_2}] = 0$, let $P = P_{M_1} P_{M_2}$. Then P is a projection. Define $Q_i = P_{M_i} - P$, for $i = 1, 2$; it is easily verified that Q_i are projections and $PQ_i = Q_i P = 0$. Therefore $Q_1 Q_2 = Q_2 Q_1 = 0$. If we define $N_i = Q_i(\mathbb{H})$, for $i = 1, 2$ and $N = P(\mathbb{H})$, then N_1, N_2, N are mutually orthogonal and $M_i = N_i \vee N$ which proves that $M_1 \leftrightarrow M_2$.

□

Theorem 14.1.2. *Let Λ be a standard logic with associated Hilbert space $\mathbb{H}$. For any $x \in$*

$\mathcal{O}(\Lambda)$, denote X the self-adjoint (not necessarily bounded) operator on $\mathbb{H}$ with spectral measure given by the mapping $\mathcal{B}(\mathbb{R}) \ni B \mapsto P_{x(B)} \in \Lambda$. Then

1. *the map $x \mapsto X$ is a bijection between $\mathcal{O}(\Lambda)$ and self-adjoint operators on $\mathbb{H}$,*
2. *the observable x is bounded if and only if $X \in \mathfrak{B}_h(\mathbb{H})$,*
3. *two bounded observables x_1 and x_2 are simultaneously observable if and only if the corresponding bounded operators X_1 and X_2 commute,*
4. *if x is a bounded observable and $Q \in \mathbb{R}[t]$, then the operator associated with $Q \circ x$ is $Q(X)$,*
5. *more generally, if $x_1, \ldots, x_r$ are bounded observables any two of them being simultaneously observable, and $Q \in \mathbb{R}[t_1, \ldots, t_2]$, then the observable $Q \circ (x_1, \ldots, x_r)$ has associated operator $Q(X_1, \ldots, X_r)$.*

Proof: Assertions 1–4 are simple exercises based on the spectral theorem for self-adjoint operators. Assertion 5 is a direct consequence of theorem 13.4.4. □

14.2 States

In chapter 2, we defined (pure) quantum states to be unit vectors of $\mathbb{H}$. In chapter 13, states have been defined as probability measures on a logic. We first show that in fact rays correspond to states viewed as probability measures on Λ.

Unit vectors of $\mathbb{H}$ are called *rays*. Let $\xi \in \mathbb{H}$, with $\|\xi\| = 1$ be a ray and denote by $p_\xi : \Lambda \to [0,1]$ the map defined by

$$\Lambda \ni M \mapsto p_\xi(M) = \langle \xi \,|\, P_M \xi \rangle = \|P_M \xi\|^2.$$

We have: $p_\xi(\mathbf{1}) \equiv p_\xi(\mathbb{H}) = 1$, $p_\xi(\mathbf{0}) \equiv p_\xi(\{0\}) = 0$, and if $(M_n)_{n\in\mathbb{N}}$ is a sequence of mutually orthogonal Hilbert subspaces of $\mathbb{H}$ and $M = \vee_{n\in\mathbb{N}} M_n$, then

$$p_\xi(M) = \|P_M \xi\|^2 = \sum_{n\in\mathbb{N}} \langle \xi \,|\, P_{M_n} \xi \rangle = \sum_{n\in\mathbb{N}} p_\xi(M_n).$$

Hence $p_\xi \in \mathcal{S}(\Lambda)$. If $c \in \mathbb{C}$, with $|c| = 1$, then $p_{c\xi} = p_\xi$.

Theorem 14.2.1. *Let $\mathbb{H}$ be a Hilbert space, $(\varepsilon_n)_{n\in\mathbb{N}}$ an orthonormal basis in it an $T \in \mathfrak{B}_+(\mathbb{H})$. We define the trace of T by*

$$\mathsf{tr}(T) = \sum_{n\in\mathbb{N}} \langle \varepsilon_n \,|\, T\varepsilon_n \rangle \in [0, +\infty].$$

Then for all $T, T_1, T_2 \in \mathfrak{B}_+(\mathbb{H})$ the trace has the following properties

1. *is independent of the chosen basis,*
2. *$\mathsf{tr}(T_1 + T_2) = \mathsf{tr}(T_1) + \mathsf{tr}(T_2)$,*
3. *$\mathsf{tr}(\lambda T) = \lambda\, \mathsf{tr}(T)$ for all $\lambda \geq 0$,*
4. *$\mathsf{tr}(UTU^*) = \mathsf{tr}(T)$, for all $U \in \mathfrak{U}(\mathbb{H})$.*

Proof: (To be filled in a later version.) □

Definition 14.2.2. Let $T \in \mathfrak{B}(\mathbb{H})$. The operator T is called *trace-class operator* if $\mathsf{tr}(|T|) < \infty$. The family of trace-class operators is denoted by $\mathfrak{T}^1(\mathbb{H})$.

Lemma 14.2.3. *The space $\mathfrak{T}^1(\mathbb{H})$ is a two-sided ideal of $\mathfrak{B}(\mathbb{H})$ and $\mathsf{tr}(TB) = \mathsf{tr}(BT)$ for all $B \in \mathfrak{B}(\mathbb{H})$.*

Proof: This will be shown in several steps.

1. Every $B \in \mathfrak{B}(\mathbb{H})$ can be decomposed as a linear combination of four unitary operators. In fact, writing $B = \frac{1}{2}(B + B^*) - \frac{i}{2}[i(B - B^*)]$, the operator B is decomposed into a sum of two self-adjoint operators. Now, if $A \in \mathfrak{B}_h(\mathbb{H})$, we can w.l.o.g. assume that $\|A\| \leq 1$ and thence $A \pm \sqrt{I - A^2}$ are unitary. We conclude that $B = c_1U_1 + \ldots + c_4U_4$ with $U_i \in \mathfrak{U}(\mathbb{H})$ and $c \in \mathbb{C}$.

2. We show then that $\mathfrak{T}^1(\mathbb{H})$ is a vector space. In fact, for every $\lambda \in \mathbb{C}$, due to the fact that $|\lambda A| = |\lambda||T|$, it follows that if $A \in \mathfrak{T}^1(\mathbb{H})$ then $\lambda A \in \mathfrak{T}^1(\mathbb{H})$ as well. For $T_1, T_2 \in \mathfrak{T}^1(\mathbb{H})$, denote by U, V, W the partial isometries arising into the polar decompositions $T_1 + T_2 = U|T_1 + T_2|$, $T_1 = C|T_1|$, and $T_2 = W|T_2|$. Then,

$$\begin{aligned}\sum_n \langle\, e_n \,|\, |T_1 + T_2|e_n \,\rangle &= \sum_n \langle\, e_n \,|\, U^*(T_1 + T_2)e_n \,\rangle \\ &= \sum_n \langle\, e_n \,|\, U^*V|T_1|e_n \,\rangle + \sum_n \langle\, e_n \,|\, U^*W|T_2|e_n \,\rangle \\ &\leq \sum_n |\langle\, e_n \,|\, U^*V|T_1|e_n \,\rangle| + \sum_n |\langle\, e_n \,|\, U^*W|T_2|e_n \,\rangle|.\end{aligned}$$

Now,

$$\begin{aligned}\sum_n \langle\, e_n \,|\, U^*V|T_1|e_n \,\rangle &= \sum_n \langle\, |T_1|^{\frac{1}{2}}V^*Ue_n \,|\, |T_1|^{\frac{1}{2}}e_n \,\rangle \\ &\leq \sum_n \||T_1|^{\frac{1}{2}}V^*Ue_n\|\||T_1|^{\frac{1}{2}}e_n\| \text{ Cauchy-Scwharz on } \mathbb{H} \\ &\leq (\sum_n \||T_1|^{\frac{1}{2}}V^*Ue_n\|^2)^{1/2}(\sum_n \||T_1|^{\frac{1}{2}}e_n\|^2)^{1/2} \text{ Cauchy-Scwharz on } \ell^2(\mathbb{N}\end{aligned}$$

We conclude that

$$\begin{aligned}\sum_n \||T_1|^{\frac{1}{2}}V^*Ue_n\|^2 &= \sum_n \langle\, |T_1|^{\frac{1}{2}}V^*Ue_n \,|\, |T_1|^{\frac{1}{2}}V^*Ue_n \,\rangle \\ &= \sum_n \langle\, e_n \,|\, U^*V|T_1|V^*Ue_n \,\rangle \\ &\leq \sum_n \langle\, e_n \,|\, V|T_1|V^*e_n \,\rangle \\ &\leq \sum_n \langle\, e_n \,|\, |T_1|e_n \,\rangle \\ &= \mathsf{tr}(|T_1|),\end{aligned}$$

because U, V are partial isometries. The second term is majorised similarly so that $\mathsf{tr}(|T_1 + T_2|) \leq \mathsf{tr}(|T_1|) + \mathsf{tr}(|T_2|) < \infty$, showing that $T_1 + T_2 \in \mathfrak{T}^1(\mathbb{H})$.

3. Using the decomposition of every $B \in \mathfrak{B}(\mathbb{H})$ into the combination of four unitary operators $B = \sum_{i=1}^{4} c_i U_i$, we get $\mathrm{tr}(TB) = \sum_{i=1}^{4} c_i \,\mathrm{tr}(TU_i)$ so that it becomes sufficient to prove that $T \in \mathfrak{T}^1(\mathbb{H})$ and $U \in \mathfrak{U}(\mathbb{H})$ implies that $TU, UT \in \mathfrak{T}^1(\mathbb{H})$. But $|UT| = \sqrt{(UT)^* UT} = \sqrt{T^*T} = |T|$ and $|TU| = \sqrt{(TU)^* TU} = \sqrt{U^*|T|^2 U} = U^*|T|U$; furthemore $U^*|T|U \geq 0$. Hence $\mathrm{tr}(|TU|) = \mathrm{tr}\,|T| = \mathrm{tr}(|UT|)$.

□

Exercise 14.2.4. Show the $T \in \mathfrak{T}^1(\mathbb{H})$ implies that $T^* \in \mathfrak{T}^1(\mathbb{H})$ (hence $T^1(\mathbb{H})$ is a bilateral $*$-ideal of $\mathfrak{T}^1(\mathbb{H})$.

Exercise 14.2.5. Show that $T \in \mathfrak{T}^1(\mathbb{H})$ is not necessarily closed with respect to the operator norm stemming from the Hilbert norm. Nevertheless, $\mathfrak{T}^1(\mathbb{H})$ is a Banach space for the $\|\cdot\|_1$ norm defined by $\|T\|_1 = \mathrm{tr}\,|T|$.

Definition 14.2.6. If D is a bounded, self-adjoint, non-negative, trace-class operator on $\mathbb{H}$, then D is called a *von Neumann* operator. If further $\mathrm{tr}(D) = 1$, then D is said to be a *density matrix (operator)*. The set of density matrices on $\mathbb{H}$ is denoted by $\mathfrak{D}(\mathbb{H})$.

The states p_ξ, for ξ a ray of $\mathbb{H}$, can also be described in another way. Let D_ξ be the projection operator on the one-dimensional subspace [1] $\mathbb{C}\xi$. Then D_ξ is trace-class and for every $X \in \mathfrak{B}(\mathbb{H})$, it follows that $D_\xi X$ is also trace-class. Let $(\varepsilon_n)_{n\in\mathbb{N}}$ be an arbitrary orthonormal basis of $\mathbb{H}$; without loss of generality, we can then assume that $\varepsilon_1 = \xi$. We have

$$\begin{aligned} \mathrm{tr}(D_\xi X) &= \mathrm{tr}(X D_\xi) \\ &= \sum_{n\in\mathbb{N}} \langle\, \varepsilon_n \,|\, X D_\xi \varepsilon_n \,\rangle \\ &= \langle\, \xi \,|\, X\xi \,\rangle \\ &= \mathbb{E}_\xi(X). \end{aligned}$$

In particular, if $X = P_M$ for $M \in \Lambda$,

$$p_\xi(M) = \langle\, \xi \,|\, P_M \xi \,\rangle = \mathrm{tr}(D_\xi P_M).$$

Lemma 14.2.7. *Let $(\xi_n)_{n\in\mathbb{N}}$ be an arbitrary sequence of rays in $\mathbb{H}$ and $(c_n)_{n\in\mathbb{N}}$ an arbitrary sequence of non-negative reals such that $\sum_{n\in\mathbb{N}} c_n = 1$. Denote by D_n the projection operator on the one-dimensional subspace $\mathbb{C}\xi_n$, for $n \in \mathbb{N}$. Then*

$$D = \sum_{n\in\mathbb{N}} c_n D_n$$

is a well defined density matrix.

Proof: Exercise. □

Exercise 14.2.8. Show that $\mathfrak{D}(\mathbb{H})$ is convex.

Lemma 14.2.9. *Let D be a density matrix defined as in lemma 14.2.7 and $p : \Lambda \to \mathbb{R}$ the mapping defined by $\Lambda \ni M \mapsto p(M) = \mathrm{tr}(P_M D)$. Then $p \in \mathcal{S}(\Lambda)$ and moreover it can be decomposed into $p = \sum_{n\in\mathbb{N}} c_n p_{\xi_n}$.*

1. We recall that the term subspace always means closed subspace.

Proof: First the superposition property follows from the linearity of the trace: for all $M \in \Lambda$, we have $p(M) = \mathrm{tr}(P_M D) = \sum_{n\in\mathbb{N}} c_n \,\mathrm{tr}(P_M D_n) = \sum_{n\in\mathbb{N}} c_n p_{\xi_n}(M)$. It is now obvious that p is a state: in fact, $p(\mathbf{0}) = p(\{0\}) = 0$ and $p(\mathbf{1}) = p(\mathbb{H}) = 1$. □

Conversely, if D is any density matrix, then the map $\Lambda \ni M \mapsto p(M) = \mathrm{tr}(DP_M)$ is a state in $\mathcal{S}(\Lambda)$. States of this type are called *tracial states*. The natural question is whether every state in $\mathcal{S}(\Lambda)$ arises as a tracial state. The answer to this question is one of the most profound results in the mathematical foundations of quantum mechanics, the celebrated Gleason's theorem:

Theorem 14.2.10 (Gleason)**.** *Let $\mathbb{H}$ be a complex separable Hilbert space with $3 \leq \dim \mathbb{H} \leq \aleph_0$, $\mathfrak{D}(\mathbb{H})$ the convex set of density matrices on $\mathbb{H}$, and Λ the logic of subspaces of $\mathbb{H}$. Then*

1. *the map $\mathfrak{D}(\mathbb{H}) \ni D \mapsto \rho_D \in \mathcal{S}(\Lambda)$, defined by $\rho_D(M) = \mathrm{tr}(DP_M)$ for all $M \in \Lambda$, is a convex isomorphism of $\mathfrak{D}(\mathbb{H})$ on $\mathcal{S}(\Lambda)$,*
2. *a state $p \in \mathcal{S}(\Lambda)$ is pure if and only if $p = p_\xi$ for some ray ξ in$\mathbb{H}$,*
3. *two pure states p_ξ and p_ζ are equal if and only if there exists a complex number c with $|c| = 1$ such that the rays ξ and ζ verify $\xi = c\zeta$.*

The proof, lengthy and tricky, is omitted. It can be found, extending over 13 pages (!), in [146].

14.3 Symmetries

Definition 14.3.1. A linear map $S : \mathbb{H} \to \mathbb{H}$ is a *symmetry* if

1. S is bijective, and
2. for all $f, g \in \mathbb{H}$, the scalar product is preserved: $\langle Sf \,|\, Sg \rangle = \langle f \,|\, g \rangle$.

Exercise 14.3.2. Let $\alpha \in \mathrm{Aut}(\Lambda)$ where Λ is the standard quantum logic associated with a given Hilbert space $\mathbb{H}$. Show that

1. there exists a symmetry $S \in \mathfrak{B}(\mathbb{H})$ such that for all $M \in \Lambda$, $\alpha(M) = SM$,
2. if S' is another symmetry corresponding to the same automorphism α, then there exists a complex number c, with $|c| = 1$ such that $S' = cS$,
3. if S is any symmetry of $\mathbb{H}$, the map $\Lambda \ni M \mapsto SM \in \Lambda$ is an automorphism of Λ.

Notice that unitaries are obviously symmetries. It turns out that they are the only symmetries encountered in elementary quantum systems[2].

2. In general, anti-unitaries may also occur as symmetries. They are not considered in this course.

15

States, effects, and the corresponding quantum formalism

15.1 States and effects

15.2 Operations

15.3 General quantum transformations, complete positivity, Kraus theorem

16

Some illustrating examples

16.1 The harmonic oscillator

In chapter 13, a general formalism, covering both classical and quantum logics, has been introduced. Here we present a simple physical example, the harmonic oscillator, in its classical and quantum descriptions. Beyond providing a concrete illustration of the formalism developed so far, this example has the advantage of being completely solvable and illustrating the main similarities and differences between classical and quantum physics.

16.1.1 The classical harmonic oscillator

Exercise 16.1.1. À re-écrire. Determine the phase space for a point mass in dimension 1 subject to the force exerted by a spring of elastic constant k.

Solution: Recall that a point mass m in dimension 1 obeys Newton's equation:

$$m\frac{d^2x}{dt^2}(t) = F(x(t)),$$

subject to the initial conditions $x(0) = x_0$ and $\dot{x}(0) = v_0$, where $x(t)$ denotes the position of the mass at instant t and $F(y)$ denotes the force exerted by the spring on the particle when it is at position y. It reads $F(y) = k(y - y_0)$ where y_0 is the equilibrium elongation of the spring. The kinetic energy, K, of the particle is a quadratic form in the velocity

$$K(\dot{x}) = \frac{m}{2}\dot{x}^2$$

and the potential energy, U, is given by

$$U(x) = -\int_{x_0}^{x} F(y)dy.$$

In order to conclude, we need the following

Theorem 16.1.2. *The total energy $H(x, \dot{x}) = K(\dot{x}) + U(x)$ is a constant of motion, i.e. does not depend on t.*

Proof.

$$\begin{aligned}\frac{d}{dt}(K(\dot{x}) + U(x)) &= m\dot{x}\ddot{x} + \frac{\partial U}{\partial x}(x)\dot{x} \\ &= \dot{x}(m\ddot{x} - F(x)) \\ &= 0.\end{aligned}$$

□

Hence the Newton's equation is equivalent to the system of first order differential equations, known as **Hamilton's equations**:

$$\begin{aligned}\frac{dp}{dt} &= -\frac{\partial H}{\partial q} \\ \frac{dq}{dt} &= \frac{\partial H}{\partial p},\end{aligned}$$

subject to the initial condition

$$\begin{pmatrix} q(0) \\ p(0) \end{pmatrix} = \begin{pmatrix} q_0 \\ p_0 \end{pmatrix},$$

where $p = m\dot{x}$, $q = x$, and $H = \frac{p^2}{2m} + U(q)$. Therefore, the phase space for the point mass in dimension one is $\mathbb{R}^2$ (one dimension for the position, q, and one for the momentum p.) Moreover, this space is stratified according to constant energy surfaces that are ellipses for the case of elastic spring, because potential energy is quadratic in q (see figure 16.1.)

If $\omega(t) = \begin{pmatrix} q(t) \\ p(t) \end{pmatrix} \in \mathbb{R}^2$ represents the coordinate and momentum of the system at time t, the time evolution induced by the system of Hamilton's equations can be thought as the flow on $\mathbb{R}^2$, described by $\omega(t) = T_t\omega(0)$, with initial condition $\omega(0) = \begin{pmatrix} q_0 \\ p_0 \end{pmatrix}$.

The system is described by a mass m attached to a spring of elastic constant k. The motion is assumed frictionless on the horizontal direction and the mass originally equilibrates at point 0. The spring is originally elongated to position q_0 and the system evolves then freely under the equations of motion. The setting is described in figure 16.2. The system was already studied in chapter 2. The equation of motion, giving the

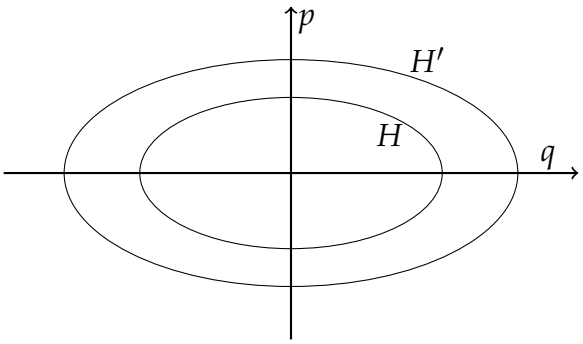


Figure 16.1 – The phase space for a point mass in dimension one.

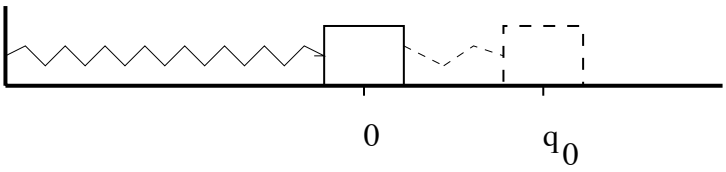


Figure 16.2 – The experimental setting of the one-dimensional harmonic oscillator.

elongation $q(t)$ as a function of time t, is

$$\begin{aligned} m\ddot{q}(t) &= f(q(t)) = -kq(t) \\ q(0) &= q_0 \\ \dot{q}(0) &= v_0 = 0. \end{aligned}$$

Introducing the new variable $p = m\dot{q}$ and transforming the second order differential equation into a system of first order equations, we get the vector equation

$$\frac{d\omega}{dt}(t) = A\omega(t), \qquad (*)$$

where

$$\omega(t) = \begin{pmatrix} q(t) \\ p(t) \end{pmatrix}, \text{ with initial condition } \omega(0) = \begin{pmatrix} q_0 \\ p_0 \end{pmatrix}$$

and

$$A = \begin{pmatrix} 0 & \frac{1}{m} \\ -k & 0 \end{pmatrix}.$$

The solution to equation $(*)$ is given by a flow on the phase space $\Omega = \mathbb{R}^2$ given by

$$\omega(t) = T^t\omega(0),$$

where

$$T^t = \exp(tA) = \begin{pmatrix} \cos(\mu t) & \frac{\sin(\mu t)}{m\mu} \\ -\frac{k}{\mu}\sin(\mu t) & \cos(\mu t) \end{pmatrix},$$

and $\mu = \sqrt{k/m}$. Since $\det T^t = 1$, it follows that the evolution is invertible and $(T^t)^{-1} = T^{-t}$. The orbit of the initial condition $\omega(0) = \begin{pmatrix} q_0 \\ 0 \end{pmatrix}$ under the flow reads $(T^t\omega)_{t\in\mathbb{R}}$, where $\omega(t) = T^t\omega = \begin{pmatrix} q_0\cos(\mu t) \\ -q_0\frac{k}{\mu}\sin(\mu t) \end{pmatrix}$.

The system is classical, hence its logic Λ is a Boolean σ-algebra; the natural choice is $\Lambda = \mathcal{B}(\mathbb{R}^2)$. Now observables in $\mathcal{O}(\Lambda)$ are mappings $x : \mathcal{B}(\mathbb{R}) \to \Lambda \equiv \mathcal{B}(\mathbb{R}^2)$. Identify henceforth indicator functions with Borel sets in $\mathcal{B}(\mathbb{R}^2)$ (i.e. for any Borel set $B \in \mathcal{B}(\mathbb{R})$, instead of considering $x(B) = F \in \mathcal{B}(\mathbb{R}^2)$ we shall identify $x(B) = \mathbb{1}_F$.)

Let now $X : \Omega \to \mathbb{R}$ be any measurable bounded mapping and chose as $x(B) = \mathbb{1}_{X^{-1}(B)}$ for all $B \in \mathcal{B}(\mathbb{R})$. Then, on defining $X = \int \lambda x(d\lambda)$, a bijection is established between x and X. Now since $(T^t\omega)_{t\in\mathbb{R}} = (\exp(tA)\omega)_{t\in\mathbb{R}}$ is the orbit of the initial condition ω_0 in Ω, the value $X(T^t\omega)$ is well defined for all $t \in \mathbb{R}$; we denote by $X_t(\omega) \equiv X(T^t\omega)$. Then

$$\begin{aligned} \frac{dX_t}{dt}(\omega) &= \partial_1 X(T^t\omega)\frac{d(T^t\omega)_1}{dt} + \partial_2 X(T^t\omega)\frac{d(T^t\omega)_2}{dt} \\ &= \partial_1 X(T^t\omega)\frac{dq}{dt}(t) + \partial_2 X(T^t\omega)\frac{dp}{dt}(t), \end{aligned}$$

provides the evolution of X under the flow $(T^t)_t$.

The Hamiltonian is a very particular measurable bounded map on the phase space (hence an observable) $H : \Omega \to \mathbb{R}$, having the formula $H(\omega) = k\omega_1^2/2 + \omega_2^2/2m$. It evolves also under the flow $(T^t)_t$: Then

$$\begin{aligned} \frac{dH_t}{dt}(\omega) &= kq(t)\dot{q}(t) + \frac{p(t)}{m}\dot{p}(t) \\ &= kq(t)\dot{q}(t) + \dot{q}(t)(-k\dot{q}(t)) \\ &= 0. \end{aligned}$$

Thus, the Hamiltonian is a constant of motion. Physically it represents the energy of the system. Initially, $H(q_0, p_0) = \frac{kq_0^2}{2} = E$ and during the flow, the energy always remains E, so that *the energy takes arbitrary (but constant with respect to the flow) values* $E \in \mathbb{R}_+$. Moreover, $\partial_1 H(T^t\omega) = kq(t) = -\dot{p}(t)$ and $\partial_2 H(T^t\omega) = \frac{p(t)}{m} = \dot{q}(t)$. Hence we recover the Hamilton equations

$$\begin{aligned} \frac{dq}{dt}(t) &= \frac{\partial H}{\partial p} = \partial_2 H \\ \frac{dp}{dt}(t) &= -\frac{\partial H}{\partial q} = -\partial_1 H. \end{aligned}$$

Denote for every two functions $f, g \in C^1(\Omega)$ by $\{f, g\} := \partial_1 f\partial_2 g - \partial_2 f\partial_1 g$ their **Poisson's bracket**. The Poisson bracket $\{f, g\}$ is also often denoted by $\mathcal{L}_f(g)$ in the literature. Remark that the time derivative of the observable can now be expressed as $\frac{dX_t}{dt} = \partial_1 X\partial_2 H + \partial_2 X(-\partial_1 H) = L_H X$ where $L_H = -(\partial_1 H\partial_2 - \partial_2 H\partial_1)$. Assuming integrability of the evolution equation, the flow now becomes $X_t = \exp(tL_H)X$. This

means that the flow $(T^t\omega)_t)$ on Ω induces a flow $(\exp(tL_H)X)_t$ on observables. Notice also that $X_t = \exp(tL_H)X$ is a shorthand notation for

$$X_t = \sum_{n=0}^{\infty} \frac{(-t)^n}{n!}\{H, \{H, \dots \{H, X\} \dots\}\}.$$

Theorem 16.1.3 (Liouville's theorem). *Let μ be the Lebesgue measure on Ω, i.e. $\mu(d\omega_1 d\omega_2) = d\omega_1 d\omega_2$. Then*

1. *the measure μ is invariant under T^t, i.e. $\mu(T^t B) = \mu(B)$ for all $B \in \mathcal{B}(\mathbb{R}^2)$ and all $t \in \mathbb{R}$,*
2. *the operator L_H is formally skew-adjoint on $L^2(\Omega, \mathcal{F}, \mu)$.*

Proof:

1. $\mu(T^t B) = \int_{T^t B} d\omega_1 d\omega_2$. Now, if $\omega \in T^t B \Rightarrow T^{-t}\omega \in B$. Hence, denoting $(x_1, x_2) = T^{-t}(\omega_1, \omega_2)$, we have

$$\begin{aligned}\int_{T^t B} d\omega_1 d\omega_2 &= \int_B \frac{\partial(\omega_1, \omega_2)}{\partial(x_1, x_2)} dx_1 dx_2 \\ &= \int_B dx_1 dx_2 = \mu(B),\end{aligned}$$

   because the Jacobian verifies

$$\frac{\partial(\omega_1, \omega_2)}{\partial(x_1, x_2)} = \det \exp(tA) = 1.$$

2. L_H is not bounded on $L^2(\Omega, \mathcal{F}, \mu)$. It can be defined on dense subset of $L^2(\Omega, \mathcal{F}, \mu)$, for instance the Schwartz space $\mathbf{S}(\mathbb{R}^2)$. For $f, g \in \mathbf{S}(\mathbb{R}^2)$, we have

$$\begin{aligned}\langle f \,|\, L_H g \rangle &= \int \overline{f}(\omega) L_H g(\omega) \mu(d\omega) \\ &= -\int \overline{L_H f}(\omega) g(\omega) \mu(d\omega) + \text{ bdry terms.}\end{aligned}$$

   Now the boundary terms vanish because f and g vanish at infinity. Hence, on $\mathbf{S}(\mathbb{R}^2)$, the operator is skew-adjoint $L_H^* = -L_H$ and hence formally skew-adjoint on $L^2(\Omega, \mathcal{F}, \mu)$.

□

Notice that, as a consequence of the previous theorem, $\exp(tL_H)$ is formally unitary on $L^2(\Omega, \mathcal{F}, \mu)$.

Any probability measure p on Λ is a state. We have for all $B \in \mathcal{B}(\mathbb{R})$, $\rho_x(B) = p(x(B)) = p(X^{-1}(B))$ while $\rho_{x_t} = p(x_t(B)) = p(X_t^{-1}(T^{-t}B)) = p(x(T^{-t}B))$. Hence the flow T^t on Ω induces a convex automorphism $\tilde{\alpha}(p)(x(B)) = p(x((T^{-t}B))$ on states.

16.1.2 Quantum harmonic oscillator

Standard quantum logic Λ coincides with the family of subspaces of an infinite-dimensional Hilbert space $\mathbb{H}$. Since all separable Hilbert spaces are isomorphic, we

can chose any of them. The Schrödinger's choice for the one-dimensional harmonic oscillator is $\mathbb{H} = L^2(\mathbb{R})$. States are probability measures $p : \Lambda \to [0,1]$ and thanks to Gleason's theorem, we can limit ourselves to tracial states, i.e.

$$\Lambda \ni M \mapsto p(M) = \mathsf{tr}(P_M D) = p_D(M),$$

for some $D \in \mathcal{D}(\mathbb{H})$. Symmetries are implemented by unitary operators on $\mathbb{H}$ (automorphisms on Λ.) Let $U \in \mathfrak{U}(\mathbb{H})$. Then $\alpha : M \mapsto \alpha(M) = UM$ induces a projection $P_{UM} = U^* P_M U$. Subsequently, the automorphism α induces a convex automorphism on $\mathbf{S}(\Lambda)$, given by

$$\begin{aligned} \tilde{\alpha}(p)(M) &= p_D(\alpha(M)) \\ &= \mathsf{tr}(P_{UM} D) \\ &= \mathsf{tr}(U^* P_M U D) \\ &= \mathsf{tr}(P_M D^{(U)}), \end{aligned}$$

with $D^{(U)} = UDU^*$. Physics remains invariant under time translations. Hence time translation (evolution) must be a symmetry implemented by a unitary operator $U(t)$ acting on $\mathbb{H}$. Define $U(t) = \exp(-itH/\hbar)$ (this a definition of H.) Then H is formally self-adjoint, hence an observable (a very particular one!) generating the Lie group of time translations. It will be shown below that H is time invariant. Now $U(t)$ acts on rays of $\mathbb{H}$ to give a flow. Denoting $\psi(t) = U(t)\psi$, we have the *Schrödinger's evolution equation* in the *Schrödinger's picture*:

$$i\hbar \frac{d\psi}{dt}(t) = H\psi(t).$$

Thanks to the spectral theorem (and, identifying for $x \in \mathcal{O}(\Lambda)$ and $B \in \mathcal{B}(\mathbb{R})$, $x(B)$ with the projection-valued measure corresponding to the subspace $x(B)$), there is a bijection between $x \in \mathcal{O}(\Lambda)$ and self-adjoint operators on $\mathbb{H}$ through $X = \int \lambda x(d\lambda)$. For every tracial states p_D, we have $\mathbb{E}_{p_D}(X) = \int \lambda \,\mathsf{tr}(x(d\lambda)D)$ and

$$\begin{aligned} \mathbb{E}_{\tilde{\alpha}(p_D)}(X) &= \int \lambda \,\mathsf{tr}(x(d\lambda) D^{U(t)}) \\ &= \int \lambda \,\mathsf{tr}(U^*(t) x(d\lambda) U(t) D) \\ &= \mathbb{E}_{p_D}(X_t), \end{aligned}$$

where we defined $X_t = U^*(t) X U(t)$. Hence the flow $U(t)\psi$ on $\mathbb{H}$ induces a flow on observables satisfying

$$\frac{dX_t}{dt} = \frac{i}{\hbar}[H, X] = L_H X$$

with $L_H(\cdot) = \frac{i}{\hbar}[H, \cdot]$. Notice incidentally that $dH_t/dt = 0$ proving the claim that H is a constant of motion. Moreover, H has dimensions $M \cdot L^2/T^2$ (energy), therefore H is interpreted as the quantum Hamiltonian. If the flow is integrable, we have

$$\begin{aligned} X_t &= \exp(tL_H) X \\ &= \sum_{n=0}^{\infty} \frac{(it)^n}{\hbar^n n!} [H, [H, \ldots, [H, X] \ldots]]. \end{aligned}$$

Physics remains invariant also by space translations. Hence they must correspond to a symmetry implemented by a unitary transformation.

Lemma 16.1.4. *The operator ∇_x is formally skew-adjoint on $L^2(\mathbb{R})$.*

Proof: For all $f, g \in \mathbf{S}(\mathbb{R})$ (dense in $L^2(\mathbb{R})$), we have, $\langle f \mid \nabla_x g \rangle = \int \overline{f}(x) \frac{d}{dx} g(x) dx = -\int \frac{d}{dx} \overline{f}(x) g(x) dx + fg|_{-\infty}^{\infty}$. □

Consequently, the operator $\exp(x \cdot \nabla_x)$ is formally unitary and since $\exp(x \cdot \nabla_x)\psi(y) = \psi(y + x)$, ∇_x is the generator of space translations. If we write $p = \frac{\hbar}{i}\nabla_x$ then p is formally self-adjoint, has dimensions $L \cdot M \cdot (L/T^2) \cdot (1/L) = M \cdot L/T$ (momentum), and $\exp(ix \cdot p/\hbar)$ is unitary and implements space translations.

Define $H_{\text{osc}} = p^2/2m + kq^2$ as the formally self-adjoint operator on $L^2(\mathbb{R})$, with $p = \frac{\hbar}{i}\nabla_x$ and $q\psi(x) = x\psi(x)$, the multiplication operator. Introduce $\mu = \sqrt{k/m}$, $Q = \sqrt{m\mu/\hbar}q$, $P = (1/\sqrt{m\mu\hbar})p$, and $H = (1/\hbar\mu)H_{\text{osc}}$. Then $H = (1/2)(P^2 + Q^2)$ where $P = -i\nabla$ and Q is the multiplication operator; these two latter operators are formally self-adjoint and verify the commutation relation $[P, Q] = -i\mathbb{1}$.

Definition 16.1.5. (Creation and annihilation operators) Define the *creation operator* $A^* = \frac{1}{\sqrt{2}}(P + iQ)$ and the *annihilation operator* $A = \frac{1}{\sqrt{2}}(P - iQ)$.

Exercise 16.1.6. For the creation and annihilation operators, show

1. $[A, A^*] = \mathbb{1}$,
2. $H = A^*A + \mathbb{1}/2$,
3. $[H, A] = -A$,
4. $[H, A^*] = A^*$,
5. for $n \in \mathbb{N}$, $[H, (A^*)^n] = n(A^*)^n$.

Lemma 16.1.7. *If $\psi_0 \in \mathbf{S}(\mathbb{R})$ is a ray (in the L^2 sense) satisfying $A\psi_0 = 0$ then*

1. $\psi_0(x) = \pi^{-1/4} \exp(-x^2/2)$,
2. $H\psi_0 = \psi_0/2$, *and*
3. $H(A^*)^n\psi_0 = (1/2 + n)A^{*n}\psi_0$, *for all $n \in \mathbb{N}$.*

Proof:

$$\begin{aligned} A\psi_0 = 0 \quad &\Rightarrow \quad \frac{1}{\sqrt{2}}(P - iQ)\psi_0 \\ &\Rightarrow \quad -i\frac{d}{dx}\psi_0(x) - ix\psi_0(x) = 0 \\ &\Rightarrow \quad \psi_0(x) = c\exp(-x^2/2), \end{aligned}$$

and by normalisation, $c = \pi^{-1/4}$. □

Lemma 16.1.8. *Denote, for $n \in \mathbb{N}$, $\psi_n = \frac{1}{\sqrt{n!}}A^{*n}\psi_0$. Then*

1. *$(\psi_n)_{n\in\mathbb{N}}$ is an orthonormal sequence,*
2. *$A^*\psi_n = \sqrt{n+1}\psi_{n+1}$, for $n \geq 0$,*
3. *$A\psi_n = \sqrt{n}\psi_{n-1}$, for $n \geq 1$, and*
4. *$A^*A\psi_n = n\psi_n$, for $n \geq 0$.*

Proof: All the assertions can be shown by similar arguments. It is enough to show the arguments leading to orthonormality:

$$\begin{aligned}\langle\,\psi_0\,|\,A^nA^{*n}\psi_0\,\rangle &= \langle\,\psi_0\,|\,A^{n-1}AA^*A^{*n-1}\psi_0\,\rangle\\ &= \langle\,\psi_0\,|\,A^{n-1}(\mathbb{1}+A^*A)A^{*n-1}\psi_0\,\rangle\\ &\vdots\\ &= n\langle\,\psi_0\,|\,A^{n-1}A^{*n-1}\psi_0\,\rangle\\ &\vdots\\ &= n!\langle\,\psi_0\,|\,\psi_0\,\rangle.\end{aligned}$$

□

Theorem 16.1.9. *The sequence $(\psi_n)_{n\in\mathbb{N}}$ is a complete orthonormal sequence in $\mathbb{H}$.*

The proof is based on an analogous result for Hermite polynomials that can be shown using the two following lemmata.

Lemma 16.1.10. *Let $c_{n,j} = \frac{n!}{(n-2j)!2^j j!}$, for $n \in \mathbb{N}$, and $j \in \mathbb{N}$ such that $0 \le j \le n/2$. Then*

$$c_{n,j} = (1 - \frac{2j}{n+1})c_{n+1,j} = \frac{2(j+1)}{(n+1)(n-2j)})c_{n+1,j+1}$$

and if

$$\eta_n(x) = \sum_{j=0}^{[n/2]} (-1)^j c_{n,j} x^{n-2j},$$

then

$$(x - \frac{d}{dx})\eta_n(x) = \eta_{n+1}(x)$$

while $x^n = \sum_{j=0}^{[n/2]} c_{n,j}\eta_{n-2j}(x)$.

Proof: Substitute and make induction. □

Lemma 16.1.11. $(A^{*n}\psi_0)(x) = \eta_n(\sqrt{2}x)\psi_0(x)$.

Proof: True for $n = 0$. Conclude by induction. □

Corollary 16.1.12. $\mathrm{spec}(H) = 1/2 + \mathbb{N}$.

Therefore the energy is quantised in quantum mechanics i.e. it can take only discrete values. It is this surprising phenomenon that gave its adjective *quantum* to the term quantum mechanics.

Exercise 16.1.13. Using Dirac's notation $|\,n\,\rangle \equiv \psi_n$, for $n \in \mathbb{N}$,

1. $H|\,n\,\rangle = (1/2+n)|\,n\,\rangle$,
2. $A^*|\,n\,\rangle = \sqrt{n+1}|\,n+1\,\rangle$,
3. $A|\,n\,\rangle = \sqrt{n}|\,n-1\,\rangle$, and
4. $A^*A|\,n\,\rangle = n|\,n\,\rangle$.

16.1.3 Comparison of classical and quantum harmonic oscillators

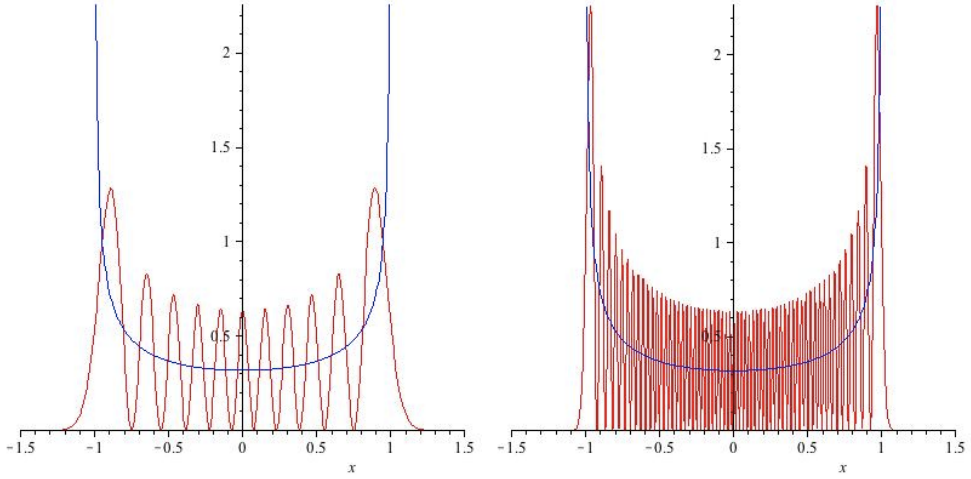


Figure 16.3 – Comparison of probability densities. In blue is depicted the probability density of the classical oscillator. In red the corresponding density for the quantum oscillator for $n = 10$ (left) and $n = 60$ (right).

16.2 Schrödinger's equation in the general case, rigged Hilbert spaces

16.3 Potential barriers, tunnel effect

16.4 Rotations in the classical and quantum settings

16.4.1 Rotations for classical particles

Classical rotations in $\mathbb{R}^2$

It is instructive to consider first the motion of a particle of mass m evolving in $\mathbb{R}^2$ subject to central potential V. The state of the particle is completely described if we know its position $\mathbf{x} \in \mathbb{R}^2$ and its momentum $\mathbf{p} \in \mathbb{R}^2$ hence its phase space is $\mathbb{R}^4$.

The angular momentum of the particle reads $L = x_1 p_2 - x_2 p_1 \in \mathbb{R}$. Since the potential V is assumed central (i.e. invariant under rotations of $\mathrm{SO}(2, \mathbb{R})$) it follows that the angular momentum is conserved (i.e. is a constant of motion). This result

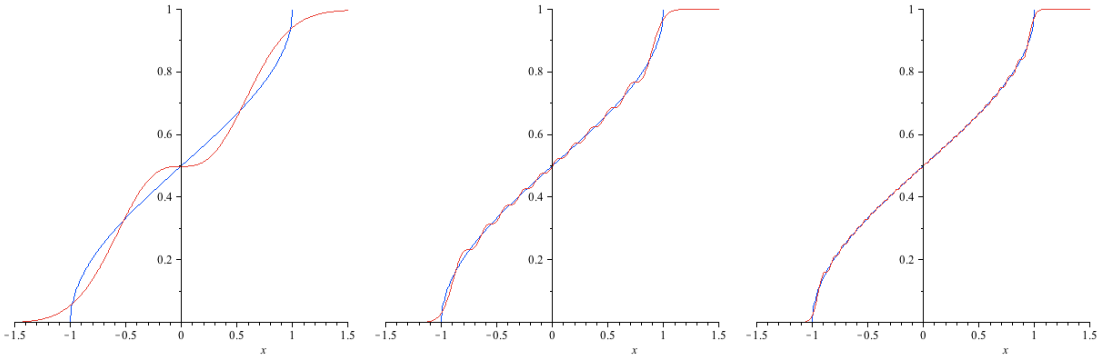


Figure 16.4 – Comparison of distribution functions. In blue is depicted the distribution of the classical oscillator. In red the corresponding distribution for the quantum oscillator for $n = 1$ (left), $n = 10$ (middle), and $n = 30$ (right). Already for $n = 30$, the classical and quantum distributions are almost indistinguishable.

can be obtained as a corollary of the celebrated Noether's theorem [111]. Instead of appealing to this general result, we provide with an elementary proof of this statement here. Namely

Theorem 16.4.1. *Consider the 2-dimensional system described by equations of motion*

$$\dot{\mathbf{x}}(t) - = \frac{\mathbf{p}(t)}{m}, \quad \dot{\mathbf{p}}(t) = -\nabla V(\mathbf{x}) = \begin{pmatrix} -\frac{\partial V}{\partial x_1} \\ -\frac{\partial V}{\partial x_2} \end{pmatrix}.$$

We have

$$[V \ \textit{invariant under rotations}] \ \Leftrightarrow [\dot{L} = 0].$$

Proof. Let R be a rotation of $\mathsf{SO}(2, \mathbb{R})$, the special orthogonal group. Since the rotation is orthogonal, it follows that $R^t R = \mathbb{I}_2$; since the rotation is special, it follows that $\det R = 1$. Hence the set of such rotations is parametrised by a real parameter $\theta \in \mathbb{R}$ in the sense that $\{R_\theta, \theta \in \mathbb{R}\} \simeq \mathsf{SO}(2, \mathbb{R})$. It is elementary to show that

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

The rotation R_θ acts on the space $\mathbb{R}^2$ and transforms vectors $\mathbf{x} \in \mathbb{R}^2$ into $\mathbf{y}$ by

$$\mathbf{x} \to R_\theta \mathbf{x} = \begin{pmatrix} x_1 \cos\theta - x_2 \sin\theta \\ x_1 \sin\theta + x_2 \cos\theta \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \mathbf{y}.$$

Now

$$\begin{aligned} \frac{\mathrm{d}}{\mathrm{d}\theta} V(R_\theta \mathbf{x}) &= \frac{\partial V}{\partial x_1}\frac{\mathrm{d}y_1}{\mathrm{d}\theta} + \frac{\partial V}{\partial x_2}\frac{\mathrm{d}y_2}{\mathrm{d}\theta} \\ &= \frac{\partial V}{\partial x_1}(-x_1 \sin\theta - x_2 \cos\theta) + \frac{\partial V}{\partial x_2}(-x_1 \cos\theta - x_2 \sin\theta). \end{aligned}$$

Hence

$$\frac{\mathrm{d}}{\mathrm{d}\theta}V(R_\theta \mathbf{x})|_{\theta=0} = -\frac{\partial V}{\partial x_1}x_2 + \frac{\partial V}{\partial x_2}x_1.$$

Now, computing the time derivative of L and using the equation of motion, we obtain

$$\begin{aligned}\frac{\mathrm{d}L}{\mathrm{d}t} &= \dot{x}_1 p_2 + x_1 \dot{p}_2 - \dot{x}_2 p_1 - x_2 \dot{p}_1 \\ &= -\frac{\partial V}{\partial x_1}x_2 + \frac{\partial V}{\partial x_2}x_1 = \frac{\mathrm{d}}{\mathrm{d}\theta}V(R_\theta \mathbf{x})|_{\theta=0}.\end{aligned}$$

□

Generalisation to higher dimension

The general form of the angular momentum in dimension n is given by the $n \times n$ matrix $\mathbf{L} = (L_{kl})_{k,l=1,\dots,n}$ where $L_{kl} = x_k p_l - x_l p_k$. Note that in dimension $n = 3$, this matrix simplifies into the form $\mathbf{J} = \begin{pmatrix} 0 & L_1 & -L_2 \\ -L_3 & 0 & L_1 \\ L_2 & -L_1 & 0 \end{pmatrix}$, where $(J_k)_{k=1,2,3}$ are the Cartesian components of the vector $\mathbf{J} = \mathbf{x} \wedge \mathbf{p}$ (i.e. we can identify the angular momentum — the matrix $\mathbf{J}$ — with the vector $\mathbf{J}$).

We have introduced the notion of Poisson bracket on page 242 for differentiable functions in two variables. The notion can be extended to arbitrary dimension.

Notation 16.4.2. Let $f \in C^\infty(\mathbb{R}^{2n})$ and denote $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$ and $\mathbf{p} = (p_1, \dots, p_j) \in \mathbb{R}^n$ the arguments of the function f. We denote by $\mathcal{L}_f$ the differential operator, acting on $C^\infty(\mathbb{R}^{2n})$, defined by

$$\mathcal{L}_f = \sum_{k=1}^{n} \frac{\partial f}{\partial x_k}\frac{\partial}{\partial p_k} - \frac{\partial f}{\partial p_k}\frac{\partial}{\partial x_k}.$$

With the above notation, the Poisson bracket of f and g becomes $\{f, g\} = \mathcal{L}_f(g)$.

We derive a useful relationship for the components of the angular momentum in dimension 3.

Lemma 16.4.3. *For a particle in $\mathbb{R}^3$, identify its angular momentum with the vector $\mathbf{L} = \mathbf{x} \wedge \mathbf{p}$ as stated above. Then*

$$\{L_k, L_l\} = \varepsilon_{klm} L_m, \quad k, l, m = 1, 2, 3,$$

where ε_{klm} is the totally antisymmetric tensor (equal to 0 if there is a repeated index and being equal to $(-1)^s$, where s is the signature of the permutation needed to transform the triplet (klm) into (123)).

Exercise 16.4.4. Prove the previous lemma.

Definition 16.4.5. For N particles evolving in space $\mathbb{R}^n$, the **total angular momentum** is the $n \times n$ matrix defined by its matrix elements $L_{k,l} = \sum_{r=1}^{N}(x_k^r p_l^r - x_l^r p_k^r)$, where $\mathbf{x}^r$ and $\mathbf{p}^r$ are the position and the momentum of the r-th particle.

Note also that the theorem 16.4.1 has a straightforward generalisation in arbitrary dimension n, given without proof in

Theorem 16.4.6. *Suppose N particles evolve in $\mathbb{R}^n$ under the influence of conservative forces stemming from a potential $V : \mathbb{R}^{nN} \to \mathbb{R}$. Then the following statements are equivalent:*

1. *For all $R \in \mathsf{SO}(n, \mathbb{R})$ and all points $\mathbf{x}_1, \ldots, \mathbf{x}_N \in \mathbb{R}^n$, the mutli-particle potential V remains invariant, i.e. $V(R\mathbf{x}_1, \ldots, R\mathbf{x}_N) = V(\mathbf{x}_1, \ldots, \mathbf{x}_N)$.*
2. *The total angular momentum is conserved, i.e. for all $k, l = 1, \ldots, n$, $\dot{L}_{k,l} = 0$.*

16.4.2 Lie groups and algebras

We follow [80] in this subsection.

We denote, as usual, $\mathsf{GL}(n, \mathbb{C})$ the group of invertible $n \times n$ matrices with complex coefficients, viewed as an open subset of the space $\mathbb{M}_n(\mathbb{C}) \simeq \mathbb{C}^{n^2}$ of all $n \times n$ matrices with complex coefficients.

Definition 16.4.7. A closed subgroup G of $\mathsf{GL}(n, \mathbb{C})$ is termed a **matrix Lie group**; it is viewed as a smooth submanifold of $\mathbb{M}_n(\mathbb{C})$. A matrix Lie group G is

— **connected** if for any two $A, B \in \mathsf{G}$, there exists a continuous path $\gamma : [0, 1] \to \mathbb{M}_n(\mathbb{C})$, such that $\gamma(0) = A$ and $\gamma(1) = B$,
— **simply connected** if every closed path (loop) γ in G is continuously contractible to one point in G,
— **compact** if, viewed as a subset of $\mathbb{M}_n(\mathbb{C})$, G is compact.

Example 16.4.8. The matrix Lie group

$$\mathsf{SU}(2, \mathbb{C}) = \{M \in \mathsf{GL}(2, \mathbb{C}) : M^* M = I_2, \det M = 1\} = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}, a, b \in \mathbb{C}, |a|^2 + |b|^2 = 1 \right\}$$

is conncected, simply connected, and compact.

We shall mainly be interested in the closely related groups $\mathsf{SO}(3, \mathbb{R})$ and $\mathsf{SU}(2, \mathbb{C})$, abbreviated into $\mathsf{SO}(3)$ and $\mathsf{SU}(2)$, in the sequel.

Definition 16.4.9. A complex or real vector space $\mathfrak{g}$ is termed a **Lie algebra** if it is equipped with an internal multiplication $[\cdot, \cdot] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ that is

— bilinear,
— antisymmetric, i.e. $[X, Y] = -[Y, X]$ for all $X, Y \in \mathfrak{g}$,
— fulfilling the Jacobi identity, i.e. $[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0$, for all $X, Y, Z \in \mathfrak{g}$.

Example 16.4.10. The functional real space $C^\infty(\mathbb{R}^n)$ equipped with the internal product $[f, g] = \mathcal{L}_f(g) = \{f, g\}$ is an infinite-dimensional Lie algebra.

Definition 16.4.11. Let $\mathfrak{g}_1$ and $\mathfrak{g}_2$ be two Lie algebras. A **Lie algebra homomorphism** is a linear map $\phi : \mathfrak{g}_1 \to \mathfrak{g}_2$ preserving internal mulitplication, i.e. $\phi([X, Y]_{\mathfrak{g}_1}) = [\phi(X), \phi(Y)]_{\mathfrak{g}_2}$ for all $X, Y \in \mathfrak{g}_1$.

We remark that for every $X \in \mathbb{M}_n(\mathbb{C})$, the **exponential map** $\exp(X)$ is well defined by its formal power series $\exp(X) = \sum_{m\in\mathbb{N}} \frac{X^m}{m!}$ (which converges normally since $\|X^m\| \leq \|X\|^m$ for all $m \in \mathbb{N}$). For example, if $X = \begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix}$, with $a \in \mathbb{R}$, then $\exp(X) = \begin{pmatrix} \cos a & \sin a \\ -\sin a & \cos a \end{pmatrix}$.

Lemma 16.4.12. *Let $\mathfrak{g} \subseteq \mathbb{M}_n(\mathbb{C})$ be a Lie algebra and $X, Y \in \mathfrak{g}$. Then*

1. $\exp(0X) = I_n$,
2. $\exp(X^t) = (\exp(X))^t$ *and* $\exp(X^*) = (\exp(X))^*$,
3. *for all* $B \in \mathsf{GL}(n,\mathbb{C})$, *we have* $\exp(BXB^{-1}) = B\exp(X)B^{-1}$,
4. $\det(\exp(X)) = \exp(\operatorname{tr} X)$,
5. *if* $[X,Y] = 0$, *then* [1] $\exp(X)\exp(Y) = \exp(X+Y)$, *and*
6. $\exp(X)$ *in invertible and* $(\exp(X))^{-1} = \exp(-X)$.

Exercise 16.4.13.
1. Prove the previous lemma.
2. Conclude that, for all $X \in \mathfrak{g}$, the set $\{\exp(tX), t \in \mathbb{R}\}$ is a subgroup of $\mathsf{GL}(n,\mathbb{C})$.
3. Show that $\frac{\mathrm{d}}{\mathrm{d}t}\exp(tX)|_{t=0} = X$.

Definition 16.4.14. Let $\mathsf{G} \subseteq \mathsf{GL}(n,\mathbb{C})$ a matrix Lie group. The **Lie algebra of the group** G is the set (as a matter of fact the Lie algebra)

$$\mathfrak{g} = \{X \in \mathbb{M}_n(\mathbb{C}) : \exp(tX) \in \mathsf{G}, \forall t \in \mathbb{R}\}.$$

Exercise 16.4.15. Show that the following sets are are the (finite-dimensional) Lie algebras of the classical matrix groups.

1. $\mathfrak{gl}(n,\mathbb{K}) = \mathbb{M}_n(\mathbb{K})$, for $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$,
2. $\mathfrak{sl}(n,\mathbb{K}) = \{X \in \mathbb{M}_n(\mathbb{K}), \operatorname{tr} X = 0\}$, for $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$,
3. $\mathfrak{u}(n) = \{X \in \mathbb{M}_n(\mathbb{C}) : X^* = -X\}$,
4. $\mathfrak{su}(n) = \{X \in \mathfrak{u}(n) : \operatorname{tr} X = 0\}$,
5. $\mathfrak{o}(n) = \{X \in \mathbb{M}_n(\mathbb{R}) : X^t = -X\}$,
6. $\mathfrak{so}(n) = \{X \in \mathfrak{o}(n) : \operatorname{tr} X = 0\} = \mathfrak{o}(n)$, because the condtion $\operatorname{tr} X = 0$ is automatically fulfilled for $X \in \mathfrak{o}(n)$.

Since the operation $[\cdot,\cdot]$ is an internal multiplication and $\mathfrak{g}$ is a (finite-dimensional) vector space, if $(X_k)_{k\in I}$ is a basis of $\mathfrak{g}$, it follows that we can always write

$$[X_k, X_l] = \sum_{m\in I} {c_{kl}}^m X_m,$$

where the constants $({c_{kl}}^m)_{k,l,m\in I}$ are known as the **structure constants** of the Lie algebra; they determine the Lie algebra $\mathfrak{g}$.

1. Note that if X and Y do not commute, then $Z = \log(\exp(X)\exp(Y))$ is known as the Baker-Cambell-Hausdorff formula and is given by a complicated combinatorial expression. Its general form has be determined by Dynkin [50] (a more easily accessible reference is [51, pp. 31–35]) and reads

$$Z = \sum_{n\geq 1} \frac{(-1)^{n-1}}{n} \sum^{*} \frac{X^{r_1}Y^{s_1}\cdots X^{r_n}Y^{s_n}}{\sum_{i=1}^n (r_i+s_i)\prod_{k=1}^n r_k! s_k!},$$

where $\sum^{*}$ denotes summation over indices such that $r_1 + s_1 > 0, \ldots, r_n + s_n > 0$.

Exercise 16.4.16. 1. Show that the vector space $\mathfrak{so}(3)$ admits as basis the matrices

$$F_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}, F_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix}, F_3 = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

2. Verify that $[F_i, F_j] = \varepsilon_{ijk} F_k$ and conclude that the matrices of the basis (F_1, F_2, F_3) fulfill the Jacobi identity.

Proposition 16.4.17. *Let G_1 and G_2 be matrix Lie groups and $\mathfrak{g}_1$ and $\mathfrak{g}_2$ their Lie algebras. For every Lie group homomorphism $\Phi : \mathsf{G}_1 \to \mathsf{G}_2$, there exists a linear map $\phi : \mathfrak{g}_1 \to \mathfrak{g}_2$ such that*

$$\Phi(\exp(tX)) = \exp(t\phi(X)), \forall t \in \mathbb{R}, \forall X \in \mathfrak{g}_1.$$

Moreover, forall $X, Y \in \mathfrak{g}_1$ and all $A \in \mathsf{G}_1$,

1. *$\phi([X,Y]) = [\phi(X), \phi(Y)]$ (i.e. ϕ is a Lie algebra homomorphism),*
2. *$\phi(AXA^{-1}) = \Phi(A)\phi(X)\Phi(A^{-1})$, and*
3. *$\phi(X) = \frac{d}{dt}\Phi(\exp(tX))|_{t=0}$.*

Corollary 16.4.18. *If G_1 and G_2 are homomorphic matrix Lie groups then their Lie algebras $\mathfrak{g}_1$ and $\mathfrak{g}_2$ are homomorphic.*

In view of the previous corollary, a natural question is whether two homomorphic Lie algebras give rise, by exponentiation, to homomorphic Lie groups. The answer is in general negative as the following exercise shows.

Exercise 16.4.19. 1. Show that the vector space $\mathfrak{su}(2)$ admits as basis the matrices

$$E_1 = \frac{1}{2}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, E_2 = \frac{1}{2}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, E_3 = \frac{1}{2}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

2. Verify that $[E_j, E_k] = \varepsilon_{jkl} F_l$ and conclude that the matrices of the basis [2] (E_1, E_2, E_3) fulfill the Jacobi identity.
3. Denote by $\Phi : \mathsf{SU}(2) \to \mathsf{SO}(3)$ the unique Lie group homomorphism for which the associated Lie algebra homomorphism ϕ (see proposition 16.4.17) is defined by $\phi(E_k) = F_k$, for $k = 1, 2, 3$, where (F_1, F_2, F_3) are the basis of $\mathfrak{so}(3)$ (obtained in exercise 16.4.16). Show that $\ker(\Phi) = \{I, -I\}$.
4. Conclude that although $\mathfrak{su}(2) \simeq \mathfrak{so}(3)$, it is not true that $\mathsf{SU}(2) \simeq \mathsf{SO}(3)$.

Therefore, the following theorem is interesting since it states the conditions under which the Lie algebra uniquely determines the corresponding group.

Theorem 16.4.20. *Let G_1 and G_2 be matrix Lie groups and $\mathfrak{g}_1$ and $\mathfrak{g}_2$ the corresponding Lie algebras. If*

1. *G_1 and G_2 are connected, and*
2. *$\mathfrak{g}_1 \simeq \mathfrak{g}_2$,*

then $\mathsf{G}_1 \simeq G_2$.

2. It is worth noticing that those matrices are closely related to — although not coinciding with — Pauli matrices. As a matter of fact, $E_k = \frac{i\sigma_k}{2}$, for $k = 1, 2, 3$, where (σ_k) are the Puali matrices.

The previous results give also a non trivial significance to the following definition.

Definition 16.4.21. Let G be a connected matrix Lie group and $\mathfrak{g}$ its Lie algebra. A **universal cover** of G is a pair $(\tilde{\mathsf{G}}, \Phi)$ where $\tilde{\mathsf{G}}$ is a simply connected matrix Lie group and $\Phi : \tilde{\mathsf{G}} \to \mathsf{G}$ is a Lie group homomorphism such that the Lie algebra homomorphism $\phi : \tilde{\mathfrak{g}} \to \mathfrak{g}$ between the corresponding Lie algebras is as a matter of fact an isomorphism. The map Φ is termed the **covering map**.

Example 16.4.22. The universal cover of $\mathsf{SO}(3)$ is $\mathsf{SU}(2), \Phi)$, with Φ defined in exercise 16.4.19.

Definition 16.4.23. Let $\mathsf{G} \subseteq \mathsf{GL}(n, \mathbb{C})$ be a matrix Lie group and $\mathfrak{g} \subseteq \mathfrak{gl}(n, \mathbb{C})$ its Lie algebra. A finite-dimensional **representation**

1. of G is a continuous homomorphism $A : \mathsf{G} \to \mathsf{GL}(\mathbb{V})$ where $\mathbb{V}$ is a finite dimensional vector space,
2. of $\mathfrak{g}$ is a Lie algebra homomorphism $\alpha : \mathfrak{g} \to \mathfrak{gl}(\mathbb{V})$, where $\mathfrak{gl}(\mathbb{V})$ is the space of all linear mappings on $\mathbb{V}$ equipped with the internal product $[X, Y] = XY - YX$ for X, Y arbitrary linear mappings.

Remark 16.4.24. Let $A : \mathsf{G} \to \mathsf{GL}(\mathbb{V})$ be a finite-dimensional representation of G.

1. When A is injective, then G is isomorphic with $A(\mathsf{G}) \subseteq \mathsf{GL}(\mathbb{V})$, i.e. the map A serves to "represent" every element of G by an invertible matrix acting on $\mathbb{V}$. Nevertheless, the term representation is used even if A fails to be injective.
2. We say that G acts on a set $\mathbb{X}$ if there exists a mapping $\bullet : \mathsf{G} \times \mathbb{X} \to \mathbb{X}$, the **action**, denoted multiplicatively as $g \bullet x \in \mathbb{X}$, for all $g \in \mathsf{G}$ and $x \in \mathbb{X}$, verifying

$$e \bullet x = x \text{ and } g \bullet (h \bullet x) = (gh) \bullet x,$$

   for all $g, h \in \mathsf{G}$, $x \in \mathbb{X}$, and on denoting e the neutral element of G.
   Every representation $A : \mathsf{G} \to \mathsf{GL}(\mathbb{V})$ induces a linear action on $\mathbb{V}$ by

$$g \bullet v = A(g)v.$$

3. In general, we view $\mathfrak{gl}(\mathbb{V})$ as a real vector space. If $\mathbb{V}$ is a complex vector space and $\mathfrak{g}$ a real Lie algebra, we require that $\alpha : \mathfrak{g} \to \mathfrak{gl}(\mathbb{V})$ be a real linear function.

Definition 16.4.25. Let $A : \mathsf{G} \to \mathsf{GL}(\mathbb{V})$ (respectively $\alpha : \mathfrak{g} \to \mathfrak{gl}(\mathbb{V})$) be a representation of a Lie group G (respectively a Lie algebra $\mathfrak{g}$).

1. A vector subspace $\mathbb{W} \subset \mathbb{V}$ is called **invariant for the representation** if for all $g \in \mathsf{G}$, $w \in \mathbb{W}$, $X \in \mathfrak{g}$, we have

$$A(g)w \in \mathbb{W}, \quad \alpha(X)w \in \mathbb{W}.$$

2. A representation is called **irreducible** if it has only trivial invariant subspaces, i.e. the only invariant subspaces are $\{0\}$ and $\mathbb{V}$.
3. Let $(A_1, \mathbb{V}_1)$ and $(A_2, \mathbb{V}_2)$ be two representations of G. A morphism $\Phi : \mathbb{V}_1 \to \mathbb{V}_2$ is called an **intertwining** if $\Phi(A_1(g)v) = A_2(g)\Phi(v)$, for all $g \in \mathsf{G}$ and all $v \in \mathbb{V}_1$.

16.4.3 Rotations for quantum particles

A classical text for this section — where basic results of representation theory are re-proven — is [52]; a more modern textbook is [80].

We deal only with rotations in dimension 3. Rotations in dimension 2 can be defined analogously in a simpler fashion. Since classically the generators of the rotations are the components of the angular momentum $\mathbf{L} = \mathbf{x} \wedge \mathbf{p}$ and the quantisation of the system is obtained by the formal assignments $\mathbf{x} \to$ multiplication operator and $\mathbf{p} \to -i\hbar\nabla_{\mathbf{x}}$ on $L^2(\mathbb{R}^3)$, we get the assignment $\mathbf{L} = -i\hbar\mathbf{x} \wedge \nabla_{\mathbf{x}}$. Of course, this operator is not defined on the whole space $\mathbb{H} = L^2(\mathbb{R}^3)$ but only to a dense subset, for instance on $\mathbf{S}(\mathbb{R}^3)$. For example, the third component of $\mathbf{L}$ can be defined through a differential operator and be given a significance in terms of rotations as shown in the following formula:

$$L_3\psi(\mathbf{x}) = -i\hbar(x_1\frac{\partial}{\partial x_2} - x_2\frac{\partial}{\partial x_1})\psi(\mathbf{x}) = -i\hbar\frac{\mathrm{d}}{\mathrm{d}\theta}\psi(R_\theta\mathbf{x})|_{\theta=0},$$

where R_θ denotes the rotation by θ (measured in the positive sense) on the plane defined by the axes 1 and 2.

On $\mathbf{S}(\mathbb{R}^3)$, we verify easily that the components $(L_k)_{k\in\{1,2,3\}}$ of the angular momentum operator fulfil the commutation relations

$$[L_k, L_l] = i\hbar\varepsilon_{klm}L_m.$$

These commutation relations are compatible with the Lie algebra structure. It will be prove important to consider the above commutation relations as the defining property of the components of the angular momentum instead of the previous differential operator definition. As a matter of fact, the differential form of the angular momentum operator will be associated with the classical notion of a particle rotating around a given axis. However, quantum particles have also internal degrees of freedom, without classical counterparts, obeying at precisely the same commutation relations. In the sequel, we reserve the symbol $\mathbf{L} = (L_k)_{k=1,2,3}$ for the angular momentum stemming from the differential operator of particle rotation around an axis, and we use the symbol $\mathbf{J} = (J_k)_{k=1,2,3}$ for the family of operators defined algebraically through the commutation relations

$$[J_k, J_l] = i\hbar\varepsilon_{klm}J_m,$$

without reference to differentiation. These operators denote generically angular momentum or "generalised angular momentum" corresponding to internal degrees of freedom — known as **spin of the particle** — or "sums" of the previous observables.

Definition 16.4.26. For $R \in \mathsf{SO}(3)$, define $A : \mathsf{SO}(3) \to \mathfrak{B}(L^2(\mathbb{R}^3))$ an (infinite)-dimensional representation of $\mathsf{SO}(3)$, by

$$A(R)\psi(\mathbf{x}) = \psi(R^{-1}\mathbf{x}).$$

Proposition 16.4.27. *The representation A defined in 16.4.26 is unitary and a strongly continuous homomorphism.*

Proof. The unitarity follows from the invariance to rotations of the Lebesgue measure on $\mathcal{B}(\mathbb{R}^3)$. To establish the second statement, remark that for all $\psi \in L^2(\mathbb{R}^3)$ and all

$R_1, R_2 \in \mathsf{SO}(3)$,

$$\begin{aligned} A(R_1R_2)\psi(\mathbf{x}) &= \psi((R_2 \circ R_1)^{-1}(\mathbf{x})) = \psi(R_1^{-1} \circ R_2^{-1}\mathbf{x}) \\ &= A(R_1)\psi(R_2^{-1}\mathbf{x}) = A(R_1)A(R_2)\psi(\mathbf{x}). \end{aligned}$$

Hence $A(R_1R_2) = A(R_1)A(R_2)$ establishing the homomorphism property.

To establish strong continuity, remark that $C(\mathbb{R}^3)$ is dense in $L^2(\mathbb{R}^3)$, i.e. for every $\varepsilon > 0$, there exists $\phi \in C(\mathbb{R}^3)$ such that $\|\psi - \phi\|_2 < \varepsilon/3$. Hence, for $R, S \in \mathsf{SO}(3)$ such that $\|R - S\| \to 0$,

$$\begin{aligned} \|A(R)\psi - A(S)\psi\| &\leq \|A(R)(\psi - \phi)\| + \|A(R)\phi - A(S)\phi\| + \|A(S)\phi - A(S)\psi\| \\ &\leq \|\psi - \phi\| + \|A(S)(A(S^{-1}R) - I)\phi\| + \|\phi - \psi\| \leq \varepsilon. \end{aligned}$$

□

Since the representation A defined in **??** is (formally) unitary, it follows that if we define the representation α on the algebra $\mathfrak{so}(3)$ by

$$A(\exp(tX)) = \exp(t\alpha(X)), \quad \text{for } X \in \mathfrak{so}(3), t \in \mathbb{R},$$

then $\mathbf{S}(\mathbb{R}^3) \subseteq \mathsf{dom}(F_k)$ for $k = 1, 2, 3$ and on this domain, $J_k = i\hbar\alpha(F_k)$.

Theorem 16.4.28. *Let $\alpha : \mathfrak{so}(3) \to \mathfrak{gl}(\mathbb{V})$ be an irreducible representation of $\mathfrak{so}(3)$ in the finite-dimensional space $\mathbb{V}$ with $\dim \mathbb{V} = 2l + 1$ (this expression defines l as a non-negative integer or half-integer). Define $J_k = i\alpha(F_k)$, for $k = 1, 2, 3$ and $J_\pm = L_1 \pm iL_2 = i\alpha(F_1) \mp \alpha(F_2)$. Then there exists a basis $(v_0, \ldots, v_{2l})$ of $\mathbb{V}$ satistying*

$$\begin{aligned} J_3 v_j &= (l - j)v_j \\ J_+ v_j &= \begin{cases} j(2l + 1 - j)v_{j-1} & \text{if } j > 0, \\ 0 & \text{if } j = 0, \end{cases} \\ J_- v_j &= \begin{cases} v_{j+1} & \text{if } j < 2l, \\ 0 & \text{if } j = 2l. \end{cases} \end{aligned}$$

Proof. The map α is a Lie algebra homomorphism; therefore, $(\alpha(F_k))$ have the same commutation properties as (F_k) for $k = 1, 2, 3$. Hence

$$[J_3, J_\pm] = J_\pm, \quad [J_+, J_-] = 2J_3.$$

Since the number field $\mathbb{C}$ is algebraically closed, it follows that J_3 has at least one eign-vector v with some eigenvalue λ. Using the commutation relation, we get

$$J_3(J_+v) = (J_+J_3 + J_+)v = (\lambda + 1)J_+v.$$

Consequently, either $J_+v = 0$, or it is an eigenvector of J_3 with eigenvalue $\lambda + 1$.

Since $\mathbb{V}$ is finite-dimensional, there are only finitely many eigenvalues. Therefore, there eixsts an integer $K \geq 0$ such that $J_+^K v \neq 0$ but $J_+^{K+1}v = 0$. Introduce henceforth $v_0 := J_+^k v$ and $\mu := \lambda + K$. Obviously $v_0 \neq 0$, $J_+v_0 = 0$, and $L_3v_0 = \mu v_0$.

In the sequel, forget about v and consider solely v_0. Define $v_j = J_-^j v_0$ for $j = 0, 1, 2, \ldots$. By exactly the same arguments as above, either J_- yields a null vector or an eigenvector of J_3 with eigenvalue decreased by 1. Therefore, $J_3 v_j = (\mu - j)v_j$. We show by recurrence that $J_+ v_j j(2\mu + 1 - j)$, for $j = 1, 2, \ldots$. Since J_3 has finitely many eigenvalues, there exists an integer $N \geq 0$ such that $v_N \neq 0$ and $v_{N+1} = 0$. Hence,

$$0 = J_+ v_{N+1} = (N+1)(2\mu + 1 - N - 1)v_N = (N+1)(2\mu - N)v_N \Longrightarrow 2\mu = N.$$

Defining $l = N/2$ and $\mu = N/2 = l$, we get the formulae stated in the theorem.

Now, the vectors v_j are eigenvectors of J_3 corresponding to distinct eigenvalues; therefore they are linearly independent and $\mathbb{W} := \text{vect}\{v_j, j = 0, 1, \ldots, N\}$ is invariant under the action of J_3, J_+, J_-. Since the latter span $\mathfrak{so}(3)$, it follows that $\mathbb{W}$ is invariant under $\mathfrak{so}(3)$. The representation is assumed irreducible; hence $\mathbb{W} = \mathbb{V}$ and consequently, $\dim \mathbb{V} = N + 1 = 2l + 1$. □

Definition 16.4.29. Let $(\alpha, \mathbb{V})$ be a finite-dimensional irreducible representation of $\mathfrak{so}(3)$. We call **spin of the representation** the maximal eigenvalue of $J_3 = i\alpha(F_3)$. Equivalently, l is the unique non-negative integer or half-integer such that $\dim \mathbb{V} = 2l + 1$.

Exercise 16.4.30. Show that for every $l \in \mathbb{N}/2$, there exists an irreducible representation of $\mathfrak{so}(3)$ of dimension $2l + 1$.

Hint: For a given $l \in \mathbb{N}/2$, construct a vector space $\mathbb{V}$ by defining its basis $\{v_0, v_1, \ldots, v_{2l}\}$. Let $\mathfrak{so}(3)$ act on it as in theorem 16.4.28 and check that J_3, J_+, J_- verify the correct commutation relations so that $\mathbb{V}$ is indeed a representation space of $\mathfrak{so}(3)$. Then one concludes by showing irreducibility.

Proposition 16.4.31. *Let $\alpha : \mathfrak{so}(3) \to \mathfrak{gl}(\mathbb{V})$ be an irreducible representation of spin l. Then, the vector space $\mathbb{V}$ can be equipped with a scalar product, unique up to multiplication by constants, such that $\alpha(X)$ is skew-adjoint for all $X \in \mathfrak{so}(3)$.*

Proof. Suppose first that such a scalar product, guaranteeing skew-adjointness of all $\alpha(X)$, exists. Then, recalling that $J_3 = i\alpha(F_3)$ and $J_\pm = i\alpha(F_1) \mp \alpha(F_2)$, skew adjointness of all $\alpha(X)$ implies that $J_3^* = J_3$ and $J_\pm^* = J_\mp$. Let (v_j) be the set of eigenvectors corresponding to the different eigenvalues $l - j$ of J_3. By adjointness of J_3 it follows that (v_j) must be orthogonal. Conversely, if $\langle \cdot \,|\, \cdot \rangle$ is a scalar product such that the eigenvectors (v_j) of J_3 are orthogonal, it follows that $J_3^* = J_3$.

Suppose henceforth the aforementioned properties for the adjoints of J_3 and $J_\pm$. We get, using the identity $[J_+, J_-] = 2J_3$, that

$$\begin{aligned}
\langle v_j \,|\, v_j \rangle &= \langle J_- v_{j-1} \,|\, J_- v_{j-1} \rangle = \langle v_{j-1} \,|\, J_+ J_- v_{j-1} \rangle \\
&= (j-1)(2l + 1 - (j-1))\langle v_{j_1} \,|\, J_- v_{j-2} \rangle + 2(l - j + 1)\langle v_{j-1} \,|\, v_{j-1} \rangle \\
&= [(j-1)(2l + 2 - j) + 2(l - j + 1)]\langle v_{j-1} \,|\, v_{j-1} \rangle = j(2l - j + 2)\langle v_{j-1} \,|\, v_{j-1} \rangle.
\end{aligned}$$

This recurrence must be valid for all $l = 1, \ldots, 2l$. Now, since $j(2l - j + 2) > 0$ for all these values of j, there is no obstacle preventing this recurrence from holding. In order to completely determine the scalar product, it is enough to fix the constant $c = \langle v_0 \,|\, v_0 \rangle$. □

For a finite-dimensional irreducible representation $\alpha : \mathfrak{so}(3) \to \mathfrak{gl}(\mathbb{V})$ on a vector space $\mathbb{V}$ equipped with a non-degenerate invariant bilinear form b, there exists a linear operator C_α acting on $\mathbb{V}$ in the centre of the representation (i.e. commutes with all $\alpha(F_k)$). This operator is called **Casimir operator**.

Theorem 16.4.32. *Let $\alpha : \mathfrak{so}(3) \to \mathfrak{gl}(\mathbb{V})$ be an irreducible representation of spin l (equivalently $\dim \mathbb{V} = 2l+1$). Then $C_\alpha = \sum_{k=1}^3 \alpha(F_k)^2$ is a Casimir operator for α. Moreover for all $v \in \mathbb{V}$, $C_\alpha v = -l(l+1)v$.*

Before proving this theorem, we need a standard result in the theory of Lie algebras:

Theorem 16.4.33 (Schur's lemma)**.** *Let $(\alpha, \mathbb{V})$ be a finite-dimensional representation of a complex Lie algebra $\mathfrak{g}$.*

1. *If α is irreducible then any operator T on $\mathbb{V}$ commuting with all $\alpha(X), X \in \mathfrak{g}$, has the form $T = \lambda \mathbb{1}$, for some $\lambda \in \mathbb{C}$.*
2. *It α is fully reducible (i.e. every invariant subspace has an invariant complement) and is such that every operator T acting on $\mathbb{V}$ that commutes with all $\alpha(X), X \in \mathfrak{g}$, has the form $T = \lambda \mathbb{I}$ for some $\lambda \in \mathbb{C}$ then α is irreducible.*

Proof of the theorem 16.4.32. To show that C_α is in the centre of $\mathfrak{so}(3)$, we use the commutation relations to show that $\forall k = 1,2,3$, $[C_\alpha, \alpha(F_k)] = 0$. Since (F_k) is basis of $\mathfrak{so}(3)$, it follows that $[C_\alpha, \alpha(X)] = 0$ for every $X \in \mathfrak{so}(3)$, hence, by Schur's lemma, there exists a $\lambda \in \mathbb{C}$, such that $C_\alpha v = \lambda v$, for all $v \in \mathbb{V}$. Let v_0 be the non-vanishing vector introduced in the proof of theorem 16.4.28 and use the standard re-writing $C_\alpha = -\sum_{k=1}^3 J_k^2 = -(J_3^2 + J_- J_+ + J_3)$ to establish that $C_\alpha v_0 = -l(l+1)v_0$. Since this equation holds for the non-vanishing vector v_0, it holds for all vectors. □

16.4.4 Irreducible representations of SO(3) and notion of the spin of a particle

The natural invariance group for rotation is $\mathsf{SO}(3)$. We have already seen that its Lie algebra $\mathfrak{so}(3)$ is isomorphic to the Lie algebra $\mathfrak{su}(2)$ of its universal covering group$\mathsf{SU}(2)$. Moreover, the representations of $\mathsf{SO}(3)$ can be obtained from those of $so(3)$ by using the exponential map. The following theorem clarifies this statement.

Theorem 16.4.34. *Denote by $\alpha_l : \mathfrak{so}(3) \to \mathfrak{gl}(\mathbb{V})$, the irreducible representation whose spin is $l = \frac{1}{2}(\dim \mathbb{V} - 1)$.*

— *If $l \in \mathbb{N}$ (i.e. $\dim \mathbb{V}$ is odd), there exists a representation $A_l : \mathsf{SO}(3) \to \mathsf{GL}(\mathbb{V})$ such that*

$$A_l(\exp(tX)) = \exp(t\alpha_l(X)),\ \forall X \in \mathfrak{so}(3), t \in \mathbb{R}.$$

— *If $l \in \mathbb{N} + \frac{1}{2}$ (i.e. $\dim \mathbb{V}$ is even), there does not exist such a representation.*

Remark 16.4.35. The representations of $\mathsf{SO}(3)$ are those precisely with integer spin. Nevertheless, a natural question remains: do the other representations with spin in $\mathbb{N} + \frac{1}{2}$ have any physical meaning? These representations are termed **half-integer spin representations** in the literature. We will see that those representations are responsible for internal rotational degrees of freedom of the particle, present even in the absence of any physical rotation in $\mathbb{R}^3$, known as spin of the particle.

Proof ot the theorem 16.4.34. — Let $l \in \mathbb{N} + \frac{1}{2}$. In the eigenbasis $(v_j)_{j=0,\dots,2l}$ of J_3, we have $J_3 v_j = (l-j)v_j$. For $t = 2\pi$,

$$\exp(t\alpha_l(F_3)) = \exp(2i\pi\alpha_l(F_3)) = \exp(-2\pi J_3),$$

and applying this operator on v_j, we get $\exp(-2\pi J_3)v_j = -v_j$ for all $j = 0, \dots, 2l$ because the eigenvalues $l - j \in \mathbb{N} + \frac{1}{2}$. I.e. $\exp(-2i\pi J_3) = -I$. It is an elementary computation to show that $\exp(2\pi F_3) = e$ (e the neutral element of $\mathsf{SO}(3)$). Hence, if it was be possible to express the representation A_l in terms of α_l, we should have

$$A_l(e) = A_l(\exp(-2\pi J_3)) = \exp(2\pi\alpha_l(F_3)) = \exp(-2i\pi J_3) = -I.$$

This is impossible because A_l must be an homomorphism.

— Let now $l \in \mathbb{N}$. Use the isomorphism $\phi : \mathfrak{su}(2) \to \mathfrak{so}(3)$ to transform the basis (E_1, E_2, E_3) of $\mathfrak{su}(2)$ into the basis (F_1, F_2, F_3) of $\mathfrak{so}(3)$. If α_l is a representation of $\mathfrak{so}(3)$, the aforementioned isomorphism induces a representation $\alpha'_l : \mathfrak{su}(2) \to \mathfrak{gl}(\mathbb{V})$ by $\alpha'_l = \alpha_l \circ \phi$. Since $\mathsf{SU}(2)$ is simply connected, there exists a representation A'_l of $\mathsf{SU}(2)$ obtained by exponentiation, i.e. $A'_l(\exp(X)) = \exp(\alpha'_l(X)) = \exp(\alpha_l(\phi(X)))$ for all $X \in \mathfrak{su}(2)$. It is easy to verify that $\exp(2\pi E_3) = -e$. Therefore,

$$A'_l(-e) = A'_l(\exp(2\pi E_3)) = \exp(2\pi\alpha_l(\phi(E_3))) = \exp(2\pi\alpha_l(F_3)) = \exp(2\pi i J_3).$$

But now the eigenvalues of J_3 are integers. Hence $\exp(2\pi J_3))v_j = v_j$ for all j. Consequently, $\exp(2\pi J_3) = I$.
Now recall that $\mathsf{SU}(2)$ is the universal cover of $\mathsf{SO}(3)$. There exists a surjective homomorphism $\Phi : \mathsf{SU}(2) \to \mathsf{SO}(3)$, whose kernel is $\ker(\Phi) = \{e, -e\}$ that leads to the previously mentioned Lie algebra isomorphism ϕ. We have established in the previous lines that $\ker A'_l \supseteq \{-e, e\}$. Hence Φ factors, on $\mathsf{SO}(3)$, into two components so that the representation $A'_l = A_l \circ \Phi$ leads to $A_l = A'_l \circ \Phi^{-1}$.

□

Irreducible representations of $\mathsf{SO}(3)$ in $L^2(\mathbb{S}^2)$

We have seen, in 16.4.27, that the mapping $A : \mathsf{SO}(3) \to \mathfrak{B}(L^2(\mathbb{R}^3))$ defined by

$$\mathsf{SO}(3) \ni R \mapsto A(R) \text{ s.t. } (A(R)\psi)(\mathbf{x}) = \psi(R^{-1}\mathbf{x}),$$

for all $\psi \in L^2(\mathbb{R}^3)$ and $\mathbf{x} \in \mathbb{R}^3$, is a unitary representation. Now, if the problem under consideration has rotational symmetry and we split the $\mathbf{x}$ dependence into radial and angular coordinates, the action of $\mathsf{SO}(3)$ manifests itself only by its action on angular coordinates. It is therefore possible to split the action of $\mathsf{SO}(3)$ into its action on $L^2(\mathbb{S}^2)$ — equipped with area measure on $\mathbb{S}^2$ that is invariant under $\mathsf{SO}(3)$ — and on the angular part. The representation reads on the angular part $(A(R)\psi)(\mathbf{u}) = \psi(R^{-1}\mathbf{u})$ for $\mathbf{u} \in \mathbb{S}^2$. Once the angular action will be determined, the full action on $L^2(\mathbb{R}^3)$ will be easily recovered.

The Laplacian on $\mathbb{R}^d$ is defined as being the differential operator defined formally on $L^2(\mathbb{R}^d)$ by

$$\Delta = \sum_{k=1}^{d} \partial_k^2,$$

i.e. Δ is only defined on a dense domain (for instance $\mathbf{S}(\mathbb{R}^d)$.

Definition 16.4.36. A polynomial on $\mathbb{R}^d$ with complex coefficients is called
— **harmonic** if $\Delta p = 0$,
— **homogeneous of degree** l if $p(\lambda x_1, \dots, \lambda x_d) = \lambda^l p(x_1, \dots x_d)$ for all $\mathbf{x} = (x_1, \dots, x_d) \in \mathbb{R}^d$ and all $\lambda \in \mathbb{R}$.
The set of polynomials on $\mathbb{R}^d$, homogeneous of degree l, is denoted by HP_l^d while the set of harmonic polynomials on $\mathbb{R}^d$ homogeneous of degree l by HHP_l^d.

Exercise 16.4.37. Show that

1. HP_l^d is a vector space,
2. $\dim \mathsf{HP}_l^2 = l + 1$,
3. $\dim HP_l^3 = \frac{(l+1)(l+2)}{2}$.

Hint: Look at figure **??**.

Let $l \in \mathbb{N}$ and

$$\mathbb{V}_l = \mathsf{vect}\{p\restriction_{\mathbb{S}^2} : p \in \mathsf{HHP}_l^3\} \subseteq L^2(\mathbb{S}^2).$$

The set $\mathbb{V}_l$ constitutes the **space of spherical harmonics** of degree l.

Exercise 16.4.38. Let p be an homogeneous polynomial on $\mathbb{R}^3$. Show that its restriction $p\restriction_{\mathbb{S}^2} \equiv 0$ if, and only if, $p \equiv 0$.

Exercise 16.4.39. Show that all homogeneous polynomials of degree 0 and 1 are harmonic. Determine $\mathbb{V}_0^3$, $\mathbb{V}_1^3$, and $\mathbb{V}_2^3$.

Theorem 16.4.40. *The spaces $\mathbb{V}_l$ defined in 16.4.36 have the following properties:*

1. $\dim \mathbb{V}_l = 2l + 1$,
2. $\mathbb{V}_l$ *is invariant under* $\mathsf{SO}(3)$ *and irreducible*
3. $l \neq m \Longrightarrow \mathbb{V}_l \perp \mathbb{V}_m$ *in* $L^2(\mathbb{S})^2$,
4. $L^2(\mathbb{S}^2) = \oplus_{l \in \mathbb{N}} \mathbb{V}_l$.

The proof is split into various intermediate results.

Lemma 16.4.41. *The set P_l is the space of homogeneous polynomials of degree l on $\mathbb{R}^3$. Moreover, for $l \geq 2$,*

1. $\Delta : P_l \to P_{l-2}$, *and*
2. $\dim \mathbb{V}_l = \dim P_l - \dim P_{l-2} = 2l + 1$.

Proof. 1. For $l \geq 2$, we have obviously $\Delta(P_l) \subseteq P_{l-2}$ since the action of the Laplacian decreases powers by two.

2. All homogeneous polynomials of degree 0 and 1 are harmonic. Since there is only one such polynomial of degree 0 and there are 3 monomials of degree 1, namely x_1, x_2, x_3, the formula is satisfied.

Now, equip P_l with the scalar product of Bargmann-Segal. Instanciating the identity $\ker(X^*) = \mathrm{im}(X)^\perp$, valid for all operators X acting on P_l, to the case $X = \Delta$ and using the fact that Δ^* is the multiplication operator by $\|\mathbf{x}\|^2$, we conclude that Δ^* is injective. In fact, $\|\mathbf{x}\|^2 = 0 \Leftrightarrow x_1^2 + x_2^2 + x_3^2 = 0 \Leftrightarrow \mathbf{x} = \mathbf{0}$. □

Corollary 16.4.42. *Let $l \in \mathbb{N}$ and $k = l/2$ (if l is even) or $k = (l-1)/2$ (if l is odd). Then every $p \in P_l$ can be decomposed into a superposition of polynomials of the form*

$$p(\mathbf{x}) = \sum_{m=0}^{k} \|\mathbf{x}\|^{2m} p_m(\mathbf{x}),$$

where p_m is a harmonic polynomial homogeneous of degree $l - 2m$. In particular, if $\mathbf{x} \in \mathbb{S}^2$, then $p\restriction_{\mathbb{S}^2} = (\sum_{m=0}^{k} p_m)\restriction_{\mathbb{S}^2}$.

Remark 16.4.43. Mind that the polynomial $\sum_{m=0}^{k} p_m(\mathbf{x})$ is not homogeneous for general $\mathbf{x} \in \mathbb{R}^3$. However, given any polynomial p there exists a harmonic polynomial p' such that p and p' have the same restriction on $\mathbb{S}^2$.

Exercise 16.4.44. Let, as usual, $J_k = i\alpha(F_k)$ and $J_\pm = J_1 \pm iJ_2$. Show that for any $l \in \mathbb{N}$, the polynomial $p(\mathbf{x}) = (x_1 + ix_2)^l$ belongs to $\mathbb{V}_l$. Moreover, show:
— $J_3 p = lp$,
— $J_+ p = 0$,
— $\mathbb{V}_l$ is irreducible under the action of $\mathrm{SO}(3)$ (hint: repeatedly act on p with J_-),
— and conclude by completing the proof of the theorem 16.4.40.

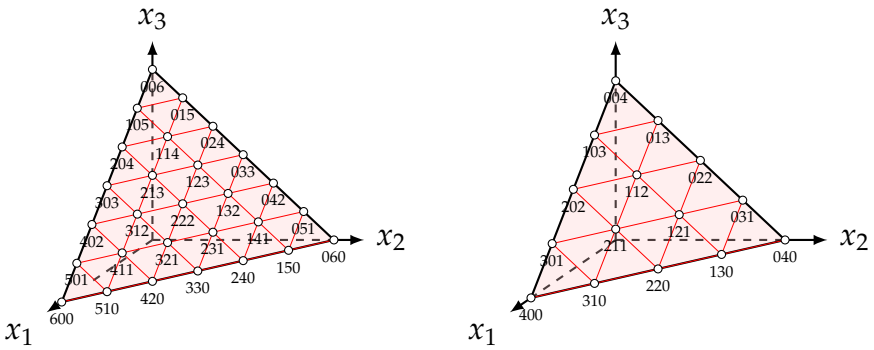


Figure 16.5 – The set of homogeneous polynomials of degree l in 3 variables $\mathbf{x} = (x_1, x_2, x_3)$ is spanned by monomials of the form $x_1^{l_1} x_2^{l_2} x_3^{l_3}$, with $l_1, l_2, l_3 \in \mathbb{N}$ and $l_1 + l_2 + l_3 = l$. This remark allows the bijective representation of the spanning monomials by the points depicted in the above figures for the cases of $l = 6$ and $l = 4$.

Irreducible representations of $\mathrm{SO}(3)$ in $L^2(\mathbb{R}^3)$

In the previous subsection, it has been established that $L^2(\mathbb{S}^2) = \oplus_{l \in \mathbb{N}} \mathbb{V}_l$. Moreover, it was shown that $\dim \mathbb{V}_l = 2l + 1$ by exhibiting a basis of $\mathbb{V}_l$. Although the so con-

structed basis can be used to obtain an orthonormal basis of $\mathbb{V}_l$, this construction is a little tedious. We shall follow below a slightly different approach.

Using spherical coordinates (r, θ, ϕ) in $\mathbb{R}^3$ instead of Cartesian (x_1, x_2, x_3) ones, i.e.

$$x_1 = r\sin\theta\cos\phi, x_2 = r\sin\theta\sin\phi, x_3 = r\cos\phi,$$

where

$$r = \|\mathbf{x}\|, \theta = \arccos\left(\frac{x_3}{r}\right) \in [0, \pi], \phi = \arctan\left(\frac{x_2}{x_1}\right) \in [0, 2\pi],$$

we observe that, expressing any $\psi \in L^2(\mathbb{R}^3)$ in spherical coordinates, we get

$$\|\psi\|_2^2 = \int_0^\infty \mathrm{d}r\, r^2 \int_0^\pi \mathrm{d}\theta\ \sin\theta \int_0^{2\pi} \mathrm{d}\phi\ \psi(r, \theta, \phi).$$

The previous equation means that for almost all r, the function $\psi(r, \theta, \phi)$ must be square integrable with respect to the measure to the $\sin\theta \mathrm{d}\theta\mathrm{d}\phi$ acting on the angular variables (θ, ϕ), i.e. for almost all r, $\psi(r, \cdot, \cdot) \in L^2(\mathbb{S}^2)$. Here the scalar product on $L^2(\mathbb{S}^2)$ is given by

$$L^2(\mathbb{S}^2) \times L^2(\mathbb{S}^2) \ni \langle f \,|\, g \rangle := \int_0^\pi \mathrm{d}\theta \sin\theta \int_0^{2\pi} \mathrm{d}\phi\ \overline{f(\theta, \phi)} g(\theta, \phi).$$

In summarising, we have thus identified the Hilbert space $L^2(\mathbb{R}^3)$ with the Hilbert space $L^2([0, \infty[; L^2(\mathbb{S}^2), r^2\mathrm{d}r)$ of $L^2(\mathbb{S}^2)$-valued measurable functions defined on the interval $[0, \infty[$ that are square integrable with respect to the measure $r^2\mathrm{d}r$.

Let $l \in \mathbb{N}$ and f a measurable function such that $\int_0^\infty |f(r)|^2 r^{2l+2}\mathrm{d}r < \infty$. Since every $\mathbf{x} \neq 0$ can be written as $\mathbf{x} = \hat{\mathbf{x}}\|\mathbf{x}\|$, where $\hat{\mathbf{x}} = \frac{\mathbf{x}}{\|\mathbf{x}\|} \in \mathbb{S}^2$, any function of the form $\psi(\mathbf{x}) = p(\mathbf{x})f(\|\mathbf{x}\|)$, with $p \in \mathbb{V}_l$, can be rewritten in the equivalent form $\psi(\mathbf{x}) = p(\hat{\mathbf{x}})\|\mathbf{x}\|^l f(\|\mathbf{x}\|)$, establishing thus that ψ is both measurable and square integrable. It is therefore meaningful to define the subspace

$$\mathbb{V}_l^f = \{\psi \in L^2(\mathbb{R}^3) : \psi(\mathbf{x}) = p(\mathbf{x})f(\|\mathbf{x}\|), p \in \mathbb{V}_l\}$$

where the dependence of ψ in $\mathbf{x}$ is split into an angular and a radial part. It is therefore clear that the representations in $L^2(\mathbb{S}^2)$ can serve as germs of the representations in $L^3(\mathbb{R}^3)$.

Now $H(\mathbf{r}; \mathbf{p})$ is invariant under the rotations of the group $\mathsf{SO}(3, \mathbb{R})$. Hence the angular momentum $\mathbf{J} = \mathbf{r} \wedge \mathbf{p}$ is conserved by Noether's theorem [111]. Decomposing $\mathbf{J}$ into its Cartesian components $M_1 = r_2p_3 - r_3p_2$ (and cyclically for the others) we easily check that $\{H, M_i\} = 0$ for $i = 1, 2, 3$ and additionally, $J_j = i\hbar\alpha(F_j)$.

16.5 The hydrogen atom

16.5.1 Classical planetary model and its inconsistencies

After the experimental confirmation of the existence of atoms [3] in 1908 by Perrin [4] [117] (reprinted in [118]), that has been made possible thanks to the mathematical description of Brownian motion by Einstein [53], various models for the chemical atoms have been proposed. The *plum pudding model* of the atom, proposed by J.J. Thomson in 1904, was experimentally shown to be totally unrealistic by Ernest Rutherford in 1909. Rutherford's experiments were compatible only with a planetary model for the atom.

The planetary model of the hydrogen atom considers a positively charged (with charge e) massive proton having mass m_1 around which gravitates a light negatively charged (with charge $-e$) electron of mass m_2, with $m_2 \ll m_1$. According to classical electrodynamics, the total energy of the system is given by the Hamiltonian function

$$H(\mathbf{x}_1, \mathbf{x}_2; \mathbf{p}_1, \mathbf{p}_2) := \frac{\|\mathbf{p}_1\|^2}{2m_1} + \frac{\|\mathbf{p}_2\|^2}{2m_2} + V(\|\mathbf{x}_1 - \mathbf{x}_2\|),$$

where $\mathbf{x}_i$, $i = 1, 2$ designate the positions of the (centres of mass) of the particles and $\mathbf{p}_i = m_i \dot{\mathbf{x}}_i$ their moments. V stands for the Coulomb electrostatic potential $V(\|x\|) = -k_e \frac{e^2}{\|\mathbf{x}\|}$, where $k_e = \frac{1}{4\pi\varepsilon_0}$ is the Coulomb constant [5].

Due to the large disparity of the masses [6] the system is approximately decoupled. Introducing new coordinates $(\mathbf{X}, \mathbf{r})$ for the centre of mass of the system $\mathbf{X} = \frac{m_1\mathbf{x}_1 + m_2\mathbf{x}_2}{M}$, where $M = m_1 + m_2$ is the total mass and $\mathbf{P} = M\dot{\mathbf{X}}$, and relative coordinates $\mathbf{x} = \mathbf{x}_1 - \mathbf{x}_2$ and $\mathbf{p} = m\dot{\mathbf{x}}$, where [7] $m = \frac{m_1 m_2}{M}$, the Hamiltonian decouples into

$$H(\mathbf{x}, \mathbf{X}; \mathbf{p}, \mathbf{P}) := \frac{\|\mathbf{P}\|^2}{2M} + H(\mathbf{x}; \mathbf{p}),$$

where the first term describes to free motion of the centre of mass and the second one

$$H(\mathbf{x}; \mathbf{p}) = \frac{\|\mathbf{p}\|^2}{2m} + V(\|\mathbf{x}\|)$$

describes the motion of a fictitious particle (having almost the same mass as the electron) of reduced mass m in the central potential V.

Although this form will be shown to be the right starting point for a genuine quantum description, the classical model is flawed by two major inconsistencies:

3. The hypothesis of their existence has been issued by the British scientist John Dalton in 1802.
4. The 1926 Nobel Prize in Physics has been awarded to French physicist Jean Perrin for this discovery.
5. Its value is $9.9875517873681764 \times 10^9$ $\mathrm{Nm^2C^{-2}}$.
6. The electron mass is $m_2 = 9.10938356 \times 10^{31}$ kg while the proton mass is $m_1 = 1.6726219 \times 10{-}27$ kg.
7. Note that $m = 0.999449819 m_2$.

— Since the electrons are charged and supposed to turn around the nucleus, they emit constantly electromagnetic radiation as a consequence of Maxwell equations. Should the electrons — considered as classical particles — gravitate around the nucleus, they rapidly would loose all their energy and collapse on the nucleus. The (classically computed) collapse time for the hydrogen atom (in the planetary model) is 16 ps $= 1.6 \times 10^{-11}$ s, while this atom is experimentally known to be stable!

— The experimental observation of absorption and emission phenomena occur at discrete very precise frequencies. For instance, the hydrogen in higher solar atmosphere absorbs light at very specific frequencies so that the spectrum of solar light when analysed by a prism does not only show the familiar *rainbow-like* continuous spectrum; some specific colours are totally missing instead. On the other hand, hydrogen lamps emit only at some very specific frequencies, precisely located at the positions of the spectrum where absorption is observed in the solar spectrum (see figure 16.6). These observations are incompatible with

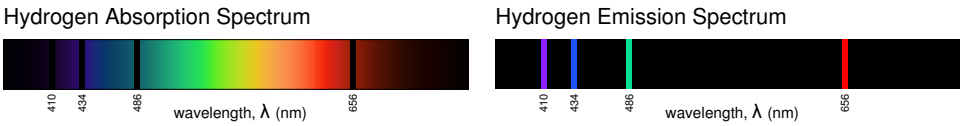


Figure 16.6 – The absorption and emission lines of hydrogen.

classical physics since classically energy can take continuous values (compare with classical harmonic oscillator).

It will be shown below that both inconsistencies disappear in the quantum description.

16.5.2 The quantum description

The quantum description of the energy spectrum of the hydrogen atom constituted one of the major triumph of the quantum formalism since all its predictions were experimentally verified with unprecedented accuracy. It paved the way of the unified description of all atomic and molecular Physics, explaining thus the fundamentals of Chemistry (and hence Biology).

Absorption and emission spectra from atoms other than hydrogen (or from molecules) display the same features and their frequencies are so precise that can serve as signatures of the existence of these elements. The figure 16.8 give such an example.

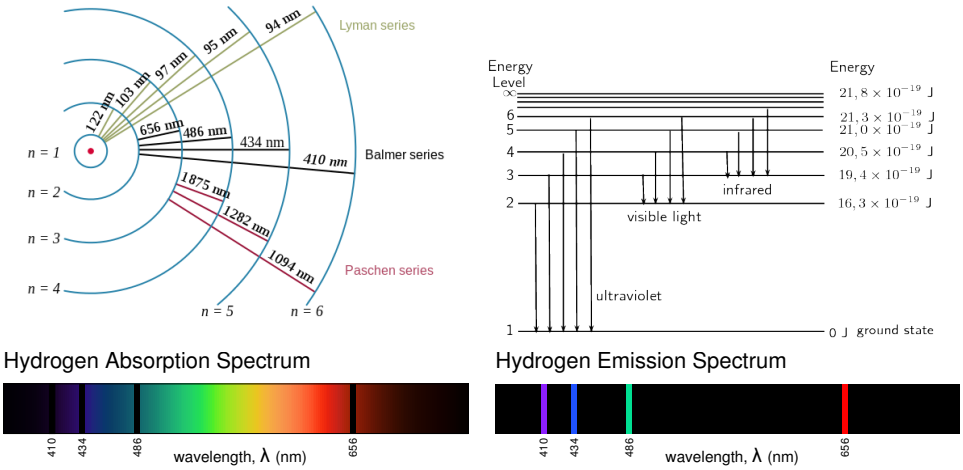


Figure 16.7 – Explanation of the absorption/emission lines of hydrogen.

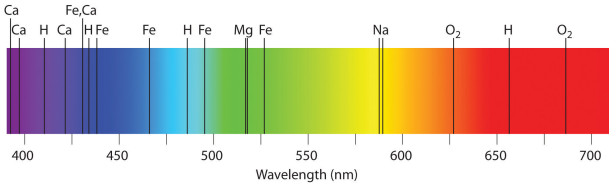


Figure 16.8 – Absorption lines of other atoms or molecules used as signature of these elements.

16.6 Related results

16.6.1 Mechanism of classifying atomic elements into the periodic table

16.7 Stern-Gerlach experiment and the spin of electron

Short video explaining the Stern-Gerlach experiment.

16.7.1 Principle of nuclear magnetic resonance imaging

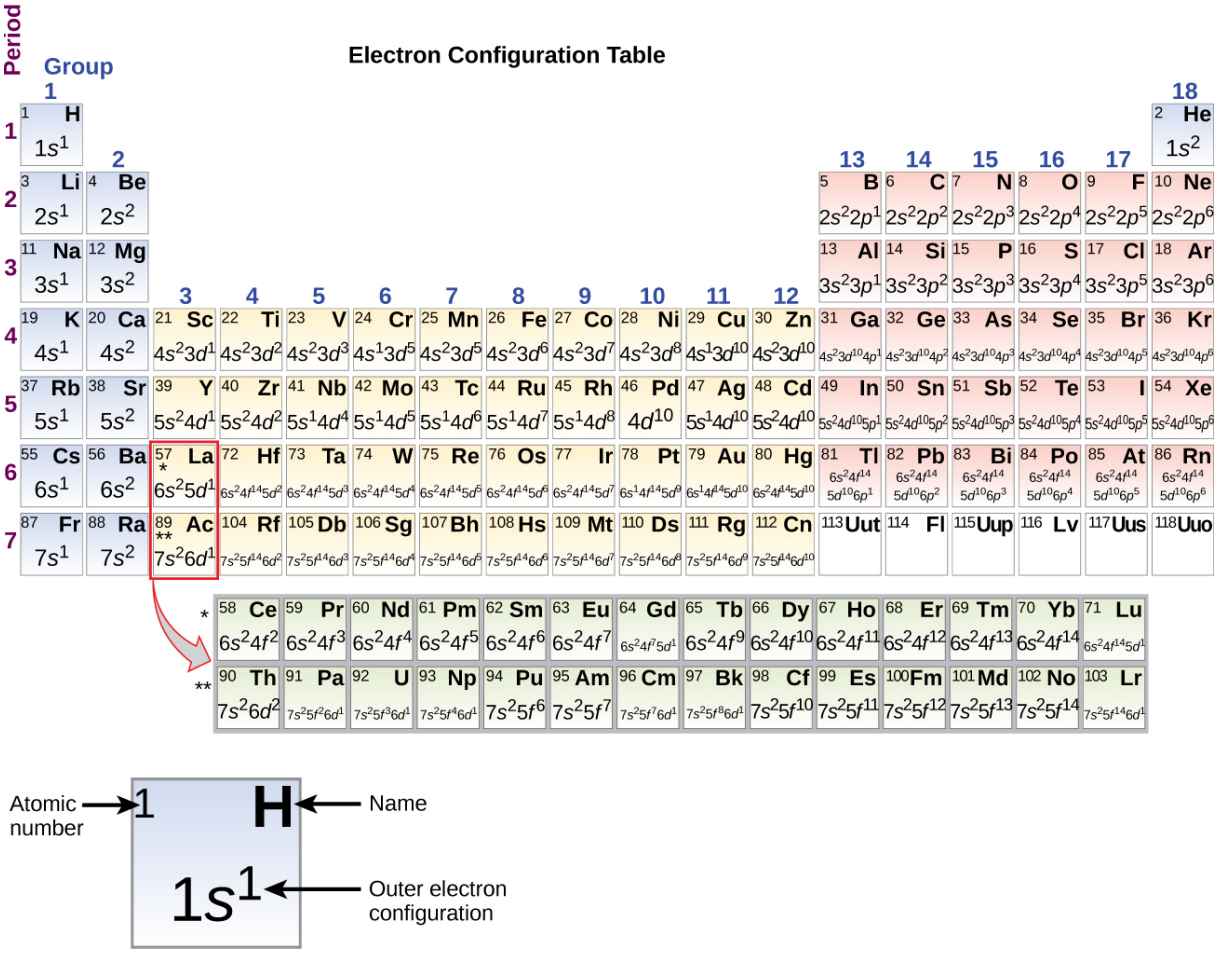
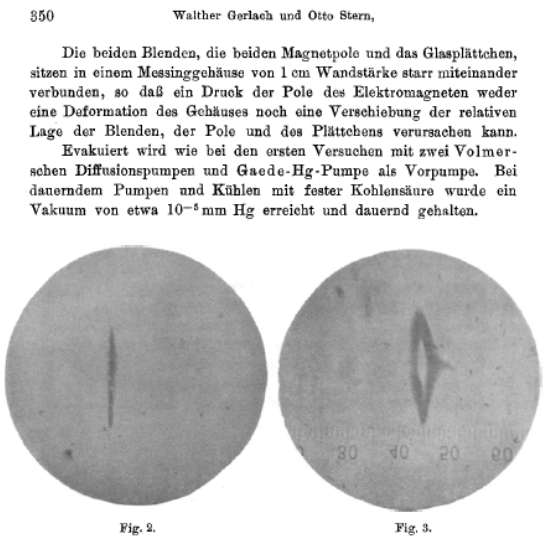


Figure 16.9 – Mendele'ev periodic table of elements displaying the electronic configuration of the outer shell.



350 Walther Gerlach und Otto Stern,

Die beiden Blenden, die beiden Magnetpole und das Glasplättchen, sitzen in einem Messinggehäuse von 1 cm Wandstärke starr miteinander verbunden, so daß ein Druck der Pole des Elektromagneten weder eine Deformation des Gehäuses noch eine Verschiebung der relativen Lage der Blenden, der Pole und des Plättchens verursachen kann.

Evakuiert wird wie bei den ersten Versuchen mit zwei Volmer-schen Diffusionspumpen und Gaede-Hg-Pumpe als Vorpumpe. Bei dauerndem Pumpen und Kühlen mit fester Kohlensäure wurde ein Vakuum von etwa 10^{-5} mm Hg erreicht und dauernd gehalten.

Fig. 2. Fig. 3.

Figure 16.10 – Facsimile from the 1922 original article of Stern-Gerlach [69, 68], displaying the experimentally observed beam splitting.

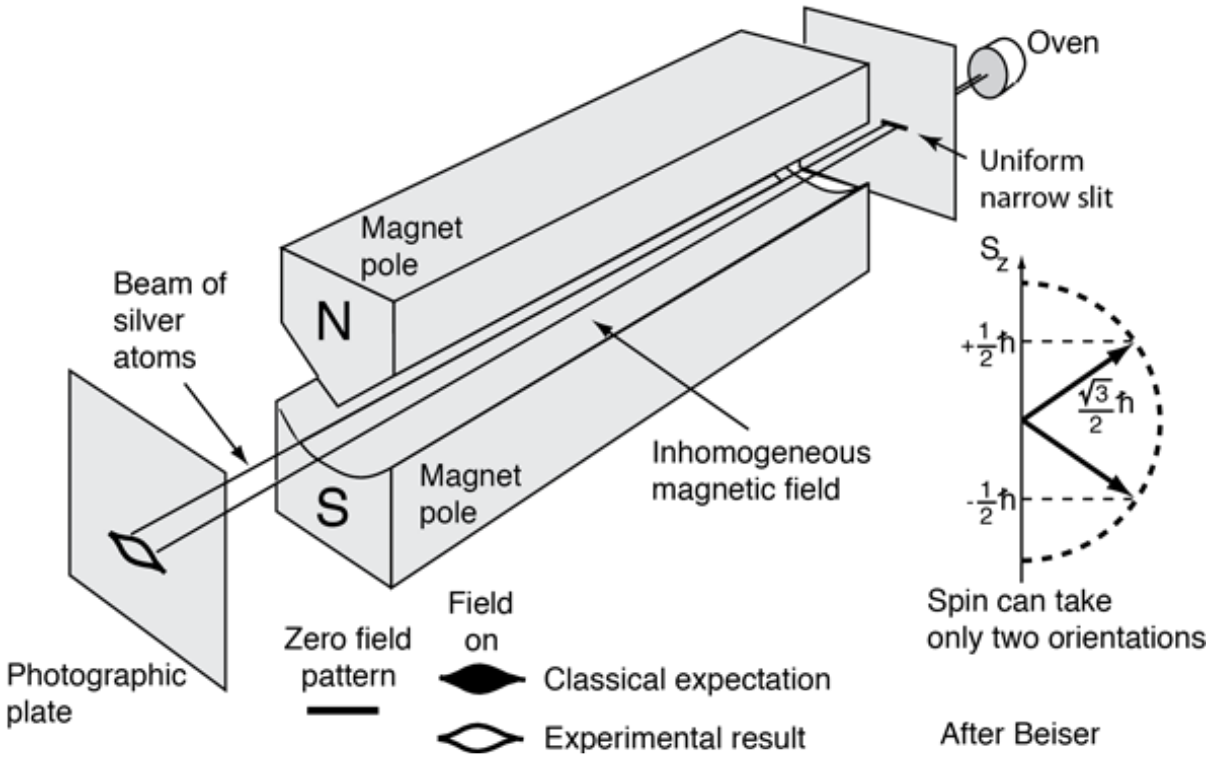


Figure 16.11 – Experimental setup of the Stern-Gerlach experiment. The elecrtronic configuration of silver is [Kr]$5s^1$; the full shells up to [Kr] contribute with 0 total spin. The nucleus spin has en effect below the detection threshold because its Bohr magneton is 2000 times smaller that for the electron.

17

Quantum formalism based on the informational approach

Conditioning as disintegration [35], regular conditional probabilities, standard Borel spaces.

Projective limits [109]. Probabilities on lattices [103]. Effect algebras [81, 90].

A

What is light?

Most of the experiments investigating the nature of the quantum, at the crux of the most important foundational questions of quantum formalism, although in principle possible to realise with electrons or atoms, are more easily implemented using light. Moreover, in these days, light plays a key role in the transmission, storage, processing, and protection of digital information (let it be classical or quantum). It is therefore important both for practitioners of cryptography and digital communication and for those interested to the foundational aspects of quantum formalism to know some basic facts about nature of light and its properties.

The major difficulty towards such a goal is that the nature of light cannot be easily explained; *stricto sensu* its description lies outside the realm of pure (non-relativistic) quantum mechanics since its speed (constant in all inertial frames) is not small compared to the speed c of ... light; it is precisely equal to c. Hence the correct framework of its description is quantum field theory. We know these days that a beam of light is a flow of a huge number of light quanta, called photons [1].

We start with a brief history ot Light. We continue then with its description as electromagnetic waves — solutions of the sourceless Maxwell equations — and give some hints towards the (classical, i.e. non-quantum) relativistic rewriting of Maxwell equations in a relativistically covariant form. Then a step towards the quantisation of the electromagnetic field is made and the description of the most common optical devices is made in the framework of quantum optics.

The reader is warned however that this appendix is necessarily of phenomenological nature, intending to give the basic necessary tools to handle phenomena involving

1. Within the quantum field theoretical framework photons are massless (hence travelling at the speed c in all inertial frames) particles, with spin 1 (hence bosons) particles, and interacting with charged matter. Since they cannot be stopped, the possible eigenvalues of their spin are only $+1$ and -1 (the valued 0 is forbidden); it is therefore improper to speak about their polarisation, they bear only helicity.

light. Readers interested in the full-fledged microscopic description of light within quantum electrodynamics are invited to consult textbooks on quantum electrodynamics (for instance [24, 57, 88, 91]).

A.1 History

The conjectured nature of light has undergone several profound changes during centuries.

Ancient times: For Egyptians (ca. 10th century before our era) light was "ocular fire" for the eye of the god of sun Ra. For the ancient Greeks (ca. 4 century before our era) sight was an interaction of light rays emitted both by the eye and the luminous source; rays were supposed to travel in straight lines. For the ancient Indians (ca. 1–2 century of our era), light was a stream of high velocity "fire" atoms.

Arabic golden age: Hasan Ibn al-Haytham (ca. 965–ca. 1040), Latinised as Alhazen, mathematician, physicist, physician, astronomer, and philosopher, is considered as the father of modern geometric optics. In a highly influential book, the *Kitab al-Manazir* (Book of optics), he explained that vision occurs when light bounces on an object and then is directed to the eyes. In the same book, among other things, he formalises and investigates in detail refraction i.e. the phenomenon of change of the direction of propagation when light crosses an interface of two different optical media, e.g. air-water. Additionally, he gave the correct explanation (as we now know) of this phenomenon, namely that light travel slower in the denser medium.

Early 17th century: Light is particles. René Descartes (1596–1650) explained refraction of light by a modification of its speed in the two media based on the wrong conjecture (6 centuries after the correct prediction of al-Haytham!) that light travels faster in the denser medium. Pierre Gassendi (1592–1655) proposed a particle theory of light.

Late 17th century: In 1676, the Danish astronomer Ole Rømer (1644–1710), working at the *Observatoire royal de Paris*, by timing the eclipses of the Jupiter moon Io, determined [2] that light travels at finite speed, he estimated at ca. 220000 km/s, about 26% lower than the now known precise speed c. Sir Isaac Newton (1642–1727) published in 1704 his treatise *Opticks* [3] where he provides a particle explanation of refraction making the same mistake as Descartes by assuming that light travels faster in water than in the air. Among other things, he established that white light is a mixture of all colours.

Late 17th–19th centuries: Light is waves. Christiaan Huygens (1629-1695) proposed a wave theory of light and introduced the fallacious idea of the luminiferous ether as the medium into which light propagates. Leonhard Euler (1707–1738) and Augustin-Jean Fresnel (1788–1827), independently, developed a consistent wave theory of light explaining many observed experimental facts. The

2. Démonstration touchant le mouvement de la lumière, Journal des sçavants, Académie des inscriptions et belles-lettres, 1676, Accessible sur Gallica.

3. Opticks: or a treatise of the reflexions, refractions, inflexions and colours of light, Sam. Smith & Benj. Walford, printers to the Royal Society, London (1704), Accessible on internet archive.

wave description culminated with the theory of electromagnetic radiation of James Clerk Maxwell (1831–1879) who considered light as a very specific subset of all possible electromagnetic waves providing a coherent classical theory that is still instrumental for the description of electromagnetic radiation of frequencies less than 1THz or for some specific phenomena concerning light in frequencies even in the region of visible light.

1900 and onwards: Light is quantum relativistic particles. Monochromatic light beams in vacuum are streams of a very large number of elementary particles of zero mass, the **photons** [4] travelling at the ... speed of light c **in all inertial frames**. Every individual photon interacts with matter charged particles and the result of such interactions is described probabilistically. Photon-photon interaction is a second order effect and can be safely omitted in all the phenomena discussed in this course.

A.2 Classical description

A.2.1 Maxwell equations

The mathematically rigorous solution of Maxwell equations is quite demanding and lies outside the scope of this short appendix. The main reason is that we must use Fourier transform but plane waves are not $L^1(\mathbb{R}^4)$ functions; therefore we have two alternatives: either seek generalised (distributional) solutions as is done in [39, pp. 432–436], or pass through a decomposition into spherical harmonics as is done in [94, chap. 2]. In this section, we follow the more intuitive approach of [43] (that can be made perfectly rigorous in the distributional sense) and use the term "light" in a very broad sense, meaning electromagnetic radiation of every frequency.

Electromagnetic phenomena are described by a system of partial differential equations, known these days as **Maxwell equations** [5]. These equations are the local (differential) counterpart of global (integral) relationships between flux and circulations [6], connecting time and space derivatives of electric (**E**) and magnetic fields (**B**) with charge (ρ)

4. A name coined in 1926 by the chemist Gilbert Newton Lewis (1875–1946).

5. The differential form of the equations, in spite of their name, is due to Oliver Heaviside (1850–1925).

6. Let V be a bounded domain in $\mathbb{R}^3$ with smooth boundary ∂V and S a bounded smooth surface embedded in $\mathbb{R}^3$ with boundary ∂S. The integral form of Maxwell equations is

$$\oiint_{\partial V} \mathbf{E}\cdot \mathrm{d}\boldsymbol{s} = \frac{1}{\varepsilon_0}\iiint_V \rho\,\mathrm{d}v \quad ; \quad \oint_{\partial S} \mathbf{E}\cdot \mathrm{d}\boldsymbol{l} = -\frac{\mathrm{d}}{\mathrm{d}t}\iint_S \mathbf{B}\cdot \mathrm{d}\boldsymbol{s}$$
$$\oiint_{\partial V} \mathbf{B}\cdot \mathrm{d}\boldsymbol{s} = 0 \quad ; \quad \oint_{\partial S} \mathbf{B}\cdot \mathrm{d}\boldsymbol{l} = \mu_0\left(\iint_S \mathbf{j}\cdot \mathrm{d}\boldsymbol{s} + \varepsilon_0\frac{\mathrm{d}}{\mathrm{d}t}\iint_S \mathbf{E}\cdot \mathrm{d}\boldsymbol{s}\right),$$

where $\mathrm{d}v$, $\mathrm{d}\boldsymbol{s}$, and $\mathrm{d}\boldsymbol{l}$ are the volume, surface and length differential elements.

and current ($\mathbf{j}$) densities. The parameters ε_0 and μ_0 are physical constants[7].

$$\nabla \cdot \mathbf{E} = \frac{\rho}{\varepsilon_0} \text{ (Gauss law for electricity)} \quad ; \quad \nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t} \text{ (Faraday's induction law)}$$
$$\nabla \cdot \mathbf{B} = 0 \text{ (Gauss law for magnetism)} \quad ; \quad \nabla \times \mathbf{B} = \mu_0(\mathbf{j} + \varepsilon_0 \frac{\partial \mathbf{E}}{\partial t}) \text{ (Ampère's law)}$$

Deriving with respect to time the Gauss law for electricity, we get the equation of local conservation of electric charge:

$$\frac{\partial \rho}{\partial t} + \nabla \cdot \mathbf{j} = 0.$$

The equations governing the evolution of electric and magnetic fields are coupled with the evolution equations for charged particles in these fields. If Γ is a family of charged particles of masses $m_\gamma, \gamma \in \Gamma$, the matter-field coupling is expressed by the equation

$$m_\gamma \frac{\mathrm{d}^2 \mathbf{v}_\gamma(t)}{\mathrm{d}t^2} = q_\gamma[\mathbf{E}(t, \mathbf{r}_\gamma(t)) + \mathbf{v}_\gamma(t) \times \mathbf{B}(t, \mathbf{r}_\gamma(t))),$$

where m_γ, q_γ are the mass and electric charge of particle γ and $\mathbf{r}_\gamma, \mathbf{v}_\gamma$ its instantaneous position and velocity. It is elementary to check tha the global evolution leaves certain quantities invariant. Namely

$$H = \frac{1}{2} \sum_{\gamma \in \Gamma} m_\gamma \|\mathbf{v}_\gamma\|^2 + \frac{\varepsilon_0}{2} \int_{\mathbb{R}^3} \left(\|\mathbf{E}\|^2 + c^2 \|\mathbf{B}\|^2 \right) \mathrm{d}\mathbf{r} \quad \text{(total energy)}$$
$$\mathbf{P} = \sum_{\gamma \in \Gamma} \mathbf{r}_\gamma \times (m_\gamma \mathbf{v}_\gamma) + \varepsilon_0 \int_{\mathbb{R}^3} (\mathbf{E} \times \mathbf{B}) \, \mathrm{d}\mathbf{r} \quad \text{(total momentum)}$$
$$\mathbf{J} = \sum_{\gamma \in \Gamma} \mathbf{r} \times (m_\gamma \mathbf{v}_\gamma) + \varepsilon_0 \int_{\mathbb{R}^3} \mathbf{r} \times (\mathbf{E} \times \mathbf{B}) \, \mathrm{d}\mathbf{r} \quad \text{(total angular momentum)}$$

are constants of motion.

Since $\nabla \cdot \mathbf{B} = 0$ and $\nabla \times \mathbf{E} = -\frac{\partial}{\partial t}\mathbf{B}$, it follows that there exists a vector field (vector potential) $\mathbf{A}$ and a scalar field (scalar potential) U such that, locally, we can write

$$\mathbf{B} = \nabla \times \mathbf{A}$$
$$\mathbf{E} = -\frac{\partial}{\partial t}\mathbf{A} - \nabla U.$$

Substituting into the Maxwell equations, they become the coupled equations for the vector and scalar potentials:

$$\Delta U = -\frac{\rho}{\varepsilon_0} - \nabla \cdot \frac{\partial}{\partial t}\mathbf{A}$$
$$\left(\frac{1}{c^2}\frac{\partial^2}{\partial t^2} - \Delta \right) \mathbf{A} = \mu_0 \mathbf{j} - \nabla \left(\nabla \cdot \mathbf{A} + \frac{1}{c^2}\frac{\partial}{\partial t} U \right),$$

7. Known respectively as **electric permittivity** $\varepsilon_0 = 8.8541878128(13) \times 10^{-12}\ \mathrm{F \cdot m^{-1}}$ and **magnetic permeability** $\mu_0 = 1.2566370614 \times 10^{-6}\ \mathrm{N/A^2}$.

where $c^2 = \frac{1}{\varepsilon_0\mu_0}$ is the speed of light. Obviously, the potentials U and $\mathbf{A}$ are not uniquely determined, since these equations remain unaltered if the gradient of a smooth function f is added to $\mathbf{A}$ or its time derivative subtracted from the scalar potential U, i.e. the so called **gauge transformation**

$$\mathbf{A} \to \mathbf{A}' = \mathbf{A} + \nabla f$$
$$U \to U - \frac{1}{c}\frac{\partial f}{\partial t}$$

leave the equations invariant. This indeterminacy can be removed by imposing an additional constraint on the potentials, either of the form of

the Lorentz gauge: $\nabla \cdot \mathbf{A} + \frac{1}{c^2}\frac{\partial U}{\partial t} = 0$, or

the Coulomb gauge: $\nabla \cdot \mathbf{A} = 0$.

The Lorentz gauge has the advantage of being relativistically covariant. As a matter of fact, introducing the quadrivectors $\mathsf{A} = (A^0, \mathbf{A}) := (U/c, \mathbf{A})$ and $\mathsf{j} = (j^0, \mathbf{j}) := (c\rho, \mathbf{j})$, the Lorentz gauge takes the form[8]: $\partial_\alpha A^\alpha = 0$, where $\partial_\alpha = \frac{1}{c}\frac{\partial}{\partial t}$ if $\alpha = 0$ and $\partial_\alpha = \frac{\partial}{\partial x^\alpha}$ when $\alpha = 1, 2, 3$.The Maxwell equations take the particularly simple relativistically covariant expression

$$\Box A^\beta = \frac{1}{\varepsilon_0 c^2} j^\beta, \quad \beta = 0, \ldots, 3,$$

where $\Box$ denotes the differential operator $\Box = \partial_\alpha \partial^\alpha = \frac{1}{c^2}\frac{\partial^2}{\partial t} - \Delta$, known as d'Alembertian. In the vacuum this equation can be further simplified into

$$\Box \mathsf{A} = 0.$$

The Coulomb gauge breaks the relativistic covariance since the Maxwell equations become:

$$\Delta U = -\frac{\rho}{\varepsilon_0}$$
$$\Box \mathbf{A} = \frac{1}{\varepsilon_0 c^2}\mathbf{j} - \frac{1}{c^2}\nabla\frac{\partial U}{\partial t}.$$

However, the Coulomb gauge is more adapted in a semi-classical approach of the radiation field.

In the vacuum, there are no sources, i.e. the densities of charge, ρ, and of current, $\mathbf{j}$, vanish. Since the four differential equations form a linear differential homogeneous system, the space of solutions constitutes a vector space. Assume now that sufficiently smooth (C^2) solutions exist for the sourceless equations. Such solutions[9] must then satisfy

$$\begin{aligned}
\boldsymbol{\nabla} \times (\boldsymbol{\nabla} \times \mathbf{B}) &= \boldsymbol{\nabla}(\boldsymbol{\nabla} \cdot \mathbf{B}) - \Delta\mathbf{B} \\
&= -\Delta\mathbf{B} \ \ (\text{since } \boldsymbol{\nabla} \cdot \mathbf{B} = 0) \\
&= \mu_0\varepsilon_0\frac{\partial}{\partial t}\boldsymbol{\nabla} \times \mathbf{E} \\
&= -\mu_0\varepsilon_0\frac{\partial^2}{\partial t^2}\mathbf{B},
\end{aligned}$$

8. We use the Einstein's convention for summing repeated indices: $B^\alpha C_\alpha := \sum_{\alpha=0}^{3} B^\alpha C_\alpha$.
9. Recall that $\boldsymbol{\nabla} \times (\boldsymbol{\nabla} \times \mathbf{V}) = \boldsymbol{\nabla}(\boldsymbol{\nabla} \cdot \mathbf{V}) - \Delta\mathbf{V}$.

hence a solution of the sourceless Maxwell equations for the magnetic field $\mathbf{B}$ fulfils the wave equation

$$\frac{1}{c^2}\frac{\partial^2 \mathbf{B}}{\partial t^2} - \Delta \mathbf{B} = 0 \text{ (wave equation for magnetic field).}$$

With similar arguments, and using again the Maxwell equations, we get that a solution for the electric field fulfils an analogous wave equation

$$\frac{1}{c^2}\frac{\partial^2 \mathbf{E}}{\partial t^2} - \Delta \mathbf{E} = 0 \text{ (wave equation for electric field).}$$

In other words, if smooth solutions exist, they must satisfy the two aforementioned wave equations.

We work henceforth within the Coulomb gauge and seek solutions in the vacuum (i.e. $\rho = 0$ and $\mathbf{j} = 0$). Seek tentatively a solution of the wave equation for the electric field in the form

$$\mathbf{E}(t, \mathbf{r}) = \mathbf{E}_0 \exp(i(\omega t - \boldsymbol{k} \cdot \mathbf{r} - \phi)),$$

where $\mathbf{E}_0$ stands for the amplitude of the solution, ω has dimensions of **frequency** and $k := \|\boldsymbol{k}\|$ of inverse length while ϕ is an arbitrary phase. As a matter of fact, only the real part of the field $\mathrm{Re}(\mathbf{E}(t, \mathbf{r}))$ has a physical significance but it is more convenient to take the real part only at the end of the computations.

Fixing the total phase $\omega t - \boldsymbol{k} \cdot \mathbf{r} - \phi$ at a constant value, the phase front of the wave travels in direction $\boldsymbol{k}$ at the speed $v_{\text{phase}} = \omega/k$. The **wavelength**, λ, is defined as the length $\|\mathbf{r}' - \mathbf{r}''\|$ between the positions $\mathbf{r}'$ and $\mathbf{r}''$ of two successive maxima of the modulus of the field; it reads $\lambda = \frac{2\pi}{k}$.

For the above expression to satisfy the wave equation, ω and k must be related through the linear **dispersion relation** $\omega = ck$ as determined by substituting the tentative solution into the wave equation for $\mathbf{E}$. We obtain thus that the speed of the phase front reads $v_{\text{phase}} = \frac{1}{\sqrt{\varepsilon_0 \mu_0}} = c$, where c is the speed of light in vacuum: $c = 299792458$ m/s. Substituting the elementary solution into the Maxwell equation $\boldsymbol{\nabla} \cdot \mathbf{E} = 0$, we get further $\boldsymbol{k} \cdot \mathbf{E} = 0$, meaning that the vectors $\boldsymbol{k}$ and $\mathbf{E}$ are orthogonal.

We can repeat the same arguments with a tentative solution

$$\mathbf{B}(t, \mathbf{r}) = \mathbf{B}_0 \exp(i(\omega' t - \boldsymbol{k}' \cdot \mathbf{r} - \phi'))$$

for the magnetic field. We obtain again the dispersion relation $\omega' = ck'$ (thus the phase front of the magnetic field travels also at the speed of light). Substituting into the Maxwell equation $\boldsymbol{\nabla} \cdot \mathbf{B} = 0$ we get again orthogonality of $\boldsymbol{k}'$ and $\mathbf{B}$.

Still, tentative solutions for $\mathbf{E}$ and $\mathbf{B}$ of the wave equations are not necessarily solutions of the Maxwell equations. Inserting these tentative solutions into the sourceless Maxwell equation $\nabla \times \mathbf{B} = \mu_0 \varepsilon_0 \frac{\partial \mathbf{E}}{\partial t}$, we get that the condition

$$-\boldsymbol{k}' \times \mathbf{B}_0 \exp(i(\omega' t - \boldsymbol{k}' \cdot \mathbf{r} - \phi')) = \frac{\omega}{c^2} \mathbf{E}_0 \exp(i(\omega t - \boldsymbol{k} \cdot \mathbf{r} - \phi)),$$

must hold for every $\mathbf{r}', \mathbf{r}, t', t$, Due to the orthogonality of complex exponentials, it follows that $\omega' = \omega$, $\boldsymbol{k}' = \boldsymbol{k}$, and

$$\mathbf{B}_0 \exp(-i\phi') \times \boldsymbol{k} = \frac{\omega}{c}\mathbf{E}_0 \exp(-i\phi).$$

We conclude that elementary solutions of the Maxwell equations must have the same frequency ω and wavevector $\boldsymbol{k}$ for both electric and magnetic components.

A general solution of the sourceless Maxwell equations is given by a linear combination of elementary solutions determined above. Electromagnetic radiation arises at very different frequencies. (Human) eye is differentially sensitive to frequency ω (or wavelength λ since, due to the dispersion relation, fequency and wavelenght are connected trhough: $\omega/c = 2\pi\lambda$). Electromagnetic waves carrying a single wavelength λ in the range ca. $[400, 700]$ nm, are physiologically perceived as light of a single colour (ranging from violet to red). Mind however that electromagnetic spectrum has a much broader range from 0.01 nm to some kilometres but only the spectrum within $[400, 700]$ nm is perceived as visible light. The figure A.1 gives information about frequencies and wavelengths of different types of radiation and locates the region of the visible spectrum in the whole frequency range of electromagnetic radiation. Nevertheless, we use the adjective **monochromatic** to signify an electromagnetic wave carrying a single frequency (wavelentgth), even if it lies outside the visible range.

A.2.2 Polarisation

Substituting a monochromatic solution into the equations in vacuum, we get further

$$\begin{aligned} \boldsymbol{k} \cdot \mathbf{E} = 0 \quad ; \quad \boldsymbol{k} \times \mathbf{E} &= \omega\mu_0\mathbf{B} \\ \boldsymbol{k} \cdot \mathbf{B} = 0 \quad ; \quad \boldsymbol{k} \times \mathbf{B} &= -\omega\varepsilon_0\mathbf{E}. \end{aligned}$$

The first column of these equations means that, for all $t, \mathbf{r}$, both vectors $\mathbf{E}(t, \mathbf{r})$ and $\mathbf{B}(t, \mathbf{r})$ are orthogonal to the vector $\boldsymbol{k}$. From the second column we get

$$\mathbf{B} \cdot \mathbf{E} = -\frac{1}{\omega^2\mu_0\varepsilon_0}(\boldsymbol{k} \times \mathbf{E}) \cdot (\boldsymbol{k} \times \mathbf{B}),$$

from where [10] we conclude that $\mathbf{B} \cdot \mathbf{E} = 0$, i.e. the electric and magnetic field are mutually orthogonal so that the triple $(\mathbf{E}, \mathbf{B}, \boldsymbol{k})$ defines a positively oriented orthogonal system. Additionally, $\hat{\boldsymbol{k}} = \frac{\boldsymbol{k}}{k} = \frac{\mathbf{E}\times\mathbf{B}}{\|\mathbf{E}\|\|\mathbf{B}\|}$ is proportional to the vector of Poynting, $\frac{1}{\mu_0}\mathbf{E} \times \mathbf{B}$, pointing [11] in the direction of propagation.

Assume henceforth that $\hat{\boldsymbol{k}}$ is in the direction of the z axis. Orthogonality of $\mathbf{E}$ and $\mathbf{B}$ with $\hat{\boldsymbol{k}}$ means that the field vectors are evolving in the xy plane. Concentrate on the electric field vector. Since it evolves in the xy plane, it is enough to consider its two

10. Recall that $(\mathbf{a} \times \mathbf{b}) \cdot \mathbf{c} = \mathbf{a} \cdot (\mathbf{b} \times \mathbf{c})$.
11. This vector has been introduced by the British physicist with the ... predestined name John Henry Poynting (1852–1914).

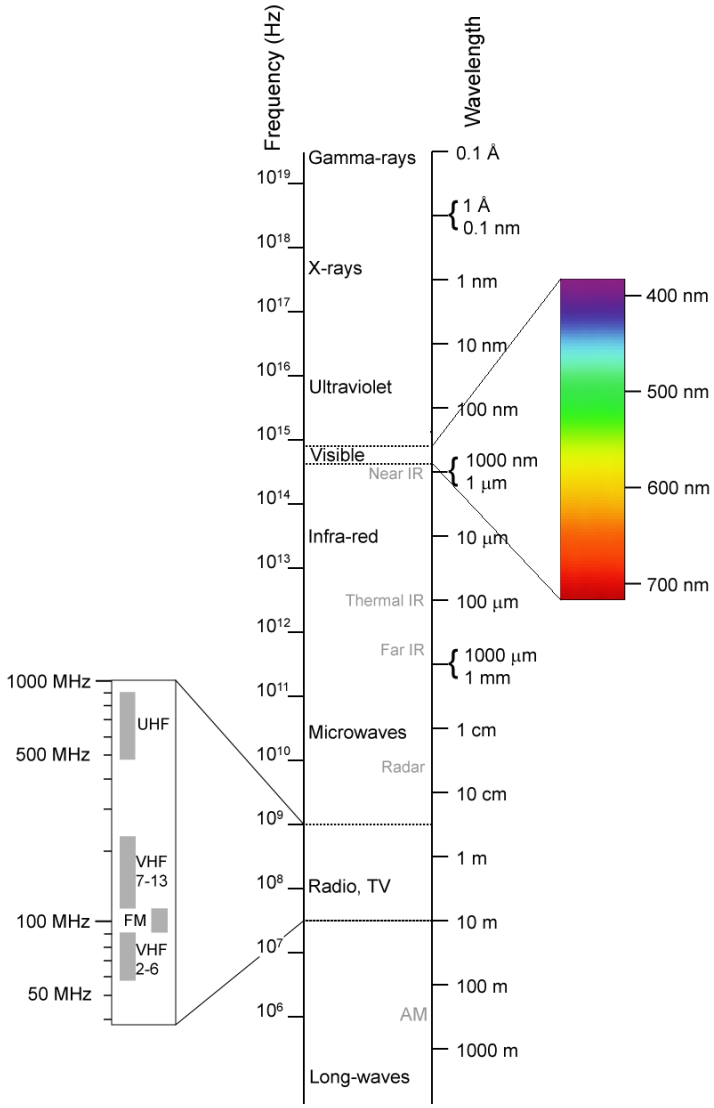


Figure A.1 – Spectrum of visible light occupies only a tiny portion of the frequency range of electromagnetic radiation. (Source: Wikipedia).

dimensional restriction and write, with a slight abuse of notation, the more general form [12] of the electric field as

$$\mathbf{E}(t,z) = \begin{pmatrix} E_x \exp(i\phi_x) \\ E_y \exp(i\phi_y) \end{pmatrix} \exp(i(\omega t - kz)),$$

where $E_x = \langle\, \mathbf{e}_x \,|\, \mathbf{E}_0 \,\rangle = E_0 \cos(\theta)$ and $E_y = \langle\, \mathbf{e}_y \,|\, \mathbf{E}_0 \,\rangle = E_0 \sin(\theta)$, with $E_0 = \|\mathbf{E}\| = \sqrt{E_x^2 + E_y^2}$ and $\theta \in [0, 2\pi]$, are the components of the amplitude $\mathbf{E}_0$ relative to the $\mathbf{e}_x$ and $\mathbf{e}_y$ directions while ϕ_x and ϕ_y are arbitrary phases. The magnetic field, as always orthogonal to $\mathbf{E}$ and to $\hat{\boldsymbol{k}}$, reads $\mathbf{B}(t,z) = \frac{1}{c}\mathbf{e}_z \times \mathbf{E}(z,t)$.

12. As a matter of fact, the electric field is given by the three dimensional vector

$$\mathbf{E}(t,z) = \begin{pmatrix} E_x \exp(i\phi_x) \\ E_y \exp(i\phi_y) \\ 0 \end{pmatrix} \exp(i(\omega t - kz)),$$

whose expression we trivially restrict in the xy plane.

On the xy-plane passing through $z_0 = \phi_x/k$, and on introducing the relative phase $\phi = \phi_y - \phi_x$, and taking real part, we get

$$\boldsymbol{\xi}(t) = \begin{pmatrix} \xi_x(t) \\ \xi_y(t) \end{pmatrix} := \frac{\mathsf{Re}(\mathbf{E}(t, z_0))}{E_0} = \begin{pmatrix} \cos(\theta)\cos(\omega t) \\ \sin(\theta)\cos(\omega t + \phi) \end{pmatrix}.$$

The locus on the xy-plane passing through z_0 of the projection of $\mathbf{E}(t, z_0)$ is a periodic function of time described by the parametric curve $E_0\xi(t), t \in [0, 2\pi]$. Eliminating the time coordinate, we get the quadratic equation for the shape of the curve $\xi(t), t \in [0, 2\pi]$:

$$\frac{\xi_x^2}{\cos^2(\theta)} + \frac{\xi_y^2}{\sin^2(\theta)} - 2\frac{\xi_x\xi_y}{\cos(\theta)\sin(\theta)}\cos(\phi) = \sin^2(\phi),$$

that can be also expressed by the geometric condition $\langle\, \boldsymbol{\xi} \,|\, \mathbf{Q}\boldsymbol{\xi} \,\rangle = \sin^2(\phi)$, where $\mathbf{Q} := \mathbf{Q}(\theta, \phi)$ is the matrix

$$\mathbf{Q}(\theta, \phi) = \begin{pmatrix} \frac{1}{\cos^2(\theta)} & -\frac{1}{\cos(\theta)\sin(\theta)} \\ -\frac{1}{\cos(\theta)\sin(\theta)} & \frac{1}{\sin^2(\theta)} \end{pmatrix}.$$

The matrix $\mathbf{Q}$ is symmetric, hence it admits a spectral decomposition with real eigenvalues. We compute them explicitly: $v_\pm = \frac{2(1\pm\sqrt{D})}{\sin^2(2\theta)}$, where $D = 1 - \sin^2(\phi)\sin^2(2\theta)$. Denote $\mathbf{V}_\pm$ the corresponding eigenvectors. Hence

$$M = v_-|\,\mathbf{V}_-\,\rangle\langle\,\mathbf{V}_-\,| + v_+|\,\mathbf{V}_+\,\rangle\langle\,\mathbf{V}_+\,|;$$

consequently, the geometric condition becomes

$$\begin{aligned} \sin^2(\phi) &= \langle\, \boldsymbol{\xi} \,|\, \mathbf{Q}\boldsymbol{\xi} \,\rangle \\ &= v_-|\langle\, \mathbf{V}_- \,|\, \boldsymbol{\xi} \,\rangle|^2 + v_+|\langle\, \mathbf{V}_+ \,|\, \boldsymbol{\xi} \,\rangle|^2 \\ &= v_-|\xi_-|^2 + v_+|\xi_+|^2, \end{aligned}$$

where $\xi_\pm = \langle\, \mathbf{V}_\pm \,|\, \boldsymbol{\xi} \,\rangle$. Equivalently, the geometric condition reads $\frac{\xi_-^2}{a^2} + \frac{\xi_+^2}{b^2} = 1$, where $a^2 = \frac{1}{\sin^2(\phi)v_-}$ and $b^2 = \frac{1}{\sin^2(\phi)v_+}$ (note that the eigenvalues are necessarily non-negative because $D \leq 1$).

Elliptic polarisation

Since $0 \leq D \leq 1$, the eigenvalues are non-negative. and the normalised shape of the projection of the electric field corresponds generically to a (tilted with respect to the x and y axes) ellipse. The directions of the major and minor axes of the ellipse are determined by the eigenvectors of $\mathbf{Q}$; the length of the major semi-axis is $a := \frac{|\sin(2\theta)|}{|\sin(\phi)|\sqrt{2(1-\sqrt{D})}}$ and of the minor semi-axis $b := \frac{|\sin(2\theta)|}{|\sin(\phi)|\sqrt{2(1+\sqrt{D})}}$.

The figure A.3 gives some examples of profiles for various values of the parameters θ and ϕ.

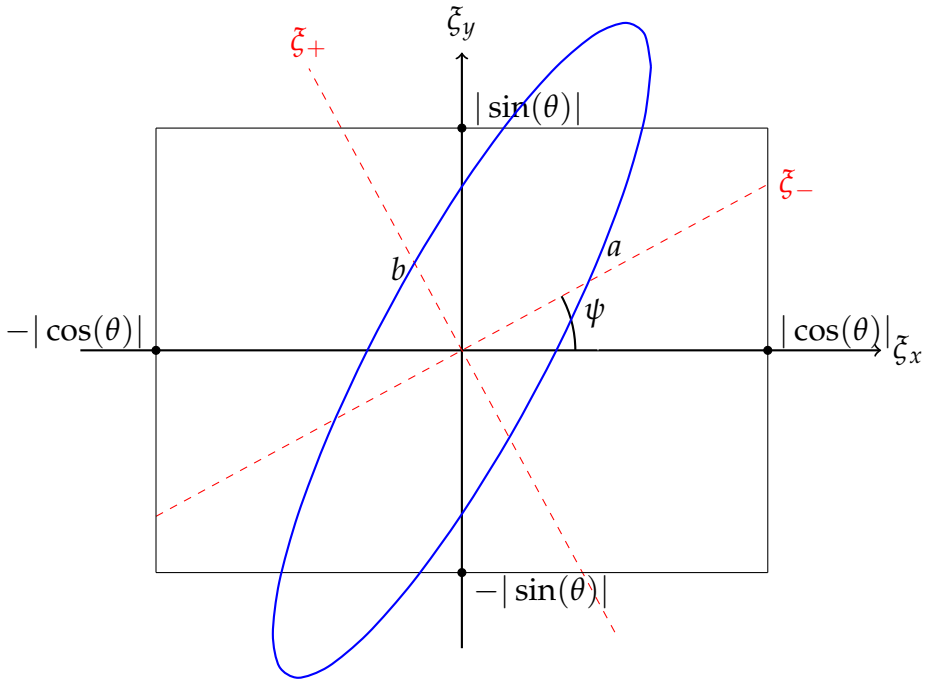


Figure A.2 – The locus of the projection of electric field on the xy-plane is the homothetic image of the above ellipse with dilation ratio $E_0 = \|\mathbf{E}_0\|$. This ellipse is tilted with respect to the canonical basis and is inscribed in the rectangle of sides $2|\cos(\theta)|$ and $2|\sin(\theta)|$. The major and minor semi-axes (of length a and b respectively) of the ellipse are determined by the eigenvectors $\mathbf{V}_-$ and $\mathbf{V}_+$. The angle ψ formed by the major semi-axis with the Ox direction is given by $\psi = \frac{1}{2}\arctan\big(\tan(2\theta)\cos(\phi)\big) - \frac{\pi}{2}$.

Linear polarisation

The ratio of the minor over the major axis of the polarisation ellipse reads $\frac{b}{a} = \frac{\sqrt{1-\sqrt{D}}}{\sqrt{1+\sqrt{D}}}$. It follows that this ratio vanishes when $\phi = k\pi$, with $k \in \mathbb{Z}$ since then $D = 1$ and the ellipse degenerates to a segment. The light is then called **linearly polarised** and the figure A.4 below gives some examples of such polarisation.

In that situation, the electric field oscillates remaining constantly in a plane defined by the direction of the linear polarisation (the magnetic field oscillates constantly in the perpendicular plane) and the propagation in space of the plane electromagnetic wave is depicted in the figure A.5.

Circular polarisation

When the lengths of the minor and major axes are equal, i.e. $a = b$, the locus of the projections of $\mathbf{E}$ on the xy-plane is circle (see figure A.6 below). This happens when the rectangle circumscribing the projection of the field on the xy-plane becomes a square — which occurs whenever $|\cos(\theta)| = |\sin(\theta)|$, i.e. $\theta = \frac{\pi}{4} + k\pi$, $k \in \mathbb{Z}$ — and when the two eigenvalues $v_\pm$ of $\mathbf{Q}$ become equal — which occurs when $D = 0$, i.e. $\sin^2(2\theta)\sin^2(\phi) = \sin^2(\phi) = 1$, or $\phi = \pi/2 + k\pi$, for $k \in \mathbb{Z}$.

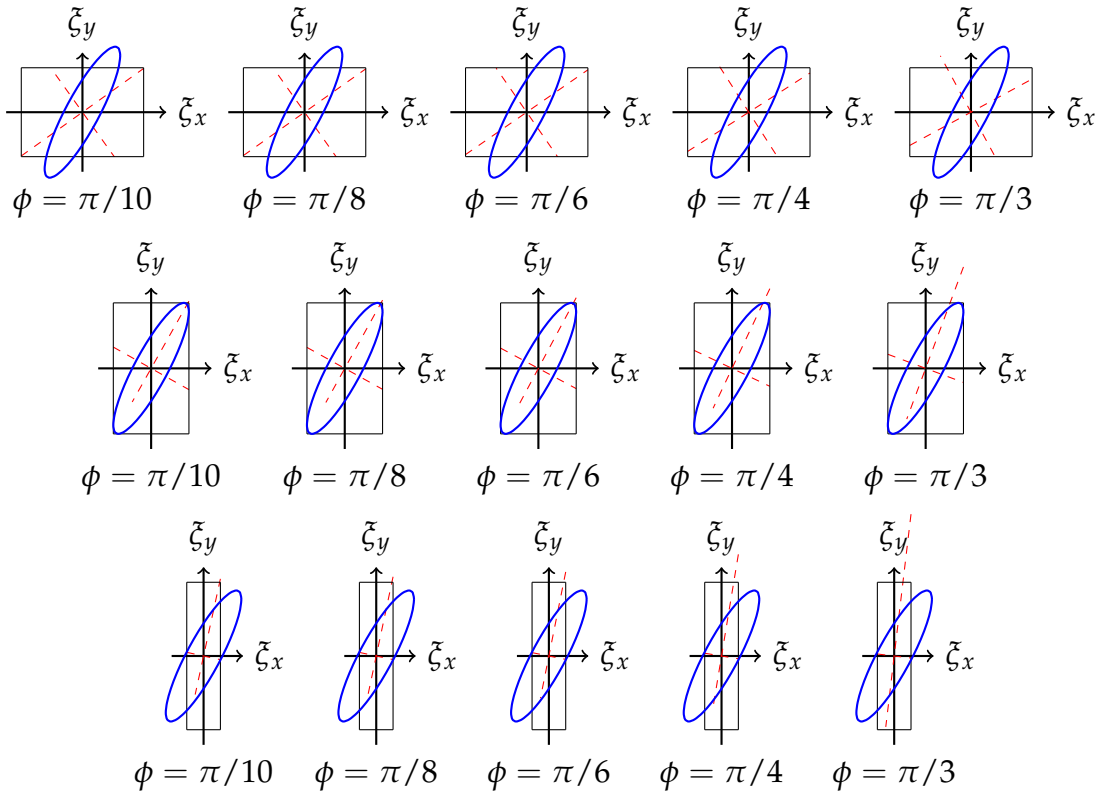


Figure A.3 – The shape of the projection for different values of θ and ϕ. First row corresponds to $\theta = \pi/5$, second row to $\pi/3$, and third row to $3\pi/7$.

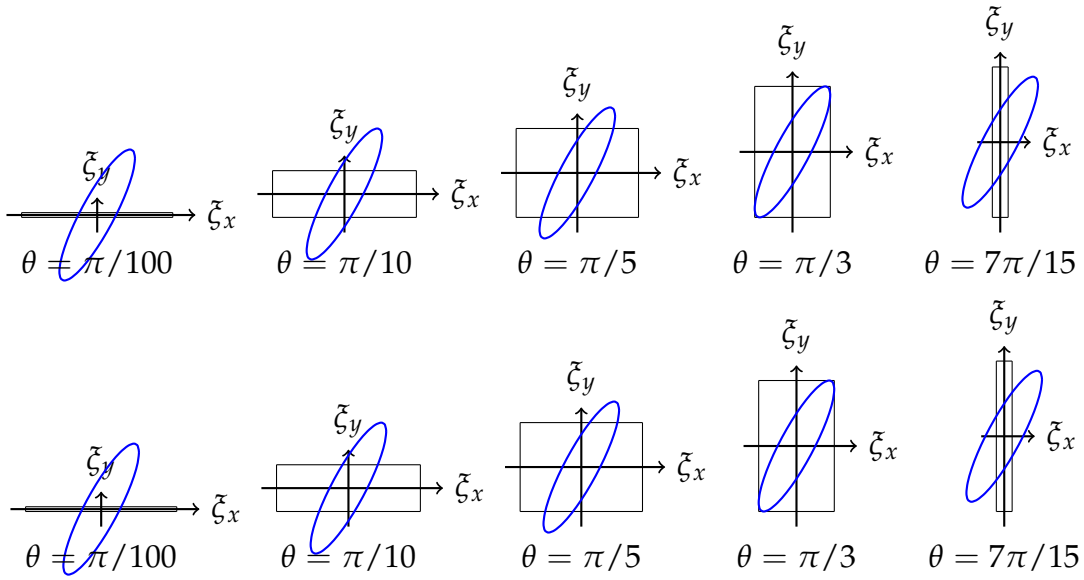


Figure A.4 – Examples of linear polarisations for different values of the parameters θ and ϕ. First row corresponds to $\phi = 0$ and second one to $\phi = \pi$.

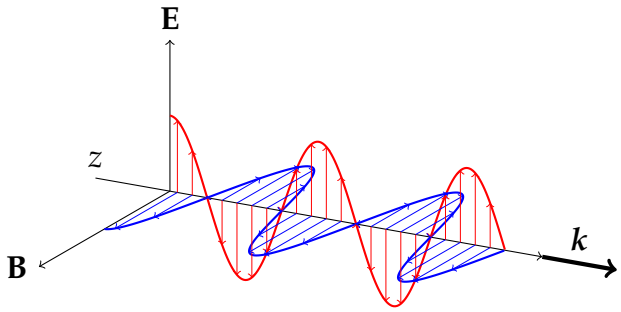


Figure A.5 – The planes of oscillation of electric (red, $\mathbf{E}$) and magnetic (blue, $\mathbf{B}$) fields are mutually perpendicular and intersect at the axis of propagation of the electromagnetic wave, determined by the Poynting's pointing vector $\boldsymbol{k} = \frac{\mathbf{E}\times\mathbf{B}}{\|\mathbf{E}\|\|\mathbf{B}\|}$. We call classical transversal polarisation the plane of oscillation of the electric field. For instance, the wave depicted above has vertical polarisation.

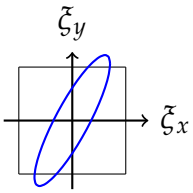


Figure A.6 – When $\theta = \frac{\pi}{4} + k\pi$ with $k \in \mathbb{Z}$, $\phi = \pi/2 + \ell\pi$, with $\ell \in \mathbb{Z}$ and the projection of the electric field on the xy-plane degenerates into a circle.

The three dimensional profile of the electric field in a circularly polarized light beam is depicted in figure A.7.

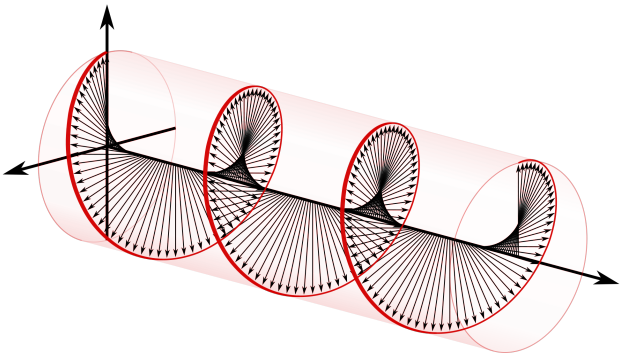


Figure A.7 – Snapshot of the three dimensional profile of circularly polarised plane wave. Only the electric field is depicted. (Source: Wikipedia).

A.2.3 Helicity and chirality

For elliptic (or circular) polarisation an additional degree of freedom in describing the polarisation profile is the sense of gyration on the projection ellipse. As a matter of fact, as we can observe on the figure A.7, the end-point of the electric field vector sweeps

an helix progressing in space towards the $\boldsymbol{k}$ direction of propagation. For an observer on the z axis and looking against the propagation (i.e. towards the source), assuming that the vertical direction is x and the horizontal y, the helix of this example is left-handed. In other words the circle of polarisation is swept counter-clockwise. The sense of sweeping determines the **chirality** of the polarisation (counterclockwise/left-handed versus clockwise/right-handed). The **helicity** of the polarisation is the sign of advancement of a screw in the direction $\boldsymbol{k}$ when the screw is turned positively (counterclockwise). For a left-handed helix, the sign is $+1$, for a right-handed helix it is -1. The helicity is governed by the parameters θ and ϕ as shown in figure A.8.

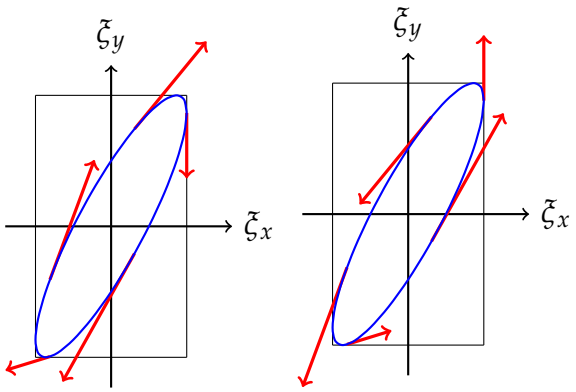


Figure A.8 – The ellipse is swept clockwise or counterclockwise, depending on the parameters θ and ϕ. In this example, $\theta = \pi/3$ while $\phi = \pi/6$ on the left side and $\phi = -\pi/6$ on the right side.

A.2.4 Hilbert space description of classical polarisation

We have seen on page 276 that the polarisation is *in fine* determined by the vector $\begin{pmatrix} E_x \exp(i\phi_x) \\ E_y \exp(i\phi_y) \end{pmatrix} = E_0 \xi$, where $\mathbf{E}_0 = E_x \mathbf{e}_x + E_y \mathbf{e}_y$, $E_0 = \|\mathbf{E}_0\|$, and ξ is the so called **Jones vector**:

$$\xi := \begin{pmatrix} \cos(\theta) \\ \sin(\theta) \exp(i\phi) \end{pmatrix} \exp(i\phi_x).$$

Obviously ξ is a unit vector (ray) in a Hilbert space $\mathbb{H} \simeq \mathbb{C}^2$ (we can even forget the global phase $\exp(i\phi_x)$). Sourceless solutions of the Maxwell equations constitute a vector space. Hence, linear combinations of solutions have a counterpart on linear combinations of Jones vectors. Moreover, we can choose a basis in $\mathbb{H}$. For instance, the canonical basis $(\varepsilon_x, \varepsilon_y)$. The Jones vector corresponding to a linear polarisation can be expressed as $|\, \xi^{(l)} \,\rangle = \cos(\theta) |\, \varepsilon_x \,\rangle \pm \sin(\theta)) |\, \varepsilon_y \,\rangle$. Similarly, the Jones vector corresponding to a circular polarisation can be expressed as $|\, \xi^{(c)} \,\rangle = \frac{1}{\sqrt{2}} \left(|\, \varepsilon_x \,\rangle \pm i |\, \varepsilon_y \,\rangle \right)$. But the canonical basis has nothing special; every other orthonormal basis of $\mathbb{H}$ allows for an equivalent description. For instance the **chiral basis** $(|\, L \,\rangle, |\, R \,\rangle)$, with

$$|\, L \,\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \quad \text{and} \quad |\, R \,\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix},$$

is equally adapted for expressing any Jones vector. It is also worth noting that as a unit vector (ray) of the Hilbert space $\mathbb{H}$, it can be interpreted *quantum mechanically* as

corresponding to a pure polarisation state. It is outside the scope of this text to show that this formal analogy is in fact more profound so that ξ can in fact be interpreted as a quantum mechanical state vector *abusively* called polarisation vector. Recall now (see exercise 3.12.21) that Pauli matrices $(\sigma_\alpha)_{\alpha=0,\dots,3}$, defined on page 105, constitute a basis of the set of self-adjoint operators on $\mathbb{H}$. In particular, for every θ and ϕ, the projector $|\,\xi\,\rangle\langle\,\xi\,|$ on the one dimensional subspace of $\mathbb{H}$ spanned by ξ can be decomposed on the basis of Pauli matrices:

$$|\,\xi\,\rangle\langle\,\xi\,| = \begin{pmatrix} \cos^2(\theta) & \cos(\theta)\sin(\theta)\exp(-i\phi) \\ \cos(\theta)\sin(\theta)\exp(i\phi) & \sin^2(\theta) \end{pmatrix}$$
$$= \frac{1}{2}\sum_{\alpha=0}^{3} s_\alpha\sigma_\alpha = \begin{pmatrix} 1+s_3 & s_1-is_2 \\ 1-s_3 & s_1+is_2 \end{pmatrix},$$

where the components of the quadrivector $\mathsf{s} = (s_0, \mathbf{s})$ are

$$s_0 = 1,\ s_1 = \sin(2\theta)\cos(\phi),\ s_2 = \sin(2\theta)\sin(\phi),\ s_3 = \cos(2\theta).$$

The quadrivector s is called the **Stokes vector** corresponding to the polarisation of light. Contrary to the Jones vector ξ, the components of s are directly accessible to intensity measurements on the light source.

Active optical devices act on light and modify its polarisation state ξ into a new state ξ'. The transformation is implemented by the **Jones matrix M** i.e. $\xi' = \mathbf{M}\xi$. The most common such devices include linear polarisers, circular polarisers, phase shifters and mirrors, beam splitters.

The table A.1 summarises the Jones matrices (projectors) corresponding to the action of such devices, represented in the canonical basis.

Now the passage from the canonical basis to the chiral one is implemented by a a unitary transformation. It turns out that this unitary transformation can be physically implemented by an optical device called **half wavelength plate** or $\lambda/2$-plate. Inserting such a $\lambda/2$ plate (with an appropriate orientation) in a monochromatic linearly polarised beam, results in transforming the beam to a circularly polarised one.

Other useful optical devices are the beam splitters, i.e. devices with two input and two output channels (see figure A.9).

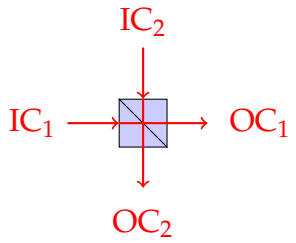


Figure A.9 – The input and output channels for a beam splitter.

They are available into two different species: polarising and non-polarising ones. Classically a lossless polarising beam splitter sacts as a mirror on the horizontal polarisation

Device	Jones matrix $\mathbf{M}$
Horizontal linear polariser	$\left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right]$
Linear polariser at $\pm\pi/4$	$\frac{1}{2}\left[\begin{smallmatrix} 1 & \pm 1 \\ \pm 1 & 1 \end{smallmatrix}\right]$
Vertical linear polariser	$\left[\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right]$
Left circular polariser	$\frac{1}{2}\left[\begin{smallmatrix} 1 & -i \\ i & 1 \end{smallmatrix}\right]$
Right circular polariser	$\frac{1}{2}\left[\begin{smallmatrix} 1 & i \\ -i & 1 \end{smallmatrix}\right]$
$\lambda/2$ plate vertically retarding	$\left[\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right]$
$\lambda/4$ plate vertically retarding	$e^{-i\pi/4}\left[\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right]$
Mirror (normal incidence)	$\left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$

Table A.1 – Jones matrices representing the most common optical devices. Note that the first group of four devices correspond to projective transformations while the second group of three devices to unitary transformations that are unitary. Hence they can be viewed as basis transformations.

of the input and as a free transmitter for the vertical polarisation. Since the device has two input and two output channels, the input polarisation is determined by the tensor product of the corresponding Jones vectors $\xi^{(1)}$ or $\xi^{(2)}$ with the choice of the channel (and similarly for the output). Hence the Jones vector for the input channel is given by $\xi^{\text{in}} = \begin{bmatrix} \xi_h^{(1)} \\ \xi_v^{(1)} \\ \xi_h^{(2)} \\ \xi_v^{(2)} \end{bmatrix}$ and analogously for the output. The Jones matrix $\mathbf{M}_{\text{PBS}}$ of the lossless polarising beam splitter is therefore defined by

$$\mathbf{M}_{\text{PBS}} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

For example, if a linearly polarised beam at angle $\pi/4$ enters the separator through the input channel 1, the action of the PBS is summarised below:

$$\xi^{\text{out}} = \mathbf{M}\xi^{\text{in}} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1/\sqrt{2} \\ -1/\sqrt{2} \\ 0 \end{pmatrix}.$$

Classically, electromagnetic radiation is produced by the electric dipole oscillations

inside antennas or atoms. The polarisation of light is hence determined by the axis of the emitting antenna or of the electric atomic dipole. While the orientation of an antenna is usually kept fixed, atoms are in all possible orientations in matter. Hence the light produced by the Sun (or by incandescent bulbs) for instance arises in all possible polarisations; the corresponding electromagnetic wave comes as a superposition of all possible waves of different polarisations (unpolarised light).

A.3 Simplified quantum descriprtion

Since $\mathbf{B} = \nabla \times \mathbf{A}$ and (in the Coulomb gauge) $\mathbf{E} = -\frac{\partial \mathbf{A}}{\partial t}$, the wave equations for electric and magnetic fields can be replaced by a single wave equation for the vectot potential

$$\frac{1}{c^2}\frac{\partial^2 \mathbf{A}}{\partial t^2} - \Delta \mathbf{A} = 0.$$

Assume that the wace is Seeking for an elementary solution of this equation in the form of a plane wave $\mathbf{A}(t, \mathbf{r}) = \mathbf{A}_0 \exp(i(\omega t - \boldsymbol{k} \cdot \mathbf{r} - \phi)$, where $\mathbf{A}_0$ stands for the amplitude of the solution, ω has dimensions of a **frequency**, $k := \|\boldsymbol{k}\|$ of an inverse length while ϕ is an arbitrary phase.

Consider the wave confined within a cubic volume of size L and impose (for simplicity) a periodic boundary condition. Periodisation of the space induces a discretisation of the allowed wavevectors $\boldsymbol{k} = (k_x, k_y, k_z) = \frac{2\pi}{L}(n_x, n_y, n_z)$, with $(n_x, n_y, n_z) \in \mathbb{Z}$. Denote by $\hat{\cdot}$ the spatial Fourier transform of the fields appearing in the Maxwell equations. For instance $\hat{\mathbf{E}}(\boldsymbol{k}, t) = \int_{\mathbb{R}^3} \mathbf{E}(\mathbf{r}, t) \exp(-i\boldsymbol{k} \cdot \mathbf{r}) \mathrm{d}^3 r$. The Coulomb gauge ($\nabla \cdot \mathbf{A} = 0$) implies the transversality condition $\boldsymbol{k} \cdot \mathbf{A}_0$ to hold (as is the case for $\mathbf{B}$ and $\mathbf{E}$). Assume (for simplicity) that the electromagnetic wave is linearly polarised, i.e. there exists a transverse polarisation vector $\boldsymbol{\xi}$ in the xy plane such that an elementary solution to the wave equation for $\mathbf{A}$ reads

$$\mathbf{A}(t, \mathbf{r}) = A_0 \boldsymbol{\xi} \exp(-i(\omega t - \boldsymbol{k} \cdot \mathbf{r})),$$

and (hence)

$$\begin{aligned} \mathbf{E}(t, \mathbf{r}) &= -iA_0 \omega \boldsymbol{\xi} \exp(-i(\omega t - \boldsymbol{k} \cdot \mathbf{r})) \\ \mathbf{B}(t, \mathbf{r}) &= iA_0 [\boldsymbol{k} \times \boldsymbol{\xi}] \exp(-i(\omega t - \boldsymbol{k} \cdot \mathbf{r})). \end{aligned}$$

The general solution will be expressed as a linear superposition of elementary solutions in the form

$$\mathbf{A}(t, \mathbf{r}) = L^{-3/2} \sum_{\boldsymbol{k} \in \frac{2\pi}{L}\mathbb{Z}^3} \sum_{\ell=1,2} \xi_{\boldsymbol{k},\ell} \left(q_{\boldsymbol{k},\ell}(t) \exp(-i\boldsymbol{k} \cdot \mathbf{r}) + \overline{q}_{\boldsymbol{k},\ell}(t) \exp(i\boldsymbol{k} \cdot \mathbf{r}) \right),$$

where $\xi := \xi_{\boldsymbol{k}} = \xi_{\boldsymbol{k},1}\varepsilon_1 + \xi_{\boldsymbol{k},2}\varepsilon_2$, $q_{\boldsymbol{k},\ell}(t) := A_{0,\boldsymbol{k}} \exp(i\omega_{\boldsymbol{k}} t)$, and $\omega_{\boldsymbol{k}} = c\|\boldsymbol{k}\|$. Now, since we consider the situation in vacuum, i.e. without particles having kinetic energy,

the total energy reduces merely to its electromagnetic component. Introducing the multi-index $\alpha = (\boldsymbol{k}, \ell)$, the total energy (constant of motion) reads:

$$\begin{aligned} H &= +\frac{\varepsilon_0}{2}\int_{\mathbb{R}^3}\left(\|\mathbf{E}\|^2 + c^2\|\mathbf{B}\|^2\right)\mathrm{d}\mathbf{r} \\ &= \varepsilon_0 \sum_\alpha \omega_\alpha^2 \left(\overline{q}_\alpha q_\alpha + q_\alpha \overline{q}_\alpha\right). \end{aligned}$$

Introducing the real variables $Q_\alpha(t) = q_\alpha(t) + \overline{q}_\alpha(t)$ and $\dot{(Q)}_\alpha(t) = -i\omega_\alpha(q_\alpha(t) - \overline{q}_\alpha(t))$, the energy takes the form of a classical harmonic oscillator Hamiltonian:

$$H = \frac{\varepsilon_0}{2}\sum_\alpha (\dot{Q}_\alpha^2 + \omega_\alpha^2 Q_\alpha^2).$$

Introducing the canonical coordinate $P_\alpha = \varepsilon_0 Q_\alpha$ that is conjugate to Q_α, we can formally quantise the field by replacing $P_\alpha \to -i\hbar\frac{\partial}{\partial Q_\alpha}$ to arrive to the quantised form of the Hamiltonian

$$H = \sum_\alpha \left(-\frac{\hbar^2}{2\varepsilon_0}\frac{\partial^2}{\partial Q_\alpha^2} + \frac{\varepsilon_0}{2}\omega_\alpha^2 Q_\alpha^2\right).$$

Repeat now the construction done in the study of simple harmonic oscillator for every mode α of the radiation field and introduce the creation and annihilation operators

$$\begin{aligned} a_\alpha &= \sqrt{\frac{\varepsilon_0\omega_\alpha}{2\hbar}}\left(Q_\alpha + \frac{i}{\varepsilon_0\omega_\alpha}P_\alpha\right) \\ a_\alpha^* &= \sqrt{\frac{\varepsilon_0\omega_\alpha}{2\hbar}}\left(Q_\alpha i - \frac{i}{\varepsilon_0\omega_\alpha}P_\alpha\right). \end{aligned}$$

The Hamiltonian now becomes

$$H = \sum_\alpha \hbar\omega_\alpha\left(a_\alpha^* a_\alpha + \frac{1}{2}\right),$$

i.e. it is a decoupled sum of quantum harmonic oscillators over all possible modes of the radiation field. The eigenstates of H are tensor products over all possible modes and for every mode they are indexed by non-negative integers. In other words, the eigenstates of are tensor products $\otimes_\alpha |\, n_\alpha \,\rangle$, with $n_\alpha \in \mathbb{N}$ for all α. Moreover (recall 16.1.13),

1. $a_\alpha^* a_\alpha \left[\otimes_\beta |\, n_\beta \,\rangle\right] = n_\alpha \left[\otimes_\beta |\, n_\beta \,\rangle\right]$,
2. $H \left[\otimes_\beta |\, n_\beta \,\rangle\right] = \sum_\alpha \hbar\omega_\alpha(n_\alpha + 1/2)\left[\otimes_\beta |\, n_\beta \,\rangle\right]$,
3. $a_\alpha \left[\otimes_\beta |\, n_\beta \,\rangle\right] = \begin{cases} \sqrt{n_\alpha}|\, \ldots, n_\alpha - 1, \ldots\rangle & \text{if } n_\alpha \geq 1 \\ 0 & \text{otherwise.} \end{cases}$
4. $a_\alpha^* \left[\otimes_\beta |\, n_\beta \,\rangle\right] = \sqrt{n_\alpha + 1}|\, \ldots, n_\alpha + 1, \ldots\rangle$.

A photon corresponds to the elementary excitation of a single mode. It is caracterised by its polarisation and wavenumber. It can be thought as an elementary wave packet of the form depicted in figure A.10.

White light, as the one reaching us from the Sun, has a precise mixture of photons of various frequencies. Monochromatic light, as the one emitted by a laser for instance,

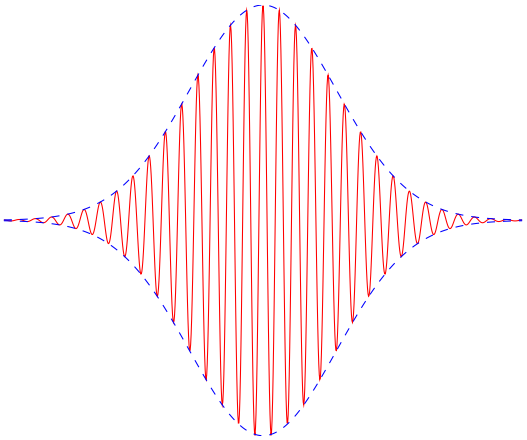


Figure A.10 – A non totally rigorous but useful mental representation of a photon as a wave packet. The envelope (dashed blue curve) gives an estimate of the"position" of the photon (at the centre of the enveloping curve) and of its "frequency" as the number of times the enveloped wave (solid red curve) changes sign per unit time. Position and frequency are determined only up to the precision allowed by Heisenberg's uncertainty principle. The direction of propagation of the depicted photon is the horizontal axis, its polarisation is vertical.

has photons of a single frequency. When the light intensity is $1\text{mW}/\text{cm}^2$, every square centimetre [13] receives 3.59×10^{20} red light photons/s and roughly half as much violet photons ($\nu = 700\text{THz}$). Huge numbers of photons being involved even for modest intensities, the appropriate method to study experimental results is through a statistical treatment of measurements.

13. Red light has a median frequency of $\nu = 420\text{THz}$. A single red photon carries an energy $E = 2\pi\hbar\nu = 2\pi \times 1.05457 \times 10^{-34}\text{Js} \times 4.2 \times 10^{14}\text{s}^{-1} = 2.783 \times 10^{-18}\text{J}$.

Bibliography

[1] B. P. Abbott et al. Observation of gravitational waves from a binary black hole merger. *Phys. Rev. Lett.*, 116:061102, Feb 2016. URL: http://link.aps.org/doi/10.1103/PhysRevLett.116.061102, doi:10.1103/PhysRevLett.116.061102. 9

[2] LM Adleman. Molecular computation of solutions to combinatorial problems. *Science*, 266(5187):1021–1024, 1994. URL: http://science.sciencemag.org/content/266/5187/1021, arXiv:http://science.sciencemag.org/content/266/5187/1021.full.pdf, doi:10.1126/science.7973651. 17

[3] N. I. Akhiezer and I. M. Glazman. *Theory of linear operators in Hilbert space*. Dover Publications Inc., New York, 1993. Translated from the Russian and with a preface by Merlynd Nestell, Reprint of the 1961 and 1963 translations, Two volumes bound as one. 64, 69

[4] William Arveson. *A short course on spectral theory*, volume 209 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002. 200, 204, 209

[5] William B. Arveson. Subalgebras of C^*-algebras. *Acta Math.*, 123:141–224, 1969b. 130

[6] R. S. Aspden, M. J. Padgett, and G. C. Spalding. Video recording true single-photon double-slit interference. *ArXiv e-prints*, February 2016. arXiv:1602.05987. 42

[7] Alain Aspect, Jean Dalibard, and Gérard Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.*, 49:1804–1807, Dec 1982. URL: http://link.aps.org/doi/10.1103/PhysRevLett.49.1804, doi:10.1103/PhysRevLett.49.1804. 13, 46, 48, 125

[8] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental tests of realistic local theories via Bell's theorem. *Phys. Rev. Lett.*, 47:460–463, Aug 1981. URL: http://link.aps.org/doi/10.1103/PhysRevLett.47.460, doi:10.1103/PhysRevLett.47.460. 46

[9] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental realization of Einstein-Podolsky-Rosen-Bohm *Gedankenexperiment*: A new violation of Bell's inequalities. *Phys. Rev. Lett.*, 49:91–94, Jul 1982. URL: http://link.aps.org/doi/10.1103/PhysRevLett.49.91, doi:10.1103/PhysRevLett.49.91. 46, 49

[10] Francisco M. Assis, Aleksandar Stojanovic, Paulo Mateus, and Yasser Omar. Improving classical authentication over a quantum channel. *Entropy*, 14(12):2531–2549, 2012. URL: http://www.mdpi.com/1099-4300/14/12/2531, doi:10.3390/e14122531. 158

[11] Alexia Auffèves and Philippe Grangier. Contexts, systems and modalities: a new ontology for quantum mechanics. *Found. Phys.*, 46(2):121–137, 2016. URL: https://doi.org/10.1007/s10701-015-9952-z. 12

[12] Guido Bacciagaluppi and Antony Valentini. *Quantum theory at the crossroads*. Cambridge University Press, Cambridge, 2009. Reconsidering the 1927 Solvay Conference, Translation of the proceedings, with a historical introduction and commentary. URL: http://dx.doi.org/10.1017/CBO9781139194983, doi:10.1017/CBO9781139194983. 51

[13] Stefan Banach. *Théorie des opérations linéaires*. Instytut Matematyczny Polskiej Akademi Nauk, Monografje Matematatyczne, 1932. URL: http://eudml.org/doc/268537. 63

[14] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp. Authentication of quantum messages. In *Foundations of Computer Science, 2002. Proceedings. The 43rd Annual IEEE Symposium on*, pages 449–458, 2002. doi:10.1109/SFCS.2002.1181969. 158

[15] David Beckman, Amalavoyal N. Chari, Srikrishna Devabhaktuni, and John Preskill. Efficient networks for quantum factoring. *Phys. Rev. A (3)*, 54(2):1034–1063, 1996. URL: http://dx.doi.org/10.1103/PhysRevA.54.1034, doi:10.1103/PhysRevA.54.1034. 191

[16] John Bell. Against 'measurement'. *Physics World*, 3(8):33–41, aug 1990. doi:10.1088/2058-7058/3/8/26. 109

[17] John S. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1(3):195–200, 1964. 46, 124

[18] John S. Bell. On the problem of hidden variables in quantum mechanics. *Rev. Modern Phys.*, 38:447–452, 1966. 45, 122, 124

[19] John S. Bell. Bertlmann's socks and nature of reality. Technical Report CERN-TH-2926, CERN, 1980. CERN Library. URL: http://cdsweb.cern.ch/record/142461/files/198009299.pdf. 118

[20] C. H. Bennett and G. Brassard. Quantum public key distribution system. *IBM Technical disclosure bulletin*, 28:3153–3163, 1985. 149

[21] Charles H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68(21):3121–3124, 1992. URL: http://dx.doi.org/10.1103/PhysRevLett.68.3121, doi:10.1103/PhysRevLett.68.3121. 152

[22] F. A. Berezin. *The method of second quantization*. Translated from the Russian by Nobumichi Mugibayashi and Alan Jeffrey. Pure and Applied Physics, Vol. 24. Academic Press, New York-London, 1966. 95

[23] A. S. Besicovitch. *Almost periodic functions*. Dover Publications, Inc., New York, 1955. 69

[24] James D. Bjorken and Sidney D. Drell. *Relativistic quantum fields*. McGraw-Hill Book Co., New York-Toronto-London-Sydney, 1965. 270

[25] David Bohm. A suggested interpretation of the quantum theory in terms of "hidden" variables. I. *Phys. Rev.*, 85:166–179, Jan 1952. URL: http://link.aps.org/doi/10.1103/PhysRev.85.166, doi:10.1103/PhysRev.85.166. 45

[26] David Bohm. A suggested interpretation of the quantum theory in terms of "hidden" variables. II. *Phys. Rev.*, 85:180–193, Jan 1952. URL: http://link.aps.org/doi/10.1103/PhysRev.85.180, doi:10.1103/PhysRev.85.180. 45

[27] Harald Bohr. *Almost periodic functions*. Chelsea Publishing Company, New York, N.Y., 1947. 69

[28] Ludwig Boltzmann. *Vorlesungen über Gastheorie, 1. Theil*. Verlag von Johann Ambrosius Barth, Leipzig, 1896. 139, 141, 142

[29] Ludwig Boltzmann. *Leçons sur la théorie cinétique des gaz*. Traduit de l'original allemand par A. Galloti. Gauthiers-Villars, Paris, 1902. Ré-imprimé par les Éditions Jacques Gabay, Paris (1987). 142

[30] George Boole. *An investigation of the laws of thought*. Walton and Maberly, Cambridge, 1854. 60

[31] M. Brune, E. Hagley, J. Dreyer, X. Maître, A. Maali, C. Wunderlich, J. M. Raimond, and S. Haroche. Observing the progressive decoherence of the "meter" in a quantum measurement. *Phys. Rev. Lett.*, 77:4887–4890, Dec 1996. URL: https://link.aps.org/doi/10.1103/PhysRevLett.77.4887, doi:10.1103/PhysRevLett.77.4887. 134

[32] S. Bugajski, K.-E. Hellwig, and W. Stulpe. On fuzzy random variables and statistical maps. *Rep. Math. Phys.*, 41(1):1–11, 1998. URL: http://dx.doi.org/10.1016/S0034-4877(98)80180-8, doi:10.1016/S0034-4877(98)80180-8. 31

[33] Jerome R. Busemeyer and Peter D. Bruza. *Quantum models of cognition and decision*. Cambridge University Press, Cambridge, 2012. URL: http://dx.doi.org/10.1017/CBO9780511997716, doi:10.1017/CBO9780511997716. 17

[34] C. Carathéodory. Untersuchungen über die Grundlagen der Thermodynamik. *Mathematische Annalen*, 67(3):355–386, Sep 1909. URL: https://doi.org/10.1007/BF01450409, doi:10.1007/BF01450409. 141

[35] J. T. Chang and D. Pollard. Conditioning as disintegration. *Statist. Neerlandica*, 51(3):287–317, 1997. URL: http://dx.doi.org/10.1111/1467-9574.00056, doi:10.1111/1467-9574.00056. 30, 267

[36] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Theoretical framework for quantum networks. *Phys. Rev. A (3)*, 80(2):022339, 20, 2009. URL: http://dx.doi.org/10.1103/PhysRevA.80.022339, doi:10.1103/PhysRevA.80.022339. 51

[37] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Informational derivation of quantum theory. *Phys. Rev. A*, 84:012311, Jul 2011. URL: http://link.aps.org/doi/10.1103/PhysRevA.84.012311, doi:10.1103/PhysRevA.84.012311. 51

[38] Man Duen Choi. Completely positive linear maps on complex matrices. *Linear Algebra and Appl.*, 10:285–290, 1975. 129, 130

[39] Yvonne Choquet-Bruhat, Cécile DeWitt-Morette, and Margaret Dillard-Bleick. *Analysis, manifolds and physics, Part I*. North-Holland Publishing Co., Amsterdam-New York, second edition, 1982. 271

[40] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23(15):880–884, 1969. doi:10.1103/PhysRevLett.23.880. 124

[41] R. Clausius. Über verschiedene für die Anwendung bequeme Formen der Hauptgleichungen der mechanischen Wärmetheorie. *Annalen der Physik*, 201(7):353–400, 1865. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/andp.18652010702, arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/andp.18652010702, doi:10.1002/andp.18652010702. 141

[42] Rudolf Clausius. *The mechanical theory of heat*. McMillan and Co., London, 1879. Translated by Walter R. Browne. Available at internet archive. 141

[43] Claude Cohen-Tannoudji, Jacques Dupont-Roc, and Gilbert Grynberg. *Photons et atomes - Introduction à l'électrodynamique quantique*. CNRS Éditions, Paris, 2001. Translation of the French origina: Photons et atomes - Introduction à l'électrpdynamique quantique, CNRS Éditions, Paris 1987. 271

[44] N. S. Dattani and N. Bryans. Quantum factorization of 56153 with only 4 qubits. *ArXiv e-prints*, November 2014. arXiv:1411.6758. 191

[45] E. B. Davies and J. T. Lewis. An operational approach to quantum probability. *Comm. Math. Phys.*, 17:239–260, 1970. 51

[46] Michel Demazure. *Cours d'algèbre*. Nouvelle Bibliothèque Mathématique [New Mathematics Library], 1. Cassini, Paris, 1997. Primalité. Divisibilité. Codes. [Primality. Divisibility. Codes]. 147

[47] Ian Duck and E. C. G. Sudarshan. *Pauli and the spin-statistics theorem*. World Scientific Publishing Co., Inc., River Edge, NJ, 1997. 52

[48] Anatolij Dvurečenskij and Sylvia Pulmannová. *New trends in quantum structures*, volume 516 of *Mathematics and its Applications*. Kluwer Academic Publishers, Dordrecht; Ister Science, Bratislava, 2000. URL: http://dx.doi.org/10.1007/978-94-017-2422-7, doi:10.1007/978-94-017-2422-7. 59

[49] Anatolij Dvurečenskij. Quantum observables and effect algebras. *Internat. J. Theoret. Phys.*, 57(3):637–651, 2018. URL: https://doi.org/10.1007/s10773-017-3594-1, doi:10.1007/s10773-017-3594-1. 59

[50] E. B. Dynkin. Calculation of the coefficients in the Campbell-Hausdorff formula. *Doklady Akad. Nauk SSSR (N.S.)*, 57:323–326, 1947. 251

[51] E. B. Dynkin. *Selected papers of E. B. Dynkin with commentary*. American Mathematical Society, Providence, RI; International Press, Cambridge, MA, 2000. Edited by A. A. Yushkevich, G. M. Seitz and A. L. Onishchik. 251

[52] A. R. Edmonds. *Angular momentum in quantum mechanics*. Princeton Landmarks in Physics. Princeton University Press, Princeton, NJ, 1996. Revised reprint of the 1960 edition. 254

[53] A. Einstein. Über die von der molekularkinetischen Theorie der Wärme geforderte Bewegung von in ruhenden Flüssigkeiten suspendierten Teilchen. *Annalen der Physik*, 322(8):549–560, 1905. URL: http://dx.doi.org/10.1002/andp.19053220806, doi:10.1002/andp.19053220806. 262

[54] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935. URL: http://link.aps.org/doi/10.1103/PhysRev.47.777, doi:10.1103/PhysRev.47.777. 44

[55] Albert Einstein, Max Born, and Hedwig Born. *Briefwechsel: 1916–1955*. Nympehnburger, München, 1969. Mit einem Geleitwort von Bertrand Russel. 44

[56] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991. URL: http://link.aps.org/doi/10.1103/PhysRevLett.67.661, doi:10.1103/PhysRevLett.67.661. 152

[57] R. P. Feynman. *Quantum electrodynamics*. Notes corrected by E. R. Huggins and H. T. Yura. Frontiers in Physics: Lecture Note and Reprint Volume. W. A. Benjamin, Inc., New York, 1961. 270

[58] Richard P. Feynman, Robert B. Leighton, and Matthew Sands. *The Feynman lectures on physics. Vol. 3: Quantum mechanics*. Addison-Wesley Publishing Co., Inc., Reading, Mass.-London, 1964. The new millenium edition, published by Basic Books. 41

[59] Ernst Fischer. Applications d'un théorème sur la convergence en moyenne. *CRAS*, 144:1148–1151, 1907. 63

[60] Ernst Fischer. Sur la convergence en moyenne. *CRAS*, 144:1022–1024 1022–1024, 1907. 63

[61] V. Fock. Konfigurationsraum und zweite Quantelung. *Zeitschrift für Physik*, 75(9):622–647, Sep 1932. URL: https://doi.org/10.1007/BF01344458, doi:10.1007/BF01344458. 95

[62] D. J. Foulis and M. K. Bennett. Effect algebras and unsharp quantum logics. *Found. Phys.*, 24(10):1331–1352, 1994. Special issue dedicated to Constantin Piron on the occasion of his sixtieth birthday. URL: http://dx.doi.org/10.1007/BF02283036, doi:10.1007/BF02283036. 59

[63] Maurice Fréchet. Sur les opérations linéaires. *Trans. Amer. Math. Soc.*, 5(4):493–499, 1904. URL: https://doi.org/10.2307/1986278, doi:10.2307/1986278. 63

[64] Maurice Fréchet. Sur les opérations linéaires. II. *Trans. Amer. Math. Soc.*, 6(2):134–140, 1905. URL: https://doi.org/10.2307/1986291, doi:10.2307/1986291. 63

[65] Maurice Fréchet. Sur les opérations linéaires. III. *Trans. Amer. Math. Soc.*, 8(4):433–446, 1907. URL: https://doi.org/10.2307/1988727, doi:10.2307/1988727. 63

[66] Maurice Fréchet. Sur l'approximation des fonctions continues périodiques par les sommes trigonométriques limitées. *Ann. Sci. École Norm. Sup. (3)*, 25:43–56, 1908. URL: http://www.numdam.org/item?id=ASENS_1908_3_25__43_0. 63

[67] Ivar Fredholm. Sur une classe d'équations fonctionnelles. *Acta Math.*, 27:365–390, 1903. URL: https://doi.org/10.1007/BF02421317, doi:10.1007/BF02421317. 63

[68] Walther Gerlach and Otto Stern. Das magnetische Moment des Silberatoms. *Zeitschrift fur Physik*, 9:353–355, December 1922. doi:10.1007/BF01326984. 265

[69] Walther Gerlach and Otto Stern. Der experimentelle Nachweis der Richtungsquantelung im Magnetfeld. *Zeitschrift fur Physik*, 9:349–352, December 1922. doi:10.1007/BF01326983. 265

[70] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002. URL: http://link.aps.org/doi/10.1103/RevModPhys.74.145, doi:10.1103/RevModPhys.74.145. 56

[71] Jonathan S. Golan. *The linear algebra a beginning graduate student ought to know*. Springer, Dordrecht, third edition, 2012. URL: http://dx.doi.org/10.1007/978-94-007-2636-9, doi:10.1007/978-94-007-2636-9. 78

[72] Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. Going beyond Bell's theorem. In *Bell's Theorem, Quantum Theory and Conceptions of the Universe (Cesena, 1991)*, pages 69–72. Kluwer Academic Publishers, M. Kafatos (ed.), 1989. 126

[73] Werner Greub. *Multilinear algebra*. Springer-Verlag, New York-Heidelberg, second edition, 1978. Universitext. 79

[74] A. Grothendieck. Produits tensoriels topologiques et espaces nucléaires. In *Séminaire Bourbaki, Vol. 2*, pages Exp. No. 69, 193–200. Soc. Math. France, Paris, 1952. 91

[75] A. Grothendieck. Résumé des résultats essentiels dans la théorie des produits tensoriels topologiques et des espaces nucléaires. *Ann. Inst. Fourier Grenoble*, 4:73–112 (1954), 1952. URL: http://www.numdam.org/item?id=AIF_1952__4__73_0. 91

[76] Alexandre Grothendieck. Produits tensoriels topologiques et espaces nucléaires. *Mem. Amer. Math. Soc.*, No. 16:336, 1955. 91

[77] S. Gudder, S. Pulmannová, S. Bugajski, and E. Beltrametti. Convex and linear effect algebras. *Rep. Math. Phys.*, 44(3):359–379, 1999. URL: https://doi.org/10.1016/S0034-4877(00)87245-6, doi:10.1016/S0034-4877(00)87245-6. 59

[78] Stanley P. Gudder. *Stochastic methods in quantum mechanics*. North-Holland, New York, 1979. North-Holland Series in Probability and Applied Mathematics. 19, 95

[79] Alain Guichardet. *Intégration et analyse hilbertienne*. Ellipses, Paris, 1989. 64

[80] Brian C. Hall. *Quantum theory for mathematicians*, volume 267 of *Graduate Texts in Mathematics*. Springer, New York, 2013. URL: http://dx.doi.org/10.1007/978-1-4614-7116-5, doi:10.1007/978-1-4614-7116-5. 250, 254

[81] Teiko Heinosaari and Mário Ziman. *The mathematical language of quantum theory*. Cambridge University Press, Cambridge, 2012. From uncertainty to entanglement. 129, 267

[82] B. Hensen et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015. Supplementary information. doi:10.1038/nature15759. 126

[83] Anthony J.G. Hey. *Feynman and computation*. Perseus Books Publishing, 1998. 50

[84] D. Hilbert, J. v. Neumann, and L. Nordheim. Über die Grundlagen der Quantenmechanik. *Math. Ann.*, 98(1):1–30, 1928. URL: https://doi.org/10.1007/BF01451579, doi:10.1007/BF01451579. 63

[85] David Hilbert. *Gesammelte Abhandlungen. Band III: Analysis, Grundlagen der Mathematik, Physik, Verschiedenes, Lebensgeschichte*. Zweite Auflage. Springer-Verlag, Berlin-New York, 1970. 63

[86] Yun-Feng Huang, Chuan-Feng Li, Yong-Sheng Zhang, Jian-Wei Pan, and Guang-Can Guo. Experimental test of the Kochen-Specker theorem with single photons. *Phys. Rev. Lett.*, 90:250401, Jun 2003. URL: https://link.aps.org/doi/10.1103/PhysRevLett.90.250401, doi:10.1103/PhysRevLett.90.250401. 124

[87] John K. Hunter and Bruno Nachtergaele. *Applied analysis*. World Scientific Publishing Co. Inc., River Edge, NJ, 2001. 64, 66

[88] Claude Itzykson and Jean Bernard Zuber. *Quantum field theory*. McGraw-Hill International Book Co., New York, 1980. International Series in Pure and Applied Physics. 270

[89] A. Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Rep. Mathematical Phys.*, 3(4):275–278, 1972. 129

[90] Peter Janotta and Haye Hinrichsen. Generalized probability theories: what determines the structure of quantum theory? *J. Phys. A*, 47(32):323001, 32, 2014. URL: http://dx.doi.org/10.1088/1751-8113/47/32/323001, doi:10.1088/1751-8113/47/32/323001. 267

[91] J. M. Jauch and F. Rohrlich. *The theory of photons and electrons*. Springer-Verlag, New York-Heidelberg, expanded edition, 1976. The relativistic quantum field theory of charged particles with spin one-half, Texts and Monographs in Physics. 270

[92] Richard V. Kadison and John R. Ringrose. *Fundamentals of the theory of operator algebras. Vol. I*, volume 15 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1997a. Elementary theory, Reprint of the 1983 original. 91, 201

[93] Alexander S. Kechris. *Classical descriptive set theory*, volume 156 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. URL: http://dx.doi.org/10.1007/978-1-4612-4190-4, doi:10.1007/978-1-4612-4190-4. 37

[94] Andreas Kirsch and Frank Hettlich. *The mathematical theory of time-harmonic Maxwell's equations*, volume 190 of *Applied Mathematical Sciences*. Springer, Cham, 2015. Expansion-, integral-, and variational methods. URL: https://doi.org/10.1007/978-3-319-11086-8, doi:10.1007/978-3-319-11086-8. 271

[95] Simon Kochen and E. P. Specker. The problem of hidden variables in quantum mechanics. *J. Math. Mech.*, 17:59–87, 1967. 123

[96] Carl A. Kocher and Eugene D. Commins. Polarization correlation of photons emitted in an atomic cascade. *Phys. Rev. Lett.*, 18:575–577, Apr 1967. URL: https://link.aps.org/doi/10.1103/PhysRevLett.18.575, doi:10.1103/PhysRevLett.18.575. 124

[97] Andrei Nikolaevich Kolmogorov. *Foundations of the theory of probability*. Chelsea Publishing Co., New York, 1956. Translation edited by Nathan Morrison of the original *Grundbegriffe der Wahrscheinlichkeitsrechnung* published in 1933, with an added bibliography by A. T. Bharucha-Reid. 22

[98] Franck Laloë. Commentaires sur le paradoxe EPR, Septembre 2010. https://www.bibnum.education.fr/physique/physique-quantique/le-paradoxe-epr. URL: https://www.bibnum.education.fr/physique/physique-quantique/le-paradoxe-epr. 118

[99] Serge Lang. *Introduction to Diophantine approximations*. Springer-Verlag, New York, second edition, 1995. URL: http://dx.doi.org/10.1007/978-1-4612-4220-8, doi:10.1007/978-1-4612-4220-8. 187

[100] A. K. Lenstra and H. W. Lenstra, Jr. Algorithms in number theory. In *Handbook of theoretical computer science, Vol. A*, pages 673–715. Elsevier, Amsterdam, 1990. 14, 148

[101] A. K. Lenstra and H. W. Lenstra, Jr., editors. *The development of the number field sieve*, volume 1554 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1993. URL: http://dx.doi.org/10.1007/BFb0091534, doi:10.1007/BFb0091534. 15

[102] Arjen K. Lenstra. Integer factoring. *Des. Codes Cryptogr.*, 19(2-3):101–128, 2000. Towards a quarter-century of public key cryptography. URL: http://dx.doi.org/10.1023/A:1008397921377, doi:10.1023/A:1008397921377. 148

[103] L. H. Loomis. The lattice theoretic background of the dimension theory of operator algebras. *Mem. Amer. Math. Soc.*, 1955(18):36, 1955. 220, 267

[104] H. Maassen. Quantum probability and quantum information theory. In *Quantum information, computation and cryptography*, volume 808 of *Lecture Notes in Phys.*, pages 65–108. Springer, Berlin, 2010. URL: http://dx.doi.org/10.1007/978-3-642-11914-9_3, doi:10.1007/978-3-642-11914-9_3. 46, 48, 49

[105] A. Manju and M. J. Nigam. Applications of quantum inspired computational intelligence: a survey. *Artificial Intelligence Review*, 42(1):79–156, 2014. URL: http://dx.doi.org/10.1007/s10462-012-9330-6, doi:10.1007/s10462-012-9330-6. 17

[106] Enrique Martín-López, Anthony Laing, Thomas Lawson, Roberto Alvarez, Xiao-Qi Zhou, and Jeremy L. O'Brien. Experimental realization of Shor's quantum factoring algorithm using qubit recycling. *Nature Photonics*, 6, 10 2012. doi:10.1038/nphoton.2012.259. 169, 191

[107] N. David Mermin. Is the moon there when nobody looks? reality and the quantum theory. *Physics Today*, April:38–47, 1985. URL: http://dx.doi.org/10.1103/PhysRevLett.65.1838. 117

[108] N. David Mermin. Hidden variables and the two theorems of John Bell. *Rev. Modern Phys.*, 65(3, part 1):803–815, 1993. See Errata: Rev. Mod. Phys. 85, 919 (2013); Rev. Mod. Phys. 88, 039902 (2016); Rev. Mod. Phys. 89, 049901 (2017). URL: https://doi.org/10.1103/RevModPhys.65.803, doi:10.1103/RevModPhys.65.803. 110, 123

[109] Michel Métivier. Limites projectives de mesures. Martingales. Applications. *Ann. Mat. Pura Appl. (4)*, 63:225–352, 1963. 267

[110] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2000. 190

[111] Emmy Noether. Invariante Variationsprobleme. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 1918:235–257, 1918. URL: http://eudml.org/doc/59024. 248, 261

[112] Masanao Ozawa. An operational approach to quantum state reduction. *Ann. Physics*, 259(1):121–137, 1997. URL: http://dx.doi.org/10.1006/aphy.1997.5706, doi:10.1006/aphy.1997.5706. 51

[113] C. Pacher, A. Abidin, T. Lorünser, M. Peev, R. Ursin, A. Zeilinger, and J-A. Larsson. Attacks on quantum key distribution protocols that employ non-ITS authentication, 2012. URL: http://arxiv.org/pdf/1209.0365. 158

[114] Juha-Pekka Pellonpää. Quantum instruments: I. Extreme instruments. *J. Phys. A*, 46(2):025302, 16, 2013. URL: http://dx.doi.org/10.1088/1751-8113/46/2/025302, doi:10.1088/1751-8113/46/2/025302. 51

[115] Juha-Pekka Pellonpää. Quantum instruments: II. Measurement theory. *J. Phys. A*, 46(2):025303, 15, 2013. URL: http://dx.doi.org/10.1088/1751-8113/46/2/025303, doi:10.1088/1751-8113/46/2/025303. 51

[116] Asher Peres. *Quantum theory: concepts and methods*, volume 57 of *Fundamental Theories of Physics*. Kluwer Academic Publishers Group, Dordrecht, 1993. 12

[117] Jean Perrin. *Les atomes*. Librairie Félix Alcan, 1913. Accessible sur Gallica. 262

[118] Jean Perrin. *Les atomes*. Nouveau Monde Editions, 2012. 262

[119] Dimitri Petritis. Markov chains on measurable spaces, 2015. Preminimary draft of lecture notes taught at the University of Rennes 1. URL: http://perso.univ-rennes1.fr/dimitri.petritis/enseignement/markov/2_pdfsam_markov.pdf. 50

[120] Dimitri Petritis. Probabilités pour la thórie de l'information, 2018. Notes de cours pour le master de cryptographie - version préliminaire, Université de Rennes 1. URL: http://perso.univ-rennes1.fr/dimitri.petritis/enseignement/ptin/ptin.pdf. 22, 140, 154

[121] Dimitri Petritis. Théorie de la complexité, 2018. Notes de cours pour le master de cryptographie - version préliminaire, Université de Rennes 1. URL: http://perso.univ-rennes1.fr/dimitri.petritis/enseignement/lcm1/lcm1.pdf. 22, 115

[122] Miklós Rédei. Why John von Neumann did not like the Hilbert space formalism of quantum mechanics (and what he liked instead). *Stud. Hist. Philos. Sci. B Stud. Hist. Philos. Modern Phys.*, 27(4):493–510 (1997), 1996. URL: http://dx.doi.org/10.1016/S1355-2198(96)00017-2, doi:10.1016/S1355-2198(96)00017-2. 51, 63

[123] Michael Reed and Barry Simon. *Methods of modern mathematical physics. I. Functional analysis*. Academic Press, New York, 1972. 64, 67

[124] Frédéric Riesz. Sur les systèmes orthogonaux de fonctions. *CRAS*, 144:615–619, 1907. 63

[125] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2):120–126, 1978. URL: http://dx.doi.org/10.1145/359340.359342, doi:10.1145/359340.359342. 15, 147

[126] Carlo Rovelli and Francesca Vidotto. *Covariant loop quantum gravity: an elementary introduction to quantum gravity and spinfoam theory*. Cambridge Monographs on Mathematical Physics. Cambridge University Press, 1 edition, 2014. 12

[127] Walter Rudin. *Real and complex analysis*. McGraw-Hill Book Co., New York, third edition, 1987. 64

[128] Walter Rudin. *Functional analysis*. International Series in Pure and Applied Mathematics. McGraw-Hill Inc., New York, second edition, 1991. 200

[129] Maximilian Schlosshauer. Decoherence, the measurement problem, and interpretations of quantum mechanics. *Rev. Mod. Phys.*, 76:1267–1305, Feb 2005. URL: https://link.aps.org/doi/10.1103/RevModPhys.76.1267, doi:10.1103/RevModPhys.76.1267. 133

[130] Erhard Schmidt. Über die Auflösung linearer Gleichungen mit unendlich vielen unbekannten. *Rendiconti del Circolo Matematico di Palermo (1884-1940)*, 25(1):53–77, Dec 1908. URL: https://doi.org/10.1007/BF03029116, doi:10.1007/BF03029116. 63

[131] Erwin Schrödinger. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31:555–563, 10 1935. URL: http://gen.lib.rus.ec/scimag/index.php?s=10.1017/S0305004100013554, doi:10.1017/S0305004100013554. 45

[132] Erwin Schrödinger and Paul Adrien Maurice Dirac. Probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 32:446–452, 10 1936. URL: http://gen.lib.rus.ec/scimag/index.php?s=10.1017/S0305004100019137, doi:10.1017/S0305004100019137. 45

[133] Denis Serre. *Matrices*, volume 216 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2010. Theory and applications, 2nd edition, Translated from the 2001 French original. doi:10.1007/978-1-4419-7683-3. 99

[134] Claude Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, 1949. 146

[135] Claude E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27:379–423, 623–656, 1948. 139

[136] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997. 14, 15, 145

[137] Thomas Sierocinski, Nathalie Théret, and Dimitri Petritis. Fuzzy and quantum methods of information retrieval to analyse genomic data from patients at different stages of fibrosis. In *2008 First International Symposium on Applied Sciences on Biomedical and Communication Technologies*, pages 1–5, Oct 2008. doi:10.1109/ISABEL.2008.4712599. 17

[138] Christoph Simon, Marek Żukowski, Harald Weinfurter, and Anton Zeilinger. Feasible Kochen-Specker experiment with single particles. *Phys. Rev. Lett.*, 85:1783–1786, Aug 2000. URL: https://link.aps.org/doi/10.1103/PhysRevLett.85.1783, doi:10.1103/PhysRevLett.85.1783. 124

[139] Instituts Solvay. *La structure de la matière: Rapports et discussions du Conseil de physique tenu à Bruxelles du 27 au 31 octobre 1913*. Gauthier-Villars, Paris, 1921. URL: http://catalog.hathitrust.org/Record/012292677. 51

[140] Instituts Solvay. *La structure de la matière: Rapports et discussions du Conseil de physique tenu à Bruxelles du 29 au 29 octobre 1933*. Gauthier-Villars, Paris, 1934. URL: http://catalog.hathitrust.org/Record/012292677. 51

[141] Instituts Solvay, Maurice de Broglie, Paul Langevin, and Ernest Solvay. *La théorie du rayonnement et les quanta: Rapports et discussions de la réunion tenue à Bruxelles, du 30 Octobre au 3 Novembre 1911, sous les auspices de E. Solvay*. Gauthier-Villars, Paris, 1912. URL: http://catalog.hathitrust.org/Record/012292676. 51

[142] W. Forrest Stinespring. Positive functions on C^*-algebras. *Proc. Amer. Math. Soc.*, 6:211–216, 1955. 128, 129, 130

[143] François Trèves. *Topological vector spaces, distributions and kernels*. Academic Press, New York-London, 1967. 80

[144] V. A. Uspenskiĭ, A. L. Semenov, and A. Kh. Shen'. Can an (individual) sequence of zeros and ones be random? *Uspekhi Mat. Nauk*, 45(1(271)):105–162, 222, 1990. URL: http://dx.doi.org/10.1070/RM1990v045n01ABEH002321, doi:10.1070/RM1990v045n01ABEH002321. 22

[145] C. J. van Rijsbergen. *The geometry of information retrieval*. Cambridge University Press, Cambridge, 2004. 17

[146] V. S. Varadarajan. *Geometry of quantum theory*. Springer-Verlag, New York, second edition, 1985. Reprint of the original edition published in two volumes, volume I in 1968 and volume 2 in 1970. 51, 220, 235

[147] Gilbert S. Vernam. *Cipher printing telegraph systems for secret wire and radio telegraphic communications*, volume 55. 1926. 146

[148] J. von Neumann. Über einen Satz von Herrn M. H. Stone. *Ann. of Math. (2)*, 33(3):567–573, 1932. URL: http://dx.doi.org/10.2307/1968535, doi:10.2307/1968535. 20

[149] Johann von Neumann. *Mathematische Grundlagen der Quantenmechanik*. Die Grundlehren der mathematischen Wissenschaften, Band 38. Springer-Verlag, Berlin, 1968. Unveränderter Nachdruck der ersten Auflage von 1932. 45, 51, 63, 122, 139

[150] John von Neumann. *Mathematical foundations of quantum mechanics*. Princeton Landmarks in Mathematics. Princeton University Press, Princeton, NJ, 1955. Translated from the German and with a preface by Robert T. Beyer, Twelfth printing, Princeton Paperbacks. 63, 122, 139

[151] John von Neumann. *Collected works. Vol. V: Design of computers, theory of automata and numerical analysis*. General editor: A. H. Taub. A Pergamon Press Book. The Macmillan Co., New York, 1963. 113

[152] John von Neumann. *Les fondements mathématiques de la mécanique quantique*. Éditions Jacques Gabay, Paris, 1988. Reprinted from the first French translation of 1946, published by the Librairie Félix Alcan. 63, 122, 139

[153] Joachim Weidmann. *Linear operators in Hilbert spaces*, volume 68 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1980. Translated from the German by Joseph Szücs. 65, 66

[154] Dirk Werner. *Funktionalanalysis*. Springer-Verlag, Berlin, 2011. 7., korrigierte une erweiterte Auflage. 69, 72

[155] D. Wineland, P. Ekstrom, and H. Dehmelt. Monoelectron oscillator. *Phys. Rev. Lett.*, 31:1279–1282, Nov 1973. URL: https://link.aps.org/doi/10.1103/PhysRevLett.31.1279, doi:10.1103/PhysRevLett.31.1279. 13

[156] Nanyang Xu, Jing Zhu, Dawei Lu, Xianyi Zhou, Xinhua Peng, and Jiangfeng Du. Quantum factorization of 143 on a dipolar-coupling nuclear magnetic resonance system. *Phys. Rev. Lett.*, 108:130501, Mar 2012. URL: http://link.aps.org/doi/10.1103/PhysRevLett.108.130501, doi:10.1103/PhysRevLett.108.130501. 191

[157] Nicholas Young. *An introduction to Hilbert space*. Cambridge Mathematical Textbooks. Cambridge University Press, Cambridge, 1988. URL: http://dx.doi.org/10.1017/CBO9781139172011, doi:10.1017/CBO9781139172011. 64

[158] W. H. Zurek. Environment-induced superselection rules. *Phys. Rev. D (3)*, 26(8):1862–1880, 1982. URL: http://dx.doi.org/10.1103/PhysRevD.26.1862, doi:10.1103/PhysRevD.26.1862. 133

Index of symbols

Index of terms and notions