UNIVERSITÉ DE RENNES I
UFR MATHÉMATIQUES

Master Sciences Technologies Santé
Année 2014–2015

Travaux dirigés de cryptographie quantique
Feuille numéro 02

Notation de Dirac

Exercice 1 Exprimer la condition de complétude d'une base orthonormée en notation de Dirac.

Exercice 2 Soient $A : \mathbb{G} \to \mathbb{H}$ un opérateur linéaire et $(\zeta_1, \ldots, \zeta_m)$ une base orthonormée de $\mathbb{G}$ et $(\eta_1, \ldots, \eta_m)$ une base orthonormée de $\mathbb{H}$.

1. Exprimer $I_{\mathbb{G}}$ et $I_{\mathbb{H}}$.
2. Déterminer les éléments de matrice de A et de A^* dans les bases respectives et exprimer l'identité $A = I_{\mathbb{H}} A I_{\mathbb{G}}$ en notation de Dirac.
3. Soit $g \in \mathbb{G}$. Déterminer ses coordonnés dans la base et exprimer l'application de A sur $|g\rangle$ en notation de Dirac.

Exercice 3 Soient $\mathbb{H}$ et $(\epsilon_1, \ldots, \epsilon_n)$ une base orthonormée de $\mathbb{H}$. On note E^{ij} l'opérateur $E^{ij} = |\epsilon_i\rangle\langle\epsilon_j|$.

1. E^{ij} est-il un orthoprojecteur ?
2. Déterminer $E^{ij}E^{kl}$.
3. Déterminer $E^{ij}|\epsilon_k\rangle$.
4. Déterminer les éléments matrice de E^{ij} dans la base.

Produit tensoriel de deux espaces de Hilbert (de dimension finie)

Exercice 4 Soit (g_k) une base orthonormée d'un espace de Hilbert $\mathbb{G}$ et et (h_l) une base orthonormée d'un espace de Hilbert $\mathbb{H}$.

1. Soit T un opérateur linéaire agissant sur $\mathbb{G} \otimes \mathbb{H}$. Calculer sa décomposition (en notation de Dirac) dans la base $(g_k \otimes h_l)$.
2. Soient A et B deux opérateurs agissant respectivement sur $\mathbb{G}$ et sur $\mathbb{H}$. On définit un opérateur S agissant sur $\mathbb{G} \otimes \mathbb{H}$ par son action sur les tenseur simples :

$$S|\phi\rangle \otimes |\psi\rangle = |A\phi\rangle \otimes |B\psi\rangle, \phi \in \mathbb{G}, \psi \in \mathbb{H},$$

étendu par linéarité sur tout l'espace $\mathbb{G} \otimes \mathbb{H}$. Comment s'écrit S dans la base $(g_k \otimes h_l)$?

Exercice 5 Soient $\mathbb{H}$ et $\mathbb{K}$ deux espaces de Hilbert et $A \in \mathfrak{B}(\mathbb{H})$, $B \in \mathfrak{B}(\mathbb{K})$ deux opérateurs auto-adjoints.

1. Monter que $\|A \otimes B\| \geq \|A\|\|B\|$.
2. Montrer que tout $\Psi \in \mathbb{H} \otimes \mathbb{K}$ peut s'écrire comme une somme finie $\Psi = \sum_{i=1}^{N} h_i \otimes k_i$, où $h_i \in \mathbb{H}$ et $k_i \in \mathbb{K}$; en outre, la famille $(k_i)_{i=1,\ldots,N}$ peut être choisie orthonormale.
3. En conclure que $\|\Psi\|^2 = \sum_{i=1}^{N} \|h_i\|^2$.
4. Montrer que $\|A \otimes I\Psi\|^2 \leq \|A\|^2\|\Psi\|^2$ et conclure que $\|A \otimes I\| \leq \|A\|$.
5. En observant que $A \otimes B = (A \otimes I_{\mathbb{K}})(I_{\mathbb{H}} \otimes B)$, établir que $\|A \otimes B\| \leq \|A\|\|B\|$ et conclure que $\|A \otimes B\| = \|A\|\|B\|$.
6. Si les dimensions respectives des espaces sont m et n, calculer $\det(A \otimes B)$.

Propriétés géométriques de l'espace des états quantiques

Exercice 6 Soit $\mathbb{H}$ un espace de Hilbert complexe de dimension d.

1. Montrer que la dimension *complexe* de $\mathfrak{L}(\mathbb{H})$ est d^2.
2. Montrer que la dimension *réelle* de l'ensemble $\mathfrak{L}_h(\mathbb{H})$ d'opérateurs auto-adjoints est d^2.
3. Conclure que l'ensemble convexe des opérateurs densité $\mathfrak{D}(\mathbb{H})$ peut être paramétré par $d^2 - 1$ paramètres réels.

Exercice 7 Soit $\mathbb{H} = \mathbb{C}^2$. On note $|0\rangle := \binom{1}{0}$ et $|1\rangle := \binom{0}{1}$ la base canonique.

1. Soit $|\psi\rangle$ un état pur. Déterminer le projecteur P_ψ sur le sous-espace unidimentionnel engendré par $|\psi\rangle$.
2. Soit $(|\psi^j\rangle)_{j\in J}$ une famille d'états purs. Déterminer la forme qu'aura une combinaison convexe ρ de tels projecteurs sur ces états.
3. Si ρ est positive (i.e. $\langle\psi|\rho\psi\rangle \geq 0$ pour tout $\psi \in \mathbb{H}$), déterminer ce que cette condition impose sur la représentation de ρ.
   Remarque : Cette expression constitue la forme la plus générale d'un état $\rho \in \mathbf{S}(\mathbb{C}^2)$; elle décrit l'état de préparation d'un système quantique binaire appelé **qubit**.
4. Montrer que l'espace vectoriel $\mathfrak{L}(\mathbb{H})$ muni de la forme sesquilinéaire $\mathfrak{L}(\mathbb{H}) \times \mathfrak{L}(\mathbb{H}) \ni (A, B) \mapsto \mathrm{tr}(A^*B) \in \mathbb{C}$ devient un espace de Hilbert. Cette forme est dite produit-scalaire de Hilbert-Schmidt.
5. On note
$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
   les matrices de Pauli. Montrer que ces matrices forment une base orthogonale de l'espace vectoriel $\mathfrak{L}(\mathbb{H})$ pour le produit scalaire de Hilbert-Schmidt. *Suggestion : on peut utiliser l'identité $\sigma_k\sigma_l = i\epsilon_{klm}\sigma_m$ pour $k, l, m = 1, 2, 3$ où $\epsilon_{klm} \in \{-1, 0, 1\}$ est le tenseur totalement antisymétrique qui vaut 0 si deux indices se répètent et vaut -1 ou $+1$ selon que la signature de la permutation nécessaire pour écrire les indices sous une forme cyclique est impaire ou paire.*

6. En décomposant $\rho = \frac{1}{2}\sum_{\alpha=0}^{3} r_\alpha \sigma_\alpha$ sur la base des matrices de Pauli, Quelle contrainte impose la condition $\mathrm{tr}(\rho) = 1$ sur les coefficients de la décomposition ? Dans la suite de l'exercice, on suppose que $\mathrm{tr}(\rho) = 1$.
7. Montrer que $r_i = \mathrm{tr}(\rho\sigma_i)$ pour $i = 1,2,3$.
8. Quelle contrainte impose la positivité de ρ sur les coefficients de la décomposition ?
9. Montrer que ρ est un projecteur si, et seulement si, $\|\mathbf{r}\| = \sqrt{r_1^2 + r_2^2 + r_3^2} = 1$.

Remarque : La représentation déterminée dans cet exercice donne une signification géométrique très intuitive de l'état d'un qubit ($\mathbb{H} = \mathbb{C}^2$). Malheureusement, la représentation correspondante aux qutrits ($\mathbb{H} = \mathbb{C}^3$), ou plus généralement aux qudits ($\mathbb{H} = \mathbb{C}^d$) sont des variétés de dimension $d^2 - 1$ qui n'ont pas de description intuitive dès que $d \geq 3$.

Marginales quantiques

Exercice 8 Soient $\rho_1 \in \mathfrak{D}(\mathbb{H}_1)$, $\rho_2 \in \mathfrak{D}(\mathbb{H}_2)$, $X_1 \in \mathfrak{B}(\mathbb{H}_1)$ et $X_2 \in \mathfrak{B}(\mathbb{H}_2)$.

1. Montrer que $\rho := \rho_1 \otimes \rho_2 \in \mathfrak{D}(\mathbb{H}_1 \otimes \mathbb{H}_2)$.
2. Quelles sont les marginales quantiques de ρ ?
3. Calculer $\mathrm{tr}(X_1 \otimes I_2\rho)$, $\mathrm{tr}(I_1 \otimes X_2\rho)$ et $\mathrm{tr}(X_1 \otimes X_2\rho)$, où I_1, I_2 sont les opérateurs identité sur $\mathbb{H}_1$ et $\mathbb{H}_2$ respectivement.
4. Quelle est l'interprétation de ρ ?

Exercice 9 Soient Ψ un vecteur unité sur $\mathbb{H}_1 \otimes \mathbb{H}_2$ et $\rho = |\Psi\rangle\langle\Psi|$ l'état pur correspondant. On note $(|\epsilon_i\rangle)_{i\in\mathbb{B}_1}$ et $(|\zeta_j\rangle)_{j\in\mathbb{B}_2}$ des bases orthonormées des espaces $\mathbb{H}_1$ et $\mathbb{H}_2$ respectivement.

1. Décomposer Ψ sur la base naturelle de $\mathbb{H}_1 \otimes \mathbb{H}_2$ et former la matrice $W = (W_{ij})_{i\in I, j1, J}$ des composantes de Fourier de Ψ dans cette base.
2. Soit A un opérateur auto-adjoint agissant sur $\mathbb{H}_1$. Calculer $\langle\Psi|(A \otimes I_{\mathbb{H}_2})\Psi\rangle$.
3. Noter $\rho_1 = WW^*$ et calculer $\mathrm{tr}(A\rho_1)$ (vérifier que les matrices A et ρ_1 ont des dimensions adéquates). Comparer ce résultat avec le résultat de la question précédente.
4. Soit B un opérateur auto-adjoint sur $\mathbb{H}_2$.Calculer $\langle\Psi|(I_{\mathbb{H}_1} \otimes B)\Psi\rangle$.
5. Noter $\rho_2 = W^*W$ et calculer $\mathrm{tr}(B\rho_2)$ (vérifier que les matrices B et ρ_2 ont des dimensions adéquates). Comparer ce résultat avec le résultat de la question précédente.
6. ρ_1 et ρ_2 sont-elles positives ? Sont-elles de trace normalisée ? Montrer qu'elle peuvent être interprétées comme des matrices-densité.
7. ρ_1 et ρ_2 correspondent-elles à des états purs ?
8. Quelle est votre conclusion ?

Exercice 10 Soient $\mathbb{H} = \mathbb{C}^d$ et $(\epsilon_1, \ldots, \epsilon_d)$ la base orthonormale canonique.

1. Les unités matricielles sont définies par $E^{kl}\epsilon_m = \delta_{lm}\epsilon_k$ pour $k, l = 1, \ldots, d$. Obtenir l'expression de E^{kl} en notation de Dirac.
2. Montrer que les $E^{kl}, k, l = 1, \ldots, d$ forment une base orthonormée de $\mathfrak{B}(\mathbb{H})$ pour le produit scalaire de Hilbert-Schmidt.

3. Soit $F = (F_\alpha)_{\alpha=1,\ldots,d^2}$ une base ortonormée arbitraire de $\mathfrak{B}(\mathbb{H})$. Obtenir les coefficients du développement de $A \in \mathfrak{B}(\mathbb{H})$ dans la base F.
4. Pour une base orthonormée arbitraire F, obtenir une expression simplifiée de $\sum_{\alpha=1}^{d^2} F_j^* A F_j$. *(Suggestion : commencer par établir cette expression simplifiée pour la base $E^{kl}, k, l = 1, \ldots, d$).*