HOW ARITHMETIC AND GEOMETRY MAKE ERROR CORRECTING CODES BETTER?

ALAIN COUVREUR

In the late 70's, V.D. Goppa proposed a new construction of codes. These so–called *algebraic geometry* benefit from pleasant features: their dimension and minimum distance can be bounded from below using elementary geometric properties of the curve. The very simple nature of these bounds led to a very concise criterion for a family of curves to provide sequences of codes whose dimension and minimum distance grow linearly in the code length: their number of rational points should grow linearly with their genus. Subsequently, Ihara and independently Tsfasman, Vlăduţ and Zink proved that some sequences of modular and Shimura curves achieve an optimal ratio of number of rational points with respect to the curves' genus. This led to an impressive and totally unexpected breakthrough in coding theory: some sequences of codes have better asymptotic parameters than "random codes".

In the spirit of this remarkable result, the objective of this talk is to shed light on various issues raised in coding theory for which the use of number theory and algebraic geometry brought a novel point of view and yielded remarkable results. Starting from a short overview of the design of families of curves leading to asymptotically good codes, we then focus on three coding theoretic questions where algebraic geometry brought relevant answers. First we discuss the behaviour of algebraic geometry codes with respect to the component wise product: a problem with a strong additive combinatorics flavour which has various applications such as decoding, secret sharing or public key cryptography. Second, we treat the constructions of codes with "good local properties", a question motivated by cloud storage and for which Galois covers of curves bring new solutions. The third question is more combinatorial and relies to the theoretical limits of list-decodability of codes where some close to optimal constructions are achieved using codes derived from algebraic geometry codes.

INRIA & LIX, UMR 7161, École Polytechnique, 91128 Palaiseau Cedex, France

Email address: alain.couvreur@inria.fr

Date: May 5, 2021.