Stage M2
Information set decoding of lee-metric codes over finite rings

P. Véron

A (k, n) binary code is a k-dimensional linear subspace of $\mathbb{F}_2^n$. The task of decoding a given code also known as syndrome decoding problem(SDP), is a fundamental issue in coding theory. In formula, given an $(n-k) \times n$ binary matrix H , a vector $s \in \mathbb{F}_2^{n-k}$, and an integer w, solving the syndrome decoding problem (SDP) consists in finding a vector $e \in \mathbb{F}_2^n$, whose weight is bounded by w, such that $He = s$. Note that such a formulation does not depend on the metric used to specify what is the weight of a vector. A well-studied case is that of the Hamming metric. In this metric, the weight of a vector is the number of non-zero coordinates of the vector. In Hamming metric, the SDP has been proven to be NP-hard; recently, the same hardness result has been extended to the rank metric case. The rationale of this work is to introduce techniques to solve the SDP for general codes in the Lee metric. In coding theory, the Lee distance is a distance between two vectors $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ over the q-ary alphabet $\{0, 1, \ldots, q-1\}$ of size $q \geqslant 2$. It is a metric, defined as :

$$\sum_{i=1}^{n} \min(|x_i - y_i|, q - |x_i - y_i|)$$

If $q = 2$ or $q = 3$ the Lee distance coincides with the Hamming distance. For $q > 3$ this is not the case anymore. Studying algorithms to solve the SDP problem in the Lee metric can be useful to address potential applicability of the Lee metric to design new code-based cryptosystems. Code-based cryptosystems are nowadays characterized by a renewed interest, because of their intrinsic resistance against quantum attacks. In fact, there is no known way to exploit quantum algorithms to efficiently solve the SDP: quantum versions of algorithms which can solve SDP are still characterized by a complexity that grows exponentially in the weight of the unknown vector e. This well-assessed security makes code-based cryptosystems among the most promising solutions for the post-quantum world.