Reduction from the decoding problem to EDCP

Agathe Blanvillain*[1]

[1]Inria de Paris – Université Paris-Sorbonne - Paris IV – France

Résumé

We revisit the quantum reduction from LWE to the extended Dihedral Coset Problem (EDCP) of Brakerski, Kirshanova, Stehl'e and Wen (BKSW18). In their paper, they show that LWE is equivalent to EDCP which is a generalized version of the dihedral coset problem, under quantum polynomial time reductions.

We adapt this reduction to coding theory and show in a general setting how to reduce the decoding problem to EDCP. The decoding problem is central in many classical cryptosystems submitted to the NIST competition, be they encryption schemes as Bike, McEliece or HQC or signature schemes as SDitH as it is supposed to be hard even for quantum adversaries. This reduction gives potentially a new way to quantumly solve the decoding problem. In essence, this reduction uses the fact that it might be easier to group together all noisy codewords c + e (where c ranges over all codewords and e ∈ Fq) that correspond to the same codeword c than decoding c + e. This operation can be done by using a suitable auxiliary code that we can decode easily and associate to c + e

the nearest (or close enough) auxiliary codeword. This can be done for any metric. We study in particular the Hamming metric, where we show that in a certain regime of parameters we obtain a reduction from the decoding problem to EDCP with a polynomial number of samples. Unfortunately, we also show that this reduction holds for a regime of parameters where decoding can be performed classically in polynomial time with the Prange decoder. We perform a general study of this reduction and show that it gives a non trivial reduction for other metrics such as the Lee metric.

*Intervenant