Probabilistic Analysis of LLL-based Decoder of Interleaved Chinese Remainder Codes

Matteo Abbondati, Antoine Afflatet, Eleonora Guerrini and Romain Lebreton

Chinese Remainder Codes (CR codes) are the integer counterpart of Reed-Solomon codes. They share similar correction capability and decoders.

Interleaving techniques are used to improve the unique decoding radius of a given code at the price of possible decoding failure. The most famous example is the case of Interleaved Reed Solomon (IRS) codes.

One can find in the literature a decoder for Interleaved Chinese Remainder codes that works in a similar way [3]. In both cases, the decoder tries to simultaneously correct ℓ codewords and build a system of linear equations, seeking for solutions satisfying some size constraints. The general idea of interleaved codes is that increasing ℓ means increasing the number of errors we can correct. But correcting beyond half the minimum distance of the code can lead to decoding failure.

The main difference between the polynomial decoder of IRS codes and the integer decoder of ICR codes is that the problem of finding the smallest degree solution becomes the problem of finding the shortest non-zero vector in a lattice, which is an NP-hard problem . In the original paper of [3], the authors present the idea of using LLL for the decoding of ICR codes. However, the proof of the correctness of their decoder is justified by heuristic arguments.

In this work, we prove an upper-bound on the decoding failure probability of the LLL-based decoder. Our main result expresses precisely the decoding failure of the algorithm in terms of its error correction capability. We consider this as a first step towards possible extensions of ICR codes to rational codes, and application to the design of a fault-tolerant integer linear system solver, similarly to the existing work in the polynomial case [1, 2].

References

1. Eleonora Guerrini, Romain Lebreton, and Ilaria Zappatore. Polynomial Linear System Solving with Errors by Simultaneous Polynomial Reconstruction of Interleaved Reed-Solomon Codes. In *2019 IEEE International Symposium on Information Theory*, pages 1542–1546, 2019.
2. Eleonora Guerrini, Romain Lebreton, and Ilaria Zappatore. Polynomial Linear System Solving with Random Errors: New Bounds and Early Termination Technique. In *Proceedings of ISSAC'21*, pages 171–178, 2021.
3. Wenhui Li, Vladimir Sidorenko, and Johan S. R. Nielsen. On decoding interleaved chinese remainder codes. In *2013 IEEE International Symposium on Information Theory*, pages 1052–1056, 2013.