Polynomial Linear System Solving with Errors by Simultaneous Polynomial Reconstruction of Interleaved Reed-Solomon Codes.

Ilaria Zappatore Eleonora Guerrini

A classical method for solving full rank consistent systems of linear equations $A(x)y(x) = b(x)$ with polynomial coefficients over a field $\mathbb{K}$, consists in evaluating the system at a certain number of evaluation points and then recovering the solution by interpolation. Some recent works, [1], [2], analyze this problem in a scenario where the evaluations are done by some black boxes that can output some erroneous values. They provide some algorithms that use a certain number of points, L, which depends on the number of errors E. Their approach is a generalization of the Berlekamp-Welch decoding of Reed-Solomon codes, which can be seen as a method to solve the Polynomial Reconstruction Problem (shortly PR).

In our work, we study the problem of solving a system of linear equations with polynomial coefficients in the same scenario, focusing on a finite field $\mathbb{F}_q$. Our aim is to use a smaller number of evaluation points than L. Since L depends on the number of errors, this is equivalent to increase the amount of errors that we can correct, i.e. the error correction capability. In order to do so, we reexamine our problem as a generalization of the Simultaneous Polynomial Reconstruction problem (SPR). The SPR was introduced in [3], as a variation of PR problem. It was associated to the decoding of Interleaved Reed-Solomon codes. Instead of the separate reconstruction of each interleaved codeword (using for example the Berlekamp-Welch algorithm for the PR solving), they proposed a probabilistic algorithm that uniquely decode all the codewords, simultaneously, with a certain probability. In particular, the error probability, i.e. the probability that the algorithm fails, is upper bounded by $\frac{E}{q}$. In [4], this bound was improved to $\mathcal{O}(\frac{1}{q})$. The advantage of this technique is the increasing error correction capability with respect to the Berlekamp-Welch one.
Therefore, following these approaches, we propose an algorithm which allows to recover the solution of the linear system using less evaluation points than L, with an error probability that depends on the order of the field. In this way, we achieve a bigger error correction capability than [1], [2]. We will also show, some experimental comparisons between the different algorithms, implemented in `SageMath`.

References

[1] Brice B. Boyer, Erich L. Kaltofen. *Numerical Linear System Solving With Parametric Entries By Error Correction.* SNC'14 Proceedings 2014 International Workshopon Symbolic-Numeric Computation, pp. 33-38.

[2] Erich L. Kaltofen, Clément Pernet, Arne Storjohann, Cleveland Waddell. *Early Termination in Parametric Linear System Solving and Rational Function Vector Recovery with Error Correction.* ISSAC '17 Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation, p. 237.

[3] Daniel Bleichenbacher, Aggelos Kiayias, Moti Yung. *Decoding interleaved Reed-Solomon codes over Noisy Data.* ICALP Springer, 2003, pp. 97-108.

[4] Andrew Brown, Lorenz Minder, Amin Shokrollahi. *Probabilistic Decoding of Interleaved RS-Codes on the Q-ary symmetric channel.* In Proc. of IEEE Intern. Symposium on Inf. Theory, 2004, p. 327.