Computing minimal interpolation bases

Vincent Neiger[†‡],
joint work with Claude-Pierre Jeannerod[†], Éric Schost[‡] and Gilles Villard[†]
[†] LIP, ENS de Lyon, France
[‡] University of Waterloo, Ontario, Canada

The first step in Guruswami and Sudan's list decoding algorithm for Reed-Solomon codes [8] amounts to bivariate interpolation with prescribed multiplicities and degree constraints. Later, variants of this problem arose in Koetter and Vardy's soft-decision decoding algorithm [9] (where constraints on the points are weakened), in Guruswami and Rudra's list decoding algorithm for folded Reed-Solomon codes [7] (where more variables are involved), and more recently in Devet, Goldberg, and Heninger's work on Private Information Retrieval [5].

In quest of fast algorithms, essentially two approaches have been proposed so far in the literature: one [3] uses fast structured system solving [2] while the other one [4] uses fast polynomial lattice reduction [6], which itself relies on fast order basis computations [11]. In this talk, we will first introduce the problem, give a quick overview of those fast algorithms, and discuss possible improvements. Then, noting the analogy between the quadratic iterative algorithms by Kötter [10] and by Beckermann and Labahn [1] respectively for constrained multivariate interpolation and order basis computation, we will present our recent work on a fast divide-and-conquer algorithm which gives a unified solution to these two problems.

Bibliography

[1] B. Beckermann and G. Labahn. A uniform approach for the fast computation of matrix-type Padé approximants. *SIAM J. Matrix Anal. Appl.*, 15(3):804–823, July 1994.

[2] A. Bostan, C.-P. Jeannerod, and É. Schost. Solving structured linear systems with large displacement rank. *Theor. Comput. Sci.*, 407(1-3):155–181, 2008.

[3] M. Chowdhury, C.-P. Jeannerod, V. Neiger, É. Schost, and G. Villard. Faster algorithms for multivariate interpolation with multiplicities and simultaneous polynomial approximations. *IEEE Trans. Inf. Theory*, 61(5):2370–2387, 2015.

[4] H. Cohn and N. Heninger. Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding. *Adv. Math. Comm.*, 9(3):311–339, 2015.

[5] Casey Devet, Ian Goldberg, and Nadia Heninger. Optimally robust private information retrieval. Cryptology ePrint Archive, Report 2012/083, 2012. http://eprint.iacr.org/.

[6] S. Gupta, S. Sarkar, A. Storjohann, and J. Valeriote. Triangular x-basis decompositions and derandomization of linear algebra algorithms over $K[x]$. *J. Symbolic Comput.*, 47(4):422–453, 2012.

[7] V. Guruswami and A. Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Trans. Inf. Theory*, 54(1):135–150, 2008.

[8] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Trans. Inf. Theory*, 45(6):1757–1767, 1999.

[9] R. Koetter and A. Vardy. Algebraic soft-decision decoding of Reed-Solomon codes. *IEEE Trans. Inf. Theory*, 49(11):2809–2825, 2003.

[10] R. Kötter. Fast generalized minimum-distance decoding of algebraic-geometry and Reed-Solomon codes. *IEEE Trans. Inf. Theory*, 42(3):721–737, 1996.

[11] W. Zhou and G. Labahn. Efficient algorithms for order basis computation. *J. Symbolic Comput.*, 47(7):793–819, 2012.