A Hybrid Ben-Or/Tiwari-Zippel Sparse Interpolation Algorithm

Erich Kaltofen and Wen-shin Lee
Department of Mathematics
North Carolina State University
Raleigh, N.C. 27695-8205
Email: {kaltofen,wlee1}@eos.ncsu.edu
URL: www.math.ncsu.edu/~{kaltofen,wlee1}

Abstract

A probabilistic algorithm is developed for minimizing the number of black box probes in sparse multivariate interpolation.

The Ben-Or/Tiwari interpolation [1, 4, 3] algorithm needs as input an upper bound of the number of terms in the polynomial. This algorithm proceeds in two stages. It first determines the terms by error correcting coding, and then their coefficients are obtained. Without such upper bound, we show how one can probabilistically determine the correct so-called error-locator polynomial. This we call the early termination version of Ben-Or/Tiwari algorithm. (Austin Lobo first employed early termination in the Wiedemann algorithm [6]. The same method should also be applicable to other sparse interpolation algorithms [5].)

Zippel's algorithm [7, 8] interpolates one variable at a time: only when the polynomial in a subset of variables is fully interpolated, do we start to interpolate the coefficient of each monimial in the next variable. In deciding which terms are to be considered, whose coefficient need to be interpolated for the next variable, the Zippel algorithm is used to probabilistically prune all those monomials, whose coefficients are zero, and only keep the present non-zero monomials (see also [2] for a pruning method which we employ here). In contrast to Zippel, however, when interpolating each coefficient polynomial in the new variable, we use simultaneously the Newton and our early termination Ben-Or/Tiwari algorithms, that on the same set of black box probes. When the coefficient has just a few terms, the Ben-Or/Tiwari algorithm determines the coefficient earlier than Newton interpolation. In other words, we race these two algorithm, and take advantage of both algorithms, or compensate for the disadvantage for either algorithm.

Our new hybrid algorithm is implemented in a Maple program.

References

[1] M. Ben-Or and P. Tiwari. A deterministic algorithm for sparse multivariate polynomial interpolation. In *Proc. Twentieth Annual ACM Symp. Theory Comput.*, pages 301–309, New York, N.Y., 1988. ACM Press.

[2] A. Díaz and E. Kaltofen. FoxBox a system for manipulating symbolic objects in black box representation. In O. Gloor, editor, *ISSAC 98 Proc. 1998 Internat. Symp. Symbolic Algebraic Comput.*, pages 30–37, New York, N. Y., 1998. ACM Press.

[3] E. Kaltofen, Lakshman Y. N., and J. M. Wiley. Modular rational sparse multivariate polynomial interpolation. In S. Watanabe and M. Nagata, editors, *ISSAC '90 Internat. Symp. Symbolic Algebraic Comput.*, pages 135–139. ACM Press, 1990.

[4] E. Kaltofen and Lakshman Yagati. Improved sparse multivariate polynomial interpolation algorithms. In P. Gianni, editor, *Symbolic Algebraic Comput. Internat. Symp. ISSAC '88 Proc.*, volume 358 of *Lect. Notes Comput. Sci.*, pages 467–474, Heidelberg, Germany, 1988. Springer Verlag.

[5] Lakshman Y. N. and B. D. Saunders. Sparse polynomial interpolation in non-standard bases. *SIAM J. Comput.*, 24(2):387–397, 1995.

[6] D. Wiedemann. Solving sparse linear equations over finite fields. *IEEE Trans. Inf. Theory*, IT-32:54–62, 1986.

[7] R. Zippel. Probabilistic algorithms for sparse polynomials. In *Proc. EUROSAM '79*, volume 72 of *Lect. Notes Comput. Sci.*, pages 216–226, Heidelberg, Germany, 1979. Springer Verlag.

[8] R. Zippel. Interpolating polynomials from their values. *J. Symbolic Comput.*, 9(3):375–403, 1990.