Algorithms for sparse and black box matrices over finite fields (Invited talk)

Erich Kaltofen

North Carolina State University, Math. Dept., Raleigh, NC 26695-8205, USA
URL: `http://www.kaltofen.net`, e-mail: `kaltofen@math.ncsu.edu`

Abstract. Sparse and structured matrices over finite fields occur in many settings. Sparse linear systems arise in sieve-based integer factoring and discrete logarithm algorithms. Structured matrices arise in polynomial factoring algorithms; one example is the famous Q-matrix from Berlekamp's method. Sparse diophantine linear problems, like computing the Smith canonical form of an integer matrix or computing an integer solution to a sparse linear system, are reduced via p-adic lifting to sparse matrix analysis over a finite field.

In the past 10 years there has been substantial activity on the improvement of a solution proposed by Wiedemann in 1986. The main new ingredients are faster preconditioners, projections by an entire block of random vectors, Lanczos recurrences, and a connection to Kalman realizations of control theory. My talk surveys these developments and describe some major unresolved problems.

Bibliographic references for my talk

The transparencies of my talk on May 23, 2001 at the *Sixth International Conference on Finite Fields and Applications (Fq6)* in Oaxaca, Mexico can be retrieved from the web address `http://www.math.ncsu.edu/~kaltofen/bibliography/01/fq6.pdf`. Following are various references to the literature of the subjects that I discussed.

Integer factoring via sieving

The classical reference to relations discovery is [25, Section 4.5.4], where references to Pomerance's quadratic sieve method and Pollard's number field sieve method can be found. The information on the arising sparse linear systems over $\mathbb{F}_2$ is for the RSA-120 challenge through private communication with Arjen K. Lenstra, and for RSA-155 by sending email to `challenge-rsa-honor-roll@rsa.com`. The latter email service also provides information on future challenges.

Berlekamp's factoring algorithm

The original paper is [3]. The Q-matrix is attributed to K. Petr in [33]. The asymptotically fastest version of Berlekamp's algorithm is given in [22]. Textbook descriptions of the method can be found in [25,12].

Black box matrices

The algorithmic significance of the linear operator view of matrices is well-know in numerical linear algebra. The Lanczos and conjugate gradient algorithms (see [15]) are sometimes referred to as "matrix-free" methods. The original paper by Wiedemann is [39]. The term "black box matrix" seems to have been coined first by [23].

Algorithms on structure matrices, like the Hilbert matrix and other Cauchy- or Toeplitz-like matrices, have a rich theory and practice, see [32,31].

Wiedemann's algorithm and applications

An essentially linear-time version of the Berlekamp/Massey algorithm can be found in [4].

The certificates of inconsistency for sparse linear systesm are in [14]. Villard's fast algorithm for the characteristic polynomial of a sparse matrix is in [38]. An even faster algorithm by Villard and Storjohann, based on blocking, is to be written up.

The relationship between the problems LinSolve0, i.e., computing a non-zero vector in the nullspace, and LinSolve1, i.e., computing a solution to a possibly singular inhomogeneous linear system, are first explored in [21]. The avoidance of nil-potent blocks by preconditioning for a solution of the problem LinSolve1 is implicit in [11] and explicit in [5].

The new sparse diophantine linear system solvers are presented in [13,30]. Hensel lifting is applied to linear system solving in [28,8] and to sparse linear systems in [21]. The fast determinant algorithms for dense integer matrices, based on Wiedemann's determinant algorithm, are in [24].

Lanczos's algorithm

Connections between the Wiedmann algorithm and the Lanczos algorithm are discussed in [27,11,34]. Dornstetter discusses the interpretation of the Berlekamp/Massey algorithm as Euclid's algorithm [9]. Gutknecht relates Lanczos recurrences to Padé approximations [16]. Early termination for the Wiedemann algorithm when the minimum polynomial has a low degree requires preconditioning and is due to Austin Lobo (cf. [19]).

Block methods

Projections by a block of vectors are analyzed in [6,7,29,17,36,37]. The different approaches for computing the matrix linear generator can be found in [7,2,17,35]. Multivariable realizations from control theory are applied to the block Wiedemann algorithm in [36,37]. A recent numerical treatment of the block Lanczos method is in [1].

Implementations

Austin Lobo's parallel implementation of the block Wiedemann algorithm is discussed in [20], Jean-Guillaume Dumas's in [10]. Information on the LinBox library project can be found at the web site `www.linalg.org`.

It appears to me that for the solution of a sparse linear system over a finite field of small or large cardinality, the (bi-directional non-symmetric) block Lanczos algorithm is superior to the block Wiedemann algorithm, the reason being that Wiedemann's bi-linear block projections for computing the sequence of low dimensional matrices and the subsequent step of evaluating the matrix polynomial linear generator are performed in the block Lanczos algorithm utilizing a single set of matrix-times-vector products. The block algorithms seem superior to the unblocked ones not only in the parallel setting but also as sequential methods, because they have a higher probability of success [36,37] and can reduce the number of matrix-times-vector products [17, Corollary after Theorem 7]. However, the block Wiedemann algorithm appears more efficient for obtaining the minimal polynomial and other information of a black box matrix, like its rank.

Open problems

The problem of computing the characteristic polynomial of a sparse or black box matrix is Problem 3 in [18].

Acknowledgement: My travel to Fq6 was supported in part by the Conference and in part by the National Science Foundation under Grant No. CCR-9988177.

References

Note: many of my publications cited below are accessible through links in my webpage listed under the title.

1. J. I. Aliaga, D. L. Boley, R. W. Freund, and V. Hernández. A Lanczos-type method for multiple starting vectors. *Mathematics of Computation*, 69:1577–1601, 2000.
2. B. Beckermann and G. Labahn. A uniform approach for fast computation of matrix-type Padé approximants. *SIAM J. Matrix Anal. Appl.*, 15(3):804–823, July 1994.
3. E. R. Berlekamp. Factoring polynomials over finite fields. *Bell Systems Tech. J.*, 46:1853–1859, 1967. Republished in revised form in: E. R. Berlekamp, *Algebraic Coding Theory*, Chapter 6, McGraw-Hill Publ., New York, 1968.
4. R. P. Brent, F. G. Gustavson, and D. Y. Y. Yun. Fast solution of Toeplitz systems of equations and computation of Padé approximants. *J. Algorithms*, 1:259–295, 1980.

5. L. Chen, W. Eberly, E. Kaltofen, B. D. Saunders, W. J. Turner, and G. Villard. Efficient matrix preconditioners for black box linear algebra. *Linear Algebra and Applications*, page to appear, 2001. Special issue on *Infinite Systems of Linear Equations Finitely Specified*.
6. D. Coppersmith. Solving linear systems over GF(2): block Lanczos algorithm. *Lin. Algebra Applic.*, 192:33–60, 1993.
7. D. Coppersmith. Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm. *Math. Comput.*, 62(205):333–350, 1994.
8. J. Dixon. Exact solution of linear equations using p-adic expansions. *Numer. Math.*, 40(1):137–141, 1982.
9. J. L. Dornstetter. On the equivalence between Berlekamp's and Euclid's algorithms. *IEEE Trans. Inf. Theory*, IT-33(3):428–431, 1987.
10. Jean-Guillaume Dumas, B. David Saunders, and Gilles Villard. On efficient sparse integer matrix Smith normal form computation. *J. Symbolic Comput.*, 32(1/2):71–99, 2001. Special issue on Computer Algebra and Mechanized Reasoning: Selected St. Andrews' ISSAC/Calculemus Contributions. Guest editors: T. Recio and M. Kerber.
11. W. Eberly and E. Kaltofen. On randomized Lanczos algorithms. In Küchlin [26], pages 176–183.
12. J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, Cambridge, New York, Melbourne, 1999.
13. M. Giesbrecht. Efficient parallel solutions of sparse systems of linear diophantine equations. In M. Hitz and E. Kaltofen, editors, *Proc. Second Internat. Symp. Parallel Symbolic Comput. PASCO '97*, pages 1–10, New York, N. Y., 1997. ACM Press.
14. M. Giesbrecht, A. Lobo, and B. D. Saunders. Certifying inconsistency of sparse linear systems. In O. Gloor, editor, *ISSAC 98 Proc. 1998 Internat. Symp. Symbolic Algebraic Comput.*, pages 113–119, New York, N. Y., 1998. ACM Press.
15. G. H. Golub and C. F. Van Loan. *Matrix Computations*. Johns Hopkins University Press, Baltimore, Maryland, third edition, 1996.
16. M. H. Gutknecht. The unsymmetric Lanczos algorithms and their relations to pade approximation, continued fractions, and the qd algorithm. Copper Mountain Conference on Iterative Methods, 1990; see `http://www.scsc.ethz.ch/~mhg/`.
17. E. Kaltofen. Analysis of Coppersmith's block Wiedemann algorithm for the parallel solution of sparse linear systems. *Math. Comput.*, 64(210):777–806, 1995.
18. E. Kaltofen. Challenges of symbolic computation my favorite open problems. *J. Symbolic Comput.*, 29(6):891–919, 2000. With an additional open problem by R. M. Corless and D. J. Jeffrey.
19. E. Kaltofen, W.-s. Lee, and A. A. Lobo. Early termination in Ben-Or/Tiwari sparse interpolation and a hybrid of Zippel's algorithm. In C. Traverso, editor, *Internat. Symp. Symbolic Algebraic Comput. ISSAC 2000 Proc. 2000 Internat. Symp. Symbolic Algebraic Comput.*, pages 192–201, New York, N. Y., 2000. ACM Press.
20. E. Kaltofen and A. Lobo. Distributed matrix-free solution of large sparse linear systems over finite fields. *Algorithmica*, 24(3–4):331–348, July–Aug. 1999. Special Issue on "Coarse Grained Parallel Algorithms".

21. E. Kaltofen and B. D. Saunders. On Wiedemann's method of solving sparse linear systems. In H. F. Mattson, T. Mora, and T. R. N. Rao, editors, *Proc. AAECC-9*, volume 539 of *Lect. Notes Comput. Sci.*, pages 29–38, Heidelberg, Germany, 1991. Springer Verlag.
22. E. Kaltofen and V. Shoup. Subquadratic-time factoring of polynomials over finite fields. *Math. Comput.*, 67(223):1179–1197, July 1998.
23. E. Kaltofen and B. Trager. Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators. *J. Symbolic Comput.*, 9(3):301–320, 1990.
24. E. Kaltofen and G. Villard. On the complexity of computing determinants. In *Proc. Fifth Asian Symposium on Computer Mathematics ASCM 2001*, page to appear. World Scientific Publishing Company, 2001. Invited contribution; extended abstract.
25. D. E. Knuth. *Seminumerical Algorithms*, volume 2 of *The Art of Computer Programming.* Addison Wesley, Reading, Massachusetts, USA, Third edition, 1997.
26. W. Küchlin, editor. *ISSAC 97 Proc. 1997 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 1997. ACM Press.
27. R. Lambert. *Computational Aspects of Discrete Logarithms.* PhD thesis, University of Waterloo, 1996.
28. R. T. Moenck and J. H. Carter. Approximate algorithms to derive exact solutions to systems of linear equations. In *Proc. EUROSAM '79*, volume 72 of *Lect. Notes Comput. Sci.*, pages 65–73, Heidelberg, Germany, 1979. Springer Verlag.
29. P. L. Montgomery. A block Lanczos algorithm for finding dependencies over GF(2). In *Proc. Eurocrypt 1995*, volume 921 of *Lect. Notes Comput. Sci.*, pages 106–120, Heidelberg, Germany, 1995. Springer Verlag.
30. T. Mulders and A. Storjohann. Diophantine linear system solving. In S. Dooley, editor, *ISSAC 99 Proc. 1999 Internat. Symp. Symbolic Algebraic Comput.*, pages 181–188, New York, N. Y., 1999. ACM Press.
31. V. Olshevsky. Pivoting on structured matrices with applications. *Linear Algebra and Its Applications*, to appear, 2001. See also `http://www.cs.gsu.edu/~matvro/papers.html`.
32. Victor Y. Pan. *Structured Matrices and Polynomials: Unified Superfast Algorithms.* Birkhäuser, 2001.
33. Št. Schwarz. On the reducibility of polynomials over a finite field. *Quart. J. Math. Oxford Ser. (2)*, 7:110–124, 1956.
34. J. Teitelbaum. Euclid's algorithm and the Lanczos method over finite fields. *Math. Comput.*, 67(224):1665–1678, October 1998.
35. E. Thomé. Fast computation of linear generators for matrix sequences and application to the block Wiedemann algorithm. pages 323–331, New York, N. Y., 2001. ACM Press.
36. G. Villard. Further analysis of Coppersmith's block Wiedemann algorithm for the solution of sparse linear systems. In Küchlin [26], pages 32–39.
37. G. Villard. A study of Coppersmith's block Wiedemann algorithm using matrix polynomials. Rapport de Recherche 975 IM, Institut d'Informatique et de Mathématiques Appliquées de Grenoble, `www.imag.fr`, April 1997.
38. Gilles Villard. Computing the Frobenius normal form of a sparse matrix. In V. G. Ganzha, E. W. Mayr, and E. V. Vorozhtsov, editors, *CASC 2000 Proc. the*

Third International Workshop on Computer Algebra in Scientific Computing, pages 395–407. Springer Verlag, 2000.

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