Tutorial

Some Recent Progress in Exact Linear Algebra and Related Questions

Gilles Villard
CNRS, Laboratoire LIP (CNRS, ENSL, INRIA, UCBL), École Normale Supérieure de Lyon, France
http://perso.ens-lyon.fr/gilles.villard

ABSTRACT

We describe some major recent progress in exact and symbolic linear algebra. These advances concern the improvement of complexity estimates for fundamental problems such as linear system solution, determinant, inversion and computation of canonical forms. The matrices are over a finite field, the integers, or univariate polynomials. We show how selected techniques are key ingredients for the new solutions: randomization and algebraic conditioning, lifting, subspace approach, divide-double and conquer, minimum matrix polynomial, matrix approximants. These algorithmic progress allow the design of new generation high performance libraries such as LinBox, and open various research directions.

We refer to [3] for an overview of methods in exact linear algebra, see also [37], [1] (in French), and [7, §2.3]. For fundamentals of computer algebra we refer to [16, 7].

Categories and Subject Descriptors: I.1.0; F.2.1; G.4.

General Terms: Algorithms.

1. Introduction. Past recent years have seen several major steps forward in linear algebra with matrices having exact or symbolic entries. For dense matrices, we illustrate this with the problem of computing the determinant of an $n \times n$ integer matrix with entries on β bits. Let $\mathsf{MM}(n)$ (between $\Omega(n^2)$ and $O(n^3)$) be the cost for multiplying to $n \times n$ matrices over a field F [4]. The "classical" use of Bareiss' algorithm or Chinese remaindering leads to a bit complexity $(n\beta\,\mathsf{MM}(n))^{1+\epsilon}$, i.e. the algebraic complexity times the bit length of the output. First estimates below the latter product are given in [14, 31] (actually, avant-garde ingredients for breaking the product were already available in [23]). We now know that the determinant can be computed in $(\beta\,\mathsf{MM}(n))^{1+\epsilon}$ bit operations [39] (randomized). In other words, and more generally (the determinant is not an isolated problem), several *polynomial or integer dense matrix problems can be solved with about the same number of operations (within* log *factors) as required to multiply two matrices having the same size (dimension and degree or bit size) as the input matrix.* We will present some of these problems and introduce the main techniques that are involved in their new solutions.

The improvements for dense matrices have arised in strong connection with those made for black box matrices (e.g. sparse matrices) over finite fields or the integers. Black box matrices have been studied intensively in various applications (polynomial systems, group computation, cryptography, etc.). We will see some new directions in this domain such as *fast basic linear algebra subroutines* and *adaptive and hybrid algorithms*, especially with the example of the dedicated design of the LinBox library.

2. Randomized algorithms and conditioning. Most of the currently fastest algorithms are randomized (Monte Carlo or Las Vegas). Randomization has led to the notion of algebraic matrix conditioning for ensuring good properties on matrices in view of easier solutions [5]. A central paper is [25] where a sort of equivalence between the Hermite and the Smith normal form of a conditioned matrix is identified. The latter is essential for understanding the recent fact that computing the Smith normal form may be surprisingly not harder than computing the determinant.

3. Hensel lifting. Lifting [9, 33] is a key iterative algorithm for system solution in symbolic linear algebra. It can be implemented at about the cost of the corresponding matrix product [38, 39]. Since the remark that system solution may be used for computing the determinant [34], lifting plays an important role for solving a lot of matrix problems. For instance, we refer to the elegant ideas of [17] for linear Diophantine systems.

4. Krylov/Lanczos subspace methods. Subspace methods such as the Krylov one are the counterpart of lifting for black box matrices. The seminal papers [45, 28, 29, 30] have established the importance and applications of the approach (see [15] for the Lanczos alternative). Blocking [8, 24, 26] and the notion of matrix minimum polynomial [43] are main ingredients for further cost improvements. For instance see [31] concerning the determinant and the Frobenius normal form, and [41] (and references therein) about the discrete logarithm.

5. Divide-double and conquer. Divide and conquer is a crucial paradigm for matrices over an abstract set of entries. Since it may not take into account the behaviour of the entry sizes during the computation, the paradigm have to be enriched for the symbolic setting. A "divide-double and conquer" strategy, which not only divides dimensions but also minimizes size rises, is used for essentially optimal polynomial matrix inversion [21], and for the outstanding determinant approach of [38, 39].

ISSAC'07, July 29–August 1, 2007, Waterloo, Ontario, Canada.
ACM 978-1-59593-743-8/07/0007.

6. Minimum matrix polynomial and approximants. The role of the uniform approach of [2] for computing polynomial matrix approximants is essential for some asymtotically fastest known algorithms on univariate polynomial matrices [22]. We rely on approximants for showing that polynomial basis reduction [19] or nullspace computation [40] can be solved at about the cost of the polynomial matrix product. Approximants complement a lifting or a subspace approach by solving the matrix reconstruction problem, and may provide minimal, if not unimodular, transformations.

7. High performance software: LinBox library. Most of the above novelties have been carried over to practical algorithms and implementations in the LinBox library [10, 32] (see also [6]). We refer to [42, 18, 20, 27, 44, 35] for presentations of the main advances in algorithm, library and code design. New concepts such as exact basic linear algebra subroutines are described in [11]. In addition to better complexity estimates, performance also relies on the use of clever adaptive and hybrid algorithms [36, 13, 12].

Related topics and perspectives. Important related topics that we do not discuss are structured matrices and numerical techniques. Some future directions will be identified.

1. REFERENCES

[1] J. Abdeljaoued and H. Lombardi. *Méthodes matricielles: Introduction à la Complexité Algébrique*. Collection Mathématique et Applications, Springer-Verlag, 2004.

[2] 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, 1994.

[3] D. Bini and V. Pan. *Polynomial and matrix computations*. Birkhäuser, 1994.

[4] P. Bürgisser, M. Clausen, and M. Shokrollahi. *Algebraic Complexity Theory*. Volume 315, Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1997.

[5] L. Chen, W. Eberly, E. Kaltofen, B. Saunders, W. Turner, and G. Villard. Efficient matrix preconditioners for black box linear algebra. *Lin. Alg. App.*, 343-344:119–146, 2002.

[6] Z. Chen and A. Storjohann. A BLAS based C library for exact linear algebra on integer matrices. *ISSAC'05, Beijing, China*, pp. 92–99. ACM Press, 2005.

[7] *Computer Algebra Handbook*, J. Grabmeier, E. Kaltofen, and V. Weispfenning editors, Springer-Verlag, 2003.

[8] D. Coppersmith. Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm. *Math. Comp.*, 62(205):333–350, 1994.

[9] J. Dixon. Exact solution of linear equations using p-adic expansions. *Numer. Math.*, 40:137–141, 1982.

[10] J. Dumas, T. Gautier, M. Giesbrecht, P. Giorgi, B. Hovinen, E. Kaltofen, B. Saunders, W. Turner, and G. Villard. LinBox: A Generic Library for Exact Linear Algebra. *ICMS'02, Beijing, China*, pp. 40–50. World Scientific, 2002.

[11] J.-G. Dumas, T. Gautier, P. Giorgi, and C. Pernet. Dense linear algebra over finite fields: the FFLAS and FFPACK packages. RRccsd-00018223, arXiv cs.SC/0601133, 2006.

[12] J.-G. Dumas, C. Pernet, and J.-L. Roch. Adaptive Triangular System Solving. In W. Decker, M. Dewar, E. Kaltofen, and S. Watt, editors, *Proc. Challenges in Symbolic Computation Software, Dagstuhl Seminar 06271, Germany*, 2006.

[13] J.-G. Dumas, C. Pernet, and Z. Wan. Efficient Computation of the Characteristic Polynomial. *ISSAC'05, Beijing, China*, pp. 92–99. ACM Press, 2005.

[14] W. Eberly, M. Giesbrecht, and G. Villard. Computing the determinant and Smith form of an integer matrix. *41st IEEE Symp. Found. Comp. Sc., Redondo Beach, USA*, pp. 675–685. IEEE Computer Society Press, Nov. 2000.

[15] W. Eberly and E. Kaltofen. On randomized Lanczos algorithms. *ISSAC'97, Maui, USA*, pp. 176–183. ACM Press, 1997.

[16] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 1999.

[17] M. Giesbrecht. Efficient parallel solution of sparse systems of linear diophantine equations. *PASCO'97, Maui, USA*, pp. 1–10, Jul 1997.

[18] P. Giorgi. Arithmétique et algorithmique en algèbre linéaire exacte pour la bibliothèque LinBox. Thèse de Doctorat, École Normale Supérieure de Lyon, France, 2004.

[19] P. Giorgi, C. Jeannerod, and G. Villard. On the complexity of polynomial matrix computations. *ISSAC'03, Philadelphia, USA*, pp. 135–142. ACM Press, 2003.

[20] B. Hovinen. Block Lanczos-Style Algorithms over Small Finite Fields. Master's Thesis, U. Waterloo, Canada, 2004.

[21] C. Jeannerod and G. Villard. Essentially optimal computation of the inverse of generic polynomial matrices. *J. Compl.*, 21(1):72–86, 2005.

[22] C. Jeannerod and G. Villard. Asymptotically fast polynomial matrix algorithms for multivariable systems. *Int. J. Control*, 79(11):1359–1367, 2006.

[23] E. Kaltofen. On computing determinants without divisions. *ISSAC'92, Berkeley, USA*, pp. 342–349. ACM Press, 1992.

[24] E. Kaltofen. Analysis of Coppersmith's block Wiedemann algorithm for the parallel solution of sparse linear systems. *Math. Comp.*, 64(210):777–806, 1995.

[25] E. Kaltofen, M. Krishnamoorthy, and B. Saunders. Fast parallel computation of Hermite and Smith forms of polynomials matrices. *SIAM J. Alg. Disc. Meth.*, 8:683–690, 1987.

[26] E. Kaltofen, and A. Lobo. Distributed matrix-free solution of large sparse linear systems over finite fields. *Algorithmica*, 24(3-4):331–348, 1999.

[27] E. Kaltofen, D. Morozov, and G. Yuhasz. Generic matrix multiplication and memory management in LinBox. *ISSAC'05, Beijing, China*, pp. 216–223. ACM Press, 2005.

[28] E. Kaltofen and V. Pan. Processor efficient parallel solution of linear systems over an abstract field. *3rd ACM Symp. Par. Alg. Arch.*, pp. 180–191. ACM-Press, 1991.

[29] E. Kaltofen and V. Pan. Processor efficient parallel solution of linear systems II: the general case. *33rd IEEE Symp. Found. Comp. Sc., Pittsburg, USA*, pp. 714–723, 1992.

[30] E. Kaltofen and B. Saunders. On Wiedemann's method of solving sparse linear systems. *AAECC-9*, LNCS 539, Springer-Verlag, pp. 29–38, 1991.

[31] E. Kaltofen and G. Villard. On the complexity of computing determinants. *Computational Complexity*, 13:91–130, 2004.

[32] LinBox. *LinBox Version 1.1,* `http://www.linalg.org`. 2007.

[33] R. Moenck and J. Carter. Approximate algorithms to derive exact solutions to systems of linear equations. *EUROSAM*, LNCS 72, Springer-Verlag, pp. 63–73, 1979.

[34] V. Pan. Complexity of parallel matrix computations. *Theor. Comp. Sc.*, 54:65–85, 1987.

[35] C. Pernet. Algèbre linéaire exacte efficace : le calcul du polynôme caractéristique. Thèse de Doctorat, U. J. Fourier, Grenoble, France, 2006.

[36] B. Saunders and Z. Wan. Smith Normal Form of Dense Integer Matrices, Fast Algorithms into Practice. *ISSAC'04, Santander, Spain*, pp. 274–281. ACM Press, 2004.

[37] A. Storjohann. *Algorithms for Matrix Canonical Forms*. PhD thesis, Institut für Wissenschaftliches Rechnen, ETH-Zentrum, Zurich, Switzerland, November 2000.

[38] A. Storjohann. High-order lifting and integrality certification. *J. Symbolic Computation*, 36(3-4):613–648, 2003.

[39] A. Storjohann. The shifted number system for fast linear algebra on integer matrices. *J. Compl.*, 21(4):609–650, 2005.

[40] A. Storjohann and G. Villard. Computing the rank and a small nullspace basis of a polynomial matrix. *ISSAC'05, Beijing, China*, pp. 309–316. ACM Press, 2005.

[41] E. Thomé. Algorithmes de calcul de logarithmes discrets dans les corps finis. Thèse de Doctorat, École Polytechnique, Palaiseau, France, 2003.

[42] W. Turner. *Black box linear algebra with the LinBox library*. PhD thesis, North Carolina State University, Raleigh, USA, May 2002.

[43] G. Villard. Further analysis of Coppersmith's block Wiedemann algorithm for the solution of sparse linear systems. *ISSAC'97, Maui, USA*, pp. 32–39. ACM Press, 1997.

[44] Z. Wan. *Computing the Smith forms of integer matrices and solving related problems*. PhD thesis, U. Delaware, USA, 2005.

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