HAL open science

Recent progress in linear algebra and lattice basis reduction (invited)

Gilles Villard

To cite this version:

Gilles Villard. Recent progress in linear algebra and lattice basis reduction (invited). ISSAC'11 - International symposium on Symbolic and algebraic computation, 2011, San Jose, United States. pp.3-4, 10.1145/1993886.1993889 . hal-00644796

HAL Id: hal-00644796

https://hal.science/hal-00644796v1

Submitted on 25 Nov 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Recent Progress in Linear Algebra and Lattice Basis Reduction

Gilles Villard
CNRS, ENS de Lyon, INRIA, UCBL, Université de Lyon
Laboratoire LIP
gilles.villard@ens-lyon.fr

Categories and Subject Descriptors

I.1.2 [**Symbolic and Algebraic Manipulation**]: Algorithms; F.2.1 [**Analysis of Algorithms and Problem Complexity**]: Numerical Algorithms and Problems

General Terms

Algorithms

ABSTRACT

A general goal concerning fundamental linear algebra problems is to reduce the complexity estimates to essentially the same as that of multiplying two matrices (plus possibly a cost related to the input and output sizes). Among the bottlenecks one usually finds the questions of designing a recursive approach and mastering the sizes of the intermediately computed data.

In this talk we are interested in two special cases of lattice basis reduction. We consider bases given by square matrices over $\mathsf{K}[x]$ or $\mathbb{Z}$, with, respectively, the notion of *reduced form* and *LLL reduction*. Our purpose is to introduce basic tools for understanding how to generalize the Lehmer and Knuth-Schönhage gcd algorithms for basis reduction. Over $\mathsf{K}[x]$ this generalization is a key ingredient for giving a basis reduction algorithm whose complexity estimate is essentially that of multiplying two polynomial matrices. Such a problem relation between integer basis reduction and integer matrix multiplication is not known. The topic receives a lot of attention, and recent results on the subject show that there might be room for progressing on the question.

Fundamental problems in linear algebra. Many matrix problems over a field K can be solved in $O\tilde{}(n^\omega)$ if ω is the exponent for matrix multiplication (see e.g. [2]). Over the last decade it became clear that the corresponding cost bounds, $O\tilde{}(n^\omega\delta)$ and $O\tilde{}(n^\omega\beta)$, for multiplying matrices of degree δ in $\mathsf{K}[x]^{n\times n}$ or with entries having bit length β in $\mathbb{Z}^{n\times n}$, may also be reached for symbolic problems. We refer for example to Storjohann's algorithms for the determinant and Smith form [21], and to the applications of polynomial approximant bases in [9]. The cost bounds have been recently improved for the characteristic polynomial [11] or matrix inverse [22]. However, as well as for integer LLL reduction, the question of reaching the bounds $O\tilde{}(n^\omega\beta)$ ($O\tilde{}(n^3\beta)$ for inversion) remains open for these problems.

Lattices. A polynomial lattice Λ_x of dimension d of $\mathsf{K}[x]^n$ is the set of the polynomial combinations of d linearly independent vectors $b_1,\ldots,b_d$ of $\mathsf{K}[x]^n$. The latter vectors form a basis of the lattice and define a matrix $B\in\mathsf{K}[x]^{n\times d}$. Any lattice admits an infinity of bases, but one may identify special ones, called minimal, with the smallest possible degrees. The matrix corresponding to a minimal basis, with degrees $\delta_1,\ldots,\delta_d$, is said to be in *reduced form* and is "orthogonal". We mean that up to a column scaling its leading coefficient matrix is full rank, and the orthogonality defect is

$$\Delta_x(b_1,\ldots,b_d)=\prod_j 2^{\delta_j}/2^{\deg\det(\Lambda_x)}=1.$$

The polynomial situation is simpler than its number theoretic analogue for which it is much harder to compute minimal quantities. A lattice Λ of $\mathbb{Z}^n$ is the set of the integer combinations of a basis $b_1,\ldots,b_d$ in $\mathbb{Z}^n$. We consider the relaxed notion of reduction introduced by Lenstra, Lenstra and Lovász in [14]. The lengths of the vectors of a *LLL reduced* basis are not minimal but fairly small. Among other properties, the lengths and the orthogonality defect satisfy

$$\Delta(b_1,\ldots,b_d)=\prod_j\|b_j\|/\det(\Lambda)\le 2^{O(d^2)}.$$

The problem of finding a reduced basis of a lattice given by an arbitrary basis is called *basis reduction*. We focus on the two above particular cases for non singular matrices. A more general setting would be reduction for discrete subgroups of $\mathbb{R}^n$ and free modules of finite rank. A rich litterature and the wide spectrum of applications of basis reduction show the importance of the domain. For the polynomial case we may refer to Kailath [10] and system theory references therein. About LLL and stronger reductions we may refer to Lovász [15] and the contributions in [16].

Basis reduction. Two matrices A and B whose columns form a basis of a given lattice are equivalent, i.e. $B=AU$ with U unimodular. A typical approach for computing a reduced B from a non reduced A is to apply successive transformations. Over $\mathsf{K}[x]$, the transformations correspond to dependencies in coefficient matrices, and decrease the column degrees. In the integer case, geometrical informations are obtained from orthogonalizations over $\mathbb{R}$ for decreasing the column norms. The basic transformations consist in reducing vectors or matrices against others, and vice versa. Reduction algorithms are seen as generalizations of Euclid's gcd or continued fraction algorithm (see [7] and seminal references therein). The intermediately computed bases play the role of "remainders", and the successive basic transformations performed on the bases play the role of "quotients".

Lehmer's & Knuth-Schönhage algorithms. Lehmer's modification of Euclid's algorithm [13], and Knuth's [12] and Schönhage's [19] algorithms, have been a crucial progress. Their idea is to employ the fact that for small quotients,

Copyright is held by the author/owner(s).
ISSAC'11, June 8–11, 2011, San Jose, California, USA.
ACM 978-1-4503-0675-1/11/06.

truncated remainders suffice to compute the quotient sequence. Via an algorithm that multiplies two integers of size β in $\mu(\beta)$ operations, this has led to the bit complexity estimate $O(\mu(\beta)\log\beta)$ for the gcd problem. Through some analogies between recent algorithms over $\mathsf{K}[x]$ and $\mathbb{Z}$, we will see how similar recursive approaches may be developed for reduction.

Reduced form over $\mathsf{K}[x]$. Beckermann and Labahn [1] has given a key generalization of the Knuth-Schönhage algorithm for Padé approximants. As a consequence one may show [9] that reconstructing a univariate and proper matrix fraction CB^{-1} from its expansion, with B column reduced of degree $O(\delta)$, can be done in $O\tilde{}(n^\omega\delta)$ field operations. This may be applied to computing a reduced form B of a non singular matrix A, by reconstructing a fraction CB^{-1} from an appropriate (proper) segment of the expansion of A^{-1} [4]. We will see that it follows that the reduction of a non singular $A \in \mathsf{K}[x]^{n\times n}$ of degree δ can be performed within about the same number $O\tilde{}(n^\omega\delta)$ of operations as that of multiplying two matrices of degree δ in $\mathsf{K}[x]^{n\times n}$. The corresponding algorithm of Giorgi *et al.* [4] is randomized. A deterministic algorithm is given in [5] where the problem of reducing A is reduced to the problem of reducing the Hermite form H of A. The latter problem may be solved in $O\tilde{}(n^\omega\delta)$ via a partial linearization of H, and using the algorithm designed in [4] for fraction reconstruction via approximants.

These reduction approaches work in two phases. A first phase transforms the problem into a "simpler"—with a small degree solution—matrix approximant problem (either via a fraction or the Hermite normal form). The second phase inherits the approximation method of [1], and works by recurrence on the approximation order. (The process may be decomposed into successive matrix factorizations over K.)

LLL reduction over $\mathbb{Z}$. For an insight into LLL reduction algorithms we may refer to the contributions of Nguyen (Ch. 2), Schnorr (Ch. 4), and Stehlé (Ch. 5) in [16]. We focus on the cost with respect to the integer bit size β, with the aim of obtaining a bit complexity estimate $O\tilde{}(\mathcal{P}oly(n)\beta)$.

We will present the gradual strategy of [8, 17] for designing a Lehmer-like algorithm in the following special case (see also [18]). Assume that B_0 is LLL reduced, and let $\sigma = \mathrm{diag}(\ell, 1, \ldots, 1)$ where $\ell > 1$. We call lift-reduction of B_0 the problem of reducing $\sigma^k B_0$, $k \in \mathbb{N}$. The lift-reduction of [17] is a recurrence on the order k of the lifting, and implements the lift-reduction as k successive elementary steps. (B_{i+1} is a reduced basis of σB_i.) With this setting, the Knuth-Schönhage algorithm may be generalized for the task of lift-reducing [17]. The truncation process of the successive bases ("remainders") relies on an LLL reduction definition that resists perturbation, and takes advantage of the numerical quality of the reduced bases that are fairly well conditioned (see [3]). The multi-dimensionality of lattice reduction leads to the manipulation of significantly differing magnitudes in the transformations themselves. The problem may be solved by truncating also the transformations. (Unlike the integer gcd case where the quotients are not truncated.)

We will see how to use lift-reduction for the LLL reduction of A in time quasi-linear in β [17] (non singular case). Lift-reduction is specialized to reducing a lift/shift of an already reduced basis. For example, appropriate reduced bases for calling the lift-reduction can be created iteratively from the Hermite form of A. The above approach takes a matrix point of view. An alternative approach to LLL reduction in time $O\tilde{}(\mathcal{P}oly(n)\beta)$ has been recently obtained [6], by using the 2-dimensional Knuth-Schönhage algorithm from [20, 23].

Acknowledgment. We are grateful to Damien Stehlé for his help during the preparation of this talk.

References

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

[3] X.-W. Chang, D. Stehlé, and G. Villard. Perturbation analysis of the QR factor R in the context of LLL lattice basis reduction. *Math. Comp.*, to appear.

[4] P. Giorgi, C. Jeannerod, and G. Villard. On the complexity of polynomial matrix computations. In *Proc. ISSAC, Philadelphia, PA*, pages 135–142. ACM Press, Aug. 2003.

[5] S. Gupta, S. Sarkar, A. Storjohann, and J. Valeriote. Triangular x-basis decompositions and derandomization of linear algebra algorithms over $\mathsf{K}[x]$. *J. Symbolic Comput.*, to appear.

[6] G. Hanrot, X. Pujol, and D. Stehlé. Personal communication, Dec. 2010.

[7] J. Hastad, B. Just, J. Lagarias, and C. Schnorr. Polynomial time algorithms for finding integer relations among real numbers. *SIAM J. Comput.*, 18(5):859–881, 1989.

[8] M. van Hoeij and A. Novocin. Gradual sub-lattice reduction and a new complexity for factoring polynomials. In *Proc. LATIN 2010*, volume 6034, pages 539–553, 2010.

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

[10] T. Kailath. *Linear systems*. Prentice Hall, 1980.

[11] E. Kaltofen and G. Villard. On the complexity of computing determinants. *Comput. Complexity*, 13(3-4):91–130, 2005.

[12] D. Knuth. The analysis of algorithms. In *Proc. International Congress of Mathematicians (Nice, 1970)*, volume 3, pages 269–274, 1971.

[13] D. Lehmer. Euclid's algorithm for large numbers. *Amer. Math. Monthly*, 45:227–233, 1938.

[14] A. Lenstra, H. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.

[15] L. Lovász. *An algorithmic theory of numbers, graphs and convexity*. CBMS-NSF Regional Conferences Series in Applied Mathematics, SIAM, 1986.

[16] P. Q. Nguyen and B. Vallée, editors. *The LLL Algorithm, Survey and Applications*. Springer-Verlag, 2010.

[17] A. Novocin, D. Stehlé, and G. Villard. An LLL-reduction algorithm with quasi-linear time complexity. In *Proc. 43rd ACM STOC, San Jose, CA*. ACM Press, June 2011.

[18] S. Radziszowski and D. Kreher. Solving subset sum problems with the L^3 algorithm. *J. Combin. Math. Combin. Comput.*, 3:49–63, 1988.

[19] A. Schönhage. Schnelle Berechnung von Kettenbruchenwicklungen. *Acta Inform.*, 1:139–144, 1971.

[20] A. Schönhage. Fast reduction and composition of binary quadratic forms. In *Proc. ISSAC, Bonn, Germany*, pages 128–133. ACM Press, 1991.

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

[22] A. Storjohann. On the complexity of inverting integer and polynomial matrices. *Comput. Complexity*, to appear.

[23] C. K. Yap. Fast unimodular reduction: planar integer lattices. In *Proc.33rd IEEE FOCS, Pittsburgh, PA*, pages 437–446, 1992.