

Exact computations on polynomial and integer matrices

*Gilles Villard**

Abstract

One may consider that the algebraic complexity of basic linear algebra over an abstract field K is well known. Indeed, if ω is the exponent of matrix multiplication over K , then for instance computing the determinant, the matrix inverse, the rank or the characteristic polynomial of an $n \times n$ matrix over K can be done in $\tilde{O}(n^\omega)$ operations in K . Here the soft “ \tilde{O} ” notation indicates some missing logarithmic factors. The same complexity estimate holds for the solution of many other problems [2, Chap. 16].

Over more concrete domains like $K[x]$ or \mathbb{Z} , the impact of data size—the degree of the polynomials or the bit length of the integers—on the problem’s complexity is much less known. Until recently it was considered that compared to n^ω , a typical extra factor n was involved in the costs. For instance the exact determinant and inverse of a polynomial matrix of degree d are computed in $\tilde{O}(n \cdot n^\omega d) = \tilde{O}(n^{\omega+1} d)$ operations in K using an evaluation/interpolation scheme or Newton’s iteration. The exact determinant and inverse of an integer matrix are computed in $\tilde{O}(n^{\omega+1} \log \|A\|)$ bit operations by Chinese remaindering. For reducing the complexity, *i.e.* the data size overhead, a main concern is to exploit the interplay of the algebraic structure with the intermediate expression swell. Several authors have successfully addressed the question during the last three years. Our aim is to survey these studies, especially around the determinant, the matrix inverse and matrix canonical forms.

New progresses for the determinant complexity have been obtained in [3, 6, 7]. It is now known that the determinant and the Smith normal form of a polynomial matrix can be computed by a certified randomized algorithm in $\tilde{O}(n^\omega d)$ operations in K [7]. We prove in [4] that the same operation count is valid for column reduction.

*CNRS / Laboratoire LIP, École Normale Supérieure de Lyon, 46, Allée d’Italie 69364 Lyon Cedex 07, France. Url: <http://www.ens-lyon.fr/~gvillard>

The corresponding bit complexity estimate for computing the determinant and the Smith normal form of an integer matrix is $O(n^\omega \log \|A\|)$ [8].

It is not clear how the reductions and equivalences between problems used in algebraic complexity can be carried over to the polynomial and integer cases. One may think in particular to the reduction of the matrix inversion problem to the determinant problem in [1]. We thus do not know how to take advantage of above cited new determinant algorithms for inverting a matrix. However, at least for generic matrices, inversion can be addressed by a different approach. In [5] we show that the inverse of a generic polynomial matrix of degree d can be computed in $O(n^3 d)$ operations in K . Asymptotically and up to the logarithmic factors, the latter operation count is the size of the output.

We remark that the new complexity estimates $O(n^\omega d)$ and $O(n^\omega \log \|A\|)$ are roughly the current estimates for polynomial or integer matrix multiplication. Also, in [4] we show that computing the determinant of a polynomial matrix is somehow harder than multiplying two polynomial matrices. Indeed, if there is a straight-line program of length $D(n, d)$ over K which computes the coefficient of degree d of the determinant, then there is a straight-line program of length no more than $8D(n, d)$ which multiplies two $n \times n$ matrices of degree d . Hence, two natural questions arise. If $MM(n, d)$ is the cost for multiplying two $n \times n$ matrices of degree d over K , which problems can be solved in $O(MM(n, d))$ operations in K ? If $MM(n, \log \|A\|)$ is the bit cost for multiplying two $n \times n$ integer matrices, which problems can be solved in $O(MM(n, \log \|A\|))$ bit operations?

Bibliography

- [1] W. BAUR AND V. STRASSEN, *The complexity of partial derivatives*, Theoretical Computer Science, 1982, 22, pp. 317–330.
- [2] P. BÜRGISSER, M. CLAUSEN AND M.A. SHOKROLLAHI, *Algebraic Complexity Theory*, Volume 315, Grundlehren der mathematischen Wissenschaften, Springer-Verlag, 1997.
- [3] W. EBERLY, M. GIESBRECHT AND G. VILLARD, *Computing the determinant and Smith form of an integer matrix*, in Proc. The 41st Annual IEEE Symposium on Foundations of Computer Science, Redondo Beach, CA USA, nov. 2000, IEEE Computer Society Press, pp. 675–685.
- [4] P. GIORGI, C.P. JEANNEROD AND G. VILLARD, *On the complexity of polynomial matrix computations*, in Proc. International Symposium on Symbolic and Algebraic Computation, Philadelphia, Pennsylvania USA, R. Sendra ed., ACM Press, aug. 2003.
- [5] C.P. JEANNEROD AND G. VILLARD, *Straight-line computation of the polynomial matrix inverse*, Research Report 2002-47, Laboratoire LIP, ENS Lyon, France, 2002, <http://www.ens-lyon.fr/LIP/Pub/rr2002.html>
- [6] E. KALTOFEN AND G. VILLARD, *On the complexity of computing determinants*, in Proc. Fifth Asian Symposium on Computer Mathematics, Lecture Notes Series on Computing 9, K. Shirayanagi and K. Yokoyama eds., World Scientific, 2001, pp. 13–27.
- [7] A. STORJOHANN, *High-order lifting and integrality certification*, Special issue 2002 Internat. Symp. Symbolic Algebraic Computation, Journal of Symbolic Computation, 2003, to appear.
- [8] A. STORJOHANN, private communication.