ARTICLE IN PRESS

Journal of Complexity ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Journal of Complexity

journal homepage: www.elsevier.com/locate/jco

Fast, deterministic computation of the Hermite normal form and determinant of a polynomial matrix☆

George Labahn[a,*], Vincent Neiger[b], Wei Zhou[a]

[a] David R. Cheriton School of Computer Science, University of Waterloo, Waterloo ON, Canada N2L 3G1

[b] ENS de Lyon (Laboratoire LIP, CNRS, Inria, UCBL, Université de Lyon), Lyon, France

ARTICLE INFO

Article history:
Received 19 July 2016
Accepted 18 March 2017
Available online xxxx

Keywords:
Hermite normal form
Determinant
Polynomial matrix

ABSTRACT

Given a nonsingular $n \times n$ matrix of univariate polynomials over a field $\mathbb{K}$, we give fast and deterministic algorithms to compute its determinant and its Hermite normal form. Our algorithms use $\widetilde{\mathcal{O}}(n^\omega \lceil s \rceil)$ operations in $\mathbb{K}$, where s is bounded from above by both the average of the degrees of the rows and that of the columns of the matrix and ω is the exponent of matrix multiplication. The soft-$\mathcal{O}$ notation indicates that logarithmic factors in the big-$\mathcal{O}$ are omitted while the ceiling function indicates that the cost is $\widetilde{\mathcal{O}}(n^\omega)$ when $s = o(1)$. Our algorithms are based on a fast and deterministic triangularization method for computing the diagonal entries of the Hermite form of a nonsingular matrix.

1. Introduction

For a given nonsingular polynomial matrix $\mathbf{A}$ in $\mathbb{K}[x]^{n\times n}$, one can find a unimodular matrix $\mathbf{U} \in \mathbb{K}[x]^{n\times n}$ such that $\mathbf{AU} = \mathbf{H}$ is triangular. Unimodular means that there is a polynomial inverse matrix, or equivalently, the determinant is a nonzero constant from $\mathbb{K}$. Triangularizing a matrix is useful for solving linear systems and computing matrix operations such as determinants or normal forms. In the

☆ Communicated by L. Pardo.

* Corresponding author.
E-mail addresses: glabahn@uwaterloo.ca (G. Labahn), vincent.neiger@ens-lyon.fr (V. Neiger), w2zhou@uwaterloo.ca (W. Zhou).

http://dx.doi.org/10.1016/j.jco.2017.03.003
0885-064X/

latter case, the best-known example is the Hermite normal form, first defined by Hermite in 1851 in the context of triangularizing integer matrices [17]. Here,

$$\mathbf{H} = \begin{bmatrix} h_{11} & & & \\ h_{21} & h_{22} & & \\ \vdots & \vdots & \ddots & \\ h_{n1} & \cdots & \cdots & h_{nn} \end{bmatrix}$$

with the added properties that each h_{ii} is monic and $\deg(h_{ij}) < \deg(h_{ii})$ for all $j < i$. Classical variations of this definition include specifying upper rather than lower triangular forms, and specifying row rather than column forms. In the latter case, the unimodular matrix multiplies on the left rather than the right, and the degree of the diagonal entries dominates that of their columns rather than their rows.

The goal of this paper is the fast, deterministic computation of the determinant and Hermite normal form of a nonsingular polynomial matrix. The common ingredient in both algorithms is a method for the fast computation of the diagonal entries of a matrix triangularization. The product of these entries gives, at least up to a constant, the determinant while Hermite forms are determined from a given triangularization by reducing the remaining entries modulo the diagonal entries.

In the case of determinant computation, there has been a number of efforts directed to obtaining algorithms whose complexities are given in terms of exponents of matrix multiplication. Interestingly enough, in the case of matrices over a field, Bunch and Hopcroft [8] showed that if there exists an algorithm which multiplies $n \times n$ matrices in $\mathcal{O}(n^\omega)$ field operations for some ω, then there also exists an algorithm for computing the determinant with the same cost bound $\mathcal{O}(n^\omega)$. In the case of an arbitrary commutative ring or of the integers, fast determinant algorithms have been given by Kaltofen [21], Abbott et al. [1] and Kaltofen and Villard [22]. We refer the reader to the last named paper and the references therein for more details on efficient determinant computation of such matrices.

In the specific case of the determinant of a matrix of polynomials $\mathbf{A}$ with $\deg(\mathbf{A}) = d$, Storjohann [28] gave a recursive deterministic algorithm making use of fraction-free Gaussian elimination with a cost of $\widetilde{\mathcal{O}}(n^{\omega+1}d)$ operations. A deterministic $\mathcal{O}(n^3d^2)$ algorithm was later given by Mulders and Storjohann [25], modifying their algorithm for weak Popov form computation. Using low rank perturbations, Eberly et al. [11] gave a randomized determinant algorithm for integer matrices which can be adapted to be used with polynomial matrices using $\widetilde{\mathcal{O}}(n^{3.5}d)$ field operations. Storjohann [29] later used high order lifting to give a randomized algorithm which computes the determinant using $\widetilde{\mathcal{O}}(n^\omega d)$ field operations. The algorithm of Giorgi et al. [12] has a similar cost but only works on a class of generic input matrices, matrices that are well behaved in the computation.

Similarly there has been considerable progress in the efficient computation of the Hermite form of a polynomial matrix. Hafner and McCurley [16] and Iliopoulos [18] give algorithms with a complexity bound of $\widetilde{\mathcal{O}}(n^4d)$ operations from $\mathbb{K}$ where $d = \deg(\mathbf{A})$. They control the size of the matrices encountered during the computation by working modulo the determinant. Using matrix multiplication the algorithms of Hafner and McCurley [16], Storjohann and Labahn [32] and Villard [35] reduce the cost to $\widetilde{\mathcal{O}}(n^{\omega+1}d)$ operations where ω is the exponent of matrix multiplication. The algorithm of Storjohann and Labahn worked with integer matrices but the results directly carry over to polynomial matrices. Mulders and Storjohann [25] then gave an iterative algorithm having complexity $\mathcal{O}(n^3d^2)$, thus reducing the exponent of n but at the cost of increasing the exponent of d.

During the past two decades, there has been a goal to design algorithms that perform various $\mathbb{K}[x]$-linear algebra operations in about the time that it takes to multiply two polynomial matrices having the same dimension and degree as the input matrix, namely at a cost $\widetilde{\mathcal{O}}(n^\omega d)$. *Randomized* algorithms with such a cost already exist for a number of polynomial matrix problems, for example for linear system solving [29], Smith normal form computation [29], row reduction [12] and small nullspace bases computation [33]. In the case of polynomial matrix inversion, the randomized algorithm in [31] costs $\widetilde{\mathcal{O}}(n^3d)$, which is quasi-linear in the number of field elements used to represent the inverse. For Hermite form computation, Gupta and Storjohann [15] gave a randomized algorithm with expected cost $\widetilde{\mathcal{O}}(n^3d)$, later improved to $\widetilde{\mathcal{O}}(n^\omega d)$ in [13]. Their algorithm was the first to be both

Please cite this article in press as: G. Labahn, et al., Fast, deterministic computation of the Hermite normal form and determinant of a polynomial matrix, Journal of Complexity (2017), http://dx.doi.org/10.1016/j.jco.2017.03.003