Fast Algorithms for Rational Forms of Integer Matrices

Mark Giesbrecht[†]
Department of Computer Science
University of Manitoba
Winnipeg, Manitoba
Canada, R3T 3T6
email: mwg@cs.umanitoba.ca

Abstract

A Monte Carlo type probabilistic algorithm is presented for finding the Frobenius rational form $F \in \mathbb{Z}^{n\times n}$ of any $A \in \mathbb{Z}^{n\times n}$ which requires an expected number of $O(n^4(\log n + \|A\|)^2)$ bit operations using standard integer and matrix arithmetic (where $\|A\|$ is the largest absolute value of any entry of A). This improves dramatically on the fastest previously known algorithm, which requires $O(n^6 \log \|A\|)$ bit operations using fast integer arithmetic. We also give a Las Vegas type probabilistic algorithm which finds the Frobenius form F and a transition matrix $U \in \mathbb{Q}^{n\times n}$ such that $U^{-1}AU = F$ and requires an expected number of $O(n^5(\log n + \log \|A\|)^{5/2}$ bit operations. Finally, a Las Vegas algorithm for computing the rational Jordan form of an integer matrix is shown, which requires about the same number of bit operations as our algorithm to find the Frobenius form, plus the time required to factor the characteristic polynomial of that matrix.

1. Introduction

Computing a canonical or normal form of a matrix is a classical mathematical problem with many practical applications. In this paper we present new probabilistic algorithms for computing exactly the Frobenius and rational Jordan normal forms of an integer matrix which are substantially faster than those previously known. We show that the Frobenius form $F \in \mathbb{Z}^{n\times n}$ of any $A \in \mathbb{Z}^{n\times n}$ can be computed with an expected number of $O(n^4(\log n + \log \|A\|)^2)$ bit operations using standard integer and matrix arithmetic. This is the lowest cost we can reasonably hope for since the best known algorithm for $\det(A)$ requires this same number of operations, and $\det(A)$ is easily obtained from F. Our algorithm is probabilistic of the Monte Carlo type: it assumes the existence of a source of random bits and, for all but an exponentially small subset of these random inputs, a correct answer is produced. A Las Vegas type probabilistic algorithm (one which always produces the correct answer) is also given which finds F and a transition matrix $U \in \mathbb{Q}^{n\times n}$ such that $F = U^{-1}AU$ using an expected number of $O(n^5(\log n + \log \|A\|)^{5/2})$ bit operations. A homomorphic imaging scheme is employed in all our algorithms: we determine the solution modulo a set of small (single-precision), randomly selected primes and recover the integral solution using the Chinese remainder algorithm. Rational forms such as the Frobenius and Jordan forms are numerically extremely sensitive, and their computation lends itself to exact, as opposed to floating point, arithmetic. The price we pay for exact arithmetic is that integers encountered in the computation may be large, especially if we wish to find a transition matrix. We show how to use modular arithmetic to avoid much of the long integer arithmetic, and get the fastest algorithms we can reasonably expect for dense matrices.

A classical theorem of linear algebra states that any $n \times n$ matrix A over any field K is similar to a unique block diagonal matrix

$$F = \begin{pmatrix} \boxed{C_{f_1}} & & & 0 \\ & \boxed{C_{f_2}} & & \\ & & \ddots & \\ 0 & & & \boxed{C_{f_k}} \end{pmatrix} \in \mathsf{K}^{n\times n}, \qquad (1)$$

where each C_{f_i} is the companion matrix of some monic $f_i \in \mathsf{K}[x]$ for $1 \le i \le k$, and $f_i \mid f_{i-1}$ for $2 \le i \le k$. That is, there exists an invertible *transition matrix* $U \in \mathsf{K}^{n\times n}$ such that $F = U^{-1}AU$. Recall that the companion matrix C_g of a monic $g = \sum_{0\le j\le r} b_i x^i \in \mathsf{K}[x]$ has the form

$$C_g = \begin{pmatrix} 0 & & & 0 & -b_0 \\ 1 & \ddots & & & -b_1 \\ & \ddots & 0 & & \vdots \\ 0 & & 1 & & -b_{r-1} \end{pmatrix} \in \mathsf{K}^{r\times r}.$$

A matrix F with the above properties, called the *Frobenius form* of A, always exists and is unique. The polynomials $f_1, \ldots, f_k \in \mathsf{K}[x]$ are the *invariant factors* of A, and the product $f_1 \cdots f_k$ is A's characteristic polynomial, while f_1 is A's minimal polynomial. Two matrices are similar if and only if they have the same Frobenius form.

When $A \in \mathbb{Z}^{n\times n}$ the Frobenius form F of A is an integer matrix as well. This suggests a simple homomor-

[†]Research was supported in part by Natural Sciences and Engineering Research Council of Canada research grant OGP0155376

Appears in: Proceedings ISSAC'94, pp. 305-311
July 20-22, 1994, Oxford, UK

phic imaging or modular approach to computing $F \in \mathbb{Z}^{n\times n}$ from $A \in \mathbb{Z}^{n\times n}$. One unavoidable difficulty in computing F exactly is that the size of its entries can be quite large: $O(n(\log n + \log \|A\|))$ bits in general. A bigger problem is that the size of intermediate values encountered in any of the previously known non-modular algorithms, can be very large — $O(n^2(\log n + \log \|A\|))$ bits — as can be the entries of a transition matrix. The modular techniques proposed here are used to avoid some of these problems, but we must be very careful to eliminate *bad* primes, modulo which the Frobenius form has an entirely different block structure.

We first present a very fast Monte Carlo type probabilistic algorithm which requires an expected number of $O(n^4(\log n + \log \|A\|)^2)$ bit operations to find the Frobenius form $F \in \mathbb{Z}^{n\times n}$ of $A \in \mathbb{Z}^{n\times n}$. The algorithm first computes F modulo a set Λ of $s = \Theta(n(\log n + \log \|A\|)/\ell)$ randomly selected primes between $2^{\ell-1}$ and 2^ℓ, where $\ell = \Theta(\log n + \log\log \|A\|)$ (we think of ℓ as the length of a word or short integer in bits and perform most of the arithmetic in our algorithms with integers of this length). We then recover F from its homomorphic images modulo these primes by Chinese remaindering. The difficulty lies in the fact that some of these primes are *bad* in the sense that the Frobenius form of A modulo p is not equal to F modulo p. Examples of this occur when $p \mid \det(A)$ when A is non-singular, or more subtly, when p divides the discriminant of the minimal polynomial of A. We show that the probability that *all* the primes we choose are bad is exponentially small, at most 2^{-s}, and as long as one good prime is selected, all bad primes can be identified and discarded. We assume in this cost analysis that "standard" arithmetic is used for this algorithm, that is, that two n bit integers can be multiplied with $O(n^2)$ bit operations, and two $n\times n$ matrices over a ring can be multiplied with $O(n^3)$ ring operations. To compute the Frobenius form of A modulo a prime p we employ the fast Las Vegas algorithm of Giesbrecht (1994), which computes the Frobenius form of A mod p with about the same number of operations as is required to multiply two $n \times n$ matrices, in this paper $O(n^3)$ operations in $\mathbb{Z}/(p)$. It is occasionally convenient, especially in summarizing results, to ignore logarithmic factors using the "soft O" notation: for any $g, h: \mathbb{R}_{>0} \to \mathbb{R}_{>0}$, $g = \tilde{O}(h)$ if and only if there exists a constant $k \geq 0$ such that $g = O(h(\log h)^k)$.

We can eliminate any possibility of error in computing F, and also compute a transition matrix $U \in \mathbb{Q}^{n\times n}$ such that $F = U^{-1}AU$ by working modulo a larger set of $O(n^2(\log n + \log \|A\|)/\ell)$ primes, where again $\ell = \Theta(\log n + \log\log \|A\|)$. This number of primes is necessary to compute U as its entries have $O(n^2(\log n + \log \|A\|))$ bits in general. We give a Las Vegas algorithm which requires an expected number of $O(n^5(\log n + \log \|A\|)\ell + n^4 \log^2 \|A\|^2)$ or $\tilde{O}(n^5 \log^2 \|A\|)$ bit operations using standard arithmetic. Entries in U will be represented modulo a basis of $\tilde{O}(n^2 \log \|A\|)$ primes. Recovery of the rational representation of U by the Chinese remainder algorithm requires $O(n^2 \mathrm{M}(n^2(\log n + \log \|A\|)) \cdot(\log n + \log \|A\|))$ or $\tilde{O}(n^2 \mathrm{M}(n^2 \log \|A\|))$ bit operations, where $\mathrm{M}(n)$ is the number of bit operations required to multiply two n-bit integers. Using standard integer arithmetic this requires $\tilde{O}(n^6 \log^2 \|A\|)$. However, for large integers such as these, faster multiplication algorithms are more efficient, such as Karatsuba & Ofman's (1962) which allows $\mathrm{M}(n) = n^{\log_2 3}$, or a 3-way generalization of this which gives $\mathrm{M}(n) = n^{\log_3 5} = O(n^{1.5})$. The latter allows us to recover U with $O(n^5(\log n + \log \|A\|)^{5/2})$ bit operations.

The Frobenius form is intimately related to the more common Jordan form of a matrix. It is well known that every matrix $A \in \mathsf{K}^{n\times n}$ over an algebraically closed field K is similar to it's Jordan form, a block diagonal matrix $J = \mathrm{diag}(J_1, \ldots, J_l)$, unique up to the order of the blocks, where J_i $(1 \leq i \leq l)$ is a Jordan block having an eigenvalue of A on the diagonal and ones on the superdiagonal. Such a J does not exist when K does not contain the eigenvalues of A. A natural generalization which always exists is the *rational Jordan form*, a block diagonal form where the eigenvalues on the diagonal are replaced by the companion matrices of their minimal polynomials in $\mathsf{K}[x]$, and the ones on the super-diagonal are replaced by identity matrices of the appropriate size. Importantly, the rational Jordan form equals the usual Jordan form whenever the latter exists. The rational Jordan form $J \in \mathbb{Z}^{n\times n}$ of a matrix $A \in \mathbb{Z}^{n\times n}$ can be found with the same cost as computing the Frobenius form of A, given a complete factorization of A's characteristic polynomial. Finding this factorization is in fact the dominant cost in computing J, and requires $\tilde{O}(n^8(\log n + \log \|A\|)^3)$ bit operations using Schönhage's (1984) algorithm with standard arithmetic, or $\tilde{O}(n^{6+\epsilon}(\log n + \log \|A\|)^{2+\epsilon})$ bit operations with fast integer arithmetic. A transition matrix X to the rational Jordan form is somewhat more complicated to compute. We demonstrate a Las Vegas algorithm which finds the rational Jordan form J and a transition matrix X such that $X^{-1}AX = J$ which requires $O(n^5(\log n + \log \|A\|)\ell + n^4 \log^2 \|A\|)$ or $\tilde{O}(n^5 \log^2 \|A\|)$ bit operations using standard arithmetic. As with the computation of the Frobenius form, within this time we can only represent the transition matrix with respect to a basis of primes, unless faster integer arithmetic is used in the Chinese remainder algorithm.

Previous Work on Computing Rational Forms

Deterministic sequential algorithms for computing the Frobenius form $F \in \mathbb{Z}^{n\times n}$ of an integer matrix $A \in \mathbb{Z}^{n\times n}$ have been proposed by Kannan (1985), Ozello (1987a), Lüneburg (1987), and Mathieu & Ford (1990). The elegant p-adic lifting algorithm of Mathieu & Ford (1990) requires $\tilde{O}(n^6 \log n(\log n + \log \|A\|))$ bit operations using fast integer arithmetic (under an unproven but experimentally justified assumption, which is most certainly true with high probability). Their algorithm does not compute a transition matrix U to F within this time. Ozello (1987a) proposes an algorithm which makes extensive use of large integers for computing the Frobenius form F of an integer matrix A and a transition matrix to F, which requires $\tilde{O}(n^8 \log^2 \|A\|)$ bit operations. Ozello also proposes a modular algorithm to compute the Frobenius form but no transition matrix. While this algorithm is not analyzed, it appears to require $\tilde{O}(n^5 \log^2 \|A\|)$ bit operations using standard arithmetic. However, Ozello does not address the question of choosing *good* primes p modulo which the Frobenius form of A mod p equals F mod p. Part of our contribution here is to show how to identify these good primes quickly. Ozello (1987b) also proposes a probabilistic algorithm, but the estimate of the probability of success is insufficient to prove a lower expected cost. Kaltofen *et al.* 1987, 1990 demonstrate fast parallel algorithms for computing the Frobenius and rational Jordan forms of matrices over abstract fields, finite fields and the rationals. While these algorithms are not particularly fast sequentially, we employ some of the techniques developed here in our fast sequential algorithms.

The fastest previously published algorithm for computing exactly the Jordan canonical form of $A \in \mathbb{Z}^{n\times n}$ is by

Gil 1992, 1993 and requires $O^{\sim}(n^9 \log^2 \|A\|)$ bit operations. It appears that a careful implementation of Kaltofen *et al.* (1990)'s parallel algorithm for the rational Jordan form requires an expected number of $O^{\sim}(n^7 \log^2 \|A\|)$ bit operations, plus the cost of factoring the characteristic polynomial. The main drawback to computing the rational Jordan form of A, both in practice and asymptotically, is that A's characteristic polynomial must be factored completely over $\mathbb{Z}[x]$. One alternative is to compute the symbolic Jordan form (see Kaltofen *et al.* 1990, Section 5, and Gómez-Díaz 1994). This looks like the usual Jordan form, where the diagonal elements contain symbols which represent eigenvalues as roots of not necessarily irreducible polynomials, and the superdiagonal contains either zeros or ones. The idea is to find the finest possible partial factorization of the invariant factors $f_1, \ldots, f_k \in \mathbb{Z}[x]$ using only GCD's and squarefree factorizations, and then to use symbolic roots of the obtained factors to represent eigenvalues. Of course, one such symbol could represent a number of (possibly non-conjugate) roots. A corresponding block-diagonal rational form of A consists of the companion matrices of these refined factors on the diagonal, and possibly identity blocks on the superdiagonal.

Considerable attention has been paid in the numerical literature to approximating the Jordan form with floating point arithmetic; see (Golub & Van Loan, 1989), though the numerical sensitivity of the problem has led to concentration on less sensitive (but less informative) rational forms, such as the real Schur form.

2. Computing the Frobenius form over an arbitrary field

In this section we briefly summarize the Las Vegas type probabilistic algorithm presented formally in (Giesbrecht 1994; see also Giesbrecht 1993) for computing the Frobenius form $F \in \mathsf{K}^{n\times n}$ of a matrix $A \in \mathsf{K}^{n\times n}$ over any field K, and a $U \in \mathsf{K}^{n\times n}$ such that $F = U^{-1}TU$. This algorithm requires an expected number of $O(\mathrm{MM}(n)\log n)$ operations in K, where $\mathrm{MM}(n)$ operations are sufficient to multiply two $n \times n$ matrices over K. In this section we will assume that K is a field with at least n^2 elements. Over such a K the aforementioned Frobenius form algorithm requires an expected number of $O(n^3)$ operations in K using standard polynomial and matrix arithmetic (see Giesbrecht 1993, Section 3.1).

The algorithm begins by finding a matrix $H \in \mathsf{K}^{n\times n}$ as follows. Vectors $w_1, \ldots, w_n$ are chosen uniformly and randomly from $L^{n\times 1}$, where L is any subset of K with $\#L \geq n^2$. We then compute

$$H = \left[w_1 | Tw_1 | \cdots | T^{d_1-1}w_1 | \cdots | w_n | \cdots | T^{d_n-1}w_n\right] \qquad (2)$$

where $d_1, \ldots, d_n$ are defined such that d_i is the minimum integer with $T^{d_i}w_i$ linearly dependent upon the vectors w_1, $Tw_1, \ldots, Tw_i, \ldots, T^{d_i-1}w_i$ to the left of it. Clearly some of the d_i's may be zero, and we let k be the smallest integer such that $d_{k+1} = \ldots = d_n = 0$. It is relatively easy to show that if H is non-singular then

$$G = H^{-1}TH = \begin{pmatrix} C_{\bar{f}_1} & B_2 & \cdots & B_k \\ & C_{\bar{f}_2} & & \\ & & \ddots & \\ \multicolumn{2}{c}{0} & & C_{\bar{f}_k} \end{pmatrix} \qquad (3)$$

where $C_{\bar{f}_i} \in \mathsf{K}^{d_i\times d_i}$ is the companion matrix of some $\bar{f}_i \in \mathsf{K}[x]$ of degree d_i (for $1 \leq i \leq k$). Each matrix B_i is zero except for its last column. If H is singular then we made an unlucky choice of $w_1, \ldots, w_n$, and in fact the last column of H must be all zeroes. This is essentially a randomized version of Danilevsky's (1937) algorithm for the characteristic polynomial of a matrix and we always have $f = \bar{f}_1 \cdots \bar{f}_k = \mathrm{char}(A) \in \mathsf{K}[x]$. G and H can be computed with $O(n^3)$ operations in K in a straightforward manner. This can also be accomplished with $O(\mathrm{MM}(n)\log n)$ operations in K using Keller-Gehrig's (1985) asymptotically fast version of Danilevsky's algorithm.

Theorem 1 (Giesbrecht 1994, Theorem 2.2). *Let K be a field and L a subset of K of size at least n^2. For randomly selected $w_1, \ldots w_n \in L^{n\times 1}$ and polynomials $\bar{f}_1, \ldots, \bar{f}_k$ from G above, with probability at least $1/4$ the Frobenius form of A is $F = \mathrm{diag}(C_{\bar{f}_1}, C_{\bar{f}_2}, \ldots, C_{\bar{f}_k})$.*

Proof. (sketch) We first show that for randomly selected $w_1 \in L^{n\times 1}$, the probability that the minimal polynomial $\bar{f}_1$ of the linearly recurring sequence $w_1, Aw_1, A^2w_1, \ldots$ equals f_1 is at least $1 - 1/n$. This is accomplished by proving that there exists an $h_1 \in \mathsf{K}[x_1, \ldots, x_n] \setminus \{0\}$ of degree at most n such that $h_1(w_1) \neq 0$ implies $f_1 = \bar{f}_1$. We then apply Corollary 1 of Schwartz (1980) to obtain the desired probability estimate.

Now let W_j be the vector space generated by $w_1, \ldots, w_j$ under left multiplication by A for $1 \leq j \leq k$. For $i > 1$ we show that there exists an $h_i \in \mathsf{K}[x_1, \ldots, x_n] \setminus \{0\}$ (dependent upon the choices of $w_1, \ldots, w_{i-1}$) such that $h_i(w_i) \neq 0$ implies that the minimal polynomial $\bar{f}_i \in \mathsf{K}[x]$ of the linearly recurring sequence

$$(w_i \bmod W_{i-1}), (Aw_i \bmod W_{i-1}), (A^2w_i \bmod W_{i-1}), \ldots \in \mathsf{K}^{n\times 1}/W_{i-1}$$

equals f_i (assuming $\bar{f}_1, \ldots, \bar{f}_{i-1}$ are correct). The companion of $\bar{f}_i$ is the ith block on the diagonal of G. This yields f_i with probability at least $1 - 1/n$, and we obtain all of $f_1, \ldots, f_k$ correctly with probability at least $(1 - 1/n)^n \geq 1/4$. □

We call a matrix $G \in \mathsf{K}^{n\times n}$ as above, such that the companion blocks on G's diagonal are the companion blocks on the diagonal of the Frobenius form of A a *modular Frobenius form* of A. The following characterization of when a set $w_1, \ldots, w_n \in \mathsf{K}^{n\times 1}$ generate an H with $H^{-1}AH$ in modular Frobenius form will be useful in the sequel.

Fact 2 (Giesbrecht 1993). *Let H be as in (2) such that $H^{-1}AH$ has blocks $C_{\bar{f}_1}, C_{\bar{f}_2}, \ldots, C_{\bar{f}_k}$ on the diagonal, with $d_i = \deg \bar{f}_i$ for $1 \leq i \leq k$. Then A has Frobenius form*

$\mathrm{diag}(C_{\bar{f}_1}, C_{\bar{f}_2}, \ldots, C_{\bar{f}_k})$ *if and only if for* $i = 1, 2, \ldots, k$ *in sequence, for all* $w \in \mathsf{K}^{n\times 1}$, $A^{d_i}w$ *is linearly dependent upon*

$$w_1, \ \ldots, A^{d_1-1}w_1, \ldots, w_{i-1}, \ldots, A^{d_{i-1}-1}w_{i-1}, w, Aw, \ldots, A^{d_i-1}w.$$

In other words, d_i *is maximal given* $w_1, \ldots, w_{i-1}$.

Of course, the procedure described above to compute the Frobenius form does not yield a matrix $U \in \mathsf{K}^{n\times n}$ with $S = \mathrm{diag}(C_{\bar{f}_1}, \ldots, C_{\bar{f}_k}) = U^{-1}AU$. It may also happen that S is not the Frobenius form of A at all, in which case no such U will exist. We next sketch a purification procedure, derived from a constructive proof for the existence of the Frobenius form (see, for example, Hoffman & Kunze 1971, Theorem 7.2.3) which will find $U \in \mathsf{K}^{n\times n}$ with $U^{-1}AU = F$. This procedure will also determine if indeed S is the Frobenius form of A.

Assume that H is non-singular and that the last column of each matrix B_i above is

$$\bar{b}_i = (b_{i,1,0}, \ldots, b_{i,1,d_1-1}, \ldots, b_{i,i-1,0}, \ldots, b_{i,i-1,d_{i-1}-1})^t \in \mathsf{K}^{t_i\times 1},$$

where $b_{ijl} \in \mathsf{K}$ for $2 \le i \le k$, $1 \le j < i$, and $0 \le l < d_j$. For $1 < j \le i \le k$, suppose $g_{ij} = \sum_{0\le l<d_j} b_{ijl}x^l$, for $b_{ijl} \in \mathsf{K}$.

Fact 3 (Giesbrecht 1993, Theorem 2.10). *Let* $w_i \in \mathsf{K}^{n\times 1}$, $\bar{f}_i \in \mathsf{K}[x]$ *and* g_{ij} *for* $1 \le i \le k$ *and* $1 \le j < i$ *be as above. Then* $S = \mathrm{diag}(C_{\bar{f}_1}, \ldots, C_{\bar{f}_k})$ *is the Frobenius form of* A *if and only if* $f_i \mid g_{ij}$ *for all* i, j *with* $1 \le j < i \le k$. *Moreover, if we let* $g_{ij} = f_i h_{ij}$ *for* $1 \le j < i \le k$, *and*

$$v_i = w_i - \sum_{1\le j<i} h_{ij}(T)w_i$$

for $1 \le i \le k$, *and*

$$U = \left[v_1|Av_1|\cdots|A^{d_1-1}v_1|\cdots|v_k|\cdots|A^{d_n-1}v_k\right] \in \mathsf{K}^{n\times n},$$

then $F = U^{-1}AU$ *is the Frobenius form of* A.

Computationally, it is straightforward to check whether $f_i \mid g_{ij}$ for $1 \le j < i \le k$ with $O(n\mathrm{M}(n))$ or $O(n^3)$ operations in K (in fact, if we are working modulo a prime p such that $2^m \mid p-1$ with $2^m > 2n-2$ then we may assume $\mathrm{M}(n) = n\log n$, using a practical implementation of the fast Fourier transform). To find $v_1, \ldots, v_k$ efficiently we first write $h_{ij} = g_{ij}/f_i = \sum_{0\le l<d_j} c_{ijl}x^l$ for $1 \le j < i \le k$ and note that $v_i = H\bar{v}_i$, where

$$\bar{v}_i = (-c_{i,1,0}, \ \ldots, -c_{i,1,d_1-1}, \ldots, -c_{i,i-1,0}, \ldots, -c_{i,i-1,d_{i-1}}, 1, 0, \ldots, 0)^t \in \mathsf{K}^{n\times 1},$$

with $\bar{v}_1 = (1, 0, \ldots, 0)$. All of $v_1, \ldots, v_k$ can now be computed with a single matrix product $H\cdot[\bar{v}_1|\cdots|\bar{v}_k]$ with $O(n^3)$ operations in K.

To execute this algorithm we simply run it with different random choices of $w_1, \ldots, w_n \in \mathsf{K}^{n\times 1}$ until it successfully completes. By Fact 1, an expected number of at most 4 attempts is required.

Theorem 4. *Let* $A \in \mathsf{K}^{n\times n}$ *where* $\#\mathsf{K} > n^2$. *The Las Vegas algorithm described above computes the Frobenius form* $F \in \mathsf{K}^{n\times n}$ *of* A *and a matrix* U *such that* $A = U^{-1}TU$ *with an expected number of* $O(n^3)$ *operations in* K *using standard matrix and polynomial arithmetic.*

3. Computing the Frobenius form over the rationals

We now examine the application of the algorithm in Section 2 to computing the Frobenius form $F \in \mathbb{Z}^{n\times n}$ of a matrix $A \in \mathbb{Z}^{n\times n}$. As discussed in the introduction, we find F by first computing $F_p \in \mathbb{Z}_p^{n\times n}$ of A mod p over $\mathbb{Z}_p$ for a set Λ of small primes p. We hope that for a sufficiently large number of these primes that $F_p = F \bmod p$; we call these *good* primes. From the set of good primes we recover F by the Chinese remainder algorithm. In this section we give a condition for which primes are potentially *bad* (that is $F_p \not\equiv F \bmod p$), show how to identify these bad primes, and prove an upper bound on the number of bad primes. We then employ these ideas in probabilistic algorithms for computing F and a transition matrix U such that $F = U^{-1}TU$.

First consider running the algorithm discussed in Section 2 over $\mathbb{Q}$ directly (it works for any field). Let $L = \{0, \ldots, n^2\}$ and choose random $w_1, \ldots, w_n \in L^{n\times 1}$. Then compute H as in (2) and $G = H^{-1}AH$ as in (3). By Fact 1, with probability at least 1/4 the blocks $C_{\bar{f}_1}, \ldots, C_{\bar{f}_k}$ on the diagonal of G are such that $F = \mathrm{diag}(C_{\bar{f}_1}, \ldots, C_{\bar{f}_k})$ is the Frobenius form of A. Assume that this is the case and let p be a prime such that $\det(H) \not\equiv 0 \bmod p$, so $H_p = H \bmod p$ is invertible in $\mathbb{Z}_p^{n\times n}$. Then if $G = H^{-1}AH$ has blocks $C_{\bar{f}_1}, \ldots, C_{\bar{f}_k}$ on the diagonal, we know $H_p^{-1}(A \bmod p)H_p \in \mathbb{Z}_p^{n\times n}$ has blocks $C_{\bar{f}_1} \bmod p, \ldots, C_{\bar{f}_k} \bmod p$ on its diagonal. Also by Fact 2, in H we know $w_i \in \mathsf{K}^{n\times 1}$ is such that $[w_1|\cdots|A^{d_1-1}w_1|\cdots|w_i|Aw_i\cdots|A^{d_i-1}w_i]$ has maximum rank. But the rank of this matrix modulo p is at most its rank in $\mathbb{Q}$. Thus, by Fact 2 we know that $\mathrm{diag}(C_{\bar{f}_1} \bmod p, \ldots, C_{\bar{f}_k} \bmod p) \in \mathbb{Z}_p^{n\times n}$ is the Frobenius form of A_p over $\mathbb{Z}_p$ and p is a good prime. In particular, the degree d_i of the ith invariant factor $\bar{f}_i$ of A equals the degree $d_i^{(p)}$ of the ith invariant factor of A mod p over $\mathbb{Z}_p$.

On the other hand, if p divides $\det(H)$ for *all* $H \in \mathbb{Z}^{n\times n}$ such that $H^{-1}AH$ is in modular Frobenius form, it must be the case that for some minimal $i \ge 1$, for all $w_1, \ldots, w_i \in \mathbb{Z}^{n\times 1}$ with $w_1, Aw_1, \ldots, A^{d_1-1}w_1, \ldots, w_i, \ldots, A^{d_i-1}w_i$ linearly independent over $\mathbb{Q}$, these same vectors are linearly dependent modulo p. In this case the degree $d_i^{(p)}$ of the ith invariant factor of A mod p is strictly less than the degree d_i of the ith invariant factor of A. We obtain the following:

Lemma 5. *Let* $A \in \mathbb{Z}^{n\times n}$ *have Frobenius form* F *as in (1), and suppose the* i*th invariant factor of* A *has degree* d_i *for* $1 \le i \le k$. *If* p *is a bad prime such that the Frobenius form* F_p *of* $A_p = A \bmod p \in \mathbb{Z}_p^{n\times n}$ *does not satisfy* $F_p \equiv F \bmod p$, *and the degree of the* i*th invariant factor of* A_p *is* $d_i^{(p)}$ *for* $1 \le i \le l$, *then* $(d_1, \ldots, d_k)$ *is lexicographically larger than* $(d_1^{(p)}, \ldots, d_l^{(p)})$.

A similar lemma to the above, for Smith normal forms of matrices of polynomials, is shown by Kaltofen *et al.* (1987), Lemma 4.1. Now we have a criteria for rejecting bad primes assuming we have one good prime: the degree sequence $(d_1^{(p)}, \ldots, d_k^{(p)})$ of the invariant factors of A modulo a good prime p will be lexicographically greater than the degree sequence of A modulo a bad prime p.

How many good primes do we need to recover the Frobenius form of A? The following fact is derived from (Mathieu & Ford, 1990).

Fact 6. *Let* $A \in \mathbb{Z}^{n\times n}$ *and* $F \in \mathbb{Z}^{n\times n}$ *its Frobenius form. Then* $\|F\| \le 2^n e^{n/2}\|A\|^n n^{n/2}$.

Thus we require at least $2\log_2(2^n e^{n/2}\|A\|^n n^{n/2})/(\ell - 1) = O(n(\log n + \log\|A\|)/\ell)$ primes between $2^{\ell-1}$ and 2^ℓ

to uniquely represent F by its images modulo these primes (the initial factor of 2 allows us to recover both positive and negative integers in F).

A Monte Carlo algorithm for the integer Frobenius form

To compute the Frobenius form, allowing an exponentially small probability of error, we first choose s random primes p (where s and the selection interval are defined below) and compute the Frobenius form $F_p \in \mathbb{Z}_p^{n\times n}$ of $A_p = A \bmod p$ using the Las Vegas algorithm of Section 2. Note that we randomly choose vectors $w_1, \ldots, w_n \in \mathbb{Z}_p^{n\times 1}$ independently for each prime p. Let p_0 be a chosen prime modulo which the Frobenius form F_{p_0} of $A \bmod p_0$ has the lexicographically largest degree sequence (p_0 will probably not be unique). We now bound the probability that p_0 is bad. Recall that p_0 is bad if and only if $p_0 \mid \det(H)$ for all H such that $H^{-1}AH$ is in modular Frobenius form. Using Hadamard's bound it is easily derived that for H constructed from $w_1, \ldots, w_n \in \{0, \ldots, n^2\}^{n\times 1}$ as in (2) above we have $|\det(H)| \le \delta = 2^{n/2}\|A\|^{n^2-n}n^{n^2+n}$. Now fix $\ell = 6 + \log\log\delta = \Theta(\log n + \log\log\|A\|)$. We will do all our computation modulo primes with ℓ bits. The following fact guarantees there are enough primes between $2^{\ell-1}$ and 2^ℓ (it follows easily from the bounds on number-theoretic functions of Rosser & Schoenfeld 1962):

Lemma 7 (Giesbrecht 1993, Theorem 1.8). *Let $x \ge 3$ and $\ell = 6 + \log\log x$. There exist at least $2\lceil\lceil\log_2(2x)\rceil/(\ell-1)\rceil$ primes p such that $2^{\ell-1} < p < 2^\ell$.*

An application of this lemma reveals that the product of all primes between $2^{\ell-1}$ and 2^ℓ is greater than δ^2 and hence greater than $|\det(H)|^2$. In particular, the probability of choosing a bad prime between $2^{\ell-1}$ and 2^ℓ is at most $1/2$. Setting $s = \log_2(2^n e^{n/2}\|A\|^n n^{n/2})/(\ell-1) = \Omega(n(\log n + \log\|A\|))$, the probability of choosing s bad primes is at most $1/2^s$. As noted above, we require s good primes between $2^{\ell-1}$ and 2^ℓ to recover F from its homomorphic images. Moreover, by Lemma 7 there are more than enough good primes between $2^{\ell-1}$ and 2^ℓ to recover F correctly.

We then proceed as follows. Choose a set Λ_0 of s primes randomly between $2^{\ell-1}$ and 2^ℓ and compute the Frobenius form F_p of $A \bmod p$ for each $p \in \Lambda_0$. Let $\Lambda_1 \subseteq \Lambda_0$ be those $p \in \Lambda_0$ modulo which the invariant factors of $A \bmod p$ have maximal degree sequence $(d_1, \ldots, d_k)$ of those degree sequences of Frobenius forms of $A \bmod p$ for $p \in \Lambda_0$. We now assume (correctly with probability $1 - 1/2^s$) that Λ_1 contains only good primes. We let $\Lambda = \Lambda_1$ initially and proceed to supplement it with more good primes until $\#\Lambda = s$: keep selecting random primes $p \notin \Lambda_0$ between $2^{\ell-1}$ and 2^ℓ and computing the Frobenius form F_p of $A \bmod p$, adding them to Λ if the degree sequence of the invariant factors equals $(d_1, \ldots, d_k)$. If we find a degree sequence lexicographically greater than $(d_1, \ldots, d_k)$ we were unlucky with our original construction of Λ_1 and must start over, but this happens with probability at most $1/2^s$.

Once we have computed F_p for the s good primes $p \in \Lambda$, we can recover $F \in \mathbb{Z}^{n\times n}$ by the Chinese remainder algorithm. This requires $O(n^2\mathrm{M}(n(\log n + \log\|A\|)))$ bit operations. We obtain the following theorem:

Theorem 8. *Let $A \in \mathbb{Z}^{n\times n}$. The Monte Carlo type probabilistic algorithm described above computes the Frobenius form $F \in \mathbb{Z}^{n\times n}$ of A with an expected number of $O(n^4(\log n + \log\|A\|)^2)$ bit operations using standard arithmetic. The probability of producing an erroneous result is at most $1/2^s$ where $s = \Omega(n(\log n + \log\|A\|))$.*

We consider the computation of a set of $2s$ primes between $2^{\ell-1}$ and 2^ℓ to be pre-computation but note that they can be extremely quickly using standard sieving methods: see (Knuth 1981, Section 4.5.4).

A Las Vegas algorithm for the integer Frobenius form

To eliminate all possibility of error in the computation of the Frobenius form we must ensure that we have selected at least one good prime in our initial set Λ_0 above. The obvious way to do this is to let Λ_0 contain more primes than can possibly divide $\det(H)$, for some $H \in \mathbb{Z}^{n\times n}$ with $G = H^{-1}AH$ a modular Frobenius form of A. Equation (2) exhibits an H with $|\det(H)| < \delta = 2^{n/2}\|A\|^{n^2-n}n^{n^2+n}$, so we require $\lceil\log_2\delta/(\ell-1)\rceil = \Omega(n^2(\log n + \log\|A\|)/\ell)$ primes between $2^{\ell-1}$ and 2^ℓ. When $\ell = 6 + \log\log\delta$ it is guaranteed by Lemma 7 that sufficiently many primes exist in this range. After computing the Frobenius form F_p for each p in this expanded Λ_0 we are guaranteed to get at least one good prime p, and the algorithm can proceed as in the Monte Carlo algorithm above with no possibility of erroneous output.

Theorem 9. *Let $A \in \mathbb{Z}^{n\times n}$. The Las Vegas type probabilistic algorithm described above computes the Frobenius form $F \in \mathbb{Z}^{n\times n}$ of A with an expected number of $O(n^5(\log n + \log\|A\|)^2)$ bit operations.*

Computing transition matrices to the Frobenius Form

Assume now that we have computed and verified correctness of the Frobenius form $F \in \mathbb{Z}^{n\times n}$ of $A \in \mathbb{Z}^{n\times n}$, and wish to compute a matrix $U \in \mathbb{Q}^{n\times n}$ such that $F = U^{-1}AU$. Consider once again the algorithm from Section 2 as run over $\mathbb{Q}$. The following theorem is easily demonstrated (see Giesbrecht 1993, Theorem 4.3).

Theorem 10. *Fix $L = \{0, \ldots, n^2\}$ and randomly choose $w_1, \ldots, w_n \in L^{n\times 1}$ and compute H as in (2). If U is constructed as in the algorithm in Section 2 then $\det(H)U \in \mathbb{Z}^{n\times n}$ and*

$$\|\det(H)U\| < \gamma = 2^{n^2+3n/2}e^{n^2/2}\|A\|^{2n^2+n+1}n^{3n^2/2+3n+3}.$$

In particular if we represent entries in U by relatively prime pairs of integers, then all the denominators divide $\det(H)$ and all numerators have absolute value less than γ. We can represent all such rational numbers uniquely modulo a set Λ of primes with product $2\gamma\delta$, where $\delta = 2^{n/2}\|A\|^{n^2-n}n^{n^2+n} \ge |\det(H)|$. By the techniques described above we construct a set Λ_0 of good primes between $2^{\ell-1}$ and 2^ℓ with product at least $2\gamma\delta^2$ (the need for the additional factor of δ is discussed below). Good primes are now easy to determine since we know the Frobenius form of A and hence know the correct degree sequence $(d_1, \ldots, d_k)$ of the invariant factors. A total of $\lceil\lceil\log_2 2\gamma\delta^2\rceil/(\ell-1)\rceil$ such primes are required in Λ_0, and if we set $\ell = 6 + \log\log(2\gamma\delta^2) = \Theta(\log n + \log\log\|A\|)$ we are guaranteed by Lemma 7 that there are enough good primes.

In the Las Vegas and Monte Carlo algorithms above for F, for each prime p we chose the vectors $w_1, \ldots, w_n \in \mathbb{Z}_p^{n\times 1}$ independently. Here we choose vectors $w_1, \ldots, w_n \in L^{n\times 1}$ and in the computation modulo p use $(w_1 \bmod p), \ldots, (w_n \bmod p)$. With probability at least $1/4$ our selection of $w_1, \ldots, w_n$ will generate an $H \in \mathbb{Z}^{n\times n}$ as in (2) such that

$H^{-1}AH$ is in modular Frobenius form. If it does not, then this will be identified modulo *all* the primes in Λ. If $H^{-1}AH$ is in modular Frobenius form then for every $p \in \Lambda_0$ such that $p \nmid \det(H)$ we can construct the matrix $U_p \in \mathbb{Z}_p^{n\times n}$ such that $U_p^{-1}AU_p \equiv F \bmod p$ using the algorithm of section 2. Note that the matrix $U \in \mathbb{Q}^{n\times n}$ constructed by the Frobenius form algorithm in Section 2 run over $\mathbb{Q}$ is uniquely determined from A and H, and in fact its entries are fixed rational functions in the entries of A and H. Thus for all $p \in \Lambda = \{q \in \Lambda : q \nmid \det(H)\}$ we have $U \equiv U_p \bmod p$. Since the primes dividing $\det(H)$ have product at most δ, the product of primes in Λ is at least $2\gamma\delta$ and we can recover all entries of U uniquely from their images modulo the primes in Λ.

As discussed in the introduction, using the Chinese remainder algorithm to recover the n^2 entries of U requires $O(n^2\,\mathrm{M}(n^2(\log n + \log\|A\|))(\log n + \log\|A\|))$ bit operations. This is prohibitive using standard integer arithmetic, but for integers of this length it is reasonable to assume that fast integer arithmetic is more efficient and we make the assumption that $\mathrm{M}(n) = O(n^{1.5})$.

Theorem 11. *Let $A \in \mathbb{Z}^{n\times n}$. The Las Vegas algorithm discussed above to compute the Frobenius form $F \in \mathbb{Z}^{n\times n}$ of A and a transition matrix $U \in \mathbb{Q}^{n\times n}$ such that $U^{-1}AU = F$ requires an expected number of $O(n^5(\log n + \log\|A\|)^{5/2})$ bit operations.*

4. Computing the rational Jordan form of an integer matrix

The rational Jordan form $J \in \mathbb{Z}^{n\times n}$ of a matrix $A \in \mathbb{Z}^{n\times n}$ is a generalization of the usual Jordan form. For any monic polynomial $g \in \mathbb{Z}[x]$ of degree r and any $m > 0$, define the *rational Jordan block* $J_g^{(m)} \in \mathbb{Z}^{mr\times mr}$ as

$$J_g^{(m)} = \begin{pmatrix} \boxed{C_g}\boxed{I_r} & & 0 \\ & \ddots & \ddots \\ & & \boxed{I_r} \\ 0 & & \boxed{C_g} \end{pmatrix} \in \mathbb{Z}^{mr\times mr}, \qquad (4)$$

where I_r is the $r\times r$ identity and C_g is the companion matrix of g. It is known (see Kaltofen *et al.* 1990) that every matrix $A \in \mathbb{Z}^{n\times n}$ is similar to a unique (up to the order of the blocks)

$$J = \mathrm{diag}(J_{g_1}^{(m_{11})}, \ldots, J_{g_1}^{(m_{1k})}, \ldots, J_{g_l}^{(m_{l1})}, \ldots, J_{g_l}^{m_(lk)}) \in \mathbb{Z}^{n\times n}$$

where $g_1, \ldots, g_l \in \mathbb{Z}[x]$ are the distinct, monic irreducible divisors of the characteristic polynomial $f \in \mathbb{Z}[x]$ of A and m_{ij} is the largest power of g_i which divides the ith invariant factor f_i of A. Thus, for any matrix $A \in \mathbb{Z}^{n\times n}$, given the Frobenius form $F \in \mathbb{Z}^{n\times n}$ and the complete factorization of the characteristic polynomial of $A \in \mathbb{Z}[x]$, we can determine the rational Jordan form immediately. Factoring the characteristic polynomial is *necessary* in this computation, since we can read off its factorization from the rational Jordan form of its companion matrix.

To construct a transition matrix $X \in \mathbb{Q}^{n\times n}$ such that $J = X^{-1}AX$ we really only need construct a transition matrix from the Frobenius form F of A to J. This is accomplished in two stages. See Giesbrecht (1993), Section 5.3 for details. We first construct a transition matrix $Q \in \mathbb{Z}^{n\times n}$ from F to its *primary rational form* $P \in \mathbb{Z}^{n\times n}$. This is a block-diagonal matrix with the companion matrices of the elementary factors along the diagonal:

$$\begin{aligned} P &= Q^{-1}FQ = Q^{-1}U^{-1}AUQ \\ &= \mathrm{diag}(C_{g_1^{m_{11}}}, \ldots, C_{g_1^{m_{1k}}}, \ldots, C_{g_l^{m_{l1}}}, \ldots, C_{g_l^{m_{lk}}}) \in \mathbb{Z}^{n\times n}. \end{aligned}$$

Q's structure is very easy to describe and compute. We can assume without loss of generality that F has only one invariant factor $f \in \mathbb{Z}[x]$ (the companion block of each factor can be treated separately), and hence has primary form $P = \mathrm{diag}(C_{g_1^{m_1}}, \ldots, C_{g_l^{m_l}})$. Then if $h_i = f/g_i^{m_i}$ and $d_i = \deg g_i$ for $1 \le i \le l$ we have

$$Q = \left[\overrightarrow{h_1}|\overrightarrow{xh_1}|\cdots|\overrightarrow{x^{m_1d_1-1}h_1}|\cdots|\overrightarrow{h_l}|\cdots|\overrightarrow{x^{m_ld_l-1}h_l}\right]$$

where $\overrightarrow{h} = (c_0, c_1, \ldots, c_{n-1})^t \in \mathbb{Q}^{n\times 1}$ for any $h = c_0 + c_1x + \cdots c_{n-1}x^{n-1} \in \mathbb{Q}[x]$. Thus, the coefficients of Q are coefficients of factors of f, and by using Mignotte's (1974) bound on the sizes of factors of integer polynomials, it is derived they are bounded in absolute value by $\beta = 2^n e^{n/2}\|A\|^n n^{n/2}$, which is the same bound we had for the elements of A.

Once we have computed the primary rational form P of A, we find a transition matrix $T \in \mathbb{Z}^{n\times n}$ such that $J = T^{-1}PT$. Without loss of generality we may assume that $P = C_{g^m}$ where $g = \sum_{0\le i\le d} b_i x^i$ is monic of degree d. . Under the standard embedding of $\mathbb{Q}^{dm}$ into $\mathbb{Q}[x]/(g^m)$ our problem is equivalent to finding an ordered basis

$$\mathcal{B} = (h_{1,0}, \ldots, h_{1,d-1}, \ldots, h_{m,0}, \ldots, h_{m,d-1}) \in \left(\mathbb{Q}[x]/(g^m)\right)^{dm}$$

for $\mathbb{Q}[x]/(g^e)$ as a $\mathbb{Q}$-vector space, satisfying the following conditions:

$$\begin{aligned}
&\text{(i)} && xh_{1,j-1} \equiv h_{1,j} \bmod g^m && \text{for } 1 \le j < d, \\
&\text{(ii)} && xh_{1,d-1} \equiv -\sum_{0\le j<d} b_j h_{1,j} \bmod g^m, && \\
&\text{(iii)} && xh_{i,j-1} \equiv h_{i,j} + h_{i-1,j-1} \bmod g^m && \text{for } 2 \le i \le m \\
& && && \text{and } 1 \le j < d, \\
&\text{(iv)} && xh_{i,d-1} \equiv h_{i-1,d-1} - \sum_{0\le j\le d-1} b_j h_{i,j} && \bmod g^m \\
& && \text{for } 2 \le i \le m. &&
\end{aligned}$$

As a solution to this system of modular polynomial equations we assign

$$\begin{aligned}
h_{1,0} &= g^{m-1}, \\
h_{1,j} &= x^j g^{m-1}, && \text{for } 1 \le j < d, \\
h_{i,0} &= \left(\sum_{0\le j\le d}\sum_{0\le l\le j-1} b_j x^{j-l-1} h_{i-1,l}\right)/g && \text{for } 2 \le i \le m, \\
h_{i,j} &= x^j h_{i,0} - \sum_{0\le l\le j-1} x^{j-l-1} h_{i-1,l} && \text{for } 2 \le i \le m \\
& && && \text{and } 1 \le j < d,
\end{aligned}$$

and claim that $h_{i,0} \in \mathbb{Z}[x]$ for $1 \le i \le m$ (for details, see Giesbrecht (1993), Section 5.3). We then let

$$T = \left[\overrightarrow{h_{1,0}}|\cdots|\overrightarrow{h_{1,m-1}}|\cdots|\overrightarrow{h_{m,0}}|\cdots|\overrightarrow{h_{m,d-1}}\right]$$

Once again using Mignotte's (1974) bound, we obtain

$$\|T\| \le d^{dm-2}\beta^m n^{(m-1)/2} 2^{(m+1)(n+1)}.$$

An algorithm to compute the entries in T and Q is easily derived from the above systems, and this algorithm requires $O(n^3)$ integer operations. Morever, all the entries in Q and T are fixed polynomials in the entries of F, and hence can be computed modulo *any* set containing a sufficient number primes and recovered by the Chinese remainder algorithm without worry of "bad" primes. We summarize the sizes of the coefficients involved and the time required to compute Q and T in the following theorem:

Theorem 12. (Giesbrecht 1993, Lemmas 5.26, 5.27 and Theorem 5.28) *Let $A \in \mathbb{Z}^{n\times n}$ have Frobenius form $F \in \mathbb{Z}^{n\times n}$ and characteristic polynomial $f \in \mathbb{Z}[x]$.*

(i) Given F and the complete factorization in $\mathbb{Z}[x]$ of f we can find the rational Jordan form J of A with $O(n^3(\log n + \log \|A\|))$ additional bit operations.

(ii) There exists an $X \in \mathbb{Q}^{n\times n}$ such that $J = X^{-1}FX$ with $\|X\| \leq 2^{3n^2+3}e^{n^2+n/2}\|A\|^{4n^2+n}n^{3n^2+7n}$. Such an X can be constructed with an expected number of $O(n^5(\log n + \log \|A\|)\ell)$ bit operations from J and U.

5. Conclusion and Open Problems

We have demonstrated fast probabilistic algorithms for computing the Frobenius and Jordan forms of integer matrices which are substantially faster than those previously known. In fact, the Monte Carlo algorithm presented in Section 3 has about the same cost as an algorithm to compute the determinant of a matrix. It would be interesting to know if this Monte Carlo algorithm ever gives an error, i.e., is it a Las Vegas algorithm? Alternatively, a new, faster verification for the correctness of the Frobenius form would be highly desirable.

References

A. Danilevsky. The numerical solution of the secular equation. *Matem. sbornik* **44**(2), pp. 169–171, 1937. In Russian.

M. Giesbrecht. *Nearly Optimal Algorithms for Canonical Matrix Forms.* PhD thesis, University of Toronto, 1993. 196 pp.

M. Giesbrecht. Nearly optimal algorithms for canonical matrix forms. *SIAM J. Comp.* , 1994. to appear. Extended abstract in Proc. 33rd IEEE Symp. Foundations of Comp. Sci., pp. 121-130, 1992.

I. Gil. Computation of the Jordan canonical form of a square matrix (using the Axiom programming language). In *Proc. ISSAC'92*, pp. 138–145, Berkeley, USA, 1992.

I. Gil. *Contribution à l'algebre linéaire formelle. Formes normales de matrices et applications.* Thesis, Intitut National Polytechnique de Grenoble, Grenoble, France, 1993.

G. Golub and C. Van Loan. *Matrix Computations.* Johns Hopkins University Press (Baltimore, USA), 1989.

T. Gómez-Díaz. *Quelques applications de l'évaluation dynamique.* Thesis, Université de Limoges, Limoges, France, 1994.

K. Hoffman and R. Kunze. *Linear Algebra.* Prentice-Hall (Englewood Cliffs, N.J.), 1971.

E. Kaltofen, M. S. Krishnamoorthy, and B. D. Saunders. Fast parallel computation of Hermite and Smith forms of polynomial matrices. *SIAM J. Algebraic and Discrete Methods* **8**, pp. 683–690, 1987.

E. Kaltofen, M. S. Krishnamoorthy, and B. D. Saunders. Parallel algorithms for matrix normal forms. *Linear Algebra and its Applications* **136**, pp. 189–208, 1990.

R. Kannan. Polynomial-time algorithms for solving systems of linear equations over polynomials. *Theoretical Computer Science* **39**, pp. 69–88, 1985.

A. Karatsuba and Y. Ofman. **Умножение многозначных чисел на автоматах**. *Dokl. Akad. Nauk USSR* **145**, pp. 293–294, 1962. English translation: Multiplication of multidigit numbers on automata, Soviet Physics–Doklady **7** (1963), 595-596.

W. Keller-Gehrig. Fast algorithms for the characteristic polynomial. *Theor. Computer Science* **36**, pp. 309–317, 1985.

D. E. Knuth. *The Art of Computer Programming, Vol.2, Seminumerical Algorithms.* Addison-Wesley (Reading MA), 2 edition, 1981.

H. Lüneburg. *On Rational Normal Form of Endomorphisms: a Primer to Constructive Algebra.* Wissenschaftsverlag (Mannheim), 1987.

M. Mathieu and D. Ford. On p-adic computation of the rational form of a matrix. *J. of Symb. Comp* **10**, pp. 453–464, 1990.

M. Mignotte. An inequality about factors of polynomials. *Math. Comp.* **28**, pp. 1153–1157, 1974.

P. Ozello. *Calcul Exact Des Formes De Jordan et de Frobenius d'une Matrice.* PhD thesis, Université Scientifique Technologique et Medicale de Grenoble, 1987a.

P. Ozello. A probabilistic algorithm to compute the Frobenius form of a matrix. Technical report, Institut National Polytechnique de Grenoble, 1987b.

J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Ill. J. Math.* **6**, pp. 64–94, 1962.

A. Schönhage. Factorization of univariate integer polynomials by diophantine approximation and an improved basis reduction algorithm. In *Proc. ICALP 84, Springer Lecture Notes in Computer Science*, vol. 172, pp. 436–447, 1984.

J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. Assoc. Computing Machinery* **27**, pp. 701–717, 1980.