Quadratic-Time Certificates in Linear Algebra*

Erich L. Kaltofen
Dept. of Mathematics, NCSU
Raleigh, North Carolina 27695-8205,USA
kaltofen@math.ncsu.edu www.kaltofen.us

Michael Nehring
Dept. of Mathematics, NCSU
Raleigh, North Carolina 27695-8205,USA
michaelnehring@yahoo.com

B. David Saunders
Dept. Comput. Inform. Sci., University of Delaware
Newark, Delaware 19716, USA
saunders@udel.edu www.cis.udel.edu/~saunders/

ABSTRACT

We present certificates for the positive semidefiniteness of an $n \times n$ matrix A, whose entries are integers of binary length $\log \|A\|$, that can be verified in $O(n^{2+\epsilon}(\log \|A\|)^{1+\epsilon})$ binary operations for any $\epsilon > 0$. The question arises in Hilbert/Artin-based rational sum-of-squares certificates, i.e., proofs, for polynomial inequalities with rational coefficients. We allow certificates that are validated by Monte Carlo randomized algorithms, as in Rusins M. Freivalds's famous 1979 quadratic time certification for the matrix product. Our certificates occupy $O(n^{3+\epsilon}(\log \|A\|)^{1+\epsilon})$ bits, from which the verification algorithm randomly samples a quadratic amount.

In addition, we give certificates of the same space and randomized validation time complexity for the Frobenius form and the characteristic and minimal polynomials. For determinant and rank we have certificates of essentially-quadratic binary space and time complexity via Storjohann's algorithms.

Categories and Subject Descriptors

I.1.2 [**Computing Methodologies**]: Symbolic and Algebraic Manipulation—*Algorithms*

General Terms: theory, algorithms, verification

Keywords: randomization, probabilistic proof, matrix determinant, matrix rank, Frobenius form, output validation

1. INTRODUCTION

For many unstructured and dense linear algebra problems concerning an $n \times n$ matrix, it is not known whether there is an algorithm running in $n^{2+o(1)}$ time, in other words essentially-linearly in the input size. Motivated by the arising theme of certified ("trustworthy," "reliable") computation, in particular in numerical and hybrid symbolic numeric computation and global optimization, it is worthwhile to provide a-posteriori certificates that can be verified in time $n^{2+\epsilon}$ for any $\epsilon > 0$; see [7, 9] and the references therein. In particular the definition of what constitutes a certificate is given at the end of [9]:

> "A certificate for a problem that is given by input/output specifications is an input-dependent data structure and an algorithm that computes from that input and its certificate the specified output, and that has lower computational complexity than any known algorithm that does the same when only receiving the input. Correctness of the data structure is not assumed but validated by the algorithm (adversary-verifier model)."

Certification itself is a challenging problem for integer and rational matrices. Even the apparently straightforward thought of certifying, for $A \in \mathbb{Z}^{n\times n}$, the LU decomposition $A = LU$, by presenting the factors L and U, is problematic. Forming the product costs matrix multiplication time, $O(n^\omega)$ with $\omega > 2.37$. We accept probabilistic verification, so one could consider forming the product $(A - LU)v$ for a random vector $v \in \mathbb{Z}^n$ [2, 10]. In the algebraic model this can be done in $O(n^2)$ time, linear in input size. However, this is not at all the case in the bit model of computation given a rational or integer matrix. For instance consider the case of $A \in \mathbb{Q}^{n\times n}$. The entries of L and U are ratios of minors of A. Even when entries are integers having lengths bounded by a constant and A has determinant 1, the size of the LU decomposition is in general $n^{3+o(1)}$ and we know of no certificate to verify it in $n^{2+o(1)}$ time, deterministically or probabilistically. Here and in the following the "$n^{o(1)}$" corresponds to factors that are asymptotically bounded by a power of $\log(n)$, i.e., "$n^{\eta+o(1)}$" corresponds to a "soft big-Oh" of n^η. We shall refer to the complexity $(\log \|A\|)^{1+o(1)}$ as *essentially-linear* (in $\log \|A\|$), the complexity $n^{2+o(1)}$ as *essentially-quadratic* (in n), etc.

However, LU decomposition is primarily a means to an end, and one can in fact use LU decomposition in $n^{3+o(1)}$ space, $n^{2+o(1)}$ time, probabilistic certification, as we will show.

By *probabilistic certification* we mean a Monte Carlo randomized verification process (an algorithm whose input consists of the problem instance, the solution, and a certificate data structure). The result is "true" if the solution is verified correct with the aid of the certificate. The probability

[*] This research was supported in part by the National Science Foundation under Grants CCF-0830347, CCF-0514585 and DMS-0532140 (Kaltofen and Nehring) and under Grants CCF-1018063 (Saunders).

ISSAC'11, June 8–11, 2011, San Jose, California, USA.
Copyright 2011 ACM 978-1-4503-0675-1/11/06 ...$10.00.

of "true" output when the solution and/or certificate are incorrect must be at most 50%. The probability of incorrect verification can then be made arbitrarily small through repetition. For instance, twenty independent repetitions of a 1/2 probability verification makes the probability of error less than one part in a million.

In the next section we discuss the certification framework and give some problems that can be probabilistically certified in essentially-quadratic time and space. Section 3 concerns LU decomposition based certifications of rank and determinant which require essentially-quadratic time and essentially-cubic space. Then Section 4 presents certificates in that same time/space complexity for the invariants of matrix similarity: minimal polynomial, characteristic polynomial, and Frobenius form. This leads to certification of our original motivating problem: positive definiteness and semidefiniteness. Finally Section 5 discusses certifications based on algorithms by Kaltofen and Villard [8] and by Storjohann [15, 16]. These certificates require smaller space asymptotically than the essentially-cubic space certificates of Section 4, but the "o(1)" hides larger factors.

2. PRELIMINARIES AND $n^{2+o(1)}$ SPACE AND TIME CERTIFICATES

The sizes of entries, of the determinant, and indeed of all the minor determinants arise in in the analysis of our certificates. Let $\|A\| = \|A\|_{\infty,1} = \max_{i,j} |a_{i,j}|$, and let $\mathrm{H}_A = \max\{|M| \text{ such that } M \text{ is a minor of } A\}$.

Results in this paper are a function of the matrix dimension and of the minors bound H_A. The next lemma bounds H_A in terms of the entry size.

Lemma 1. *If A is an $m\times n$ integer matrix, and $k = \min(m, n)$, Then $\mathrm{H}_A \leq (k^{1/2}\|A\|)^k$.*

Note that $\log \mathrm{H}_A$ is essentially-linear in k when $\|A\|$ is polynomial in k.

Proof. One form of Hadamard determinant bound of an $i \times i$ minor is $(i^{1/2}\|A\|)^i$, with equality when the matrix rows or columns are pairwise orthogonal and each entry has absolute value $\|A\|$. Our bound expression is an increasing function of i, so bounds all minors when $k = \min(m, n)$. □

The magnitudes of the scalars used in our certificates are essentially-linear in $\log \mathrm{H}_A$ and the time to do basic arithmetic operations on values bounded by $\log \mathrm{H}_A$ is essentially-linear in $\mathrm{loglog}\,\mathrm{H}_A$, using fast integer arithmetic. In the remainder of the paper, for simplicity, we will state results in terms of matrix dimension and $\log \|A\|$, making use of Lemma 1. Unless subscripted by the base, all log's are to base 2.

Lemma 2. *Zero equivalence of a matrix expression over $\mathbb{Z}_p^{n\times n}$ may be verified probabilistically in time proportional to the cost of multiplying the expression times a vector and with probability of error $1/p$* [2, Freivalds].

If the matrix expression involves matrix multiplications then expanding the expression may well cost more than matrix-times-vector product. For example when the matrix order is n and the expression is $A - LU$, expanding $E = A - LU$ would cost $O(n^\omega)$ with $\omega > 2.37$, matrix multiplication time, but the matrix-vector product $Ev = Av - L(Uv)$ costs 3 matrix-times-vector products and a vector subtraction, so is $O(n^2)$ arithmetic operations.

Proof. The verification is to apply the expression E to a random vector in $\mathbb{Z}_p^n$. If E is nonzero, its nullspace is at most an $n-1$ dimensional subspace of $\mathbb{Z}_p^n$, containing p^{n-1} of the p^n possible vectors. Hence the probability of error is bounded by $1/p$. □

Kimbrel and Sinha [10] suggest for $p \geq 2n$ to use the vector $v = [1, r, r^2, \ldots, r^{n-1}]^T$ for a random residue r with $0 \leq r \leq 2n-1$. At least half of the vectors must lead to a non-zero result, since otherwise E times a non-singular Vandermonde matrix would be the zero matrix. Their approach requires only $\log(n)$ random bits.

Theorem 1. *Let $A \in \mathbb{Z}^{n\times n}$ and $b \in \mathbb{Z}^n$. The following problems have $n^{2+o(1)}(\log\|[A, b]\|)^{o(1)}$ space and $n^{2+o(1)} \times (\log\|[A, b]\|)^{o(1)}$ time probabilistic certificates.*

1. *Nonsingularity of A,*
2. *Singularity of A,*
3. *Consistency of rational linear system $Ax = b$ (and the certificate is a solution to the system),*
4. *Inconsistency of rational linear system $Ax = b$.*

Proof. For nonsingularity the certificate is (p, B), for a prime p and matrix $B = A^{-1} \mod p$. If A is singular it is not invertible modulo any prime, so one prime's testimony suffices. Verification is zero equivalence of $AB - I \mod p$. Because at most $n\left((\log n)/2 + \log\|A\|\right)$ primes divide $\det(A)$, a prime of length

$$\log\left(n\left((\log n)/2 + \log\|A\|\right)\right)$$

may be chosen, ensuring that the size of the certificate p, B is $n^{2+o(1)}(\log\|A\|)^{o(1)}$ and the cost of the zero equivalence check is $n^{2+o(1)}(\log\|A\|)^{o(1)}$ time.

For singularity the certificate is a sequence of

$$2n\left((\log n)/2 + \log\|A\|\right)$$

primes p_i and nonzero vectors v_i such that $Av_i = 0 \mod p_i$. The certificate verification is to choose index i at random and check that $Av_i = 0 \mod p_i$. At most $n\left((\log n)/2 + \log\|A\|\right)$ primes divide the determinant of A and could provide a misleading nullspace vector. So at least half of the primes can provide a nullspace vector only if A is singular. Thus with probability 1/2 the certificate is verified. The first $2n\left((\log n)/2 + \log\|A\|\right)$ primes can be used, These primes are all of bit length essentially-constant in $\log n$ and $\log\|A\|$, since the k-th prime is $\leq k(\log_e(k) + \mathrm{loglog}_e(k) - 1/2)$ for $k \geq 20$ [13].

For consistency the certificate is an integer vector x and integer $\delta \neq 0$ such that $Ax = \delta b$ and δ and the numerators in x are bounded in absolute value by $n^{n/2}\|(A, b)\|^n$. Verification is zero equivalence of $Ax - \delta b$ modulo a randomly chosen prime. It is easy to see, by Cramer's rule, that a suitably small rational solution exists when A is square and nonsingular, the entries of x are minors of (A, b) and $\delta = \det(A)$. Otherwise, for $r =$ rank(A), rows and columns of A may be permuted so that the leading principal $r \times r$ minor is nonsingular. Thus without loss of generality, A and b have conformally the forms

$$A = \begin{bmatrix} B & C \\ D & DB^{-1}C \end{bmatrix}, \quad b = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix},$$

where B is $r \times r$ nonsingular. Consistency requires $b_2 = DB^{-1}b_1$. Let x_1 be solution to $Bx_1 = \delta b_1$, where $\delta = \det(B)$. Then $x = x_1$ padded with zeroes is a solution to $Ax = \delta b$. The bit lengths of x is as required since those of x_1 and δ are. so that again the bit lengths are as required.

How many primes can testify that $Ax = \delta b$ for a incorrect solution x, δ? Let $\hat{x}, \hat{\delta}$ be a true solution. Because $n^{n/2}\|(A, b)\|^n$ bounds the entries of the true and purported solutions, $k = 1 + n\left((\log n)/2 + \log \|[A, b]\|\right)$ is a bound for bit lengths of the differences $x-\hat{x}, \delta-\hat{\delta}$ and at most k primes can falsely testify by being divisors of all $n+1$ differences. For verification we choose a prime p uniformly at random from among the first $3k+3$ primes so that the probability of a bad prime is at most 1/3. Then we reduce x and δ modulo p in $n^{2+o(1)}(\log \|[A, b]\|)^{o(1)}$ time and do two trials of zero equivalence of $Ax - \delta b \mod p$ so that zero equivalence is assured with probability of error 1/4 and overall error probability bounded by $1/3 + 2/3 \times 1/4 = 1/2$.

For inconsistency the certificate, based on [3], is a sequence of $2n\left((\log n)/2 + \log \|[A, b]\|\right)$ primes p_i and vectors v_i, such that $v_i^T A = 0 \mod p_i$, but $v_i^T b \neq 0 \mod p_i$, which contradicts $v_i^T Ax = v_i^T b$ (over the integers) for any x. Verification consists in randomly choosing one pair p_i, v_i and checking the two conditions modulo p_i. The system is inconsistent if and only if the rank of $[A, b]$ is greater than $r = \text{rank}(A)$. The only way a consistent system can be made to look inconsistent in a modular image is to have a reduced rank of A in the modular image. Let M be a nonsingular $r \times r$ minor of A. If p does not divide $\det(M) \leq H$ then p cannot falsely testify to inconsistency. Thus at most $n\left((\log n)/2 + \log \|[A, b]\|\right)$ primes must be avoided and the primes in the certificate can be taken small (among the first $3n\left((\log n)/2 + \log \|[A, b]\|\right)$ primes) to achieve the stated space and time bounds. □

3. CERTIFICATES BASED ON LU DECOMPOSITION

Definition 1. *An $m \times n$ matrix A has an LU decomposition of rank r if $A = LU$, L is a $m \times r$ unit lower triangular matrix, and U is a $r \times n$ upper triangular matrix with nonzero diagonal entries.*

LU decomposition is a common tool used in the solution of several matrix problems including rank, determinant, and system solving. The entries in the LU decomposition are ratios of minors of A. Thus if A is an $n \times n$ matrix with a minors bound of bit length $h = n^{1+o(1)}$, then the size of the LU decomposition is $n^{3+o(1)}$ (n^2 nonzero entries of length $n^{1+o(1)}$). This cubic size makes it difficult to certify LU decompositions over the integers.

Despite the fact that we do not know, for integer matrix A, how to certify $A = LU$ in $n^{2+o(1)}$ time, the LU decomposition modulo a prime is useful for several certificates. This leads us to the definition of an LU residue system.

For given $m \times n$ matrix A, a *LU residue system* of rank r and length k is a nonempty sequence of k distinct triples $(p_1, L_1, U_1), \ldots, (p_k, L_k, U_k)$ where (1) p_i is a prime, and $p_i > p_{i-1}$ for $i > 1$, (2) L_i, U_i is a LU decomposition of rank r for A modulo p_i, and (3) the entries of U_i and L_i are normalized modulo p_i ($0 \leq x < p_i$ for each entry). The primary property of a LU residue system is that $A = L_i U_i \mod p_i$. The rest of the conditions are secondary properties (that the p_i are prime and distinct, that each decomposition is of rank r and that U_i, L_i of the stated triangular and full rank forms). The secondary properties are either inherent in the presentation of the LU residue system or may be checked in $rk\ (\max \log p_i)^{1+o(1)}$ time, which is $n^{2+o(1)}$, when $k = n^{1+o(1)}$ and the primes are bounded in length by $(\operatorname{loglog} \|A\|)^{1+o(1)}$. In the sequel we will implicitly assume any verification includes checking the secondary properties.

The next lemma states that LU residue systems cannot overstate matrix rank and can understate it only if the residue system is short.

Lemma 3. *Let A have rank r and a LU residue system of rank s and let $h = n\left((\log n)/2 + \log \|A\|\right)$, which bounds the bit length of any minor of A in absolute value. Then*

1. *$s \leq r$, and*

2. *if $s < r$, then the length of the LU residue system is bounded by h.*

Proof. First observe that the leading principal $s \times s$ minor of A is the product of the leading $s \times s$ minors of L and U. By construction of the residue system, this minor is nonzero modulo a prime, hence nonzero over the integers. Thus $s \leq \text{rank}(A)$.

Second if A has rank $r > s$ then some $r \times r$ minor of A is nonzero. Only for primes p which divide this minor can A have a rank s LU decomposition modulo p. The number of such primes, thus the length of a rank s LU residue system, is bounded by the bit length of the minor which is at most h. □

A matrix A has an LU decomposition of rank r if and only if A is of rank r and has *generic rank profile* (leading principal minors are nonzero up to the rank). If A does not have generic rank profile, then there are permutation matrices P and Q such that PAQ does have generic rank profile. Define a *general* LU residue system for A to be a pair of permutations P, Q together with a LU residue system for PAQ. We use this first as a certificate for matrix rank.

Theorem 2. *Let $A \in \mathbb{Z}^{n \times n}$ and let $h = n\left((\log n)/2 + \log \|A\|\right)$, which bounds the bit length of any minor of A in absolute value. There exists a general LU residue system of length $3h$ and with primes of bit length $(\log h)^{1+o(1)}$ which is a certificate for rank(A). The certificate occupies $n^{3+o(1)}(\log \|A\|)^{1+o(1)}$ space and can be verified in $n^{2+o(1)} \times (\log \|A\|)^{1+o(1)}$ time.*

Proof. Certificate verification consists in picking one of the triples (p, L, U) and validating the decomposition $PAQ = LU \mod p$. By Lemma 3, a false certificate (wrong rank of the residue system) can have at most h triples for which the LU decomposition modulo p is valid. The probability of that is thus bounded by 1/3. In the remaining cases, the probability of an erroneous verification of a bad LU decomposition is $1/p$ by Lemma 2. Then the probability of incorrectly accepting a bad certificate is less than $1/3 + (2/3)(1/p) \leq 1/2$ when $p > 5$.

The $3h$ primes in a good certificate may be chosen among the first $4h + 3$ primes (Just excluding 2,3,5, and those that divide the largest determinantal divisor, i.e., the greatest common divisor of the $r \times r$ minors, for matrix of rank r). These primes are all of bit length $(\log h)^{1+o(1)}$ since the m-th prime is $\leq m(\log_e(m) + \log\log_e(m) - 1/2)$ for $m \geq 20$ [13]. □

Next we address determinant certification.

Theorem 3. *Let $A \in \mathbb{Z}^{n\times n}$ and let $h = n((\log n)/2 + \log \|A\|)$, which bounds the bit length of any minor of A in absolute value. There exists a certificate for the determinant of A of form $(\det(A), C)$, where C is a general LU residue system for A of length $3h + 3$ with the primes in C of length at most $(\log h)^{1+o(1)}$. The certificate occupies $n^{3+o(1)}(\log \|A\|)^{1+o(1)}$ space and can be verified in $n^{2+o(1)} \times (\log \|A\|)^{1+o(1)}$ time.*

Proof. Let d denote the purported determinant in the certificate (d, C). If the rank of the residue system is less than n, then d must be 0 and validation consists in checking the rank as in the previous theorem. If the rank of the residue system is n, chose a triple (p, L, U) and verify the LU decomposition (zero equivalence of $PAQ - LU$) and also verify that $d = \prod_{i=1}^{n} U_{i,i} \mod p$. The probability of a bad zero equivalence is $1/p$.

Since d and the true determinant have bit length h, their difference has bit length at most $h + 1$. Only primes that divide this difference can pass the $d = \prod_{i=1}^{n} U_{i,i} \mod p$ for a false d. Since at most $h+1$ such primes are in the certificate, the probability of this is bounded by $1/3$. Thus the overall validation error probability is $1/p + ((p-1)/p)(1/3) \leq 1/2$ for $p \geq 5$.

The $3h + 3$ primes in a good certificate may be chosen among the first $4h + 5$ primes. We exclude 2, 3 and those that divide the determinant, so as to present a residue system of full rank n. The selected primes are thus of bit length $(\log h)^{1+o(1)}$. For the certificate size and the verification runtime, observe that reducing d modulo p and computing the mod p determinant of U may be done in $n^{1+o(1)}(\log h)^{1+o(1)}$, so the costs are dominated by the LU residue system and are as in Theorem 2. □

We remark that if H is any bound for the minors of A with a fast verification, then $\log H$ may substitute for the bit length bound

$$h = n((\log n)/2 + \log \|A\|)$$

that we have used. Then $\log H$ substitutes for a factor of $n^{1+o(1)}(\log \|A\|)^{1+o(1)}$ in our resource bounds. The bound does have to be verified to ensure that the LU residue systems are long enough to defeat bad primes. An example of a class of matrices with non-Hadamard minors bounds verifiable in $n^{2+o(1)}$ time is the family of matrices with a constant number of rows of entries having bit length essentially n and with the remaining rows having entry lengths essentially constant.

4. CERTIFICATES BASED ON SIMILARITY

Definition 2. *A square matrix is in Frobenius normal form (rational canonical form) if it is the direct sum (block diagonal composition) of companion matrices* companion(f_1), …, companion(f_k) *for monic polynomials $f_1(x), \ldots, f_k(x)$ such that f_i divides f_{i+1}, for all i with $1 \leq i \leq k - 1$.*

Fact 1. *A square matrix over a field is similar to one and only one matrix in Frobenius normal form* [11, Corollary 2, p391, for example].

We use similarity to Frobenius form modulo primes in the following certificates. For a matrix pair $A, B \in \mathbb{Z}^{n\times n}$, define a *similarity residue system* for B with respect to A of length k to be a sequence of k tuples $(p, S, T, \bar{B})$ with distinct primes p, and matrices $S, T, \bar{B} \in \mathbb{Z}_p^{n\times n}$ such that S is invertible with $T \equiv S^{-1}$, $B \equiv \bar{B}$, and $A \equiv S\bar{B}T$ (all modulo p).

Theorem 4. *Let $A \in \mathbb{Z}^{n\times n}$. There exists a certificate for the characteristic polynomial of A of the form (f, C), in which $f(x)$ is the characteristic polynomial of A and C is a similarity residue system for the Frobenius normal form of A of length $6h_A + 6$, where $h_A = n(1 + (\log n)/2 + \log \|A\|)$ bounds the coefficient lengths in the characteristic polynomial of A, and with the primes in C of bit length $n^{o(1)} \times (\log \|A\|)^{o(1)}$. The residue system occupies*

$$n^{3+o(1)}(\log \|A\|)^{1+o(1)}$$

bit space and can be verified in $n^{2+o(1)}(\log \|A\|)^{1+o(1)}$ time.

Proof. Let $c^A(x)$ denote the characteristic polynomial of A and let $h_A = n(1 + (\log n)/2 + \log \|A\|)$. First we bound the size of $c^A(x)$. The i-th coefficient is a sum of the principal $i \times i$ minors of A. There are $\binom{n}{i}$ such minors. Thus, as the sum of less than 2^n numbers of bit length at most $h = n((\log n)/2 + \log \|A\|)$, the coefficient bit length is bounded by $n + h$ and the n coefficients of $c^A(x)$ occupy at most $n^2 + nh$ space. Better bounds are possible, see, e.g., [5]. If a polynomial f is offered that is not the characteristic polynomial but has coefficients bounded in absolute value by h_A, then $g(x) = f(x) - c^A(x)$ has coefficients of bit length $1 + h_A$. For a prime p to lie will require that g is mapped to zero modulo p.

To verify that $f(x) = c^A(x)$, do the following.

1. Choose at random a tuple $(p, S, T, \bar{B})$ in the similarity residue system C. Verify the zero equivalence (Lemma 2) of $ST - I$ and $A - S\bar{B}T$ (both modulo p) in $O(n^2)$ time and with error probability bounded by $2/p$ (which is less than $1/6$ for $p \geq 13$).

2. Verify (deterministically) that each f_i divides the next. Multiply together the polynomials of the companion matrices comprising B, obtaining $f_p(x) = \prod f_i(x) \bmod p$, Since the Frobenius form is unique, the product is necessarily the modulo p residue of $c^A(x)$. The product can be computed using $O(n^2)$ arithmetic operations modulo p, and each division is degree$(f_{i+1})^{1+o(1)}$ arithmetic operations, so the divisibility checks in total are in $n^{2+o(1)}(\log p)^{1+o(1)}$ as well.

3. Verify (deterministically) that $f(x) = f_p(x) \mod p$. Since the size of f is $n^{2+o(1)}(\log \|A\|)^{1+o(1)}$, f can be reduced modulo p in $n^{2+o(1)}(\log \|A\|)^{1+o(1)}$ time.

Since each $f_p(x)$ is a modular residue of $c^A(x)$ the certificate must have $f(x) = c^A(x) \mod p$ for each p in the residue system. Also $f(x)$ and $c^A(x)$ have coefficients of bit length at most h_A, so the bit length of the coefficients of $f(x) - c^A(x)$ is bounded by $k = 1 + h_A$. Thus this polynomial is zero modulo at most k primes. The certificate can successfully pass the verification with an incorrect purported characteristic polynomial only with probability at most $k/(6h_A + 6) = 1/6$.

Thus we may fail to detect a bad similarity with probability 1/6. In the remaining 5/6 cases we could fail to detect a bad determinant with probability 1/3, for overall probability of failure bounded by 1/2.

The first $6h_A$ primes larger than 11 can be used in the certificate, ensuring that they have bit length essentially-constant in n and $(\log \|A\|)$. □

The *signature* of matrix is the triple (n_+, n_0, n_-) indicating the number of positive, zero, and negative eigenvalues, respectively.

Corollary 1. *Let A be an $n \times n$ symmetric matrix having minors bound H of bit length $\log \mathrm{H}_A = n^{1+o(1)}$. The signature of A can be verified in $n^{2+o(1)}$ binary operations with a $n^{3+o(1)}$ bit space characteristic polynomial certificate. Thus the same certificate serves for positive or negative definiteness or semidefiniteness.*

PROOF. Verify the characteristic polynomial $c^A(x)$ with the certificate of Theorem 4. Since the matrix is symmetric, all eigenvalues are real. The number of zero eigenvalues is the largest n_0 such that x^{n_0} divides $c^A(x)$. For instance, if A has all its eigenvalues $\alpha \geq 0$, i.e., if A is positive semidefinite, then the polynomial

$$\prod_{\alpha > 0}(x + \alpha) = (-1)^{n-n_0}\frac{c^A(-x)}{(-x)^{n_0}} \qquad (1)$$

has all positive coefficients. The condition is obviously sufficient, since a polynomial (1) with all positive coefficients cannot have a positive root, so all roots $x = -\alpha$ are negative. □

We finally turn to certificates for the Frobenius form.

Fact 2. *Let $A \in \mathbb{Z}^{n\times n}$ and let $G \in \mathbb{Z}^{n\times n}$ be in Frobenius form with $\|G\| \leq 2^n e^{n/2} n^{n/2} \|A\|^n$. If the Frobenius forms for $(A \bmod p_i)$ are equal to $(G \bmod p_i)$ for distinct primes $p_1, \ldots, p_t$ with $\prod_{i=1}^t p_i \geq 8^n e^n n^{2n} \|A\|^{3n}$, then G is the Frobenius form of A* [4, Theorem 2.1].

There are at most $n^{3+o(1)} \log \|A\|$ unlucky primes q for which the Frobenius forms of $(A \bmod q)$ are not equal to the (Frobenius form of A) mod q [6]. The Frobenius form of A can be represented in $n^{2+o(1)} \log \|A\|$ binary space. The bound given in Fact 2 for $\|G\|$ is a valid bound for the Frobenius form of A [4, Lemma 2.1]. Note that any factor coefficient bound for the characteristic polynomial will work. The certificate for the Frobenius form of A has, as in the proof of Theorem 4, a matrix G in Frobenius form and similarity residues system for it. One selects a random system and verifies the modular property of Fact 2 for that prime. If we choose $2s$ prime moduli p_i in such a way that the product of any subset of s of the moduli is $\geq 8^n e^n n^{2n} \|A\|^{3n}$, then for a false G of the required entry size bound, the Frobenius form of $(A \mod p_i)$ cannot be equal to $(G \bmod p_i)$ for more than half of the moduli. Hence a false certificate will be rejected with probability $\geq 1/2$. From $2^s \geq 8^n e^n n^{2n} \|A\|^{3n}$ we deduce that an $s = n^{1+o(1)} \log \|A\|$ suffices.

Corollary 2. *Let $A \in \mathbb{Z}^{n\times n}$. The Frobenius form of A can be verified in $n^{2+o(1)}(\log \|A\|)^{1+o(1)}$ binary operations with an $n^{3+o(1)}(\log \|A\|)^{1+o(1)}$ bit space certificate.*

5. ALGORITHM-BASED CERTIFICATES OF SPACE $n^{e+o(1)}$ WITH $e < 3$

Integer matrix algorithms that have bit complexity $n^{\eta+o(1)}$ with $\eta < 3$, where η depends on the matrix multiplication complexity exponent $\omega > 2.37$ [1, 8, 15, 16], automatically lead to faster certificates. The algorithms can be randomized of the Las Vegas kind, always correct and probably fast. For example, consider Storjohann's integer matrix determinant [15] and rank [16] algorithms of Las Vegas bit complexity $n^{\omega+o(1)}(\log \|A\|)^{1+o(1)}$. A certificate records a successful (lucky) choice of the used random bits and all occurring integer matrix multiplications and their results. Since for a hypothetical matrix multiplication algorithm with $\omega = 2$, the algorithm requires $n^{2+o(1)}(\log \|A\|)^{1+o(1)}$ bit operations, the certificate bit space is no more than that. The validation procedure simply reruns the algorithm and verifies each matrix product by Freivalds's method in $n^{2+o(1)} l^{1+o(1)}$ bit operations, where l is the bit length of the occurring entries.

Note that if the rank r of A is $r = n^{2/\omega+o(1)}$, it can computed by a Monte Carlo algorithm without the help of any certificate in $n^{2+o(1)}(\log \|A\|)^{1+o(1)}$ bit steps [14].

The situation for the characteristic polynomial and the Frobenius form is somewhat different. The fastest known algorithms, assuming $\omega = 2$, have to our knowledge complexity $n^{2+1/2+o(1)}(\log \|A\|)^{1+o(1)}$ [8, Table 6.1, Line 7], and indeed need that much storage: the algorithm computes $A^{\lceil\sqrt{n}\rceil}$ which occupies $n^{2+1/2+o(1)}(\log \|A\|)^{1+o(1)}$ bit space. However, they are Monte Carlo randomized algorithms ("always fast, probably correct") which makes independent certification difficult.

We have the following theorem.

Theorem 5. *We have certificates of binary space $n^{2+o(1)} \times (\log \|A\|)^{1+o(1)}$ for the rank and determinant of an integer matrix $A \in \mathbb{Z}^{n\times n}$ that can be validated by a Monte Carlo algorithm in $n^{2+o(1)}(\log \|A\|)^{1+o(1)}$ binary operations.*

Acknowledgments: The certificate for nonsingularity in Theorem 1 was told to us by Jürgen Gerhard when discussing with him our singularity certificate at ACA 2008 in Montreal. The referees have provided comments which have improved the presentation of the paper.

Note added on June 14, 2011: 1. The signature of A in Corollary 1 is verified by Descartes's rule of signs.
2. A sharper estimate for the number of unlucky primes for the Frobenius form than ours given below Fact 2 is

$n^{2+o(1)} \log \|A\|$ [4, Lemma 2.3].

3. As pointed out to us by Allan Borodin, our certificates are related to designing programs that check their work [Manuel Blum and Sampath Kannan, J. ACM, vol. 42, nr. 1, pp. 269–291, Jan. 1995]. There, the programs can be rerun on modified inputs, as in the matrix rank check, and thus do not have quadratic complexity. However, several of their checks, such as for GCD, constitute certificates in our sense.

Note added on July 1, 2011: Corrected the bit space estimate in Theorem 4 from $n^{3+o(1)}(\log \|A\|)^{o(1)} + n^{1+o(1)} \times (\log \|A\|)^{1+o(1)}$ to $n^{3+o(1)}(\log \|A\|)^{1+o(1)}$.

6. REFERENCES

[1] Eberly, W., Giesbrecht, M., and Villard, G. On computing the determinant and Smith form of an integer matrix. In *Proc. 41stAnnual Symp. Foundations of Comp. Sci.* (Los Alamitos, California, 2000), IEEE Computer Society Press, pp. 675–685.

[2] Freivalds, R. Fast probabilistic algorithms. In *Mathematical Foundations of Computer Science 1979, Proceedings, 8th Symposium, Olomouc, Czechoslovakia, September 3-7, 1979* (1979), J. Becvár, Ed., Springer, pp. 57–69. Lecture Notes in Computer Science, vol. 74.

[3] Giesbrecht, M., Lobo, A., and Saunders, B. D. Certifying inconsistency of sparse linear systems. In *ISSAC 98 Proc. 1998 Internat. Symp. Symbolic Algebraic Comput.* (New York, N. Y., 1998), O. Gloor, Ed., ACM Press, pp. 113–119.

[4] Giesbrecht, M., and Storjohann, A. Computing rational forms of integer matrices. *J. Symbolic Comput. 34*, 3 (Sept. 2002), 157–172.

[5] Goldstein, A. J., and Graham, R. L. A Hadamard-type bound on the coefficients of a determinant of polynomials. *SIAM Rev. 16* (1974), 394–395.

[6] Kaltofen, E., Krishnamoorthy, M. S., and Saunders, B. D. Fast parallel computation of Hermite and Smith forms of polynomial matrices. *SIAM J. Alg. Discrete Math. 8* (1987), 683–690. URL: http://www.math.ncsu.edu/~kaltofen/bibliography/87/KKS87.pdf

[7] Kaltofen, E., Li, B., Yang, Z., and Zhi, L. Exact certification of global optimality of approximate factorizations via rationalizing sums-of-squares with floating point scalars. In *ISSAC 2008* (New York, N. Y., 2008), D. Jeffrey, Ed., ACM Press, pp. 155–163. URL: http://www.math.ncsu.edu/~kaltofen/bibliography/08/KLYZ08.pdf

[8] Kaltofen, E., and Villard, G. On the complexity of computing determinants. *Computational Complexity 13*, 3-4 (2004), 91–130. URL: http://www.math.ncsu.edu/~kaltofen/bibliography/04/KaVi04_2697263.pdf

[9] Kaltofen, E. L., Li, B., Yang, Z., and Zhi, L. Exact certification in global polynomial optimization via sums-of-squares of rational functions with rational coefficients, Jan. 2009. Accepted for publication in J. Symbolic Comput. URL: http://www.math.ncsu.edu/~kaltofen/bibliography/09/KLYZ09.pdf

[10] Kimbrel, T., and Sinha, R. K. A probabilistic algorithm for verifying matrix products using $O(n^2)$ time and $\log_2 n + O(1)$ random bits. *Inf. Process. Lett. 45*, 2 (1993), 107–110.

[11] MacLane, S., and Birkhoff, G. *Algebra, second edition.* Macmillan, 1979.

[12] May, J. P., Ed. *ISSAC 2009 Proc. 2009 Internat. Symp. Symbolic Algebraic Comput.* (New York, N. Y., 2009), ACM.

[13] Rosser, J. B., and Schoenfeld, L. Approximate formulas of some functions of prime numbers. *Illinois J. Math. 6* (1962), 64–94.

[14] Saunders, B. D., and Youse, B. S. Large matrix, small rank. In May [12], pp. 317–324.

[15] Storjohann, A. The shifted number system for fast linear algebra on integer matrices. *J. Complexity 21*, 5 (2005), 609–650.

[16] Storjohann, A. Integer matrix rank certification. In May [12], pp. 333–340.