A New Interactive Certificate for Matrix Rank

Eberly, Wayne

A New Interactive Certificate for Matrix Rank

Wayne Eberly
University of Calgary

June 23,, 2015

Abstract

A new interactive certificate for matrix rank, based on the certification of a maximal nonsingular submatrix, is described. Versions of this for matrices over abstract fields and integer matrices are each described.

Categories and Subject Descriptors

I.1.2 [**Symbolic and Algebraic Manipulation**]: Algorithms — *algebraic algorithms, analysis of algorithms*; F.2.1 [**Analysis of Algorithms and Problem Complexity**]: Numerical Algorithms and Problems — *computations in finite fields, computations on matrices; interactive certificates*

General Terms

Algorithms, Performance, Reliability, Theory

Keywords

Interactive certificates, black box matrix computations, randomized algorithms, computations over finite fields, matrix rank

1 Introduction

Recently a variety of "certificates in linear algebra" (and, more generally, certificates in symbolic computation) have been proposed, notably by Kaltofen, Li, Yang and Zhi [4], Kaltofen, Nehring, and Saunders [5] and by Dumas and Kaltofen [2]. As defined in this work (and, indeed, quoting Kaltofen et. al. [4]), "a 'certificate' 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 receiving the input. Correctness of the data structure is not assumed

but validated by the algorithm (adversary-verifier model)." This motivates the following, which will be used to investigate certificates in this report. The first two criteria concern the reliability of certificates while the third concerns efficiency. All three are taken from the recent literature on certificates and have been used to assess them in this work. The fourth and fifth have received less attention but merit consideration when the first three are insufficient to compare certificates.

Criterion #1 — Perfect Completeness: A correct certificate will always be accepted by a verifier.

Criterion #2 — Soundness: The probability that an incorrect certificate is accepted by a verifier can be made to be arbitrarily small.

Criterion #3 — Efficiency of Verification: Resources required by a verifier to (with high probability) confirm that a static certificate is accurate — or, as suggested below, confirm that a "prover" is providing correct information in an interactive protocol — is minimized.

Criterion #4 — Certificate Size: The size of the data structure provided as a certificate.

Dumas and Kaltofen also considered "interactive certificates" — interactive protocols in which information is being exchanged, in multiple rounds, between provers and resource-limited verifiers. As they note, these can be converted to (non-interactive) certificates — with the validity of verification procedures "subject to standard computation hardness assumptions from cryptography." See Dumas and Kaltofen [2] for an extensive discussion of this and references.

In any case, this motivates another criterion that might be used to assess interactive certificates:

Criterion #5 — Communication Complexity: The number of bits of information (or, for computations over an abstract field, the number of field elements) that must be passed between the prover and the verifier during the protocol.

In the following, a new interactive certificate for the rank of a matrix, based on the certification of a maximal nonsingular submatrix, is provided. This is inspired by — and uses many of the same ideas — as interactive certificates for the rank of a matrix over an abstract field, and for an integer matrix, given by Dumas and Kaltofen [2], as well as an earlier non-interactive certificate for the rank of an integer matrix given by Kaltofen, Nehring and Saunders [5].

The new certificate is — arguably — a little bit simpler than these earlier certificates for matrix rank. When verifying the rank of a matrix over an abstract field the cost of verification is also — very slightly — reduced: While the required number of matrix-times-vector products is unchanged, the number of additional arithmetic operations required to certify the rank of a matrix $A \in \mathsf{F}^{n \times m}$ for a large field F drops to a number that is linear in $n + m$; if A has rank r then $O(r \log_2 \max(n, m)) \subseteq O(\min(n, m) \log_2 \max(n, m))$

additional operations on bits are also used. In the small field case this suffices to ensure that an incorrect certificate is incorrectly certified with probability at most $1/|\mathsf{F}|$. Since the new certificate uses the same method to certify that a submatrix is nonsingular as the certificate of Dumas and Kaltofen, the probability that an incorrect certificate is accepted is the same, for both certificates, in this case.

Similar — modest — improvements are obtained for the cost to verify an interactive certificate for the rank of an integer matrix. The cost to verify is most significantly reduced if the verifier has access to a "black box" to compute $Ax \bmod p$ for a vector $x \in \mathbb{Z}^{m\times 1}$ and a positive integer prime p that the verifier can specify. In this case, the cost to verify drops to two applications of this black box along with a small number of additional operations on bits: If one wishes to bound the probability that an incorrect certificate is accepted by a positive constant ϵ such that ϵ^{-1} is at most polynomial in $n+m+\log_2 \|A\|$ then the expected number of these additional operations is linear in the sum of $(n+m)(\log_2 n+\log_2 m+\log_2 \log_2 \|A\|)$ and a polynomial function of $\log_2 n+\log_2 m+\log_2 \log_2 \|A\|$. The expected number of additional operations on bits increases if the verifier has access to a black box for the computation of Ax, instead, simply because the entries of a product Ax may be significantly larger than a prime p, when the vector $Ax \bmod p \in \mathbb{Z}_p^{n\times 1}$ is required to complete the protocol.

It should be noted that it is also possible to certify the rank of a matrix by certifying the evaluation of a Boolean or arithmetic circuit using the techniques of Goldwasser, Kalai and Rothblum [3] and Thaler [9]. This may result in further reductions of the cost for verification, at least when the matrix whose rank to be verified is dense and unstructured. However, as Dumas and Kaltofen note, these methods require a prover and verifier to share access to a trusted Boolean or arithmetic circuit for the computation to be verified. Since the certificates presented by Kaltofen, Nehring and Saunders, Dumas and Kaltofen, and in this report do not require this, these latter certificates are more generally applicable.

The version of the new certificate for matrices over abstract fields is presented in Section 2, while the version for integer matrices is found in Section 3. It should be confessed that that there has been no attempt to optimize various functions or constants included in the description of the certificate for the rank of an integer matrix. Instead, a version of the protocol whose soundness is easily proved has been presented.

Acknowledgments: Jean-Guillaume Dumas has commented on a previous draft of this report. His corrections and comments were extremely helpful.

2 Certifying the Rank of a Matrix over an Abstract Field

Suppose now that $A \in \mathsf{F}^{n\times m}$ for positive integers n and m. An interactive protocol that can be used to certify that A has rank r is as follows.

Commitment: The prover sends the rank r to the verifier along with the location of a maximal nonsingular submatrix of A, that is, integers $i_1, i_2, \ldots, i_r$ and $j_1, j_2, \ldots, j_r$ such

that $1 \leq i_1 < i_2 < \cdots < i_r \leq n$, $1 \leq j_1 < j_2 < \ldots j_r \leq m$, and the $r \times r$ submatrix of A with rows $i_1, i_2, \ldots, i_r$ and columns $j_1, j_2, \ldots, j_r$ is nonsingular.

Challenge: The verifier sends values $\alpha_1, \alpha_2, \ldots, \alpha_r, \beta_1, \beta_2, \ldots, \beta_{m-r} \in \mathsf{F}$ to the prover. If F is a small finite field then these should be chosen uniformly and independently from F; they should be chosen uniformly and independently from a finite subset S of F otherwise.

Response: The prover returns a pair of vectors

$$x = \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_m \end{bmatrix} \in \mathsf{F}^{m \times 1} \quad \text{and} \quad y = \begin{bmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_m \end{bmatrix} \in \mathsf{F}^{m \times 1}$$

satisfying the following properties — all of which are checked by the verifier, who accepts the certificate if and only if they are all satisfied.

(a) For $1 \leq h \leq m$, if $h \notin \{j_1, j_2, \ldots, j_r\}$ then $\lambda_h = 0$ — so that Ax is a linear combination of columns $j_1, j_2, \ldots, j_r$ of A.

(b) For $1 \leq h \leq r$ the i_h^{th} entry of the vector Ax is equal to α_h.

(c) Let $k_1, k_2, \ldots, k_{m-r}$ be integers such that $1 \leq k_1 < k_2 < \cdots < k_{m-r} \leq m$ and $\{j_1, j_2, \ldots, j_r\} \cup \{k_1, k_2, \ldots, k_{m-r}\} = \{1, 2, \ldots, m\}$ — so that

$$\{j_1, j_2, \ldots, j_r\} \cap \{k_1, k_2, \ldots, k_{m-r}\} = \emptyset.$$

Then, for $1 \leq h \leq m - r$, $\mu_{k_h} = \beta_h$.

(d) $Ay = 0$.

Henceforth let $C \in \mathsf{F}^{r \times r}$ be the submatrix of A with rows $i_1, i_2, \ldots, i_r$ and columns $j_1, j_2, \ldots, j_r$ that is specified by the prover during the commitment phase of this protocol.

Lemma 2.1. *The above protocol is perfectly complete.*

Proof. Suppose that A has rank r. Then it is certainly possible to identify a maximal nonsingular submatrix during the commitment phase of this protocol. It can therefore be assumed that C is such a matrix, so that C also has rank r.

Consider any sequence of values $\alpha_1, \alpha_2, \ldots, \alpha_r, \beta_1, \beta_2, \ldots, \beta_{m-r} \in \mathsf{F}$ returned by the verifier as a challenge to a prover. It is necessary and sufficient to confirm that these values can be used by the prover to produce vectors $x, y \in \mathsf{F}^{m \times 1}$ satisfying properties (a)–(d) as given above.

A vector $x \in \mathsf{F}^{m\times 1}$ satisfying properties (a) and (b) can be obtained by setting the j_h^{th} entry of x to be the h^{th} entry of

$$C^{-1}\begin{bmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_r\end{bmatrix} \in \mathsf{F}^{r\times 1}$$

for $1 \leq h \leq r$, and by setting all other entries of x to be zero— it is immediate from the above definition of C that properties (a) and (b) are then satisfied.

Let $D \in \mathsf{F}^{r\times m}$ be the submatrix of A including rows $i_1, i_2, \ldots, i_r$. Let $E \in \mathsf{F}^{r\times(m-r)}$ be the submatrix of D including columns $k_1, k_2, \ldots, k_{m-r}$ (as defined in property (c), above). Let

$$\begin{bmatrix}\nu_1\\ \nu_2\\ \vdots\\ \nu_r\end{bmatrix} = C^{-1} \times E \times \begin{bmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_{m-r}\end{bmatrix} \in \mathsf{F}^{r\times 1}. \tag{2.1}$$

A vector $y \in \mathsf{F}^{m\times 1}$ satisfying properties (c)–(d) can now be produced by setting the j_h^{th} entry of y to be $-\nu_h$ for $1 \leq h \leq r$, and setting the k_ℓ^{th} entry of y to be β_ℓ for $1 \leq \ell \leq m-r$. It is immediate from the above definition that property (c) is satisfied. Since the columns of C are columns $j_1, j_2, \ldots, j_r$ of the above matrix D, it follows by the definition of $\nu_1, \nu_2, \ldots, \nu_r$ at line (2.1), above that $Dy = 0$. Since every row of A is a linear combination of the rows of D, $Ay = 0$ as well, as needed to establish property (d). □

Lemma 2.2. *Suppose that information provided by the prover during the commitment stage is incorrect, that is, either the matrix C is singular, or C is nonsingular but the rank of A is strictly greater than r.*

(a) *If F is a small finite field and the verifier chooses values $\alpha_1, \alpha_2, \ldots, \alpha_r, \beta_1, \beta_2, \ldots, \beta_{m-r}$ uniformly and independently from F, then the verifier mistakenly accepts the certificate with probability at most $|\mathsf{F}|^{-1}$.*

(b) *If the verifier chooses values $\alpha_1, \alpha_2, \ldots, \alpha_r, \beta_1, \beta_2, \ldots, \beta_{m-r}$ uniformly and independently from a finite subset S of F, then the verifier mistakenly accepts the certificate with probability at most $|S|^{-1}$.*

Proof. It suffices to establish part (b) of the claim; part (a) follows directly by setting S to be F when F is a small finite field.

Suppose the matrix C is singular, and let $s < r$ be the rank of C. Let $z_1, z_2, \ldots, z_{s+1}$ be indeterminates over F and consider a matrix $D \in \mathsf{F}[z_1, z_2, \ldots, z_{s+1}]^{(s+1)\times(s+1)}$ such that

- the $(s+1) \times s$ submatrix of D including the first s columns is a submatrix of C whose principal $s \times s$ submatrix is nonsingular. That is, this is a submatrix of A including rows $\widehat{\imath}_1, \widehat{\imath}_2, \ldots, \widehat{\imath}_{s+1}$ and columns $\widehat{\jmath}_1, \widehat{\jmath}_2, \ldots, \widehat{\jmath}_s$ such that

$$1 \leq \widehat{\imath}_1 < \widehat{\imath}_2 < \cdots < \widehat{\imath}_{s+1} \leq n \quad \text{and} \quad \{\widehat{\imath}_1, \widehat{\imath}_2, \ldots, \widehat{\imath}_{s+1}\} \subseteq \{i_1, i_2, \ldots, i_r\},$$

$$1 \leq \widehat{\jmath}_1 < \widehat{\jmath}_2 < \cdots < \widehat{\jmath}_s \leq m \quad \text{and} \quad \{\widehat{\jmath}_1, \widehat{\jmath}_2, \ldots, \widehat{\jmath}_s\} \subseteq \{j_1, j_2, \ldots, j_r\},$$

  and the $s \times s$ submatrix of A including rows $\widehat{\imath}_1, \widehat{\imath}_2, \ldots, \widehat{\imath}_s$ and columns $\widehat{\jmath}_1, \widehat{\jmath}_2, \ldots, \widehat{\jmath}_s$ is nonsingular.

- the final column of A has the indeterminates $z_1, z_2, \ldots, z_{s+1}$ as entries.

Let $f(z_1, z_2, \ldots, z_{s+1}) = \det(D)$. Consideration of a Laplace expansion of the determinant of D along the final column confirms that f is a polynomial with total degree at most one in $z_1, z_2, \ldots, z_{s+1}$ and also that this polynomial is not identically zero: The coefficient of z_{s+1} is the product of ± 1 and the determinant of the principal $s \times s$ submatrix of D. For $1 \leq a \leq s+1$, let $h_a \in \mathbb{Z}$ such that $1 \leq h_a \leq r$ and $\widehat{\imath}_a = i_{h_a}$. If $f(\alpha_{h_1}, \alpha_{h_2}, \ldots, \alpha_{h_{s+1}}) \neq 0$, then it is impossible for the verifier to produce a vector $x \in \mathsf{F}^{m \times 1}$ satisfying properties (a) and (b) — for the vector $\begin{bmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_r \end{bmatrix}^T \in \mathsf{F}^{m \times 1}$ is not in the column space of C. It now follows by a straightforward application of the Schwartz-Zippel lemma [8, 10] that if C is singular then the probability that verifier accepts is at most $1/|S|$.

Suppose next that C is nonsingular but the rank of A is greater than r. Let $z_1, z_2, \ldots, z_{m-r}$ be indeterminates over F and consider a matrix $E \in \mathsf{F}[z_1, z_2, \ldots, z_{m-r}]^{(r+1) \times (r+1)}$ such that

- The $(r+1) \times r$ submatrix of E including the first r columns is a submatrix of A including rows $i_1, i_2, \ldots, i_r$ and k where $1 \leq k \leq n$, $k \notin \{i_1, i_2, \ldots, i_r\}$, and the k^{th} row of A is not a linear combination or rows $i_1, i_2, \ldots, i_r$ of A; since the rank of A exceeds r, some such value k must certainly exist. This submatrix should also include columns $j_1, j_2, \ldots, j_r$, so its leading $r \times r$ submatrix is the above matrix C.

- Consider a vector $\zeta \in \mathsf{F}[z_1, z_2, \ldots, z_{m-r}]^{m \times 1}$ such that, for $1 \leq a \leq m-r$, the entry of this vector in position k_a is the indeterminate z_a — and whose remaining r entries are all 0. Let the final column of E be the column consisting of the entries in positions $i_1, i_2, \ldots, i_r, k$ of the vector $A\zeta$ — noting that each entry of this column is then a polynomial with total degree at most one in $z_1, z_2, \ldots, z_{m-r}$.

Let $g(z_1, z_2, \ldots, z_{m-r}) = \det(E)$. Once again, consideration of a Laplace expansion of the determinant of E along the final column of E confirms that g is a polynomial with total degree at most one in the indeterminates $z_1, z_2, \ldots, z_{m-r}$. Now let $\ell \in \mathbb{Z}$ such that $1 \leq \ell \leq m-r$ and the submatrix $\widehat{E} \in \mathsf{F}^{(r+1) \times (r+1)}$ of A with rows $i_1, i_2, \ldots, i_r, k$ and columns $j_1, j_2, \ldots, j_r, k_\ell$ is nonsingular — again, some such integer ℓ must now exist. To see that g is nonsingular, it suffices to note (by another consideration of the Laplace

expansion along the final column) that the coefficient of z_ℓ in g is $\pm\det(\widehat{E})$. Finally, it should be noted that if $g(\beta_1, \beta_2, \ldots, \beta_{m-r}) \neq 0$ then it is impossible for the prover to return a vector $y \in \mathsf{F}^{m\times 1}$ satisfying properties (c) and (d) — for if y satisfies property (c) and $g(\beta_1, \beta_2, \ldots, \beta_{m-r}) \neq 0$ then at least one of the entries of Ay in positions $i_1, i_2, \ldots, i_r, k$ must be nonzero. Another application of the Schwartz-Zippel lemma establishes if C is nonsingular and the rank of A exceeds r then the probability that the verifier accepts is at most $1/|S|$, once again. □

The following is easily verified by an inspection of the above protocol.

Lemma 2.3. *Let $N = \max(n, m)$. The cost to the verifier, to participate in the above protocol, includes (and is limited to)*

- *$O(r \log N) \subseteq O(\min(n, m) \log N)$ operations on bits — needed to perform $O(r)$ operations on integers between 1 and N, in order to confirm that the integers supplied by the prover during the commitment phase are as described above.*
- *the cost to choose m values uniformly and independently — from F if F is a small finite field, or from a finite subset S of F otherwise.*
- *Two matrix-times-vector products, in order to compute the vectors Ax and Ay.*
- *$(m-r)+r+(m-r)+n = 2m+n-r \leq 2m+n$ comparisons of pairs of values in F in order to confirm that properties (a)–(d) are satisfied.*

Thus the cost to verify is comparable to — and arguably, very slightly lower — than the cost to apply the protocol for matrix rank of Dumas and Kaltofen [2]. While it is necessary to apply this protocol repeatedly to obtain a desired level of soundness when F is a small finite field, this is also true of Dumas and Kaltofen's protocol: Each uses essentially the same technique to establish r as a lower bound for matrix rank (described in [2] as a protocol for nonsingularity), and this must be iterated.

3 Certifying the Rank of an Integer Matrix

The certification of the rank of an integer matrix is also of interest. With that noted, suppose that

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,m} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \ldots & a_{n,m} \end{bmatrix} \in \mathbb{Z}^{n\times m}.$$

Let $\|A\| = \|A\|_\infty = \max_{i,j} |a_{i,j}|$, so that $\log_2 \|A\|$ is the maximal bit length of any entry of A. Two classical results are of use when designing and analyzing algorithms to certify the rank of an integer matrix as given above:

- ***Hadamard's Inequality*** states that if $n = m$ then $|\det(A)| \leq n^{n/2}\|A\|^n$, so that $\log_2 |\det(A)| < n(\frac{1}{2}\log_2 n + \log_2 \|A\|)$.

- The ***Prime Number Theorem*** concerns the number $\pi(x)$ of (positive integer) primes that are less than or equal to a given positive integer x. Proofs of asymptotic bounds for this value can be found in a variety of texts. The somewhat more precise bounds given below are from Rosser and Schoenfeld [7]:

$$\frac{x}{\ln x}\left(1 + \frac{1}{2\ln x}\right) < \pi(x) < \frac{x}{\ln x}\left(1 + \frac{3}{2\ln x}\right) \quad \text{if } x \geq 59.$$

  More recent, sharper, bounds are now known for larger n as well. However, the above is sufficient for this report.

With that noted, and considering an matrix $A \in \mathbb{Z}^{n\times m}$ as above, and for a given positive constant ϵ such that $0 < \epsilon \leq 1$, set $\ell = \max(\min(n, m), 2)$,

$$\lambda = 4 \times \epsilon^{-1} \times \ell \left(\tfrac{1}{2}\log_2 \ell + \log_2 \|A\|\right), \tag{3.1}$$

and set $\mu \in \mathbb{Z}$ to be the smallest power of two such that

$$\mu \geq \max(2\lambda \ln \lambda, 64). \tag{3.2}$$

Note that if B is a square and nonsingular submatrix of A then $\|B\| \leq \|A\|$. It therefore follows by the above that

$$\begin{aligned}
\pi(4\mu) - \pi(\mu) &> \frac{4\mu}{\ln(4\mu)}\left(1 + \frac{1}{2\ln(4\mu)}\right) - \frac{\mu}{\ln\mu}\left(1 + \frac{3}{2\ln\mu}\right) \\
&\qquad \text{(by the Prime Number Theorem)} \\
&\geq \frac{3\mu}{\ln\mu}\left(1 + \frac{3/4}{2\ln\mu}\right) - \frac{\mu}{\ln\mu}\left(1 + \frac{3}{2\ln\mu}\right) \\
&\qquad \text{(since } \mu \geq 64 = 4^3\text{, so that } \ln(4\mu) \leq \tfrac{4}{3}\ln\mu\text{)} \\
&= \frac{2\mu}{\ln\mu}\left(1 - \frac{3/8}{2\ln\mu}\right) \\
&> \frac{\mu}{\ln\mu} \\
&> \lambda \qquad \text{(since } \mu \geq 2\lambda\ln\lambda\text{)} \\
&\geq 4 \times \epsilon^{-1} \times \log_2(\det(B)) \\
&\qquad \text{(by Hadamard's Inequality and the above definition of } \lambda\text{)} \\
&\geq \log_2(\det(B)) \qquad \text{(since } \det(B) \geq 1 \text{ and } \epsilon^{-1} \geq 1\text{).}
\end{aligned}$$

It follows that there exists a prime p such that $\mu < p \leq 4\mu$ that does not divide the determinant of B. Furthermore, if q is chosen uniformly from the set of primes that are greater

than μ and less than or equal to 4μ then the probability that q divides the determinant of B is at most $\epsilon/4$. This is useful for considering the following protocol to certify the rank of an integer matrix $A \in \mathsf{F}^{n\times m}$ as shown above.

Commitment: The prover sends the following information:

- the rank, r, of A;
- the location of a maximal nonsingular submatrix C of A, that is, integers $i_1, i_2, \ldots, i_r$ and $j_1, j_2, \ldots, j_r$ such that $1 \leq i_1 < i_2 < \cdots < i_r \leq n$, $1 \leq j_1 < j_2 < \cdots < j_r \leq m$, and the $r \times r$ submatrix C of A with rows $i_1, i_2, \ldots, i_r$ and columns $j_1, j_2, \ldots, j_r$ is nonsingular;
- a prime p such that $\mu < p < 4\mu$, for μ as at line (3.2), above, that does not divide the determinant of C.

Challenge: After verifying that $\mu < p < 4\mu$ and p is prime, the verifier sends the following values:

- Integers $\alpha_1, \alpha_2, \ldots, \alpha_r$ such that $0 \leq \alpha_i < p$ for $1 \leq i \leq r$;
- an integer q such that $\mu < q < 4\mu$ (which will be chosen as a prime selected uniformly from this range if the verifier is honest and wishes to detect an incorrect certificate with high probability);
- integers $\beta_1, \beta_2, \ldots, \beta_{m-r}$ such that $0 \leq \beta_j < q$ for $1 \leq j \leq m - r$.

Response: The prover responds by returning the following — which should satisfy the following properties. The certificate should be accepted if and only if all of the following (relevant) properties are satisfied.

The prover should always return a vector

$$x = \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_m \end{bmatrix} \in \mathbb{Z}^{m\times 1}$$

satisfying properties (a) and (b):

(a) For $1 \leq h \leq m$, if $h \notin \{j_1, j_2, \ldots, j_r\}$ then $\lambda_h = 0$ — so that Ax is a linear combination of columns $j_1, j_2, \ldots, j_r$ of A.

(b) For $1 \leq h \leq r$ the i_h^{th} entry of the vector Ax is congruent to α_h mod p.

The prover should also return one the messages *invalid*, *singular*, or *nonsingular* along with additional data corresponding to each.

If the message *invalid* is sent then no additional information is returned. The verifier should confirm property (c):

(c) Either $q \leq \mu$, $q \geq 4\mu$, or $\mu < q < 4\mu$ and q is composite.

If either *singular* or *nonsingular* is returned, instead, then the verifier should confirm property (d). This is, of course, trivial if the verifier used a reliable process to choose q during the challenge stage:

(d) $\mu < q < 4\mu$ and q is prime.

If the message *singular* is sent then the prover should also return a vector

$$y_s = \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_m \end{bmatrix} \in \mathbb{Z}^{m \times 1}$$

along with an integer k. The verifier should confirm that properties (e)–(g) are also satisfied:

(e) For $1 \leq h \leq m$, if $h \notin \{j_1, j_2, \ldots, j_r\}$ then $\sigma_h = 0$ — so that Ay_s is a linear combination of columns $j_1, j_2, \ldots, j_r$ of A.

(f) For $1 \leq h \leq r$, $0 \leq \sigma_{i_h} < q$. Furthermore, $1 \leq k \leq r$ and $\sigma_{i_k} \neq 0$.

(g) For $1 \leq h \leq r$ the i_h^{th} entry of Ay_s is divisible by q.

Finally, if the message *nonsingular* is sent then the prover should return a vector

$$y_n = \begin{bmatrix} \tau_1 \\ \tau_2 \\ \vdots \\ \tau_m \end{bmatrix} \in \mathbb{Z}^{m \times 1}.$$

The verifier should confirm that properties (h)–(i) are also satisfied.

(h) Let $k_1, k_2, \ldots, k_{m-r}$ be integers such that $1 \leq k_1 < k_2 < \cdots < k_{m-r} \leq m$ and $\{j_1, j_2, \ldots, j_r\} \cup \{k_1, k_2, \ldots, k_{m-r}\} = \{1, 2, \ldots, m\}$ — so that

$$\{j_1, j_2, \ldots, j_r\} \cap \{k_1, k_2, \ldots, k_{m-r}\} = \emptyset.$$

Then, for $1 \leq h \leq m - r$, $\tau_{k_h} = \beta_h$.

(i) Each entry of Ay_n is divisible by q.

The proof that this interactive certificate is perfectly complete is similar to, but a bit more complicated than, the proof of Lemma 2.1.

Lemma 3.1. *The above protocol is perfectly complete.*

Proof. Suppose A has rank r. Then it is certainly possible to identify indices $i_1, i_2, \ldots, i_r$ of rows and $j_1, j_2, \ldots, j_r$ of columns that are as described for the commitment stage, above, such that the matrix $C \in \mathbb{Z}^{r \times r}$ consisting of the entries of A in these rows and columns is nonsingular. As noted above (using C in place of the matrix B in the above analysis), if μ is as above then $\pi(4\mu) - \pi(\mu) > \log_2(\det(C))$, so that there exists a prime p such that $\mu < p < 4\mu$ and $C \bmod p$ is nonsingular in $\mathbb{Z}_p^{r \times r}$.

Consider any choice of integers $\alpha_1, \alpha_2, \ldots, \alpha_r$, q, and $\beta_1, \beta_2, \ldots, \beta_{m-r}$ with the properties included in the description of the above challenge stage that might be supplied by the verifier. It is necessary and sufficient to establish that the prover can return information during the response stage such that properties (a), (b), and whichever of properties (c)–(i) that are relevant, are all satisfied.

Since $C \bmod p$ is nonsingular in $\mathbb{Z}_p^{r \times r}$, there exist integers $\gamma_1, \gamma_2, \ldots, \gamma_r$ such that $0 \leq \gamma_i \leq p - 1$ for $1 \leq i \leq r$ and

$$C \times \begin{bmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_r \end{bmatrix} \equiv \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_r \end{bmatrix} \bmod p.$$

A vector $x \in \mathbb{Z}^{m \times 1}$ satisfying properties (a) and (b) can now be obtained by setting the j_h^{th} entry of x to be γ_h for $1 \leq h \leq r$ and by setting all other entries of x to be zero.

Suppose now that $q \leq \mu$, $q \geq 4\mu$, or q is composite. Then it suffices for the prover to send the message *invalid*. Property (c) is then satisfied as well, and properties (d)–(i) are irrelevant. It therefore remains only to consider the case that $\mu < q < 4\mu$ and q is prime — in which case property (d) is also satisfied.

Suppose first that $C \bmod q$ is singular in $\mathbb{Z}_q^{r \times r}$. In this case the prover should send the message *singular*. Properties (h) and (i) are irrelevant, so it suffices to show that it is possible for the prover to return a vector $y_s \in \mathbb{Z}^{m \times 1}$ and an integer k as described above such that properties (e)–(g) are satisfied.

Since $C \bmod q$ is singular in $\mathbb{Z}_q^{r \times r}$ there exist integers $\zeta_1, \zeta_2, \ldots, \zeta_r$ such that $0 \leq \zeta_h \leq q - 1$ for $1 \leq h \leq r$, and integer k such that $1 \leq k \leq r$, $\zeta_k \geq 1$, and

$$C \times \begin{bmatrix} \zeta_1 \\ \zeta_2 \\ \vdots \\ \zeta_r \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \bmod p.$$

It is easily checked that if $y_s \in \mathbb{Z}^{m\times 1}$, the j_h^{th} entry of y_s is ζ_h for $1 \leq h \leq r$ and all other entries of y_s are zero, then properties (e)–(g) are all satisfied.

Finally, suppose that $C \bmod q$ is nonsingular in $\mathbb{Z}_q^{r\times r}$. In this case the prover should send the message *nonsingular*. Properties (e)–(g) are irrelevant, so it suffices to show that it is possible for the prover to return a vector $y_n \in \mathbb{Z}^{m\times 1}$ such that properties (h) and (i) are satisfied.

Let $D \in \mathbb{Z}^{r\times m}$ be the submatrix of A with rows $i_1, i_2, \ldots, i_r$. Let $E \in \mathbb{Z}^{r\times(m-r)}$ be the submatrix of D including columns $k_1, k_2, \ldots, k_{m-r}$ (as defined in property (h) above). Let $\eta_1, \eta_2, \ldots, \eta_r$ be integers such that $1 \leq \eta_h \leq q$ for $1 \leq h \leq r$, and such that

$$C \times \begin{bmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_r \end{bmatrix} \equiv E \times \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{m-r} \end{bmatrix} \bmod q. \tag{3.3}$$

Since $C \bmod q$ is nonsingular in $\mathbb{Z}_q^{r\times r}$, such integers $\eta_1, \eta_2, \ldots, \eta_r$ certainly exist. A vector $y_n \in \mathbb{Z}^{m\times 1}$ satisfying properties (h) and (i) can now be produced by setting the j_h^{th} entry of y_n to be $q - \eta_h$ for $1 \leq h \leq r$ and setting the k_ℓ^{th} entry of y_n to be β_ℓ for $1 \leq \ell \leq m - r$. It is then immediate that property (h) is satisfied. Since the columns of C are columns $j_1, j_2, \ldots, j_r$ of the above matrix D, it follows by the definition of $\eta_1, \eta_2, \ldots, \eta_r$ at line (3.3) above that $Dy_n \equiv 0 \bmod q$. Since every row of $A \bmod q$ is a $\mathbb{Z}_q$-linear combination of the rows of $D \bmod q$, $Ay_n \equiv 0 \bmod q$ as well, establishing property (i). □

Similarly, some of the details of the proof of Lemma 2.2 are useful when establishing a claim about the soundness of the above certificate:

Lemma 3.2. *Suppose that the information provided during the commitment stage is incorrect, that is, either p is not a prime such that $\mu < p \leq 4\mu$, the matrix $C \bmod p \in \mathbb{Z}_p^{r\times r}$ is singular, or $C \bmod p$ is nonsingular but the rank of A is strictly greater than r.*

Suppose, as well, that

- *q is chosen uniformly from the set of primes that are greater than μ and less than 4μ,*
- *$\alpha_1, \alpha_2, \ldots, \alpha_r$ are chosen uniformly and independently from the set of nonnegative integers that are less than p, and*
- *$\beta_1, \beta_2, \ldots, \beta_{m-r}$ are chosen uniformly and independently from the set of nonnegative integers that are less than q.*

Then the verifier mistakenly accepts the certificate with probability at most ϵ.

Proof. It suffices to note that an incorrect certificate is only accepted if at least one of the following events takes place. The first of these can always be detected by the verifier. The

claim follows by the fact that each of the last four of these events occurs with probability at most $\epsilon/4$.

(a) p is not a prime such that $\mu < p < 4\mu$.

(b) p is prime, $\mu < p < 4\mu$, and $C \bmod p$ is a singular matrix in $\mathbb{Z}_p^{r \times r}$, but the vector $\begin{bmatrix}\alpha_1 & \alpha_2 & \dots & \alpha_r\end{bmatrix}^T \in \mathbb{Z}_p^{r \times 1}$ is in the column space of $C \bmod p$.

(c) p is prime, $\mu < p < 4\mu$, and $C \bmod p$ is nonsingular in $\mathbb{Z}_p^{r \times r}$, but $C \bmod q$ is singular in $\mathbb{Z}_q^{r \times r}$.

(d) $C \bmod q$ is nonsingular in $\mathbb{Z}_q^{r \times r}$ and the rank of A is greater than r, but $A \bmod q$ has rank r in $\mathbb{Z}_q^{n \times m}$.

(e) $C \bmod q$ is nonsingular in $\mathbb{Z}_q^{r \times r}$ and the rank of $A \bmod q$ is strictly greater than r, but it is possible for the prover to return a vector $y_n \in \mathbb{Z}^{m \times 1}$ satisfying the above properties (h) and (i).

The probability of event (b) can be bounded using the argument applied to prove Lemma 2.2 in the case that the matrix C is singular — applying this argument to the matrix $C \bmod p \in \mathbb{Z}_p^{r \times r}$. Since $\mathbb{Z}_p$ is a finite field with size p and $\mu < p < 4\mu$, it follows by this argument that the probability of this event is at most $p^{-1} < \mu^{-1} < \epsilon/4$.

If $C \bmod p$ is nonsingular in $\mathbb{Z}_p^{r \times r}$ then C is certainly nonsingular in $\mathbb{Z}^{r \times r}$. The probability of event (c) can therefore be shown to be less than $\epsilon/4$ by noting that the number of primes between μ and 4μ is greater than $4\epsilon^{-1} \times \log_2(\det(C))$, as noted above. Since q is chosen uniformly from this set of primes, and at most $\log_2(\det(C))$ such primes can divide the determinant of C, this establishes the claimed bound.

Suppose next that $C \bmod q$ is nonsingular in $\mathbb{Z}_q^{r \times r}$ — so that C is nonsingular in $\mathbb{Z}^{r \times r}$ as well — but the rank of A is greater than r. In this case there exist integers k and ℓ such that $1 \leq k \leq n$, $k \notin \{i_1, i_2, \dots, i_r\}$, $1 \leq \ell \leq m$, $\ell \notin \{j_1, j_2, \dots, j_r\}$, and the submatrix $D \in \mathbb{Z}^{(r+1) \times (r+1)}$ of A including entries in rows $i_1, i_2, \dots, i_r, k$ and columns $j_1, j_2, \dots, j_r, \ell$ is nonsingular. The probability of event (d) can now be shown to be at most $\epsilon/4$ by repeating the argument used to bound the probability of event (c), with D replacing C — for event (d) can only occur if $D \bmod q$ is singular in $\mathbb{Z}_q^{(r+1) \times (r+1)}$.

Finally, the probability of event (e) can be bounded using the argument applied to prove Lemma 2.2 in the case that the matrix C is nonsingular but the rank of A exceeds r — with $C \bmod q \in \mathbb{Z}_q^{r \times r}$ and $A \bmod q \in \mathbb{Z}_q^{n \times m}$ replacing C and A, respectively. Since the values $\beta_1 \bmod q, \beta_2 \bmod q, \dots, \beta_{m-r} \bmod q$ are chosen uniformly and independently from the finite field $\mathbb{Z}_q$, a bound of $q^{-1} < \mu^{-1} \leq \epsilon/4$ is immediate. □

Consider the cost to the verifier to participate in this protocol. $O(\min(m, n) \log_2(m + n))$ operations on bits can be used to verify that $1 \leq i_1 < i_2 < \cdots < i_r \leq n$, $1 \leq j_1 < j_2 <$

$\cdots < j_r \leq m$, and the indices of r rows and columns have been communicated by the prover during the commitment stage. Since

$$\log_2 \mu \in \Theta(\log_2 \lambda) \subseteq \Theta(\log_2(\min(n, m)) + \log_2 \log_2 \|A\| + \log_2 \epsilon^{-1}),$$

the binary representations of μ and p each have length that is at most linear in $\log_2 n + \log_2 m + \log_2 \log_2 \|A\|$, provided that ϵ^{-1} is at most polynomial in $n + m + \log_2 \|A\|$.

The AKS primality test [1] can therefore be used to verify that $\mu < p < 4\mu$ and p is prime using a number of bits that is polylogarithmic in the input size. Moreover, the variant of this test provided by Lenstra and Pomerance [6] can be used to check this using a number of operations on bits that is in $O((\log_2 n + \log_2 m + \log_2 \log_2 \|A\|)^7)$ in the worst case.

It is necessary to choose an prime q such that $\mu < q < 4\mu$ uniformly from the set of all such primes in order to form a challenge. An odd integer in this range can certainly be chosen using an expected number of operations on bits that is in $O(\log_2 \mu)$, which is logarithmic in the input size, once again. This is only being described as an "expected number of bits" because of the minor inconvenience of choosing the leading pair of bits of this integer, when one has access to a sequence of uniformly and independently selected bits: The leading bits should form the binary representation of either 1, 2, or 3.

Since there are $\frac{3}{2}\mu$ odd integers in this range, and $\pi(4\mu) - \pi(\mu) > \frac{\mu}{\ln \mu}$ as noted above, the probability that a uniformly selected odd integer in this range is prime is at least $\frac{2}{3 \ln \mu}$. Now, since $(1 - \frac{1}{x})^x < e^{-1}$ for every real number $x > 1$, it follows that if at least $\lceil \frac{2}{3} \ln \mu \rceil$ odd integers are selected uniformly and independently from this range then the probability that none of them is prime is at most $e^{-1} < \frac{1}{2}$. This can be used to establish that the expected number of operations on bits required to select the prime q during the challenge is at most polynomial in $O((\log_2 n + \log_2 m + \log_2 \log_2 \|A\|)^8)$.

Suppose next that ℓ_p and ℓ_q are positive integers such that $2^{\ell_p} < p < 2^{\ell_p + 1}$ and $2^{\ell_q} < q < 2^{\ell_q + 1}$ — so that $2^{\ell_p}, 2^{\ell_q} \in \{\mu, 2\mu\}$. An integer α_1 that is uniformly selected from the set of integers between 0 and $p - 1$ is easily obtained by choosing $\ell_p + 1$ bits uniformly and independently and using these to form the binary representation of a nonnegative integer β such that $0 \leq \beta < 2^{\ell_p + 1}$. If $\beta < p$ as well then α_1 can be set to be β; the process fails (with probability less than one-half) otherwise. The expected number of independent repetitions of the process needed to accumulate $\alpha_1, \alpha_2, \ldots, \alpha_r$ is at most $2r$. The expected number of repetitions of a similar process to accumulate $\beta_1, \beta_2, \ldots, \beta_{m-r}$ is at most $2(m - r)$. Since $O(\log_2 \mu)$ operations on bits are required for an application of either of these, the expected number of operations on bits needed to accumulate $\alpha_1, \alpha_2, \ldots, \alpha_r, \beta_1, \beta_2, \ldots, \beta_r$ is in $O(m \log_2 \mu)$.

It remains only to bound the number of operations on bits, and matrix-times-vector products by A, needed to verify that all of properties (a)–(i) that are relevant are satisfied. The verification of property (a) requires $O((m - r) \log_2 \mu)$ operations on bits.

Verification of property (b) requires a multiplication of A by in integer vector whose

entries have length in $O(\log_2 \mu)$, in order to produce a vector Ax whose entries are integers with length in $O(\log_2 m + \log_2 \|A\| + \log_2 \mu) = O(\log_2 m + \log_2 \|A\| + \log_2 \epsilon^{-1})$. $O(r(\log_2 m + \log_2 \|A\| + \log_2 \epsilon^{-1}) \log_2 \mu)$ operations on bits are certainly sufficient to complete the verification of this property. Property (g) can be verified at this cost as well, while the number of operations on bits needed to complete the verification of property (i) (after a matix-times-vector product) is in $O(n(\log_2 m + \log_2 \|A\| + \log_2 \epsilon^{-1}) \log_2 \mu)$.

As noted above, there is nothing that the verifier needs to do to check properties (c) and (d) — this has already been done.

Finally, properties (e), (f) and (h) can be verified using $O((m-r) \log_2 \mu)$ operations on bits, $O(r \log_2 \mu)$ operations on bits, and $O((m-r) \log_2 \mu)$ operations on bits, respectively.

As suggested in the introduction the largest of these costs — the costs to verify properties (b), (g), and (i) — drop significantly if the verifier has access to a reliable process (or "black box") for the multiplication of A by a specified vector modulo a specified prime, instead of one for multiplication of A by an integer vector. In particular, after applications of this black box, completion of the verification of property (b) requires r comparisons of integers that each have length in $O(\log \mu)$. Completion of the property (g) requires the comparison of r such integers to zero. Completion of the verification of property (i) requires the comparison of n such values to zero, instead. The number of additional operations required to complete the verification of properties (b) and (g) therefore falls to $O(r \log_2 \mu)$. The number of additional operations required to complete the verification of property (i) falls to $O(n \log_2 \mu)$ — and, indeed, to $O(n)$ such operations, if unpadded binary representations of the desired matrix-vector product are supplied by the black box.

It is never necessary to verify more than one of properties (g) and (i). The following can now be established from the above.

Lemma 3.3. *Consider the cost to verify an interactive certificate for the rank of an integer matrix $A \in \mathbb{Z}^{n \times m}$ using the above, protocol, in such a way that an incorrect certificate is accepted with probability less than ϵ. Suppose, as well, that ϵ^{-1} is at most polynomial in $n + m + \log_2 \|A\|$.*

(a) *If the verifier has access to a black box for the multiplication of A by a a given integer vector $x \in \mathbb{Z}^{m \times 1}$, then the cost to verify includes*

- *at most two applications of this black box to compute products Ax_1 and Ax_2 where the binary representations of each of the entries of the vectors x_1 and x_2 has length in $O(\log_2 n + \log_2 m + \log_2 \log_2 \|A\|)$, and*
- *an additional number of operations on bits. The expected number of such operations is in*

$$O((n+m)(\log_2 n + \log_2 m + \log_2 \|A\|)(\log_2 n + \log_2 m + \log_2 \log_2 \|A\|) + (\log_2 n + \log_2 m + \log_2 \log_2 \|A\|)^8).$$

(b) *If the verifier has access to a black box for the multiplication of A by a vector $x \in \mathbb{Z}^{m\times 1}$ modulo a prime p, where where x and p are specified by the verifier, then the cost to verify includes*

- *at most two applications of this black box to compute $Ax_1 \bmod p_1$ and $Ax_2 \bmod p_2$, where the binary representations of p_1, p_2, and each of the entries of x_1 and x_2 has length in $O(\log_2 n + \log_2 m + \log_2 \log_2 \|A\|)$, and*
- *an additional number of operations on bits. The expected number of such operations is in*

$$O((n+m)(\log_2 n + \log_2 m + \log_2 \log_2 \|A\|) + (\log_2 n + \log_2 m + \log_2 \log_2 \|A\|)^8).$$

There is no guaranteed bound for the worst-case cost to verify using the above version of the protocol. However, the protocol is easily modified to obtain such a bound — without significantly increasing the expected cost to verify — as well. To begin, one should change the definition of λ (at line (3.1)) by doubling this value — so that

$$\lambda = 8 \times \epsilon^{-1} \times \ell \left(\tfrac{1}{2}\ell + \log_2 \|A\|\right).$$

With this change, the probability that an incorrect certificate is accepted because of any of the conditions considered in the proof of Lemma 3.2, is now reduced to $\epsilon/2$.

Suppose next that one has a protocol to uniformly select a value from a fixed set that uses t operations on bits in the worst case — but that fails, instead of producing such a value, with probability at most $1/4$. Suppose, as well, that one wishes to obtain k values that are selected uniformly and independently from this set — and that the probability that this process is allowed to fail is at most $\epsilon/8$.

Note first that if one makes $3k$ independent attempts to select values then the expected number of uniformly and independently selected values is equal to ck, for a real number c such that $2 < \frac{9}{4} \leq c \leq 3$,while the maximum number of such values that can be obtained is $3k$.

Let p be the probability that fewer than k uniformly and independently selected values have been obtained. Then the expected number of values obtained is certainly at most

$$pk + 3(1-p)k = 3k - 2pk$$

so that

$$ck \leq 3k - 2pk,$$

that is,

$$2pk \leq (3-c)k \leq k$$

and $p \leq \frac{1}{2}$. It follows that if *this* process is iterated at least $\lceil \log_2(8 \times \epsilon^{-1}) \rceil$ times then the probability that all of these attempts, to obtain k uniformly and independently selected values, fail is at most $\epsilon/8$. Consequently at most $3k\lceil \log_2(8 \times \epsilon^{-1}) \rceil \in O(k \log_2 \epsilon^{-1})$ iterations of the *initial* process are required — and $O(kt \log_2 \epsilon^{-1})$ operations on bits are used, in the worst case, by a process that either returns k values sampled uniformly and independently from the desired set, or fails with probability at most $\epsilon/8$.

Consider now the process used by the verifier to select the prime q — ignoring, for the moment, the cost to select integers uniformly and independently from the set of odd integers between μ and 4μ. A continuation of the analysis given above establishes that if $\lceil \frac{2}{3} \ln \mu \rceil \times \lceil \log_2(8 \times \epsilon^{-1}) \rceil$ such integers are sampled uniformly and independently from this set, then the probability that they are all composite is at most $\epsilon/8$. Since the binary representations of these odd integers each have length in $O(\log_2 \mu)$, a process that uses a number of operations on bits that is polynomial in $O((\log_2 n + \log_2 m + \log_2 \log_2 \|A\|)^9)$ (excluding the cost to sample from a set of odd integers) in the worst case, and that fails with probability at most $\epsilon/8$, is easily obtained — assuming, as above, that ϵ^{-1} is at most polynomial in $n + m + \log_2 \|A\|$.

Now consider the problem of sampling from the above set of of odd integers — considering, in particular, the leading pair of bits of each of these integers. A process using $t \in O(1)$ operations on bits to choose these leading bits, which fails with probability $\frac{1}{4}$, is easily described: Choose a pair of random bits — accepting if these are the binary representations of either 1, 2 or 3, and failing if these are form the binary representation of 0. The number, k of integers that are required, is the number $\lceil \frac{2}{3} \ln \mu \rceil \times \lceil \log_2(8 \times \epsilon^{-1}) \rceil$ mentioned above. It now follows by the above that a process that uses $O(\log_2 n + \log_2 m + \log_2 \log_2 \|A\|)^2)$ operations on bits in the worst case can be used (with the same assumption concerning ϵ^{-1} as above) to choose the leading pairs of bits of the binary representations of the desired integers, or to fail with probability at most $\epsilon/8$. The remaining bits of the binary representations integers can then be selected — without increasing the probability of failure, and also using $O(\log_2 + \log_2 m + \log_2 \log_2 \|A\|)^2)$ operations in the worst case — simply by selecting the remaining (non-constant) bits uniformly and independently.

Next consider the uniform selection of an integer x such that $0 \leq x \leq p-1$ — or such that $0 \leq x \leq q-1$ — in order to address the uniform and independent selection of $\alpha_1, \alpha_2, \ldots, \alpha_r$ and of $\beta_1, \beta_2, \ldots, \beta_{m-r}$. Processes that sample uniformly from the desired sets, using a number of operations on bits in $O(\log_2 \mu)$ and failing with probability at most $\frac{1}{2}$, have already been described. A process (for each of p and q) with the same asymptotic worst-case cost that fails with probability at most $\frac{1}{4}$, is easily obtained: Apply the process that has already been described. If it succeeds then report its output. Otherwise repeat the process.

Setting $t \in O(\log_2 \mu)$ and $k = r$, and with the same assumption about ϵ^{-1}, a process that either produces $\alpha_1, \alpha_2, \ldots, \alpha_r$ as required, or fails with probability at most $\epsilon/8$, is now easily obtained. The number of operations used on bits in the worst case is in $O(r(\log_2 n +$

$\log_2 m + \log_2 \log_2 \|A\|)^2)$. Setting $k = m - r$ one obtains a process that either produces $\beta_1, \beta_2, \ldots, \beta_{m-r}$ as required or fails with probability at most $\epsilon/8$; the number of operations on bits used in the worst case is in $O((m-r)(\log_2 n + \log_2 m + \log_2 \log_2 \|A\|)^2)$.

Finally, consider an interactive protocol that is as described above except that the modified processes to choose q and $\alpha_1, \alpha_2, \ldots, \alpha_r, \beta_1, \beta_2, \ldots, \beta_{m-r}$ are used. If any of the modified processes fails then the verifier "gives up" and accepts the information supplied by the prover during the commitment phase. Assuming the availability of a black box to compute $Ax \bmod p$ for a specified integer vector x and prime p, the expected cost for verification is still as given in part (b) of Lemma 3.3. The number of additional operations on but used, in the worst case, is in

$$O(n(\log_2 n + \log_2 m + \log_2 \log_2 \|A\|) + m(\log_2 n + \log_2 m + \log_2 \log_2 \|A\|)^2 + (\log_2 n + \log_2 m + \log_2 \log_2 \|A\|)^9)$$

assuming, once again, that ϵ^{-1} is at most polynomial in $n + m + \log_2 \|A\|$.

It remains only to consider the communication complexity of this protocol. Since $r \leq \min(n, m)$, the following is easily proved by inspection of the above protocol.

Lemma 3.4. *Consider the cost to verify an interactive certificate for the rank of an integer matrix $A \in \mathbb{Z}^{n \times m}$ using the above protocol, in such a way that an incorrect certificate is accepted with probability less than ϵ. Suppose, as well, that ϵ^{-1} is at most polynomial in $n + m + \log_2 \|A\|$. Then — after (and excluding) the communication of the matrix A from the verifier to the prover — $O(m(\log_2 n + \log_2 m + \log_2 \log_2 \|A\|))$ bits are transmitted between the prover and verifier during the execution of this protocol.*

References

[1] M. Agrawal, N. Kayal, and N Saxena. PRIMES is in P. *Annals of Mathematics*, 160:781–793, 2004.

[2] J.-G. Dumas and E. Kaltofen. Essentially optimal interactive certificates in linear algebra. In *Proceedings, 2014 International Symposium on Symbolic and Algebraic Computation (ISSAC '14)*, pages 146–153. ACM Press, 2014.

[3] S. Goldwasser, Y. T. Kalai, and G. N. Rothblum. Delegating computation: Interactive proofs for muggles. In *2008 ACM Symposium on Theory of Computing (STOC '08)*, pages 113–122. ACM Press, 2008.

[4] E. Kaltofen, B. Li, Z. Yang, and Zhi. L. Exact certificates in global polynomial optimization via sums-of-squares of rational functions with rational coefficients. *Journal of Symbolic Computation*, 47:1–15, 2012.

[5] E. Kaltofen, M. Nehring, and B. D. Saunders. Quadratic-time certificates in linear algebra. In *Proceedings, 2011 International Symposium on Symbolic and Algebraic Computation (ISSAC '11)*, pages 171–176. ACM Press, 2011.

[6] H. W. Lenstra, Jr. and C. Pomerance. Primality testing with Gaussian periods. `https://math.dartmouth.edu/~carlp/aks041411.pdf`, April 2011. Version 20110412.

[7] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois Journal of Mathematics*, 6:64–94, 1962.

[8] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the Association of Computing Machinery*, 27:701–717, 1980.

[9] J. Thaler. Time-optimal interactive proofs for circuit evaluation. In *Advances in Crpytology — CRYPTO '13*, volume 8043 of *Lecture Notes in Computer Science*, pages 71–89. Springer Berlin Heidelberg, 2013.

[10] R. Zippel. Probabilistic algorithms for sparse polynomials. In *EUROSAM '79*, volume 72 of *Lecture Notes in Computer Science*, pages 216–226. Springer-Verlag, 1979.