PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 60 (74), 1996, 15–26

COMPUTATION OF DETERMINANTS AND INVERSES OF RECTANGULAR OR SINGULAR MATRICES USING RESIDUE ARITHMETIC

Predrag Stanimirović

Communicated by Žarko Mijajlović

Abstract. We make an application of the single or multiple modulus residue arithmetic in exact computation of the determinants and pseudoinverses of rectangular or singular matrices with rational entries, using the notions introduced by M. Stojaković and M. Radić. Proper selections of a prime modulus (or moduli) in particular algorithms are given. Also, a comparison of different estimates for the suitable choice of modulus (or moduli) is given.

1. Introduction and preliminaries. The set of $r \times s$ rational matrices with rank g is denoted by $\mathbb{Q}_g^{r\times s}$. The rank and the determinant of a matrix A will be denoted by $r(A)$ and $\det(A)$, respectively. Let $\alpha = \{\alpha_1, \dots, \alpha_t\}$ be a subset of $\{1, \dots, r\}$ and $\beta = \{\beta_1, \dots, \beta_t\}$ a subset of $\{1, \dots, s\}$. The matrix and minor of a rectangular matrix $A \in \mathbb{Q}^{r\times s}$ containing rows $\alpha_1, \dots, \alpha_t$ and columns $\beta_1, \dots, \beta_t$ is denoted by $A\begin{bmatrix} \alpha_1 \dots \alpha_t \\ \beta_1 \dots \beta_t \end{bmatrix} = A_{[\beta]}^{[\alpha]}$ and $A\begin{pmatrix} \alpha_1 \dots \alpha_t \\ \beta_1 \dots \beta_t \end{pmatrix} = \left| A_{[\beta]}^{[\alpha]} \right|$, respectively. Also, the following *algebraic complement* of the minor $A_{[\beta]}^{[\alpha]}$ is used:

$$A_{ij}\begin{pmatrix} \alpha_1 \dots \alpha_{p-1}\ i\ \alpha_{p+1} \dots \alpha_g \\ \beta_1 \dots \beta_{q-1}\ j\ \beta_{q+1} \dots \beta_g \end{pmatrix} = (-1)^{p+q} A\begin{pmatrix} \alpha_1 \dots \alpha_{p-1}\ \alpha_{p+1} \dots \alpha_t \\ \beta_1 \dots \beta_{q-1}\ \beta_{q+1} \dots \beta_t \end{pmatrix} = \frac{\partial}{\partial a_{ij}} \left| A_{[\beta]}^{[\alpha]} \right|.$$

We denote by (p) $([p])$ the permutation (combination) $p_1, \dots, p_t$. Index of the permutation (p) is denoted by $J(p)$, and the sum over all possible permutations (combinations) $p_1, \dots, p_t$ is denoted by $\sum_{(p)}$ $(\sum_{[p]})$. The absolute value of a given integer i we denote by $|i|$.

Theoretical base of presented algorithms are the notions of determinants for rectangular matrices (*rectangular determinants*) and implied definitions of generalized inverses, presented in [**3, 4, 5, 7**].

AMS Subject Classification (1991): Primary 11Y99

In an earlier paper [**9**] we establish algorithms for the exact computation of *rectangular determinants* and induced generalized inverses, for rectangular matrices with rational or complex elements. In algorithms described in [**9**] integers, real, complex and rational numbers are represented together as the elements of an adequate structure in programming language C, called the internal form of numbers. The internal form of a matrix is two-dimensional array or binary tree of the internal forms of numbers. Arithmetic operations on the internal forms of rational numbers require a considerable number of usual arithmetic operations and slow shorting of numerators and denominators. We use a possibility to replace computations on finite sets of rational numbers by corresponding computations in the ring of residues with sufficiently large modulus. Similar principles have been already used for various calculations, see [**1, 2, 11**]. In [**10**] residue arithmetic was applied in the theory of mathematical spectra, introduced by M. Petrović. Also, residue arithmetic algorithms were used in computing the Moore-Penrose inverse [**2, 6, 8**].

For the sake of completeness we provide a tutorial description of the residue arithmetic [**1, 2, 11**].

Definition 1.1. [**12**] For any given base $\beta = \{m_1, \dots, m_n\}$ the residue representation of an integer a, denoted by $|a|_\beta$ is another n-tuple $\{r_1, \dots, r_n\}$, where the r_i are integers defined by a set of n equations $a = q_i m_i + r_i\,, \quad i = 1, \dots, n\,,$ and q_i is an integer chosen so that $0 \le r_i < m_i$. The quantity r_i is the least positive remainder of the division of a by m_i and is designated as the *least residue of a modulo m_i* or $|a|_{m_i}$.

THEOREM 1.1. [**12**] *For the residue system consisting of moduli $m_1, \dots, m_n$ let a and b be represented in the residue form. If $M = \prod_{k=1}^{n} m_k$, then within the interval $[0, M-1]$ only one integer, namely $|a \circ b|_M$ has the residue representation $\{\big|\,|a|_{m_1} \circ |b|_{m_1}\big|_{m_1}, \dots, \big|\,|a|_{m_n} \circ |b|_{m_n}\big|_{m_n}\}$, where $\circ$ denotes addition $(+)$, subtraction $(-)$ or multiplication $(*)$.*

THEOREM 1.2. [**12**] *If $a \neq 0$ and $(a, M) = 1$, i.e. $(a, m_i) = 1$, $i = 1, \dots, n$, then there exists unique integer b such that $0 < b < M$ and $|ab|_M = 1$, i.e. $ab \equiv 1 (mod\ M)$. The integer b is called the multiplicative inverse of a modulo M, and is denoted by $a^{-1}(M)$.*

THEOREM 1.3. [**2**] *Let $\tilde{\mathbb{Q}}$ be the set of rational numbers invertible in $\mathbb{Z}_M = \{0, \dots,\ M-1\}$, i.e. $\tilde{\mathbb{Q}} = \{a/b\,:\,(b, M) = 1\}$. Also, let β be a base-vector which contains prime moduli $m_1, \dots m_n$, $M = \prod_{k=1}^{n} m_k$ and N the maximal nonnegative integer such that $2N^2+1 \le M$. If we define a finite subset $F_N = \{a/b \in \tilde{\mathbb{Q}}\,:\,(a,b) = 1,\quad 0 \le |a| < N,\quad 0 < |b| < N\}$ of $\tilde{\mathbb{Q}}$ and finite subset $\tilde{\mathbb{Z}}_M = \{|a/b|_M\,:\,a/b \in F_N\}$ of $\mathbb{Z}_M$, then $|\cdot|_M\,:\,F_N \mapsto \tilde{\mathbb{Z}}_M$ is a bijection.*

We also recall definitions of determinants of rectangular matrices and induced notions of generalized inverses, introduced in [**3, 4, 5, 7**]:

Definition 1.2. The element in i-th row and j-th column of generalized inverse

$A^{-1}_{(\epsilon,t)}$ of $A \in \mathbb{Q}_g^{r\times s}$, denoted by $\left(A^{-1}_{(\epsilon,t)}\right)^{-1}_{ij}$ is equal to

$$\left(A^{-1}_{(\epsilon,t)}\right)^{-1}_{ij} = \frac{A^{(\epsilon,t)}_{ij}}{\det^{\epsilon}_t(A)} = \frac{\sum\limits_{\substack{1\le\alpha_1<\ldots<j<\ldots<\alpha_t\le r\\ 1\le\beta_1<\ldots<i<\ldots<\beta_t\le s}} \epsilon^{(\alpha_1+\ldots+\alpha_t)+(\beta_1+\ldots+\beta_t)} \frac{\partial}{\partial a_{ji}} \left| A^{[\alpha]}_{[\beta]} \right|}{\sum\limits_{\substack{1\le\gamma_1<\ldots<\gamma_t\le r\\ 1\le\delta_1<\ldots<\delta_t\le s}} \epsilon^{(\gamma_1+\ldots+\gamma_t)+(\delta_1+\ldots+\delta_t)} \left| A^{[\gamma]}_{[\delta]} \right|},$$

where $\epsilon \in \{-1,1\}$ and $1 < t = r_\epsilon(A) \le r(A) \le \min\{r,s\}$ is the greatest integer such that $\det^{\epsilon}_t(A) \neq 0$. For $\epsilon = 1$ we get Stojaković's generalized inverse (denoted by $A^{-1}_{(S,t)}$), and for $\epsilon = -1$ we get Radić's generalized inverse (denoted by $A^{-1}_{(R,t)}$). The expression $\det^{\epsilon}_t(A) = \sum\limits_{\substack{1\le\alpha_1<\ldots<\alpha_t\le r\\ 1\le\beta_1<\ldots<\beta_t\le s}} \epsilon^{(\alpha_1+\ldots+\alpha_t)+(\beta_1+\ldots+\beta_t)} \left| A^{[\alpha]}_{[\beta]} \right|$ is called the *rectangular determinant* of A, and is denoted by $\det^S_t(A)$, for $\epsilon = 1$ and $\det^R_t(A)$ for $\epsilon = -1$. Similarly, the expression

$$A^{(\epsilon,t)}_{ij} = \sum_{\substack{1\le\alpha_1<\ldots<j<\ldots<\alpha_t\le r\\ 1\le\beta_1<\ldots<i<\ldots<\beta_t\le s}} \epsilon^{(\alpha_1+\ldots+\alpha_t)+(\beta_1+\ldots+\beta_t)} \frac{\partial}{\partial a_{ji}} \left| A^{[\alpha]}_{[\beta]} \right|$$

is called *generalized algebraic complement* of A corresponding to the element a_{ij}. The matrix $\mathrm{adj}^{(\epsilon,t)}(A) = \left(A^{(\epsilon,t)}_{ij}\right)$, $\left(\substack{i=1,\ldots,s\\ j=1,\ldots,r}\right)$ is called *generalized adjoint matrix* of A.

2. Several new notions. In this section, using presented theory, we introduce several notions which will be useful for the algorithms described later.

Definition 2.1. Given a matrix $A = (a_{ij}) \in \mathbb{Q}^{r\times s}$ and a modulus m, relatively prime to all denominators in A, the matrix $P = (p_{ij}) \in \mathbb{Q}^{r\times s}$ is called the residue of A modulo m if $p_{ij} = |a_{ij}|_m$, for all $i = 1,\ldots,r,\quad j = 1,\ldots,s$. The matrix P we denote by $P = |A|_m$.

Definition 2.2. Let a matrix $A = (a_{ij}) \in \mathbb{Q}^{r\times s}$ be given and $\beta = [m_1,\ldots,m_n]$ be an n-tuple, representing a base of a residue number system. If each m_i is relatively prime to all denominators in A, then the residue representation of A, denoted by $|A|_\beta$, is the ordered n-tuple of matrices $[P_1,\ldots,P_n]$, where $P_i = |A|_{m_i}$.

Definition 2.3. Residual Gaussian elimination with pivoting and modulus m of a matrix $A \in \mathbb{Q}_g^{r\times r}$ is the following transformation:

$$m_{ik} = \left| \frac{a^{(k)}_{ik}}{a^{(k)}_{kk}} \right|_m, \quad a^{(k+1)}_{ij} = \left| a^{(k)}_{ij} - \left| m_{ik} a^{(k)}_{kj} \right|_m \right|_m, \quad \left(\substack{k=1,\ldots,g-1\\ i,j=k+1,\ldots,r}\right);$$
$$a^{(1)}_{pq} = |a_{pq}|_m, \quad p,q = 1,\ldots,r.$$

Definition 2.4. For $A \in \mathbb{Q}_g^{r\times s}$ residue representation of $\det(A)$, denoted by $|\det(A)|_m$ is equal to

$$|\det(A)|_m = \left|\det(|A|_m)\right|_m = (-1)^\rho \left| \left| a^{(1)}_{11} a^{(2)}_{22} \right|_m \cdots a^{(g)}_{gg} \right|_m,$$

where ρ represents the number of interchanges of rows (and columns), performed during the residual Gaussian elimination.

Definition 2.5. Residual rank of $A \in \mathbb{C}_g^{r\times s}$ corresponding to the given modulus m, denoted by $r(A,m)$ is the number of nonvanishing elements lying on the main diagonal after the residual Gaussian elimination with modulo m.

The relation $r(A,m) \le r(A)$ is evident. In the following example we show the existence of a matrix A and modulus m which satisfy the inequality $r(A,m) < r(A)$.

Example 2.1 For the matrix $A = \begin{pmatrix} \frac{1}{2} & \frac{7}{6} & \frac{2}{3} \\ \\ -1 & \frac{95}{3} & \frac{98}{3} \end{pmatrix}$ we have $r(A) = 2$, $r(A,m) = 1$ and $r(A,17) = 1$.

Definition 2.6. Generalized rank of $A \in \mathbb{Q}_g^{r\times s}$ corresponding to the modulus m, denoted by $r(A,\epsilon,m)$ is the greatest integer $1 < r(A,\epsilon,m) \le g$ such that

$$\left|\det{}^{\epsilon}_{r(A,\epsilon,m)}(|A|_m)\right|_m \neq 0.$$

3. Computing determinants applying residue arithmetic. Let $A = \left(\frac{b_{jk}}{i_{jk}}\right)$, $\left(\begin{smallmatrix} 1\le j\le r \\ 1\le k\le s \end{smallmatrix}\right)$ be a rectangular rational matrix of rank g. Selecting the base-vector $\beta = [m_1,\dots,m_n]$ is an important item and should ensure that the numerator and the denominator of the *rectangular determinant* can be represented into the corresponding sets $\tilde{\mathbb{Z}}_M$ and F_N, introduced in Theorem 1.3. At first, we do not know the *rectangular determinant*. So, we use an adequate upper bound N for the numerator and the denominator of the result which is estimated in the procedure MODUL. Also, using the estimated value N for the result we select moduli $m_1,\dots,m_n$ in the same algorithm. The formal parameter l of the procedure MODUL is an integer representing the size of selected minors. The number n of moduli depends on N and it can be obtained from the following two conditions:

- (K_1) Elements of the base-vector $\beta = [m_1,\dots,m_n]$ are the smallest successive primes such that $M = \prod_{p=1}^{n} m_p \ge 2N^2+1$, and
- (K_2) m_1 is the smallest prime such that $m_1 \ge 2u^2+1$, where $u = \max\limits_{j,k}\{|i_{jk}|,|b_{jk}|\}$.

Remarks 3.1. 1. Note that the criterion (K_1), according to Theorem 1.3, ensures that $|\cdot|_M : F_N \mapsto \tilde{\mathbb{Z}}_M$ is a bijection, and the criterion (K_2) ensures $(m_i, i_{jk}) = 1$, for all denominators and for each of selected moduli.

2. The modulus m_1 is computed independently from N.

3. Modulus m_1 can be obtained as the smallest prime such that $m_1 \ge \max\limits_{j,k}\{|i_{jk}|\}$. But, assuming the principle: "it is desirable to have as few moduli as possible, because all the operations which involve a mixed-radix conversion have execution times proportional to n, the number of moduli" **[12]**, we use the condition (K_2).

Algorithm MODUL(l)

STEP 1. Compute values

$$IPQ = |i_{\sigma(p_1)q_1}||i_{\sigma(p_2)q_2}|\dots|i_{\sigma(p_l)q_l}| \quad \text{and} \quad BPQ = |b_{\sigma(p_1)q_1}||b_{\sigma(p_2)q_2}|\dots|b_{\sigma(p_l)q_l}|,$$

where $|i_{\sigma(p_k)q_k}|$ and $|b_{\sigma(p_k)q_k}|$, $1 \leq k \leq l$ denote the absolute values of the numbers $i_{\sigma(p_k)q_k}$ and $b_{\sigma(p_k)q_k}$ respectively, for all combinations $[p] = (1 \leq p_1 < \dots < p_l \leq r)$, $[q] = (1 \leq q_1 < \dots < q_l \leq s)$ and all permutations (σ) of the set $\{p_1, \dots, p_l\}$. The sets of corresponding values will be denoted by $\{IPQ\}$ and $\{BPQ\}$ respectivelly.

STEP 2. Compute the lowest common denominator for elements of the set $\{IPQ\}$, denoted by $\text{lcd}(\{IPQ\})$.

STEP 3. Compute $d = \sum\limits_{[q],[p]} \sum\limits_{(\sigma)} BPQ \dfrac{\text{lcd}(\{IPQ\})}{IPQ}$.

STEP 4. $N = \max\{d, \text{lcd}(\{IPQ\})\}$.

STEP 5. Determine the number of moduli n and the set of moduli $\{m_1, \dots, m_n\}$:

(5.1) $n \leftarrow 1$

(5.2) m_1 is the first prime such that $m_1 \geq 2u^2 + 1$, $u = \max\limits_{j,k}\{| i_{jk} |, |b_{jk}|\}$.

(5.3) $pr \leftarrow m_1$.

(5.4) **while** $pr < 2N^2 + 1$ **do**

$n \leftarrow n + 1$

m_n is the first prime greater than m_{n-1}

$pr \leftarrow pr * m_n$. ■

THEOREM 3.1. *The rectangular determinant* $\det_t^\epsilon(A)$ *of* $A \in \mathbb{Q}_g^{r\times s}$ *can be computed exactly using a base-vector* $\beta = [m_1, \dots, m_n]$ *which is obtained applying the algorithm* MODUL(t), for $t = r_c(A)$.

Proof. The denominator of $\det_t^\epsilon(A)$ is equal to $\text{lcd}(\{IPQ\}) \leq N$. Also, the numerator is

$$\sum_{[q],[p]} \epsilon^{(p_1+\dots+p_t)+(q_1+\dots+q_t)} \sum_{(\sigma)} (-1)^{J(\sigma)} b_{\sigma(p_1)q_1} \dots b_{\sigma(p_t)q_t} \frac{\text{lcd}(\{IPQ\})}{i_{\sigma(p_1)q_1} \dots i_{\sigma(p_t)q_t}} \leq d \leq N.$$

In view of $M = \prod_{k=1}^n m_k \geq 2N^2 + 1$, we easily conclude that selected base-vector $\beta = [m_1, \dots, m_n]$ from the Algorithm MODUL(t) satisfies the requirements of Theorem 1.3, and consequently suffices for the exact computation of $\det_t^\epsilon(A)$. □

The following function computes the residue representation of the *rectangular determinant* of a rational matrix $A \in \mathbb{Q}_g^{r\times s}$, for a given single modulus m and *generalized rank* l.

function $\mathrm{DET}(A, l, \epsilon, m)$

STEP 1. Compute $W = |A|_m$.

STEP 2. Denote by $G = G\begin{bmatrix} p_1 & \dots & p_l \\ q_1 & \dots & q_l \end{bmatrix}$ the matrix obtained applying the residual Gaussian elimination with pivoting and with module m on the submatrix $W\begin{bmatrix} p_1 & \dots & p_l \\ q_1 & \dots & q_l \end{bmatrix}$. Then

$$\mathrm{DET}(A, l, \epsilon, m) = \left| \sum_{[p],[q]} \left[\epsilon^{(p_1+\dots+p_t)+(q_1+\dots+q_t)} \left| \prod_{k=1}^{t} G_{p_k q_k} \right|_m \right] \right|_m . \qquad \blacksquare$$

Algorithm R_1, given below, for a given matrix $A \in \mathbb{Q}_g^{r\times s}$, using the procedure MODUL, computes the base-vector $\beta = [m_1, \dots, m_n]$ sufficient for exact computation of the *rectangular determinant* corresponding to the *generalized rank* $t = r(A, \epsilon, m_1)$.

Algorithm R_1

STEP 1. Compute m_1, as the smallest prime such that $m_1 \geq 2u^2 + 1$, and the residual rank $r(A, m_1)$, introduced in Definition 2.5.

STEP 2. Select moduli $m_1, \dots, m_n$ using procedure MODUL(t).

STEP 3. Compute $\mathrm{DET}(A, t, \epsilon, m_1)$.

STEP 4. **if** $\mathrm{DET}(A, t, \epsilon, m_1) \neq 0$ **then** $r(A, \epsilon, m_1) = t$
else $t = t - 1$ and **go to** STEP 2. $\blacksquare$

The algorithm DM describes the application of single-module residue arithmetic for computing the *rectangular determinant* of a given rectangular matrix $A \in \mathbb{Q}_g^{r\times s}$. This algorithm is applicable in the case $m_1 \geq 2N^2 + 1 \geq 2u^2 + 1$.

Algorithm DM

STEP 1. Applying Algorithm R_1 select prime modulus $m = m_1$ and compute $t = r(A, \epsilon, m)$ and $\mathrm{DET}(A, t, \epsilon, m)$.

STEP 2. The value of $\det_t^{\epsilon}(A)$ can be obtained converting $\mathrm{DET}(A, t, \epsilon, m)$ into corresponding fraction using modulus m. $\blacksquare$

The determinant of a rational rectangular matrix can be computed by means of the multiple-modulus residue arithmetic, as follows:

Algorithm DBETA

STEP 1. Applying the algorithm R_1 select a base-vector $\beta = [m_1, \dots, m_n]$ and compute $t = r(A, \epsilon, m_1)$.

STEP 2. **for** $i \leftarrow 1$ **to** n compute $\mathrm{DET}(A, t, \epsilon, m_i)$.

(Obtain the residue representation $|\det_t^\epsilon(A)|_\beta = \{|\det_t^\epsilon(A)|_{m_1}, \dots, |\det_t^\epsilon(A)|_{m_n}\}$).

STEP 3. Convert given multiple residue representation into the residue modulo $M = \prod_{k=1}^n m_k$, i.e., into the mixed-radix representation using the radices $m_1, \dots, m_n$.

STEP 4. Convert given mixed-radix representation into the corresponding fraction using the modulus M. ■

Example 3.1. In this example we demonstrate an exact computation of Radić's determinant of a given matrix $A = \begin{pmatrix} -\frac{1}{2} & 2 & \frac{5}{20} & 0 \\ \frac{12}{16} & -2 & \frac{9}{6} & 1 \end{pmatrix}$. The modulus m_1 is the smallest prime greater than or equal to $2*4^2+1$, i.e. $m_1 = 37$, and $r(A, m_1) = 2$. Now, using $t = 2$, according to the algorithm MODUL(2) we get

$$\begin{aligned} \mathrm{lcd}(\{IPQ\}) &= \mathrm{lcd}(\{2,\ 4,\ 4,\ 16,\ 2,\ 4,\ 2,\ 4,\ 1,\ 1,\ 4,\ 2\}) = 16; \\ \{BPQ\} &= \{2,\ 6,\ 3,\ 3,\ 1,\ 0,\ 6,\ 2,\ 2,\ 0,\ 1,\ 0\}; \\ d_{pq} &= 2\frac{16}{2} + 6\frac{48}{4} + 3\frac{48}{4} + 3\frac{48}{16} + 1\frac{48}{2} + 0 + 6\frac{48}{2} + 2\frac{48}{4} + 2\frac{48}{41} + 0 + 1\frac{48}{4} + 0 = \\ &= 155 = N. \end{aligned}$$

Applying the step 5 of the algorithm MODUL(2) we get $n = 3$, $\beta = [37, 41, 43]$. Also, in the step 3 of the algorithm R_1 we obtain $\mathrm{DET}(A, 2, \epsilon, 37) = 4 \neq 0$, and consequently $t = r(A, \epsilon, 37) = 2$.

The standard residue representation of $\det_2^R(A)$ is $|\det_2^R(A)|_\beta = (4,\ 35,\ 42)$, the mixed-radix representation is 44848. Finally, recovering this value with modulus $M = \prod_{k=1}^{3} m_k = 65231$ into the resulting fraction we get $\det_2^R(A) = 27/16$.

Example 3.2. For $A = \begin{pmatrix} \frac{1}{5} & 1 & \frac{38}{57} & -1 & 12 \\ -\frac{15}{18} & \frac{1}{4} & 2 & \frac{39}{27} & -1 \\ 2 & \frac{85}{119} & 1 & -\frac{78}{65} & 0 \end{pmatrix}$ we describe the computation of $\det_t^S(A)$. Application of the algorithm R_1 leads to: $\mathrm{lcd}(\{IPQ\}) = 18900$, $d = 4477952 = N$. This implies $n = 6$, $\beta = [347, 349, 353, 359, 367, 373]$, $t = r(A, \epsilon, 347) = 2$. Standard residue representation of $\det_2^S(A)$ is $|\det_2^S(A)|_\beta = (83,\ 239,\ 310,\ 176,\ 59,\ 298)$. Mixed-radix representation of $\det_2^S(A)$, with radices $m_1, \dots, m_6$ is 1234065952988185. Recovering this value from $\tilde{\mathbb{Z}}_M$ with modulus $M = \prod_{k=1}^{6} m_k = 2100868898529971$ we get $\det_2^S(A) = -217253/1350$.

4. Computing generalized inverses using residue arithmetic. In this section we also consider a rational matrix $A = \left(\frac{b_{jk}}{i_{jk}}\right)$, $\left(\begin{smallmatrix} 1\le j\le r \\ 1\le k\le s \end{smallmatrix}\right)$ of rank g. In the algorithms described below we use the following notations: consider two integers $1 \le u \le s$, $1 \le v \le r$. Denote by $[p^1] = \{p_1^1 < \dots < p_{t-1}^1\}$ and

$[q^1]=\{q_1^1<\dots<q_{t-1}^1\}$ the combinations derived from the combinations $[p]=\{1\le p_1<\dots<v<\dots<p_t\le r\}$ and $[q]=\{1\le p_1<\dots<v<\dots<p_t\le r\}$ deleting the elements v and u respectively. We denote by $\sigma^1(p_1^1),\dots,\sigma^1(p_{t-1}^1)$ the permutations of the set $\{p_1^1<\dots<p_{t-1}^1\}$. The set of values

$$IPQ1=|i_{\sigma^1(p_1^1)q_1^1}||i_{\sigma^1(p_2^1)q_2^1}|\dots|i_{\sigma^1(p_{t-1}^1)q_{t-1}^1}|$$
$$BPQ1=|b_{\sigma^1(p_1^1)q_1^1}||b_{\sigma^1(p_2^1)q_2^1}|\dots|b_{\sigma^1(p_{t-1}^1)q_{t-1}^1}|$$

defined for all combinations $[p^1]$ and $[q^1]$ and all permutations (σ^1) of the set $\{p_1^1,\dots,p_{t-1}^1\}$ is denoted by $\{IPQ1\}$ and $\{BPQ1\}$, respectively.

THEOREM 4.1. *Generalized adjoint matrix* $\operatorname{adj}^{(\epsilon,t)}(A)$ *of* $A\in\mathbb{Q}_g^{r\times s}$ *can be exactly computed using base-vector* $\beta=[m_1,\dots,m_n]$*, defined by* (K_1) *and* (K_2)*, where the upper bound* N *for all numerators and denominators of the inverse matrix can be computed as follows:* $N=\max\{\operatorname{lcd}(\{IPQ\}),\max\{d_{uv}:1\le u\le s;1\le v\le r\}\}$*, where*

$$d=\sum_{[q],[p]}\sum_{(\sigma)}BPQ\frac{\operatorname{lcd}(\{IPQ\})}{IPQ};$$

(*)
$$d_{uv}=\begin{cases}\left|\dfrac{i_{vu}}{b_{vu}}\right|d, & \textit{if } \operatorname{lcd}(\{IPQ1\}) \textit{ is not divisible by } i_{vu}\\ \dfrac{1}{|b_{vu}|}d, & \textit{otherwise.}\end{cases}\qquad\begin{pmatrix}1\le u\le s\\1\le v\le r\end{pmatrix}$$

Proof. The denominator of $A_{uv}^{(\epsilon,t)}$ is equal to

$$\operatorname{lcd}(\{IPQ1\})=\operatorname{lcd}(\{|i_{\sigma(p_1^1)q_1^1}||i_{\sigma(p_2^1)q_2^1}|\dots|i_{\sigma(p_{t-1}^1)q_{t-1}^1}|\})\le\operatorname{lcd}(\{IPQ\})\le N.$$

Similarly, the numerator can be estimated as follows:

$$\begin{aligned}&\sum_{[q^1],[p^1]}\epsilon^{(p_1+\dots+p_t)+(q_1+\dots+q_t)}\sum_{(\sigma^1)}(-1)^{J(\sigma^1)}b_{\sigma^1(p_1^1)q_1^1}\dots b_{\sigma^1(p_{t-1}^1)q_{t-1}^1}\\&\qquad\qquad\times\frac{\operatorname{lcd}(\{IPQ1\})}{i_{\sigma^1(p_1^1)q_1^1}\dots i_{\sigma^1(p_{t-1}^1)q_{t-1}^1}}\\&\le\sum_{[q],[p]}\sum_{(\sigma)}b_{\sigma(p_1)q_1}\dots b_{vu}\dots b_{\sigma(p_t)q_t}\frac{\operatorname{lcd}(\{IPQ1\})}{i_{\sigma(p_1)q_1}\dots i_{vu}\dots i_{\sigma(p_t)q_t}}\cdot\frac{i_{vu}}{b_{vu}}.\end{aligned}$$

Using

$$\operatorname{lcd}(\{IPQ1\})=\begin{cases}\operatorname{lcd}(\{IPQ\}), & \text{if } \operatorname{lcd}(\{IPQ1\}) \text{ is not divisible by } i_{vu}\\ \dfrac{\operatorname{lcd}(\{IPQ\})}{i_{vu}}, & \text{otherwise}\end{cases}$$

it is easy to conclude that the numerator of $A_{uv}^{(\epsilon,t)}$ is less than or equal to d_{uv}, defined in (*). Consequently, the numerators in $\operatorname{adj}^{(\epsilon,t)}(A)$ are limited by the value $\max\{d_{uv}\ :\ 1\le u\le s;\ 1\le v\le r\}\le N$.

As we mentioned above, the condition $(K2)$ ensures the existence of the residue representations for the given fractions with each of the selected moduli. Finally, the criterion $(K1)$ is generated by the requirements of Theorem 1.3. $\square$

The algorithm MODULI prevaluate an upper bound N and selects an adequate base-vector $\beta = [m_1, \ldots, m_n]$ for exact computation of $\mathrm{adj}^{(\epsilon,t)}(A)$.

Algorithm MODULI(l)

STEP 1. Generate the sets $\{IPQ\}$ and $\{BPQ\}$, and corresponding values $\mathrm{lcd}(\{IPQ\})$ and d, applying step 1, step 2 and step 3 of the algorithm MODUL(l).

STEP 2. Compute d_{uv} from $(*)$.

STEP 3. $d_1 = \max\{d_{uv} : 1 \le u \le s; 1 \le v \le r\}$, $N = \max\{\mathrm{lcd}(\{IPQ\}), d, d_1\}$.

STEP 4. Moduli $m_1, \ldots, m_n$ are the successive primes such that $M = \prod_{k=1}^{n} m_k \ge 2N^2 + 1$, and can be obtained applying step 5 of Algorithm MODUL.

Generalized inverse $A^{-1}_{(\epsilon,t)}$ of $A \in \mathbb{Q}^{r\times s}$ can be exactly computed using single modulus m according to the following algorithm.

Algorithm IM

STEP 1. Select the smallest modulus $m = m_1 \ge 2N^2 + 1 \ge 2u^2 + 1$ and find $t = r(A, \epsilon, m)$, according to the algorithm R_1, applying in his step 2 the algorithm MODULI(t).

STEP 2. Obtain fraction $I = \det_t^{\epsilon}(A)$, applying Algorithm DM.

STEP 3. **for** $j = 1$ **to** s **do**

for $i = 1$ **to** r **do**

(3.1) $\left| \left(\mathrm{adj}^{(\epsilon,t)}(W)\right)_{ji} \right|_m = \left| \sum_{[p],[q]} \left[\epsilon^{(p_1+\ldots+p_t)+(q_1+\ldots+q_t)} |S|_m\right] \right|_m,$

where $S = \begin{cases} (-1)^{u+v} W \begin{pmatrix} p_1 & \cdots & p_{u-1} & p_{u+1} & \cdots & p_t \\ q_1 & \cdots & q_{v-1} & q_{v+1} & \cdots & q_t \end{pmatrix}, & i \in [p],\ j \in [q] \\ 0, & \text{otherwise.} \end{cases}$

(3.2) Convert the value $\left| \left(\mathrm{adj}^{(\epsilon,t)}(W)\right)_{ji} \right|_m$ into fraction B, using module m.

(3.3) The value of $\left(A^{-1}_{(\epsilon,t)}\right)_{ji}$ is equal to the shorted fraction B/I. $\blacksquare$

In the following algorithm is described a computation of Radić's and Stojaković's generalized inverse using multiple modulus residue arithmetic.

Algorithm IBETA

STEP 1. Select the corresponding base-vector $\beta = [m_1, \ldots, m_n]$ and compute *generalized rank* $t = r(A, \epsilon, m)$, according to the algorithm R_1, applying in his step 2 the Algorithm MODULI(t).

STEP 2. Compute $I = \det_t^{\epsilon}(A)$, accomplishing STEP 2, STEP 3 and STEP 4 of the algorithm DBETA.

STEP 3. **for** $j = 1$ **to** s **do**

for $i = 1$ **to** r **do**

(3.1) **for** $k = 1$ **to** n **do**

compute $\left| \left(\mathrm{adj}^{(\epsilon,t)}(W)\right)_{ji} \right|_{m_i}$, according to the step (3.1) of the algorithm IM. {Thus, we get $\left| \left(\mathrm{adj}^{(\epsilon,t)}(A)\right)_{ij} \right|_{\beta}$.}

(3.2) Convert $\left| \left(\mathrm{adj}^{(\epsilon,t)}(A)\right)_{ij} \right|_{\beta}$ into the corresponding fraction B using the modulus $M = \prod_{k=1}^{n} m_k$.

(3.3) $\left(A^{-1}_{(\epsilon,t)}\right)_{ij}$ is equal to the shorted fraction B/I.

Example 4.1. In this example we compute Stojaković's inverse of

$$A = \begin{bmatrix} \frac{1}{2} & -4 & 3 \\ 3 & \frac{42}{9} & -11 \\ \frac{65}{26} & \frac{130}{15} & -14 \\ 2 & \frac{266}{21} & -17 \end{bmatrix}.$$

Modulus $m_1 = 2987$ is the smallest prime greater than or equal to $2 * 38^2 + 1$. The starting value for $t = r(A, \epsilon, m_1)$ is $r(A, m_1) = 2$. Now, using the algorithm MODULI(2) we get

$$N = \max\{6, 8301, 8301\} = 8301, \quad n = 3, \quad \beta = [2897, 2903, 2909].$$

Now, $\mathrm{DET}(A, 2, \epsilon, 2897) \neq 0$, and $r(A, \epsilon, m_1) = 2$. Applying the algorithm DBETA we get $\det_2^S(A) = 1253/6$.

The standard residue representation of $\mathrm{adj}^{(S,2)}(A)$ is

$$|\mathrm{adj}(A)|_\beta = \begin{bmatrix} (2881,2887,2893) & (957,959,961) & (3,3,3) & (1944,1948,1952) \\ (1399,1402,1405) & (2859,2865,2871) & (1441,1444,1447) & (28,28,28,28) \\ (1415,1418,1421) & (1902,1906,1910) & (1438,1441,1444) & (981,983,985) \end{bmatrix}.$$

The mixed-radix representation of $\mathrm{adj}^{(S,2)}(A)$ is

$$|\mathrm{adj}^{(S,2)}(A)|_M = \begin{bmatrix} 167375697 & 111583800 & 3 & 55791917 \\ 83687807 & 167375675 & 83687849 & 28 \\ 83687823 & 55791875 & 83687846 & 11583824 \end{bmatrix}.$$

Converting all elements with module M into the corresponding fractions we obtain

$$\operatorname{adj}^{(S,2)}(A) = \begin{bmatrix} -16 & -\frac{26}{3} & 3 & \frac{38}{3} \\ -\frac{99}{2} & -38 & -\frac{15}{2} & 28 \\ -\frac{67}{2} & -\frac{88}{3} & -\frac{21}{2} & \frac{46}{3} \end{bmatrix}.$$

Finally,

$$A^{-1}_{(S,2)} = \begin{bmatrix} \frac{-96}{1253} & -\frac{52}{1253} & \frac{18}{1253} & \frac{76}{1253} \\ -\frac{297}{1253} & -\frac{228}{1253} & -\frac{45}{1253} & \frac{24}{179} \\ -\frac{201}{1253} & -\frac{176}{1253} & -\frac{9}{179} & \frac{92}{1253} \end{bmatrix}.$$

5. The efficiency. In [**9**] we obtained the following number of operations on the internal representation of rational numbers sufficient for exact computation of rectangular determinants and induced generalized inverses: Let $r_\epsilon(A)$ be shortly denoted by t and let $D_t(A),\ K_t(A),\ U_t(A)$ be the number of such operations sufficient for the computations of determinant, adjoint matrix and inverse of $A \in \mathbb{Q}_g^{r\times s}$, according to Stojaković's and Radić's definition. Then:

$$D_t(A) = \binom{r}{t}\binom{s}{t}\left[\frac{1}{6}\left(4t^3 + 3t^2 - t\right) + 1\right] - 1;$$

$$\begin{aligned} K_t(A) &= rs\left\{\binom{r-1}{t-1}\binom{s-1}{t-1}\left[\frac{1}{6}\left(4(t-1)^3 + 3(t-1)^2 - (t-1)\right) + 1\right]\right\} + \\ &\quad + rs\left\{\binom{r-1}{t-1}\binom{s-1}{t-1} - 1\right\} = \\ &= rs\left\{\binom{r-1}{t-1}\binom{s-1}{t-1}\left[\frac{1}{6}\left(4t^3 - 9t^2 + 5t\right) + 2\right] - 1\right\}; \end{aligned}$$

$$U_t(A) = D_t(A) + K_t(A) + rs.$$

For a residue number system β consisting of n moduli, the execution time is proportional to n, because of the repetition of the computation for each of selected moduli from β. The main advantage of the residue arithmetic related to algorithms in [**9**] is speed-up induced by performing elementary arithmetic operations in the ring of residues instead of more complex operations on the internal forms of numbers. This compensates simple transformations of rational numbers into corresponding residues and multiplicative increase of the number of necessary operations.

The main defects of residue arithmetic are:

- a considerable number of arithmetic operations necessary for computation of an adequate base-vector;

- successive computations of $\det_n^{\epsilon}(A)$, for $n = r(A,m)$ to $n = r(A,\epsilon,m)$, during the computation of the *generalized rank* $r(A,\epsilon,m)$, in the case when $r(A,\epsilon,m) < r(A,m)$.

These algorithms can be used in the following two cases:

1. In exact computation of the Moore-Penrose inverse, in the cases when it coincides with one of the defined pseudoinverses [**11**].

2. Since the Radić's and Stojaković's pseudoinverse are the least $\{1,2\}$-inverses, in the case $r(A,\epsilon,m) = r(A)$ [**11**], described methods can be used for exact computation of $\{i,j,k\}$ generalized inverses.

Acknowledgement. The author is grateful to the referee for helpful comments and suggestions concerning the paper.

References

1. И. Я. Акушский, Д.И. Юдицкий, *Машинная арифметика в остаточных классах,* Советское Радио, 1968
2. Р. Грегори, Е. Кришнамурти, *Безошибочные вычисления, методы и приложения,* Мир, Москва, 1988
3. V.N. Joshi, *A determinant for rectangular matrices,* Bull. Austral. Math. Soc. **21** (1980), 137–146
4. M. Radić, *Inverzija pravokutnih matrica,* Doktorska disertacija, Zagreb, 1964
5. M. Radić, *A definition of the determinant of a rectangular matrix,* Glasnik Mat. **21** (1966), 17–22
6. T.M. Rao, K. Subramanian, and E. Krishnamurty *Residue arithmetic algorithms for exact computation of g-inverse of matrices,* SIAM J. Numer. Anal. **13** (1976), 155–171
7. M. Stojaković, *Determinante nekvadratnih matrica.* Vesnik DMNRS, Beograd **1/2** (1952), 9–21
8. W.T. Stallings, and T.L. Boullion, *Computation of pseudoinverse matrices using residue arithmetic,* SIAM Rev. **14** (1972), 152–163
9. P. Stanimirović, and M. Stanković, *Computing pseudoinverses of rectangular matrices in terms of square submatrices*, in: M. Jaćimović, ed., *VIII Conference on Applied Mathematics, Tivat*, 1993, pp. 207–216
10. M. Stanković, J. Madić, and P. Stanimirović, *Addition, subtraction and multiplication of sequences of fractions by means of residue arithmetic and mathematical spectra,* Math. Balkanica **9** (1995)
11. P. Stanimirović, and M. Stanković, *Determinants of rectangular matrices and Moore–Penrose inverse,* Review of Research, Novi Sad **???**
12. N. Szabo, and R. Tanaka, *Residue Arithmetic and its Applications to Computer Technology,* McGraww-Hill, New York, San Francisko, Toronto, 1967

Filozofski fakultet
Grupa za matematiku
18000 Niš
Yugoslavia

(Received 16 10 1995)