Effective Matrix Methods in Commutative Domains *

Gennadi I. Malaschonok

Tambov State University, 392622 Tambov, Russia
malaschonok@math-iu.tambov.su

Abstract. Effective matrix methods for solving standard linear algebra problems in a commutative domains are discussed. Two of them are new. There are a methods for computing adjoined matrices and solving system of linear equations in a commutative domains.

1 Introduction

Let $\mathbf{R}$ be a commutative domain with identity, $\mathbf{K}$ the field of quotients of $\mathbf{R}$. We assume that $\mathbf{R}$ is equipped with an algorithm allowing *exact division*. This means that if two elements a and b of $\mathbf{R}$ are given (a being different from zero) such that $b = ac$ with $c \in \mathbf{R}$, then this algorithm can exhibit the exact quotient c. Let $\mathbf{R}^{n\times m}$ denote the set of $n \times m$ matrices with entries in $\mathbf{R}$.

This paper is devoted to the review of effective matrix methods in the domain $\mathbf{R}$ for a solution of standard linear algebra problems. They are (1) multiplicating two matrices, (2) solving linear systems in $\mathbf{K}$, (3) solving linear systems in $\mathbf{R}$, (4) computing the adjoint matrix, (5) computing the matrix determinant, (6) computing the characteristic polynomial of a matrix.

We shall estimate algorithms according to the total number of multiplication and division operations in the ring $\mathbf{R}$.

(1). **Multiplication of two matrices**. Let $O(n^\beta)$ be the number of multiplication operations, that are necessary for multiplication of square matrices of the order n. For the standard multiplication of matrices $\beta = 3$, for Strassen [21] algorithm $\beta = \log 7$, and for the best on today algorithm $\beta < 2.376$ [9].

(2). **Solving linear systems in** K. Let $Ax = b$ be a systems of linear equations whose coefficients belong to the commutative domain $\mathbf{R}$: $A \in \mathbf{R}^{n\times m}$, $b \in \mathbf{R}^n$, $x \in \mathbf{K}^m$. The main method here is the so-called Gauss method with exact divisions with complexity $O(n^2m)$ operations in $\mathbf{R}$. First this method was published in the paper of Dodgson [11], and later it was developed in the works [5], [22], [14], [17], [18]. We adduce the asymptotic complexity of these methods: $1.5n^2m$ for Dodgson method [11], $1.5n^2m$ for Bareiss method [5], n^3 for forward

* This paper was published in the book Formal Power Series and Algebraic Combinatorics, (Ed. by D.Krob, A.A.Mikhalev, A.V.Mikhalev), Springer, 2000, 506-517.

and back-up procedures [14], $2/3n^2m$ for one-pass method [17], $7/12n^2m$ for generalized method [18]. A fast method of solving systems of linear equations over commutative domain is published in the article [19]. The complexity of this method is $O(n^{\beta-1}m)$, the same as the complexity of matrix multiplication.

(3). **Solving linear systems in** R. Let $Ax = b$ be a system of linear equations $A \in \mathbf{R}^{n\times m}$, $b \in \mathbf{R}^n$. The problem is to find all the solutions x of this system in the module $\mathbf{R}^m$. The particular cases of this problem are discussed in [15], [16]. A randomized algorithm for finding all the solutions in R is discassed in the section 3 of this paper. It is supposed that there exists an algorithm that is able to ascertain whether the finitely generated ideal $I = (a_1, a_2, \ldots, a_s)$ is unit or not. If I is unit, then there are calculated the coefficients $k_i \in \mathbf{R}$ in the expansion of the unit $1 = \sum_{i=1}^{s} k_i a_i$. It is possible to take in the capacity of such algorithm the algorithm of the Gröbner bases computation in $\mathbf{R}$.

(4). **Computing the adjoint matrix**. The best known method of computing the adjoint matrix in an arbitary commutative ring has the complexity $O(n^3\sqrt{n}\,\mathrm{log}n\,\mathrm{loglog}n)$ operations of addition, substraction and multiplication [13]. If in a commutative ring the exact division is possible, then the best method has the complexity $O(n^3)$ operations of multiplication and exact division [16], [17]. In this work in section 2 we suggest the method with the complexity, equal to the complexity of matrix multiplication, i.e. $O(n^\beta)$.

(5). **Computing the matrix determinant**. The intermediate result of each algorithm [11], [5], [14], [17], [18], [19] for solving systems in $\mathbf{K}$ is the computation of the matrix determinant. So the asymptotic complexity of determinant computation for these methods is $1.5n^3$, $1.5n^3$, n^3, $2/3n^3$, $7/12n^3$ respectively. For the methods [19] the complexity of determinant computation is $O(n^\beta)$. The best method of computing the determinant of a matrix without divisions was published by Kaltofen [13]. Complexity of this method is $n^3\sqrt{n}\log n \log\log n$.

(6). **Computing the characteristic polynomial of a matrix**. In the case of an *arbitrary commutative ring*, the best algorithms are the Chistov one [7], and the Improved Berkowitz Algorithm [1] with size $O(n^{\beta+1}\log n)$. In the paper [2] there are described two new efficient methods with $O(n^3)$ ring operations (addition, subtraction, multiplication and exact division). The first one is the Quasi-triangular method (with asymptotic multiplicative complexity $5/3n^3$) and the second one is the Tri-diagonal method (with asymptotic multiplicative complexity $3n^3$). As in the case of Hessenberg's method [12], they proceed by reducing the given matrix A to a particular upper quasi-triangular (Hessenberg) form, similar to A.

Commutative domain of principal ideals. This is the basic application field. In section 4 we discuss the problem of solving linear systems in the principal ideals domain $\mathbf{R}$ and in the field of fractions $\mathbf{K}$ Let $Ax = c$ be a system of linear equations, $A \in \mathbf{R}^{n\times m}$, $c \in \mathbf{R}^n$.

Solving linear system in the field of fractions. The best known on today method for solving determined system $Ax = c$ in the field of fractions in the case when $\mathbf{R} = Z$, $m = n$, $\det A \neq 0$, is the Dixon method [10], which uses the linear p-adic lifting. Its complexity is $O(n^3(\log n + \log\|A\| + \log p)^2)$ bit operations.

If $m > n$, $\mathbf{R} = Z$ and Gauss method with exact divisions is used then solving system $Ax = c$ in usual arithmetic needs $O(mn^4(\log n + \log\|A\|)^2)$ bit operations. $\|A\|$ denotes the absolute value of the greatest coefficient of the system. Using the Chinese remaindering method may reduce the complexity up to $O(mn^3(\log n + \log\|A\|)^2)$ bit operations [6].

My approach to this problem uses p-adic lifting like in [10]. The complexity of the algorithm in the case of the ring Z is $O((m-n+1)n^2m(\log m + \log\|A\| + \log p)^2)$ bit operations.

Solving linear system in the principal ideal domain. In [20] there is given the randomized algorithm for finding one solution of a system in the domain $\mathbf{R}$, in the cases when $\mathbf{R} = Z$ and $\mathbf{R} = F[x]$ (F[x] — ring of polynomials over a field). This method is based on the Dixon algorithm.

I suggest a randomized algorithm for finding all the solutions of a system in a commutative domain of principal ideals. It is based on using p-adic lifting. Its complexity is essentially cubic in the dimension of system like [20], but the number of matrix inversions is now $m - n$ times less.

2 Adjoint Matrix Computation

2.1 Introduction

Let $\mathcal{A} = \begin{pmatrix} A & C \\ B & D \end{pmatrix}$ be the invertible matrix and A — its invertible block. It is possible to factorize its inverse matrix $\mathcal{A}^{-1}$:

$$\begin{pmatrix} I & -A^{-1}C \\ 0 & I \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & (D - BA^{-1}C)^{-1} \end{pmatrix} \begin{pmatrix} I & 0 \\ -B & I \end{pmatrix} \begin{pmatrix} A^{-1} & 0 \\ 0 & I \end{pmatrix}. \tag{2.1}$$

Let $\mathcal{A}$ be a matrix of the order $n = 2^p$. If a block inversion by formula (2.1) is possible for the blocks up to the second order, then the computation of inverse matrix needs 2^{p-1} second order block inversions and $6 \cdot 2^{p-k-1}$ multiplications of blocks the order 2^k $(k = 1, 2, \ldots, p-1)$.

Using the Strassen [21] algorithm of matrix multiplication for such matrix inversion we need $(21n^\beta - 6n)/5$ multiplicative operations where $\beta = \log_2 7$.

The similar method is proposed in this section.

2.2 The Theorems of Adjoint Matrix Factorization

Let R be a commutative ring, $\mathcal{A} = (a_{i,j})$—a square matrix of an order n over the ring R. We denote by $A^k_{i,j}$ its square submatrix of the order k, obtained by the bordering of upper left block of order $k-1$ by the row i and the column j, $(i, j > k)$. Its determinant is denoted by $a^k_{i,j} = \det A^k_{i,j}$. Denote the corner minor of the order k by $\delta_k = a^k_{k,k}$. The determinant of the matrix, obtained from the upper left block $A^k_{k,k}$ of order k by the replacement of the column i by the column j is denoted by $\delta_{k(i,j)}$, $(1 \le i \le k, k < j \le n)$.

Consider the matrices

$$\mathcal{A}^{(s)}_t = (a^s_{i,j})^{i=s,\dots,t}_{j=s,\dots,t} \quad \text{and} \quad \mathcal{G}^{(t)}_s = (\delta_{t(i,j)})^{i=s,\dots,t}_{j=t+1,\dots,n} \tag{2.2}$$

of the order $(t-s+1)\times(t-s+1)$ and $(t-s+1)\times(n-t)$, correspondingly.

With the preceding notation the determinant Sylvester identity [3] may be written in the following way:

$$\det \mathcal{A}^{(s)}_t = \delta^{t-s}_{s-1}\delta_t \tag{2.3}$$

where $1 < s < t \le n$.

Let us prove the two main theorems of the adjoint matrix factorization.

Theorem 1. *Let a square matrix $\mathcal{A}$ of the order n over the ring R be decomposed into the blocks*

$$\mathcal{A} = \begin{pmatrix} A & C \\ B & D \end{pmatrix},$$

A is the square block of order s, $(1 < s < n)$, whose determinant δ_s is not zero or zero divisor in R. Then the adjoint matrix $\mathcal{A}^*$ can be factorized

$$\begin{pmatrix} \delta_s^{-1}\delta_n I & -\delta_s^{-1}FC \\ 0 & I \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & G \end{pmatrix} \begin{pmatrix} I & 0 \\ -B & \delta_s I \end{pmatrix} \begin{pmatrix} F & 0 \\ 0 & I \end{pmatrix}, \tag{2.4}$$

where $F = A^*$, $G = \delta_s^{-n+s+1}\mathcal{A}^{(s+1)*}_n$, I is the unit matrix and the following identity takes place:

$$\mathcal{A}^{(s+1)}_n = \delta_s D - BFC. \tag{2.5}$$

Theorem 2. *Let the square matrix $\mathcal{A}^{(s+1)}_n$ of order $n-s$, $(s > 0,$ $n-s > 2)$, over the ring R be decomposed into the blocks*

$$\mathcal{A}^{(s+1)}_n = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{B} & \mathbf{D} \end{pmatrix},$$

where $\mathbf{A}$ is the square block of the order $t-s$, $(s < t < n)$, δ_s and δ_t are not zeros or zero divisors in R. Then the matrix $\delta_s^{-n+s+1}\mathcal{A}^{(s+1)*}_n$ can be factorized:

$$\begin{pmatrix} \delta_t^{-1}\delta_n I & -\delta_t^{-1}\mathbf{FC} \\ 0 & I \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & \delta_s^{-1}\mathbf{G} \end{pmatrix} \begin{pmatrix} I & 0 \\ -\mathbf{B} & \delta_t I \end{pmatrix} \begin{pmatrix} \mathbf{F} & 0 \\ 0 & I \end{pmatrix}, \tag{2.7}$$

where $\mathbf{F} = \delta_s^{-t+s+1}\mathcal{A}^{(s+1)*}_t$, $\mathbf{G} = \delta_t^{-n+t+1}\mathcal{A}^{(t+1)*}_n$, I is the unit matrix and the following identity is true:

$$\mathcal{A}^{(t+1)}_n = \delta_s^{-1}(\delta_t\mathbf{D} - \mathbf{BFC}) \tag{2.8}$$

.

Proof. Calculate the products of matrix $\mathcal{A}_n^{(s+1)}$ by the factors of the matrix (2.7) step by step from the right to the left:

$$\mathcal{A}_n^{(s+1)} \to \begin{pmatrix} \delta_t I & \mathbf{FC} \\ \mathbf{B} & \mathbf{D} \end{pmatrix} \to \begin{pmatrix} \delta_t I & \mathbf{FC} \\ 0 & \delta_t \mathbf{D} - \mathbf{BFC} \end{pmatrix} \to \begin{pmatrix} \delta_t I & \mathbf{FC} \\ 0 & \delta_n I \end{pmatrix} \to \delta_n I.$$

It is necessary to prove the identity (2.8) and the following identities:

$$\mathbf{FA} = \delta_t I \tag{2.9}$$

$$\delta_t^{-n+t+1} \mathcal{A}_n^{(t+1)*} \mathcal{A}_n^{(t+1)} = \delta_n I \tag{2.10}$$

As $\mathbf{A} = \mathcal{A}_t^{(s+1)}$, the equality (2.9) follows from the determinant Sylvester identity $\det \mathcal{A}_t^{(s+1)} = \delta_s^{t-s-1} \delta_t$.

The identity (2.10) follows from the determinant Sylvester identity

$$\det \mathcal{A}_n^{(t+1)} = \delta_t^{n-t-1} \delta_n.$$

Let us prove the identity (2.8). Denote by $a_{l,j}^{(s+1)*}$ the cofactor of the element (l, j) in the matrix $\mathcal{A}_t^{(s+1)}$. From the determinant Sylvester identity we obtain:

$$\delta_s^{t-s-1} \delta_{t(i,j)} = \sum_{l=s+1}^{t} a_{l,i}^{(s+1)*} a_{l,j}^{s+1}.$$

Since $\mathbf{F} = \delta_s^{-t+s+1} \mathcal{A}_t^{(s+1)*}$ and $\mathbf{C}$ is the block of the matrix $\mathcal{A}_n^{(s+1)}$, the last equality for the elements implies the matrix identity $\mathcal{G}_t^{(s)} = \mathbf{FC}$. We decompose the determinant of the matrix $A_{i,j}^{s+1}$ according to the last column and obtain

$$a_{i,j}^{s+1} = a_{i,j} \delta_s - \sum_{l=1}^{s} a_{l,j} \sigma_{s(l,j)}, \tag{2.11}$$

where $\sigma_{s(l,j)}$ is the determinant of the matrix, resulted from $A_{s,s}^s$ by the replacement of the row l by the row j. Let $\sigma = (\sigma_{s(1,i)}, \sigma_{s(2,i)}, \ldots, \sigma_{s(s,i)}, 0, 0, \ldots, 0)$, $\alpha = (a_{1,j}, a_{2,j}, \ldots, a_{t,j})$, $\beta = (a_{i,1}^{s+1}, a_{i,2}^{s+1}, \ldots, a_{i,t}^{s+1})$ denote the rows with t elements. Then according to (2.11) we obtain the matrix identity

$$\begin{pmatrix} I & 0 \\ -\sigma & \delta_s \end{pmatrix} \cdot A_{i,j}^{t+1} = \begin{pmatrix} A_{t,t}^t & \alpha^T \\ \beta & a_{i,j}^{s+1} \end{pmatrix}.$$

Correspondingly, we write the following determinant identity, where the determinant of the matrix on the right is decomposed according to the last row:

$$\delta_s a_{i,j}^{t+1} = \delta_t a_{i,j}^{s+1} - \sum_{l=1}^{t} a_{i,l}^{s+1} \delta_{s(l,j)}.$$

In the matrix form it may be written as $\delta_s \mathcal{A}_n^{(t+1)} = \delta_t \mathbf{D} - \mathbf{B} \mathcal{G}_t^{(s)}$. Taking into account $\mathcal{G}_t^{(s)} = \mathbf{FC}$ we get the identity (2.9).

2.3 The Estimate of the Complexity

The dimension of the upper left block A in the process of the factorization of the matrix may be taken arbitrarily. Consider the case, when the dimension of the block A is a degree of 2. We call such decomposition of the adjoin matrix the *binary factorization*.

Let $M(n)$ be the complexity of the multiplication of two matrices of the order n and its asymptotical estimate is αn^{β}.

Then the complexity of the adjoint matrix calculation for the matrix of the order $n = 2^p$ by means of binary factorization is $C(n) = \sum_{k=0}^{p-2} 6 \cdot 2^k M(2^{n-k-1})$. We neglect the complexity of multiplication of a matrix by a scalar, i.e. the terms of the order n^2.

Therefore, the asymptotical estimate of the complexity of the adjoint matrix calculation is $3\alpha n^{\beta}/(1 - 2^{1-\beta})$.

Finally, for the relation of the complexities of the adjoint matrix calculation and of the matrix multiplication we obtain the asymptotical estimate $k(\beta) = \lim_{n\to\infty} \frac{C(n)}{M(n)} = \frac{3}{1-2^{1-\beta}}$. For example we have $k(3) = 4$ for classical multiplication, and $k(\log_2 7) = 4.2$ for Strassen's multiplication.

3 Linear System Solving in Commutative Domains

3.1 Solving Systems in a Field of Fractions

Let $\mathbf{R}$ be a commutative domain with an identity, $\mathbf{K}$ be a field of fractions of $\mathbf{R}$, $A \in \mathbf{R}^{n\times m}$, $\mathrm{rank} A = r$, $c \in \mathbf{R}^n$,

$$Ax = c \tag{3.1}$$

be a system of linear equations. Let S and T be permutation matrices, which transpose linearly independent rows and columns of the matrix A to the upper left corner. We obtain in this corner a square matrix of size $r \times r$, denote it by A_0 ($\det A_0 \neq 0$). The matrices SAT and Sc may be written in a block form:

$$SAT = \begin{pmatrix} A_0 & A_1 \\ A_2 & A_3 \end{pmatrix}, \quad Sc = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}, \quad c_0 \in \mathbf{R}^r.$$

Denote by $\mathcal{M} = \{x \mid x \in \mathbf{K}^m, Ax = c\}$ the set of all the solutions of the system (3.1).

We denote by I_r the identity matrix of order r, $E_{i,j}$—square matrices which have only one nonzero element—(i, j), that equals 1.

We need some facts from the theory of linear equations.

1. If $\mathrm{rank}(A, c) \neq r$, then $\mathcal{M} = \emptyset$. If $\mathrm{rank}(A, c) = r$, then $\mathcal{M}$ is a hyperplane of dimension $m - r$ in a space of dimension m. It is defined by $m - r + 1$ points, which do not belong to one hyperplane of lower dimension.

2. If the system (3.1) is homogeneous ($c = 0$) and $x_1, x_2, \dots, x_{m-r}$ are its linearly independent solutions then $\mathcal{M} = \{\sum_{i=1}^{m-r+1} x_i u_i \mid u_i \in \mathbf{K}\}$.

3. If the system (3.1) is nonhomogeneous ($c \neq 0$) and $x_1, x_2, \ldots, x_{m-r+1}$ are its linearly independent solutions then $\mathcal{M} = \{\sum_{i=1}^{m-r+1} x_i u_i \mid u_i \in \mathbf{K}, \sum_{i=1}^{m-r+1} u_i = 1\}$.

Definition. *A basis set of solutions of a homogeneous system of linear equations* (3.1) is a set which consists from $m - r$ linearly independent solutions of the system (3.1). *A basis set of solutions of a nonhomogeneous system of linear equations* (3.1) is a set which consists from $m - r + 1$ linearly independent solutions of the system (3.1).

The next two theorems reduce the problem of getting the basis solutions of (3.1) to several problems of solving determined systems. The first theorem considers homogeneous systems, the second — nonhomogeneous systems.

Theorem 3. *Let (3.1) be a homogeneous system of linear equations and $A_1 = (a_1, a_2, \ldots, a_{m-r})$, $a_j \in \mathbf{R}^r$. Then the systems*

$$A_0 x_j = -a_j, \quad j = 1, \ldots, m-r, \tag{3.2}$$

are determined and their solutions $x_j \in \mathbf{K}^r$ define the basis set of solutions of (3.1):

$$T \begin{pmatrix} x_j \\ e_j \end{pmatrix}, \quad j = 1, \ldots, m-r, \tag{3.3}$$

where $e_j \in \mathbf{R}^{m-r}$ are the columns of the identity matrix $I_{m-r} = (e_1, e_2, \ldots, e_{m-r})$.

Proof. Denote $y = T^{-1}x$. By the condition we have $(A_0, A_1)y = 0$. We search for the solution in the form $y = \begin{pmatrix} x_j \\ e_j \end{pmatrix}$, and get the system (3.2).

Corollary 1. *Let it be $B = A_0^{-1}A_1 = (b_1, b_2, \ldots, b_{m-r})$, $b_j \in \mathbf{K}^r$. Then $T\begin{pmatrix} -b_1 \\ e_1 \end{pmatrix}, T\begin{pmatrix} -b_2 \\ e_2 \end{pmatrix}, \ldots, T\begin{pmatrix} -b_{m-r} \\ e_{m-r} \end{pmatrix}$ is the basis set of solutions of (3.1).*

Theorem 4. *Let (3.1) be a nonhomogeneous system of linear equations, P a permutation matrix such that the last element of the vector $b = PA_0^{-1}c_0$ is not equal to 0. Let it be $B = PA_0^{-1}A_1$, $J \subset \{1, \ldots, m-r\}$ be the numbers of the columns of the matrix B with zero elements in the last row. Let it be $U = I_{m-r+1} + \sum_{j \in J} E_{1,j+1}$, $W = \mathrm{diag}(I_{r-1}, U)$, $Q = \mathrm{diag}(P, I_{m-r})$, $V = QW$, $I_{m-r+1} = (e'_0, e'_1, \ldots, e'_{m-r})$, where $e'_j \in \mathbf{R}^{m-r+1}$ are the columns of the unit matrix, and $(A'_0, a_0, a_1, a_2, \ldots, a_{m-r}) = P(A_0, A_1)V$ where $A'_0 \in \mathbf{R}^{r \times r-1}$, $a_j \in \mathbf{R}^r$. Then the systems*

$$(A'_0, a_j)x_j = Pc_0, \quad j = 0, 1, \ldots, m-r, \tag{3.4}$$

are determined. The solutions of these systems $x_j = \begin{pmatrix} x'_j \\ \xi_j \end{pmatrix}$, $x'_j \in \mathbf{K}^{r-1}$, $\xi_j \in \mathbf{K}$ define the basis set of solutions of (3.1):

$$TV \begin{pmatrix} x'_j \\ \xi_j e'_j \end{pmatrix}, \quad j = 0, 1, \ldots, m-r. \tag{3.5}$$

Proof. Denote $y = V^{-1}T^{-1}x$. By the condition we have $P(A_0, A_1)Vy = Pc_0$ and $P(A_0, A_1)V = (A'_0, a_0, a_1, \ldots, a_{m-r})$. If we search for the solution in the form $y = \begin{pmatrix} x'_j \\ \xi_j e'_j \end{pmatrix}$, then we obtain the systems (3.4).

Let us show that the systems (3.4) are determined and $\xi_j \neq 0$. Multiply them by $PA_0^{-1}P$ from the left. Since $P = P^{-1}$, we get $PA_0^{-1}P(A'_0, a_j)x_j = PA_0^{-1}c_0$, $j = 0, 1, \ldots, m-r$.

As $b = PA_0^{-1}c_0$ and $PA_0^{-1}P(A'_0, a_0) = I_r$, the first of the systems (3.4) gets the form $I_r x_0 = b$. Denote $I_r = (I', e)$, $e \in \mathbf{R}^r$. We see that $PA_0^{-1}PA'_0 = I'$, $PA_0^{-1}Pa_0 = e$.

Since $PA_0^{-1}P(a_0, \ldots, a_{m-r}) = PA_0^{-1}P(a_0, PA_1)U = (e, B)U$, we get $d_j = PA_0^{-1}Pa_j$, $j = 1, \ldots, m-r$ are the columns of the matrix $(e, B)U$. As $U = I_{m-r+1} + \sum_{j \in J} E_{1,j+1}$ and J are the numbers of the columns of the matrix B with zero elements in the last row, the last elements of all columns d_j of the matrix $(e, B)U$ do not equal zero. The systems (3.4) obtain the form

$$(I', d_j)x_j = b, \quad j = 0, 1, \ldots, m-r, \tag{3.6}$$

and $\det(I', d_j) \neq 0$. Since the last element of the vector b is nonzero, solutions $x_j = \begin{pmatrix} x'_j \\ \xi_j \end{pmatrix}$ of the systems (3.6) are such that $\xi_j \neq 0$. So the vectors $\xi_j e'_j$, $j = 1, \ldots, m-r$, are linearly independent, therefore the vectors (3.5) are linearly independent.

Corollary 2. *Let it be* $B = (b_1, b_2, \ldots, b_{m-r})$, $b = \begin{pmatrix} b' \\ \beta \end{pmatrix}$, $b_j = \begin{pmatrix} b'_j \\ \beta_j \end{pmatrix}$; $\xi_j = \beta/\beta_j$, $f_j = e'_j$ *for* $j \notin J$; $\xi_j = \beta$, $f_j = e'_j + e'_0$ *for* $j \in J$. *Then*

$$TQ \begin{pmatrix} b' \\ \beta e'_0 \end{pmatrix}, \quad TQ \begin{pmatrix} b' - \xi_j b'_j \\ \xi_j f_j \end{pmatrix}, \quad j = 1, \ldots, m-r, \tag{3.7}$$

is the basis set of solutions of (3.1).

Proof. Substitute solutions of (3.6) into (3.5). We take into account that according to the construction, $d_j = \begin{pmatrix} b'_j \\ \delta_j \end{pmatrix}$, $\delta_j = 1$ for $j \in J$ and $\delta_j = \beta_j$ for $j \notin J$. Then we multiply by the matrix W.

Corollaries 1 and 2 allow to present the algorithm to construct the basis set of solutions of a system of linear equations for an arbitrary commutative domain.

3.2 System Solving in a Domain

Now we consider a linear system solving in a commutative domain. Note that it is not a problem for homogeneous systems, since any solution in a field of fractions, been multiplied by a suitable factor, gives the solution in the domain. So further we shall consider only nonhomogeneous systems.

Let $\boldsymbol{\alpha}$ be a nonempty finite subset of $\mathbf{R}$. The intersection of principal ideals generated by elements of the set $\boldsymbol{\alpha}$, is the principal ideal $\cup_{p\in\boldsymbol{\alpha}}(p)$. We denote by $\mathrm{LCM}(\boldsymbol{\alpha})$ the generator of this ideal, i.e. $(\mathrm{LCM}(\boldsymbol{\alpha})) = \cup_{p\in\boldsymbol{\alpha}}(p)$.

Let $\mathbf{K}$ be a field of fractions of $\mathbf{R}$, x be a vector of the space $\mathbf{K}^m$, $\alpha_x \subset \mathbf{R}$ be a set of denominators of components of x.

Definition. *A denominator of a vector* x is $\chi = \mathrm{LCM}(\alpha_x)$. The vector x will be written as a product $x = \mathbf{x}\chi^{-1}$, $\mathbf{x} \in \mathbf{R}^m$, $\chi \in \mathbf{R}$.

The denominator of a vector x is denoted by $\mathrm{DEN}(x)$.

Let $\mathcal{M} = \{x \mid x \in \mathbf{K}^m, Ax = b\}$ be the set of all solutions of (3.1) in $\mathbf{K}^m$. Denote by $\mathcal{M}_D = \mathcal{M} \cup \mathbf{R}^m$ the set of solutions lying in the module $\mathbf{R}^m$. We call $\mathcal{M}_D$ *the set of Diophantine solutions.*

For $x=(x_1, x_2, \ldots, x_s)$ and $y=(y_1, y_2, \ldots, y_s)$ we denote $\langle x, y\rangle = \sum_{i=1}^{s} x_i y_i$.

Theorem 5. *Let* $\{x_i = \mathbf{x}_i\chi_i^{-1} \mid i = 1, 2, \ldots, h\}$ *be a basis set of solutions of the nonhomogeneous system (3.1),* $\hat{\mathbf{x}} = (\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_h)$, $\chi = (\chi_1, \chi_2, \ldots, \chi_h)$. *Then*

$$\mathcal{M} = \{\frac{\langle \hat{\mathbf{x}}, q\rangle}{\langle \chi, q\rangle}\bigg| q \in \mathbf{R}^h, \langle \chi, q\rangle \neq 0\}$$

Proof. Let $u = (u_1, u_2, \ldots, u_h) \in \mathbf{K}^h$ be such that $\sum_{i=1}^{s} u_i = 1$. Further we use the notations: $s_i = u_i\chi_i^{-1}$, g is LCM of denominators of all numbers $\{s_i \mid i = 1, 2, \ldots, h\}$, $q_i = gs_i \in \mathbf{R}$, $i = 1, 2, \ldots, h$, $q = (q_1, q_2, \ldots, q_h)$.

Let it be $\hat{x} = (x_1, x_2, \ldots, x_h)$, $z = \langle \hat{x}, u\rangle$, $\sum_{i=1}^{s} u_i = 1$, and so $z \in \mathcal{M}$. Then we obtain

$$z = \langle \hat{x}, u\rangle = \sum_{i=1}^{h} \mathbf{x}_i\chi_i^{-1}u_i = \sum_{i=1}^{h} \mathbf{x}_i s_i = \langle \hat{\mathbf{x}}, q\rangle g^{-1}, \tag{3.7}$$

$$1 = \sum_{i=1}^{s} u_i = \sum_{i=1}^{h} \chi_i\chi_i^{-1}u_i = \sum_{i=1}^{h} \chi_i s_i = \langle \chi, q\rangle g^{-1}. \tag{3.8}$$

So $\frac{\langle \hat{\mathbf{x}}, q\rangle}{\langle \chi, q\rangle} = z \in \mathcal{M}$.

Conversely, if $q \in \mathbf{R}^h$, $\langle \chi, q\rangle = g \neq 0$ and $z = \frac{\langle \hat{\mathbf{x}}, q\rangle}{\langle \chi, q\rangle}$, then, denoting $u_i = \chi_i q_i g^{-1}$, obtain $z = \langle \hat{x}, u\rangle$ and $\sum_{i=1}^{s} u_i = 1$. Therefore $z \in \mathcal{M}$.

Corollary 3. *The set* $I_A = \{\mathrm{DEN}(x) \mid Ax = c, x \in \mathbf{K}^m\} \cup 0$ *is an ideal in* $\mathbf{R}$.

Corollary 4. $\mathcal{M}_D \neq \emptyset$ *if and only if* $I_A = \mathbf{R}$.

Corollary 5. *A system (3.1) has Diophantine solutions if the ideal generated by the denominators of a basis set of solutions is unit.*

Corollary 6. *Let the ideal, generated by the denominators of basis solutions* $x_i = \mathbf{x}_i\chi_i^{-1}$, $i = 1, 2, \ldots, h$ *of the system (3.1) be unit,* $\chi = (\chi_1, \chi_2, \ldots, \chi_h)$. *Then there exists a nonzero vector* $q = (q_1, q_2, \ldots, q_h) \in \mathbf{R}^h$, *such that* $\langle \chi, q\rangle = 1$ *and* $\langle \mathbf{x}, q\rangle$ *is Diophantine solution of (3.1). If in addition* $q_s \neq 0$, *then*

$$x_1, \ldots, x_{s-1}, \langle \mathbf{x}, q\rangle, x_{s+1}, \ldots, x_h$$

is a basis set of solutions for this system.

Definition. We call a *Diophantine basis of solutions for a system* $Ax = b$ a basis set of solutions for this system, that wholly belongs to $\mathbf{R}^m$.

In other words a Diophantine basis consists of the $m+1-r$ linearly independent solutions of nonhomogeneous ($m-r$ for homogeneous) system, that belong to $\mathbf{R}^m$.

Corollary 7. *Let* $x_i = \mathbf{x}_i\chi_i^{-1}$, $i = 1, 2, \ldots, h$ *be a basis set of solutions of (1) and* $\chi_1 = 1$. *Then the set* $\mathbf{x}_1$, $\mathbf{x}_i - \mathbf{x}_1(\chi_i - 1)$, $i = 2, 3, \ldots, h$, *is a Diophantine basis of solutions for this system.*

Proof. : Since all $z_i = \mathbf{x}_i - \mathbf{x}_1(\chi_i - 1)$, $i = 2, 3, \ldots, h$ belong to $\mathbf{R}^m$ and are linearly independent together with x_1, it remains to show that z_i are the solutions of (1). As $\chi_1 = 1$, we have

$$z_i = \mathbf{x}_i - \mathbf{x}_1(\chi_i - 1) = \frac{\mathbf{x}_1(-\chi_i + 1) + \mathbf{x}_i \cdot 1}{\chi_1(-\chi_i + 1) + \chi_i \cdot 1}.$$

Therefore, by Theorem 3, z_i, $i = 2, 3, \ldots, h$ are the solutions of the system $Ax = b$.

Corollaries of Theorem 5 allow to present a rendomized algorithm for computing a Diophantine basis of a system solutions.

If the ideal generated by the denominators of a basis set of solutions is unit, than we compute a Diophantine basis. Else we must choose a new permutation matrices S and T and compute a new rational basis, and so on. So we get some kind of iterative Diophantine solve. As it is proved in [20] an expected number of rational solutions that are necessary for getting Diophantine solution is $O(\log n + \log\log \|(A, c)\|)$ for the ring Z. One of the question here is how to get such evaluation for another rings.

As we get $m - n + 1$ rational solutions in one iteration for rank$A = n$, so an expected number of iterations for the ring Z is $O((m - n + 1)^{-1}(\log n + \log\log \|(A, c)\|))$.

4 Solving Linear System in Principal Ideal Domain

4.1 Solving Linear System in the Field of Fractions

Theorems 3 and 4 reduce the problem of getting the basis solutions of the system (3.1) to several problems of solving determined systems. Computing a basis set of solutions of nonhomogeneous system needs to solve $m - r + 1$ systems with the matrix of coefficients of size $r \times r$ (the case of homogeneous systems needs to solve $m - r$ systems). To solve a determined system one may use the p-adic lifting.

Recall a general scheme of p-adic methods. The suitable prime element p of the ring $\mathbf{R}$ is chosen. The element p must not divide the determinant of the coefficients matrix. For example, in the ring Z this choice may appear to be unsuccessful with probability no more than $1/p$. If the check shows that the solution is incorrect, then another prime element p is chosen. The ring of residues prime modulo p is a field, and the solution in this field may be found for example using the Gauss method. The upper evaluations for numerators and denominators of system solutions is calculated by means of Hadamard inequality. According to them the upper evaluation for p^k — the boundary of lifting. Then the solution is lifted modulo p up to p^k and a rational solution is constructed. For solving one determined system we apply the algorithm given by Dixon [10], which use a linear p-adic lifting. Its complexity is $O(n^3(\log n + \log\|A\| + \log p)^2)$ bit operations. So the algorithm for getting all the rational solutions of the system $Ax = c$, when $\mathrm{rank} A = n$, has the complexity $O(n^2 m(m-n+1)(\log n + \log\|A\| + \log p)^2)$ bit operations.

4.2 Solving Linear System in the Principal Ideal Domain

A one iterative step for computing a Diophantine basis is consist in the computing a rational basis and a Diophantine solutions, due to the Corollaries of Theorem 5.

The complexity of the first is $O(mn^{\beta-1})$, of the second — $O(m(m-r)+C_G)$ operations in the ring $\mathbf{R}$. C_G is the amount of operations that are necessary for an expansion of a unit in $m-r$ generators of the unit ideal in the ring $\mathbf{R}$. Such expansion of a unit may be obtained for example with the help of the algorithm of computing the Gröbner basis. The evaluation of the complexity of such algorithm in general is not the subject of this paper. Mention that for Euclidean rings C_G it is the amount of operations in Euclidean algorithm, that calculates the GCD for $m-r$ numbers.

The more defined evaluations may be obtained for algorithms, using the linear p-adic lifting. It is known that the complexity of Dixon algorithm [20] in the case of integer numbers Z, for $n = m$ and $\det A \neq 0$ is bounded by the number $\mathcal{D}_Z = O(n^3(\log n + \log\|A\| + \log p)^2 + n(\log\|\|)^2)$ bit operations. In the case of the ring of polynomials $F[x]$ over a field F this complexity is bounded by $\mathcal{D}_{F[x]} = O(n^3(\|A\| + \|p\|)^2 + n(\|c\|)^2)$ operations in the field F. The function $\|\ \ \|$ has the next meaning: $\|\alpha\| = |\alpha|$ for $\alpha \in Z$, $\|\alpha\| = \deg\alpha$ for $\alpha \in F[x]$, for matrix A, $\|A\| = \max_{\alpha\in A}\|\alpha\|$.

Computing a basis from $m-r$ solutions needs not more than $\mathcal{C}_Z = (m-r)\mathcal{D}_Z$ and $\mathcal{C}_{F[x]} = (m-r)\mathcal{D}_{F[x]}$ operations for each case correspondingly.

The average number of matrix inversions for computing one rational solution is now $m-r$ times less than this number in the algorithm [20].

The complexity of computing a Diophantine basis for Z and $F[x]$ is the same as the complexity of computing a rational basis. An expected number of iterations is $O((m-n+1)^{-1}(\log n + \log\log\|(A,c)\|))$.

References

1. Abdeljaoued, J.: Berkowitz Algorithm, Maple and computing the characteristic polynomial in an arbitrary commutative ring. Computer Algebra MapleTech **4**,

No. 3, Birkhauser Boston (1997)
2. Abdeljaoued, J., Malaschonok, G. I.: Efficient Algorithms for Computing the Characteristic Polynomial in a Domain. Journal of Pure and Applied Algebra (to appear)
3. Akritas, A. G., Akritas, E. K., Malaschonok, G. I.: Various proofs of Sylvester's (determinant) identity. Mathematics and Computations in Simulation **42** (1996) 585–593
4. Akritas, A. G., Akritas, E. K., Malaschonok, G. I.: Matrix computation of subresultant polynomial remainder sequences in integral domain. Reliable Computing **1**, No. 4 (1995) 375–381
5. Bareiss, E. H.: Sylvester's Identity and Multistep Integer-Preserving Gaussian Elimination. Math. Comp. **22** (103) (1968) 565–578
6. Bareiss, E. H.: Computational solutions of matrix problems over an integral domain. J. Inst. Maths Applics **10** (1972) 68–104
7. Chistov, A. L.: Fast parallel calculation of the rank of matrices over a field of arbitrary characteristic. Proc. FCT'85, Springer Lecture Notes in Computer Science **199** (1985) 147–150
8. Collins, G. E. and Encarnacion, M. J.: Efficient rational number reconstruction. Journal of Symbolic Computation. **20** (1995) 287–297
9. Coppersmith, D. and Winograd, S.: Matrix multiplication via arithmetic progressions. Journal of Symbolic Computation **9** (1990) 251–280
10. Dixon, J.: Exact solution of linear equations using p-adic expansions. Numer. Math. **40** (1982) 137–141
11. Dodgson, C. L.: Condensation of determinants, being a new and brief method for computing their arithmetic values. Proc. Royal Soc. Lond. **A.15** (1866) 150–155
12. Faddeev, D. K., Faddeeva, V. M.: Computational methods of linear algebra. W.H. Freeman & Co., San Francisco (1963)
13. Kaltofen, E.: On Computing Determinants of Matrices Without Divisions. In: Wang, P. S. (ed.): Proc. Internat. Symp. Symbolic Algebraic Comput. ISSAC'92. ACM Press (1992) 342–349
14. Malaschonok, G. I.: Solution of a system of linear equations in an integral domain. USSR Journal of computational Mathematics and Mathematical Physics **23** (1983) 1497–1500
15. Malaschonok, G. I.: System of linear equations over a commutative ring. Academy of Sciences of Ukraine, Lvov (1986) (in Russian)
16. Malaschonok, G. I.: On the solution of a linear equation system over commutative rung. Math. Notes of the Acad. Sci. USSR **42**, No. 4 (1987) 543–548
17. Malaschonok, G. I.: Algorithms for the solution of systems of linear equations in commutative rings. In: Mora, T. and Traverso, C. (ed.): Effective Methods in Algebraic Geometry. Progress in Mathematics 94, Birkhauser (1991) 289–298
18. Malaschonok, G. I.: Argorithms for the Computing Determinants in a commutative rings. Diskretnaya Matematika **7**, No. 4 (1995) 68–76
19. Malaschonok, G. I.: Recursive Method for the Solution of Systems of Linear Equations. In: Sydow, A. (ed.): Computational Mathematics (Proceedings of the 15th IMACS World Congress, Vol. I, Berlin, August 1997). Wissenschaft & Technik Verlag, Berlin (1997) 475–480
20. Mulders, T., Storjohann, A.: Diophantine Linear System Solving. In: Proceedings of ISSAC'99: ACM International Symposium on Symbolic and Algebraic Computation, July 1999, Vancouver, Canada
21. Strassen, V.: Gaussian Elimination is not optimal. Numerische Mathematik **13** (1969) 354–356

22. Sasaki, T. & Murao, H.: Efficient Gaussian elimination method for symbolic determinants and linear systems. A.C.M. Trans. Math. Software **8**, No. 4 (1968) 277–289