ISSN 0361-7688, Programming and Computer Software, 2024, Vol. 50, No. 2, pp. 202–207. © Pleiades Publishing, Ltd., 2024.
Russian Text © The Author(s), 2024, published in Programmirovanie, 2024, Vol. 50, No. 2.

Lower Bounds for the Rank of a Matrix with Zeros and Ones outside the Leading Diagonal

A. V. Seliverstov[a],* (ORCID: 0000-0003-4746-6396) and O. A. Zverkov[a], (ORCID: 0000-0002-8546-364X)**

[a] *Institute for Information Transmission Problems (Kharkevich Institute),*
Russian Academy of Sciences, Bol'shoi Karetnyi per. 19/1, Moscow, 127051 Russia
**e-mail: slvstv@iitp.ru*
***e-mail: zverkov@iitp.ru*

Received July 12, 2023; revised August 10, 2023; accepted October 1, 2023

Abstract—We found a lower bound on the rank of a square matrix where every entry in the leading diagonal is neither zero nor one and every entry outside the leading diagonal is either zero or one. The rank of this matrix is at least half its order. Under an additional condition, the lower bound is higher by one. This condition means that some auxiliary system of linear equations has no binary solution. Some examples are provided that show that the lower bound can be achieved. This lower bound on the matrix rank allows the problem of finding a binary solution to a system of linear equations with a sufficiently large number of linearly independent equations to be reduced to a similar problem in a smaller number of variables. Restrictions on the existence of a large set of solutions are found, each differing from the binary one by the value of one variable. In addition, we discuss the possibility of certifying the absence of a binary solution to a large system of linear algebraic equations. Estimates of the time required for calculating the matrix rank in the SymPy computer algebra system are also provided. It is shown that the rank of a matrix over the field of residues modulo prime number is calculated faster than it generally takes to calculate the rank of a matrix of the same order over the field of rational numbers.

Keywords: matrix rank, system of linear equations, computer algebra system, and SymPy

DOI: 10.1134/S0361768824020142

1. INTRODUCTION

Suppose that K is a field computable in polynomial time [1] the characteristic of which is either zero or an odd prime number. A solution to a system of m equations in n variables is called an (0, 1)-solution if each variable takes either of two values: 0 or 1. The solution is called an almost-(0, 1)-solution if one variable is neither 0 nor 1 and the other variables are 0 or 1.

A system of linear equations defines a subspace in the ambient affine space with a fixed Cartesian coordinate system. We identify points with lists of field elements or with matrix columns. Over an unordered field, the concept of a polytope is not defined; however, we identify the set of vertices of the unit cube in an n-dimensional space with the set of 2^n points the coordinates of which belong to the set $\{0, 1\}$. Two vertices of this cube, i.e., two (0, 1)-points, are called adjacent if they differ in one coordinate. For instance, the (0, 1)-solution to the system of equations is a vertex of this cube that belongs to this subspace; its almost-(0, 1)-solution is a point in a straight line that passes through two adjacent vertices of the unit cube but does not coincide with the vertex. The point all coordinates of which are 1/2 is the center of symmetry of the unit cube.

The problem of recognizing the (0, 1)-solution is equivalent to the problem of finding the relative position of the subspace and vertices of the unit cube. This problem is NP-complete. Using estimates of the rank of a matrix of a special type, we propose a necessary condition for the existence of a sufficiently large set of almost-(0, 1)-solutions in the absence of (0, 1)-solutions to the system of equations. The existence of almost-(0, 1)-solutions is an obstacle to reducing the dimension of the (0, 1)-solution recognition problem by elimination of variables, i.e., by projection onto a coordinate subspace. Hence, the violation of the proposed condition implies the possibility of dimensionality reduction and, therefore, reduction in computational complexity. However, here, we do not consider enumeration problems, which are more difficult than problems of recognizing at least one solution [2, 3].

Recently, algorithms were proposed for recognizing (0, 1)-solutions to a system of linear equations with integer coefficients: both heuristic ones under the low density condition [4] or for a sufficiently large number of equations [5, 6] and non-deterministic ones with new upper bounds on computational complexity [7].

Our new results hold for finite fields. Over a finite field, elimination of variables is not accompanied by the lengthening of coefficients of equations. Therefore, various calculations are relatively easy to carry out in computer algebra systems, with their bit complexity being close to algebraic complexity. Moreover, over a finite field with a fixed number of variables, the exhaustive search is feasible [8].

The rank of a square matrix M is related to the dimension of the affine hull L of the points corresponding to the columns of the matrix. If L contains the origin, then $\operatorname{rank}(M) = \dim(L)$; otherwise, $\operatorname{rank}(M) = \dim(L) + 1$.

The rank of an $n \times n$ matrix over a field can be calculated using a polynomial number of processors and executing just $O(\log_2^2 n)$ operations over this field on each of them [9, 10]. On the other hand, the complexity of calculating the rank [11] and characteristic polynomial [12, 13] is close to the complexity of matrix multiplication. In addition, there is a fast probabilistic algorithm for calculating the Smith normal form of an integer matrix [14]. The calculation of the rank over rings without nontrivial zero divisors was considered in [15]. For sparse symmetric matrices, the necessary condition of nondegeneracy is convenient, which uses the Newton polytope for the quadratic form [16]. Newton polytopes are also useful for solving other problems [17].

However, in practice, calculating the rank of high-order matrices is expensive. Hence, efficiently verifiable rank estimates can be useful in a variety of applications. Some results on the rank of matrices were considered at the conference on computer algebra that was dedicated to the memory of Marko Petkovšek [18].

This paper is organized as follows. Section 2 presents new matrix rank estimates and related theoretical results. Section 3 discusses results of calculations in the SymPy computer algebra system. Section 4 provides a brief conclusion.

2. THEORETICAL RESULTS

Suppose that, for each $1 \le k \le n$, a system of equations in n variables have an almost-(0, 1)-solution with coordinate $x_k \notin \{0, 1\}$. Such solutions correspond to the columns of a matrix where each entry in the leading diagonal is neither zero nor one and each entry outside the leading diagonal is either zero or one. Estimating the rank of this matrix makes it possible to estimate the dimension of the affine subspace defined by the system of equations.

Theorem 1. *Suppose that we have an $n \times n$ matrix M over field K where each entry in the leading diagonal is neither zero nor one and each entry outside the leading diagonal is either zero or one. Then, the rank of matrix M is not less than $n/2$.*

Proof. If $n = 2$, then the rank of 2×2 matrix M is not less than $n/2$ because $\operatorname{rank}(M) \ge 1$.

Suppose that, at some $n \ge 3$, the theorem holds for all $m \times m$ matrices of order $m < n$. Let us consider $n \times n$ matrix M.

A column of matrix M corresponds to a point in a straight line that passes through two adjacent (0, 1)-points but does not coincide with these (0, 1)-points. Affine transformations of form $x_k \to 1 - x_k$ map (0, 1)-points to other (0, 1)-points and almost-(0, 1)-points to other almost-(0, 1)-points. These transformations preserve the dimension of the subspace. Transformation $x_k \to 1 - x_k$ means the replacement of all entries in the kth row of the matrix. This allows us to pass from matrix M to matrix $\hat{M}$ of the same type (in the last column of matrix $\hat{M}$, all entries, except for the entry in the leading diagonal, are zero):

$$\hat{M} = \left(\begin{array}{c|c} \\ N & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ \\ \hline * \; \cdots \; * & \alpha \end{array}\right)$$

for some $\alpha \notin \{0,1\}$. Moreover, inequality $\operatorname{rank}(M) \ge \operatorname{rank}(\hat{M}) - 1$ holds. However, if the affine hull of the columns of M contains the origin, then the rank of M may be less than the rank of $\hat{M}$.

By elementary transformations of the columns of $\hat{M}$, we obtain the matrix

$$\widetilde{M} = \left(\begin{array}{c|c} \\ N & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ \\ \hline 0 \; \cdots \; 0 & \alpha \end{array}\right)$$

of the same rank. Matrices $\hat{M}$ and $\widetilde{M}$ can differ only in the bottom rows. The entries in the bottom row of $\widetilde{M}$, except for the entry in the leading diagonal, are zero.

By removing the last column and last row of $\widetilde{M}$, we obtain an $(n - 1) \times (n - 1)$ matrix N of a lower rank. By the induction hypothesis, $\operatorname{rank}(N) \ge (n - 1)/2$. Therefore, inequality $\operatorname{rank}(\widetilde{M}) \ge n/2$ holds.

Let us denote the affine hull of the columns of $\widetilde{M}$ by L. There are two possible cases. If L passes through the origin, then $\operatorname{rank}(\widetilde{M}) = \dim(L)$. In this case, $\operatorname{rank}(M) \ge \dim(L) = \operatorname{rank}(\widetilde{M}) \ge n/2$.

If L does not pass through the origin, then $\operatorname{rank}(M) \ge \operatorname{rank}(\widetilde{M}) - 1 = \operatorname{rank}(N)$. The affine hull of the columns of matrix N does not pass through the origin. We again apply transformations of form $x_k \to 1 - x_k$ to matrix N and obtain matrix $\widetilde{N}$ of the same type: in the last column of $\widetilde{N}$, all entries, except for the entry in the leading diagonal, are zero. Moreover, rank(N) ≥ rank($\widetilde{N}$). By removing the last column and last row of $\widetilde{N}$, we obtain an $(n - 2) \times (n - 2)$ matrix U of a lower rank. By the induction hypothesis, its rank is bounded from below: rank(U) ≥ $(n - 2)/2$. Then, rank($\widetilde{N}$) = rank(U) + 1 ≥ $n/2$. Hence, rank(M) ≥ rank(N) ≥ rank($\widetilde{N}$) ≥ $n/2$.

The following result shows that this lower bound for the rank is accurate. In this case, the division by two is used, which explains the assumption that the characteristic of field K is not equal to two. By $\lceil \cdot \rceil$ we denote the result of rounding to a larger integer.

Theorem 2. *For any odd number n, there is an $n \times n$ matrix M over field K such that each entry in its leading diagonal is neither zero nor one, each entry outside its leading diagonal is either zero or one, no* (0, 1)*-point lies in the affine hull of the columns of M, and equality* $\operatorname{rank}(M) = \lceil n/2 \rceil$ *holds.*

Proof. Let us consider the $n \times n$ matrix

$$M = \begin{pmatrix} 1/2 & 0 & 1 & 0 & 1 & \cdots & 0 & 1 \\ 0 & -1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 & -1 \end{pmatrix}$$

and denote the $(n-1) \times (n-1)$ submatrix obtained by removing the first column and first row of M by N. The ranks of the matrices are related as follows: rank(M) = rank(N) + 1. Matrix N is a block-diagonal matrix with 2 × 2 blocks, each block being degenerate. Therefore, its rank is equal to the number of blocks: rank(N) = $(n - 1)/2$. Hence, rank(M) = rank(N) + 1 = $(n+1)/2 = \lceil n/2 \rceil$.

Each column of matrix M is a solution to the system of $(n+1)/2$ linearly independent equations

$$\begin{cases} 2x_1 - x_2 - \cdots - x_{2k} - \cdots - x_{n-1} = 1 \\ x_{2k} + x_{2k+1} = 0, \quad 1 \le k \le (n-1)/2. \end{cases}$$

This system has no (0, 1)-solutions. Indeed, the lower equations imply that the (0, 1)-solution should have zero coordinates, except for the first one. However, this contradicts the first equation.

For instance, the 3 × 3 matrix

$$\begin{pmatrix} 1/2 & 0 & 1 \\ 0 & -1 & 1 \\ 0 & 1 & -1 \end{pmatrix}$$

has rank 2. Three columns correspond to three points in straight line L, which is defined by the following system of two equations:

$$\begin{cases} 1 - 2x_1 + x_2 = 0 \\ x_2 + x_3 = 0. \end{cases}$$

This system has no $(0,1)$-solutions.

The 4 × 4 matrix

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 2 & 1 \\ 1 & 0 & 1 & 1/2 \end{pmatrix}$$

has rank 3. Four columns correspond to points on a plane defined by the system of two equations

$$\begin{cases} x_3 = x_1 + x_2 + 1 \\ x_4 = (-x_1 + x_2 + 1)/2. \end{cases}$$

This system has no (0, 1)-solutions.

For 2 × 2 matrices where each entry in the leading diagonal is neither zero nor one and each entry outside the leading diagonal is either zero or one, the rank is 1 only for the matrices

$$\begin{pmatrix} 1/\alpha & 1 \\ 1 & \alpha \end{pmatrix}.$$

where $\alpha \notin \{0,1\}$. The columns correspond to points in a straight line that passes through the origin and is defined by equation $x_2 = \alpha x_1$. Thus, if no (0, 1)-point belongs to the line that passes through the points corresponding to the columns of matrix M, then rank(M) = 2.

Theorem 3. *Suppose that n is an even number and M is an $n \times n$ matrix over field K with each entry in the leading diagonal being neither zero nor one and each entry outside the leading diagonal being either zero or one. If no* $(0,1)$*-point lies in the affine hull of the columns of M, then the rank of M is not less than* $(n/2) + 1$.

Proof. Transformations of form $x_k \to 1 - x_k$ applied to the rows of the matrix, as in the proof of Theorem 1, allows us to pass from matrix M to matrix $\hat{M}$ of the same type (in the last column of $\hat{M}$, all entries, except for the entry in the leading diagonal, are zero):

$$\hat{M} = \left(\begin{array}{c|c} & 0 \\ N & \vdots \\ & 0 \\ \hline * \ \cdots \ * & \alpha \end{array} \right)$$

for some $\alpha \notin \{0,1\}$. Since the affine hull of the columns of M does not contain any (0, 1)-points, the same is true for matrix $\hat{M}$. In this case, the rank does not change. Hence, rank(M) = rank($\hat{M}$) = rank(N) + 1. According to Theorem 1, rank(N) ≥ $(n - 1)/2$. Therefore, inequality rank(M) ≥ $(n + 1)/2$ holds. For even n, this inequality is equivalent to rank(M) ≥ $(n/2) + 1$.

Theorem 4. *Suppose that we have a system of m linearly independent linear equations in n variables that has no* (0, 1)-*solutions*. If $m > (n + 1)/2$, *then*, *for some* $1 \le k \le n$, *there is no almost-*(0, 1)-*solution in which* $x_k \not\in \{0,1\}$.

Proof. Suppose that, for each variable, there is an almost-(0, 1)-solution that is neither zero nor one in the value of this variable. Then, it is easy to construct a matrix M where each entry in the leading diagonal is neither zero nor one and each entry outside the leading diagonal is either zero or one. In the absence of (0, 1)-solutions, rank(M) $= n - m + 1$. If n is odd, then $n - m + 1 \ge n/2$ by Theorem 1. If n is even, then $n - m + 1 \ge (n/2) + 1$ by Theorem 3. In any case, $m \le (n + 1)/2$. Thus, we arrive at the contradiction.

By $\lfloor n/2 \rfloor$ we denote the integer part of $n/2$. The geometric interpretation of Theorem 4 is as follows. Suppose that s < $\lfloor n/2 \rfloor$. In the n-dimensional affine space, for each s-dimensional subspace L that is not incident to any vertex of the unit cube, there is a coordinate-oblivious projection onto some coordinate hyperplane whereby the image of subspace L is again not incident to any vertex of the unit cube. The coordinate-oblivious projection is easy to calculate. In this case, there are, generally speaking, several such projections; however, the selection of a good projection is nondeterministic and can have high computational complexity. In this sense, the discussed method for reducing the dimension of the problem resembles the results from [7]. However, we do not use probabilistic methods.

Theorem 5. *Suppose that we have a system of m linearly independent linear equations in n variables over field* K. *If* $n = 2m - 1$ *and the system has no* (0, 1)-*solutions but*, *for each* $1 \le k \le n$, *there is an almost-*(0, 1)-*solution in which* $x_k \not\in \{0,1\}$, *then point* (1/2, ..., 1/2), *each coordinate of which is equal to* 1/2, *is not a solution to the system*.

Proof. Suppose that point (1/2, ..., 1/2) is a solution to the system. Then, the set of the remaining solutions to this system splits into pairs of symmetric solutions that pass one into another with the simultaneous transformation of all coordinates $x_k \to 1 - x_k$. Under this transformation, the almost-(0, 1)-solution passes into another almost-(0, 1)-solution in which the same coordinate is neither zero nor one. However, point (1/2, ..., 1/2) remains fixed.

By substituting zero for the last variable $x_n = 0$, we obtain a new system of m equations that has no (0, 1)-solutions; however, for each $1 \le k \le n - 1$, there is an almost-(0, 1)-solution in which $x_k \not\in \{0, 1\}$. In the new system, the number of linearly independent equations is m, while the number of variables is $n - 1 = 2m - 2$. Thus, we arrive at a contradiction with Theorem 4. □

The following result establishes the mutual dependence of almost-(0, 1)-solutions.

Theorem 6. I*f straight line L intersects three lines each of which contains two adjacent* (0, 1)-*points and line L is not incident to any* (0, 1)-*point*, *then*, *at all points in line L*, *the coordinates*, *except for some three coordinates*, *take constant values from set* {0, 1}.

Proof. Without loss of generality, we can assume that line L intersects the first coordinate axis at point A with coordinates $(\alpha, 0, \ldots, 0)$, where all coordinates, except for the first one, are zero and $\alpha \not\in \{0, 1\}$. For some $k \ge 2$, line L passes through point W for which all coordinates, except for the k th one, belong to set {0, 1}.

Line L consists of points $tA + (1 - t)W$, where t is a parameter. If, among its coordinates except for the first one, point W has two coordinates equal to one, then, for any third point on L, these coordinates are also neither zero nor one. However, by condition, there is a third point on L that has exactly one coordinate different from zero and one. Hence, point W can have no more than three non-zero coordinates, including the first one. Therefore, line L lies in a coordinate subspace the dimension of which is no higher than three.

3. IMPLEMENTATION AND DISCUSSION

The rank of a matrix is calculated faster over the field $GF(p)$ of residues modulo p than over the field of rational numbers (cf. [19]). These calculations are implemented in many computer algebra systems, e.g., in SymPy [20].

SymPy 1.12 calculates matrices the entries of which are independently and uniformly distributed over a finite set of values; for a finite field, over the set of all elements of the field. The matrices were generated by the `randMatrix` method. If the time it takes to calculate the rank of one matrix was less than a minute, then this calculation was repeated in five series. In that case, as the calculation time, the minimum of five values was used, each of which was obtained by averaging over one series of calculations. The length of a series depended on the calculation time. If the time of one calculation exceeded two seconds, then each series consisted of one calculation. For each matrix order, the median of calculations for 25 matrices was calculated.

Calculating the rank of an $n \times n$ matrix over field $GF(p)$ for $p \le 11$ and $n \le 500$ takes less than two minutes; for $n \le 1000$, it takes less than 15 minutes. In this case, the median time for calculating the rank monotonically increases with increasing matrix order as $c(p)n^{3+\varepsilon}$, where the additive in the exponent varies on interval $0.05 < \varepsilon < 0.09$ depending on prime number p. This median increases monotonically with increasing modulus of p. The calculation results for $p \in \{3, 5, 7, 11\}$ are shown in Table 1. For $n = 500$ at large values of

Table 1. Median time (in seconds) for calculating the rank of a random $n \times n$ matrix over field $GF(p)$ for $p \in \{3, 5, 7, 11\}$

n	$GF(3)$	$GF(5)$	$GF(7)$	$GF(11)$
100	0.4	0.5	0.6	0.7
200	3.2	4.6	5.1	5.9
300	11	16	18	21
400	27	39	45	51
500	53	78	91	102
600	95	137	158	177
700	151	220	251	280
800	227	327	376	421
900	324	468	538	595
1000	447	644	737	832

Table 2. Ratios of the interquartile range $(Q_3 - Q_1)$ to the median time required for calculating the rank of a random $n \times n$ matrix over field $GF(p)$ for $p \in \{3, 5, 7, 11\}$

n	$GF(3)$	$GF(5)$	$GF(7)$	$GF(11)$
100	0.06	0.09	0.10	0.06
200	0.03	0.07	0.07	0.07
300	0.05	0.03	0.03	0.03
400	0.04	0.03	0.02	0.02
500	0.02	0.02	0.02	0.03
600	0.03	0.02	0.02	0.02
700	0.01	0.01	0.01	0.01
800	0.02	0.02	0.01	0.02
900	0.01	0.01	0.01	0.02
1000	0.02	0.01	0.01	0.01

Table 3. Median time (in seconds) for calculating the rank of a random $n \times n$ matrix with integer entries independently and uniformly distributed over the interval from zero to 10^k for $k \in \{1, 2, 3, 4, 5\}$

n	$k = 1$	$k = 2$	$k = 3$	$k = 4$	$k = 4$
100	0.184	0.262	0.345	0.426	0.513
200	2.20	3.64	5.11	6.71	8.48
300	10.5	18.3	27.0	36.5	47.2
400	32.9	60.2	91.2	126	164
500	83.9	155	237	332	439
600	178	340	526	743	990
700	341	662	1040	1480	1980
800	609	1190	1880	2700	3630
900	1010	2000	3190	4600	6220
1000	1610	3200	5140	7440	10 100

$p \in \{31, 101, 307, 1009, 3001\}$, the time required for calculating the rank depends slightly on p. Table 2 shows the ratios of the interquartile range $(Q_3 - Q_1)$ to the median for the same data.

For matrices over the field of rational numbers (in SymPy, it corresponds to the QQ domain), the time required for calculating the rank increases faster with increasing matrix order, and it also depends on the binary length of matrix entries. The entries of the generated matrices were independently and uniformly distributed over the set of integers from zero to 10^k for $k \in \{1, 2, 3, 4, 5\}$. In this case, the median time required for calculating the rank monotonically increases with increasing matrix order as $c(k)n^{4+\varepsilon}$, where the additive in the exponent varies on interval $0 < \varepsilon < 0.4$ depending on k. For $k = 1$ and $n = 1000$, the time it takes to calculate the rank of an $n \times n$ matrix does not exceed half an hour; for $k = 5$, it is approximately three hours. The results are shown in Table 3.

The calculations were carried out on a computer with Intel® Core i7-5820K 3.30GHz and 32 GB RAM.

The discussed reduction in the number of variables when searching for the (0, 1)-solution can be explained through the dialogue between the user with low computational capabilities and the web service with high computational capabilities. The user receives instructions in the form of short messages; however, the user does not trust the service and wants to verify the presence or absence of the (0, 1) solution to the system of linear equations. If the (0, 1)-solution exists, then it is returned, and it is easy to verify whether the given sequence of zeros and ones is a solution. Otherwise, the key is to select variables that can be eliminated so that the new system still does not have (0, 1)-solutions. This elimination is easy to perform. By Theorem 4, the number of variables can be reduced if the original system has sufficiently many linearly independent equations. Thus, the system is sometimes reduced to a single equation. If the further reduction is not possible, then the user is provided with a set of almost-(0, 1)-solutions. Then, it is easy to verify that the system cannot be further simplified. Theorem 2 suggests that there are obstacles to this simplification. In the worst case, the problem remains computationally complex.

4. CONCLUSIONS

The reported results are consistent with the generally accepted hypothesis about the high computational complexity of (0, 1)-solution recognition problems for systems of linear equations, because changing the problem by elimination of variables encounters the obstacle in the worst case. However, the obtained estimates leave room for certain reduction in computational complexity over finite fields. On the other hand, computer algebra systems allow one to quickly calculate the matrix rank and the dimension of the affine subspace over the field of residue modulo a prime number.

FUNDING

This work was supported by ongoing institutional funding. No additional grants to carry out or direct this particular research were obtained.

CONFLICT OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

1. Alaev, P.E., Finitely generated structures computable in polynomial time, *Sib. Math. J.,* 2022, vol. 63, pp. 801–818. https://doi.org/10.1134/S0037446622050019
2. Leontiev, V.K. and Gordeev, E.N., On the number of solutions to a system of Boolean equations, *Autom. Remote Control,* 2021, vol. 82, pp. 1581–1596. https://doi.org/10.1134/S000511792109006X
3. Gordeev, E.N. and Leont'ev, V.K., On the number of solutions to linear Diophantine equation and Frobenius problem, *Comput. Math. Math. Phys.,* 2022, vol. 62, pp. 1413–1423. https://doi.org/10.1134/S0965542522090044
4. Pan, Y. and Zhang, F., Solving low-density multiple subset sum problems with SVP oracle, *J. Syst. Sci. Complexity,* 2016, vol. 29, pp. 228–242. https://doi.org/10.1007/s11424-015-3324-9
5. Seliverstov, A.V., Binary solutions to large systems of linear equations, *Prikl. Diskretnaya Mat.,* 2021, no. 52, pp. 5–15. https://doi.org/10.17223/20710410/52/1
6. Seliverstov, A.V., Generalization of the subset sum problem and cubic forms, *Comput. Math. Math. Phys.,* 2023, vol. 63, pp. 48–56. https://doi.org/10.1134/S0965542523010116
7. Akmal, S., Chen, L., Jin, C., Raj, M., and Williams, R., Improved Merlin–Arthur protocols for central problems in fine-grained complexity, *Algorithmica,* 2023, vol. 85, pp. 2395–2426. https://doi.org/10.1007/s00453-023-01102-6
8. Stoichev, S.D. and Gezek, M., Unitals in projective planes of order 25, *Math. Comput. Sci.,* 2023, vol. 17, no. 5, pp. 1–19. https://doi.org/10.1007/s11786-023-00556-9
9. Chistov, A.L., Fast parallel calculation of the rank of matrices over a field of arbitrary characteristic, *Lect. Notes Comput. Sci.,* 1985, vol. 199, pp. 63–69. https://doi.org/10.1007/BFb0028792
10. Mulmuley, K., A fast parallel algorithm to compute the rank of a matrix over an arbitrary field, *Combinatorica,* 1987, vol. 7, no. 1, pp. 101–104. https://doi.org/10.1007/BF02579205
11. Cheung, H.Y., Kwok, T.C., and Lau, L.C., Fast matrix rank algorithms and applications, *J. ACM,* 2013, vol. 60, no. 5, pp. 1–25. https://doi.org/10.1145/2528404
12. Pereslavtseva, O.N., On calculating the characteristic polynomial of a matrix, Discrete Mathematics and Applications, 2011, vol. 21, no. 1, pp. 109–128. https://doi.org/10.1515/DMA.2011.008
13. Neiger, V. and Pernet, C., Deterministic computation of the characteristic polynomial in the time of matrix multiplication, *J. Complexity,* 2021, vol. 67, no. 101572, pp. 1–35. https://doi.org/10.1016/j.jco.2021.101572
14. Birmpilis, S., Labahn, G., and Storjohann, A., A fast algorithm for computing the Smith normal form with multipliers for a nonsingular integer matrix, *J. Symbolic Comput.,* 2023, vol. 116, pp. 146–182. https://doi.org/10.1016/j.jsc.2022.09.002
15. Abramov, S.A., Petkovšek, M., and Ryabenko, A.A., On ranks of matrices over noncommutative domains, *Comput. Math. Math. Phys.,* 2023, vol. 63, no. 5, pp. 771–778.
16. Yuran, A., Newton polytopes of non-degenerate quadratic forms, Functional Analysis and Its Applications, 2022, vol. 56, no. 2, pp. 152–158. https://doi.org/10.1134/S0016266322020095
17. Batkhin, A.B. and Bruno, A.D., Real normal form of a binary polynomial at a second-order critical point, *Comput. Math. Math. Phys.,* 2023, vol. 63, pp. 1–13. https://doi.org/10.1134/S0965542523010062
18. Seliverstov, A.V., On a simple lower bound for the matrix rank, *Komp'yuternaya algebra: materialy 5-i mezhdunarodnoi konferentsii* (Computer Algebra: Proc. 5th Int. Conf.), Abramov, S.A., Batkhin, A.B., and Sevast'yanov, L.A., Eds., Moscow: Inst. Prikl. Mat. im. Keldysha, 2023, pp. 126–128.
19. Bayramov, R.E., Blinkov, Yu.A., Levichev, I.V., Malykh, M.D., and Melezhik, V.S., Analytical study of cubature formulas on a sphere in computer algebra systems, *Comput. Math. Math. Phys.,* 2023, vol. 63, pp. 77–85. https://doi.org/10.1134/S0965542523010050
20. Meurer, A., Smith, C.P., Paprocki, M., Čertik, O., Kirpichev, S.B., Rocklin, M., Kumar, A., Ivanov, S., Moore, J.K., Singh, S., Rathnayake, T., Vig, S., Granger, B.E., Muller, R.P., Bonazzi, F., Gupta, H., Vats, S., Johansson, F., Pedregosa, F., Curry, M.J., Terrel, A.R., Roučka, Š., Saboo, A., Fernando, I., Kulal, S., Cimrman, R., and Scopatz, A., SymPy: Symbolic computing in Python, *PeerJ Comput. Sci.,* 2017, vol. 3, no. e103, pp. 1–27. https://doi.org/10.7717/peerjcs.103

Translated by Yu. Kornienko