Федеральный исследовательский центр
Информатика и Управление
Российской академии наук

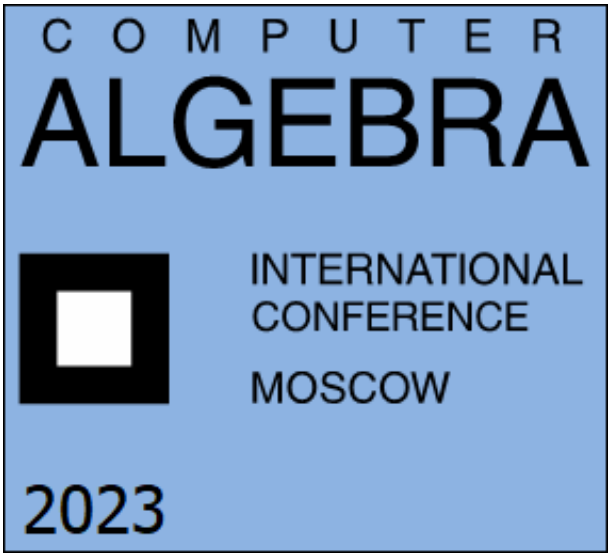
РУДН

Ордена Ленина
им. М.В. Келдыша РАН

КОМПЬЮТЕРНАЯ АЛГЕБРА

Материалы 5-й международной конференции

Москва, 26–28 июня 2023 года



ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ
«ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
«ИНФОРМАТИКА И УПРАВЛЕНИЕ»
РОССИЙСКОЙ АКАДЕМИИ НАУК»

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ
ИМЕНИ ПАТРИСА ЛУМУМБЫ»

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ
«ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ ИМ. М. В. КЕЛДЫША
РОССИЙСКОЙ АКАДЕМИИ НАУК»

КОМПЬЮТЕРНАЯ АЛГЕБРА

Материалы 5-й Международной Конференции

Москва, 26–28 июня 2023 года

COMPUTER ALGEBRA

5th International Conference Materials

Moscow, June 26–28, 2023

Москва
ИПМ им. М.В. Келдыша РАН
2023

УДК 519.6(063)
ББК 22.19;31
К637

Ответственные редакторы:
д-р физ.-мат. наук С.А. АБРАМОВ,
д-р физ.-мат. наук А.Б. БАТХИН,
д-р физ.-мат. наук Л.А. СЕВАСТЬЯНОВ

Рецензенты: канд. техн. наук Ю.О. Трусова,
канд. физ.-мат. наук К.П. Ловецкий

Компьютерная алгебра: материалы 5-й международной конференции. Москва, 26–28 июня 2023 г./ отв. ред. С.А. Абрамов, А.Б. Батхин, Л.А. Севастьянов. – Москва: ИПМ им. М.В. Келдыша, 2023.

ISBN 978-5-98354-067-5
https://doi.org/10.20948/ca-2023

Международная конференция проводится совместно ФИЦ «Информатика и управление» РАН, Российским университетом дружбы народов им. Патриса Лумумбы и ФИЦ Институтом прикладной математики им. М.В. Келдыша РАН. В представленных на конференции докладах обсуждаются актуальные вопросы компьютерной алгебры — научной дисциплины, алгоритмы которой ориентированы на точное решение математических и прикладных задач с помощью компьютера.

UDC 519.6(063)
BBC 22.19;431

Responsible editors:
Doctor of Physical and Mathematical Sciences S.A. Abramov,
Doctor of Physical and Mathematical Sciences A.B. Batkhin,
Doctor of Physical and Mathematical Sciences L.A. Sevastianov

Reviewers: PhD Yu.O. Trusova, PhD K.P. Lovetskiy

Computer algebra: 5th International Conference Materials. Moscow, 26–28 June, 2023/ ed. S.A. Abramov, A.B. Batkhin, L.A. Sevastyanov. Moscow: KIAM, 2023.

ISBN 978-5-98354-067-5
https://doi.org/10.20948/ca-2023

The international conference is organized jointly by Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, Peoples’ Friendship University of Russia named after Patrice Lumumba and Keldysh Institute of Applied Mathematics of Russian Academy of Sciences. The talks presented at the conference discuss actual problems of computer algebra — the discipline whose algorithms are focused on the exact solution of mathematical and applied problems using a computer.

On a Simple Lower Bound for the Matrix Rank

A.V. Seliverstov

Institute for Information Transmission Problems of Russian Academy of Sciences (Kharkevich Institute), Russia

e-mail: slvstv@iitp.ru

Abstract

Over a field of characteristic not equal to two, we proved a lower bound for the rank of a square matrix, where every entry outside the leading diagonal is equal to either zero or one, but every diagonal entry is neither zero nor one. This lower bound equals half of the order of the matrix. It is tight.

Keywords: matrix rank, affine subspace, computational complexity

The rank of an $n \times n$ matrix over a field can be calculated using a polynomial number of processors and performing only $O(\log_2^2 n)$ algebraic operations per processor [1, 2]. On the other hand, the computational complexity of both matrix rank [3] and the characteristic polynomial [4, 5] is equivalent in complexity to matrix multiplication. In practice, calculating the matrix rank requires a lot of time or a large number of processors. Simple lower bounds are important for planning calculations because a sufficiently large rank ensures the applicability of some algorithms for solving pseudo-Boolean programming problems [6, 7]. The distribution of the matrix rank over a finite field is used in cryptography [8].

Let us denote by K an arbitrary field of characteristic not equal to two. Let us consider an $n \times n$ matrix over the field K, where every entry outside the leading diagonal belongs to the set $\{0, 1\}$, but every diagonal entry is neither 0 nor 1. How small can its rank be?

This problem has a simple geometric interpretation. We consider an affine space over a field K with a fixed system of Cartesian coordinates. A point is identified with a column, where entries are coordinates of the point in this coordinate system. A column of zeros and ones corresponds to a $(0, 1)$-point, i.e., to a vertex of the unit cube. In matrices under consideration, each column corresponds to a point in a straight line passing through two adjacent $(0, 1)$-points, but this point does not coincide with any of $(0, 1)$-points. Moreover, different columns of the matrix correspond to non-parallel straight lines.

The rank of a matrix A is related to the dimensionality of the affine hull L of all points corresponding to columns of the matrix. If L passes through the origin, then $\operatorname{rank}(A) = \dim(L)$, else $\operatorname{rank}(A) = \dim(L) + 1$.

Theorem 1. *Given an $n \times n$ matrix A over the field K, where every entry outside the leading diagonal belongs to the set $\{0, 1\}$, but every diagonal entry is neither 0 nor 1. The rank of the matrix A is at least $n/2$.*

Proof. The theorem is obvious when the matrix A has at most two columns because $\operatorname{rank}(A) \geq 1$.

Let the theorem be proved for some $n \geq 3$ and for all $m \times m$ matrices with $m < n$. Let us consider an $n \times n$ matrix A.

A column of the matrix A corresponds to a point in a straight line passing through two adjacent $(0, 1)$-points, but this point itself is different from any $(0, 1)$-point. Changes of coordinates $x_k \to 1 - x_k$ (for different indices k) commute with each other and map each $(0, 1)$-point to some $(0, 1)$-point. Such coordinate transformations preserve the dimensionality of the affine hull of given points, as well as the number of $(0, 1)$-points belonging to this affine hull. Therefore, if no $(0, 1)$-point belongs to this affine hull, then such transformations do not affect the rank of the matrix.

By applying these transformations to the matrix A, one can obtain a matrix M of the same type so that in the last column of the matrix M all entries vanish except for the entry belonging to the leading diagonal. Removing both last column and last row from the matrix M, we get the $(n-1)\times(n-1)$ matrix B of lower rank. By the inductive hypothesis, $\operatorname{rank}(B)\geq(n-1)/2$. Thus, $\operatorname{rank}(M)\geq n/2$.

Let us denote by L the affine hull of all points corresponding to columns of M. Two cases are possible. If the origin belongs to L, then $\operatorname{rank}(M)=\dim(L)$. Therefore, the rank $\operatorname{rank}(A)\geq\dim(L)=\operatorname{rank}(M)\geq n/2$.

Else if the origin does not belong to L, then $\operatorname{rank}(A)\geq\operatorname{rank}(M)-1=\operatorname{rank}(B)$. By applying some transformations to the matrix B, one can obtain a matrix N of the same type so that in the last column of the matrix N all entries vanish except for the entry belonging to the leading diagonal. Moreover, $\operatorname{rank}(B)\geq\operatorname{rank}(N)$. Removing both last column and last row from the matrix N, we get the $(n-2)\times(n-2)$ matrix C of lower rank. By the inductive hypothesis, $\operatorname{rank}(C)\geq(n-2)/2=(n/2)-1$. Thus, $\operatorname{rank}(N)\geq n/2$. Therefore, $\operatorname{rank}(A)\geq\operatorname{rank}(B)\geq\operatorname{rank}(N)\geq n/2$. □

The lower bound is tight. Let $\lceil\cdot\rceil$ denote rounding up.

Theorem 2. *For every odd n, there is an $n\times n$ matrix A over the field K such that every entry outside the leading diagonal belongs to the set $\{0,1\}$, every diagonal entry is neither 0 nor 1, no $(0,1)$-point belongs to the affine hull of all points corresponding to columns of the matrix A, and the equality $\operatorname{rank}(A)=\lceil n/2\rceil$ holds.*

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

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

Let us denote by B an $(n-1)\times(n-1)$ matrix obtained by removing both first column and first row from the matrix A. Obviously, $\operatorname{rank}(A)=\operatorname{rank}(B)+1$. The matrix B is block-diagonal with 2×2 blocks. All blocks are degenerate. Thus, $\operatorname{rank}(B)=(n-1)/2$. Next, $\operatorname{rank}(A)=\operatorname{rank}(B)+1=(n+1)/2=\lceil n/2\rceil$.

Every column of the matrix A is a solution to the inhomogeneous system of equations

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

This system defines the affine hull, which does not pass through any $(0,1)$-point. □

Example 1. For the 3×3 matrix

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

the rank equals two. Three columns correspond to three points belonging to a straight line L. The straight line L is given by the system of two equations $1-2x_1+x_2=0$ and $x_2+x_3=0$. But the straight line L does not pass through any of the $(0,1)$-points.

Example 2. For 2×2 matrices under consideration, the rank equals one for matrices

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

where $\alpha \notin \{0, 1\}$. Two points corresponding to columns of this matrix belong to a straight line that passes through the origin, i.e., through a $(0, 1)$-point. This straight line is given by the equation $x_2 = \alpha x_1$. Therefore, if no $(0, 1)$-point belongs to the affine hull of all points corresponding to columns of the matrix A, then $\mathrm{rank}(A) = 2$.

Theorem 3. *Given an even n and an $n \times n$ matrix A over the field K, where every entry outside the leading diagonal belongs to the set $\{0, 1\}$, but every diagonal entry is neither 0 nor 1. If no $(0, 1)$-point belongs to the affine hull of all points corresponding to columns of the matrix A, then the rank of the matrix A is at least $(n/2) + 1$.*

References

[1] *Chistov A.L.* Fast parallel calculation of the rank of matrices over a field of arbitrary characteristic. In: L. Budach (eds) Fundamentals of Computation Theory. FCT 1985. Lecture Notes in Computer Science, vol. 199. Springer, Heidelberg, 1985, pp. 63–69. https://doi.org/10.1007/BFb0028792

[2] *Mulmuley K.* A fast parallel algorithm to compute the rank of a matrix over an arbitrary field. Combinatorica. 1987. Vol. 7, N. 1, pp. 101–104. https://doi.org/10.1007/BF02579205

[3] *Cheung H.Y., Kwok T.C., Lau L.C.* Fast matrix rank algorithms and applications. Journal of the ACM. 2013. Vol. 60, N. 5, Article 31, pp 1–25. https://doi.org/10.1145/2528404

[4] *Pereslavtseva O.N.* Calculation of the characteristic polynomial of a matrix. Discrete Mathematics and Applications. 2011. Vol. 21, N. 1, pp. 109–128. https://doi.org/10.1515/DMA.2011.008

[5] *Neiger V., Pernet C.* Deterministic computation of the characteristic polynomial in the time of matrix multiplication. Journal of Complexity. 2021. Vol. 67, N. 101572, pp. 1–35. https://doi.org/10.1016/j.jco.2021.101572

[6] *Seliverstov A.V.* Binary solutions to large systems of linear equations. Prikladnaya Diskretnaya Matematika. 2021. N. 52, pp. 5–15. (In Russian) https://doi.org/10.17223/20710410/52/1

[7] *Seliverstov A.V.* Generalization of the subset sum problem and cubic forms. Computational Mathematics and Mathematical Physics. 2023. Vol. 63, N. 1, pp. 48–56. https://doi.org/10.1134/S0965542523010116

[8] *Kruglov V.I., Mikhailov V.G.* On the rank of random matrix over prime field consisting of independent rows with given numbers of nonzero elements. Matematicheskie Voprosy Kriptografii. 2020. Vol. 11, N. 3, pp. 41–52. (In Russian) https://doi.org/10.4213/mvk331