ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ
«ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
«ИНФОРМАТИКА И УПРАВЛЕНИЕ»
РОССИЙСКОЙ АКАДЕМИИ НАУК»
ВЫЧИСЛИТЕЛЬНЫЙ ЦЕНТР им. А. А. ДОРОДНИЦЫНА
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ»

КОМПЬЮТЕРНАЯ АЛГЕБРА

Материалы 4-й международной конференции

Москва, 28–29 июня 2021 г.

COMPUTER ALGEBRA

4th International Conference Materials

Moscow, June 28–29, 2021

МАКС ПРЕСС

МОСКВА – 2021

УДК 519.6(063)
ББК 22.19;31
К63

Ответственные редакторы:
С.А. Абрамов – д-р физ.-мат. наук
Л.А. Севастьянов – д-р физ.-мат. наук

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

Компьютерная алгебра. Материалы 4-й международной конференции. Москва, 28–29 июня 2021 г./ под ред. С.А. Абрамова, Л.А. Севастьянова. – Москва : МАКС Пресс, 2021. – 124 с.
ISBN 978-5-317-06623-9
https://doi/org/10.29003/m2019.978-5-317-06623-9

Международная конференция проводится совместно Вычислительным центром им. А.А.Дородницына ФИЦ “Информатика и управление” РАН и Российским университетом дружбы народов. 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.

УДК 519.6(063)
ББК 22.19;31

Computer algebra: 4th International Conference Materials. Moscow, June 28–29, 2021/ Ed. S.A. Abramov, L.A. Sevastyanov. Moscow : MAKS Press, 2021. – 124 p.
ISBN 978-5-317-06623-9
https://doi/org/10.29003/m2019.978-5-317-06623-9

The international conference is organized jointly by Dorodnicyn Computing Center of Federal Research Center “Computer Science and Control” of Russian Academy of Science and Peoples’ Friendship University of Russia. 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.

ISBN 978-5-317-06623-9

A Plain Note on Binary Solutions to Large Systems of Linear Equations

A.V. Seliverstov[1]

[1]*Institute for Information Transmission Problems of RAS (Kharkevich Institute), Russia*
e-mail: slvstv@iitp.ru

Abstract. A generic-case algorithm is proposed to recognize systems of linear equations without any binary solution, when the number of equations is close to the number of unknowns. This problem corresponds to a well-known optimization problem, i.e., the multidimensional knapsack problem. In 1994 Nikolai Kuzyurin discovered an average-case polynomial-time optimization algorithm. His proof is based on binomial tail bounds. Contrariwise, our algebraic approach allows to specify the structure of the set of inconvenient inputs. For any fixed dimension, this set is included in the set of zeros of an explicit nonzero multivariate polynomial.

Keywords: binary solution, linear equation, generic-case complexity

Introduction

Let us consider the decision problem whether there exists a binary solution (also known as a $(0,1)$-solution) to a system of inhomogeneous linear equations with integer coefficients. The problem is NP-complete and can be reduced to its particular case containing only one linear equation [1]. In some cases, the equation has small integer coefficients [2, 3]. Furthermore, a binary solution to one linear equation can be found using a pseudopolynomial-time algorithm [1, 4–7]. Without any restriction on the coefficients, Horowitz and Sahni [8] had introduced the meet-in-the-middle approach and gave an exact $O^*(2^{n/2})$ time and space algorithm. A few years later, Schroeppel and Shamir [9] improved the space complexity to $O^*(2^{n/4})$. Recently a probabilistic $O^*(2^{0.86n})$ time and polynomial-space algorithm was found [10]. The O^* notation suppresses a factor that is polynomial in the input size. There is also known a polynomial upper bound on the average-case complexity of the multidimensional knapsack problem [11].

By means of Gaussian elimination, searching for a binary solution to a system of m linearly independent linear equations in n unknowns is reduced to a parallel check whether a binary solution to a subsystem in $n-m$ unknowns can be extended to a binary solution to the whole system of equations in n unknowns. Hence, the initial problem is polynomial-time solvable when the difference between the number of unknowns and the number of linearly independent equations is bounded by a function of the type $n - m = O(\log n)$. Let us consider the case when the difference between the number of unknowns n and the number of equations m is bounded by a function of the type $n - m = O(\sqrt{n})$. So, the previously obtained estimate is improved, although the proposed method is generally useless for one equation.

An easy generalization of this problem is searching for binary solutions to a system of linear equations over an arbitrary field $(K, 0, 1, +, -, \times, ()^{-1}, =)$ of characteristic zero. Let us define $0^{-1} = 0$. In contrast to previous works [11], we consider not only ordered fields but also arbitrary fields of characteristic zero, including the field of complex numbers. Let us use either generalized register machines [12] or BSS-machines over reals [13]. These machines over an algebraic extension of the field of rational numbers naturally correspond to the idea of symbolic computations. Every register contains an element of K. The machine also has index registers containing non-negative integers. The running time is polynomial when the total number of operations performed by the machine is bounded by a polynomial in the number of registers containing the input. Initially, this number is written in the zeroth index register.

A predicate holds almost everywhere when it holds on every instance x satisfying an inequality of the type $f(x) \neq 0$, where f denotes a nonzero polynomial [14]. This restriction is more rigorous than any upper bound on the measure. Let us consider so-called generic generalized register machines over K. The machine halts at every input and gives a meaningful answer at almost every input, but it can abandon the calculation using explicit notification, that is, there exists the vague halting state. More precisely, a generalized register machine over K is called generic when two conditions hold: (1) the machine halts at every input and (2) for every positive integer k and for almost all inputs, each of which occupies exactly k registers, the machine accepts or rejects the input, but does not halt in the vague state. Generic machines that compute non-trivial output in registers are defined similarly. If the machine halts in the vague state, then the output recorded in the registers is considered meaningless. Note that the machine does not make any error. For detailed description of generic-case computation on classical computational models refer to [15–16].

Results

Let us consider systems of linear equations of the type $x_j = \ell_j(1, x_1, \cdots, x_{n-m})$, where $j > n - m$ and every $\ell_j(x_0, x_1, \cdots, x_{n-m})$ denotes a linear form over K.

Theorem. *There exists a polynomial-time generic generalized register machine over K such that for all positive integers n and m satisfying the inequality $2n \geq (n-m+1)(n-m+2)$, and for almost every m-tuple of linear forms $\ell_j(x_0, \cdots, x_{n-m})$, where $j > n - m$, if the machine accepts the input, then there exists no binary solution to the system of all equations of the type $x_j = \ell_j(1, x_1, \cdots, x_{n-m})$. Moreover, for every n, there exists a polynomial of degree at most $2n$ in coefficients of all the linear forms ℓ_j such that if the machine halts in the vague state, then the polynomial vanishes.*

Proof. If $2n < (n-m+1)(n-m+2)$, then the machine rejects the input. Else, in accordance with Theorem 1, some polynomial time generic machine calculates numbers $\lambda_1, \ldots, \lambda_n$ such that the equality

$$\sum_{k=1}^{n-m} \lambda_k x_k (x_k - x_0) + \sum_{j=n-m+1}^{n} \lambda_j \ell_j (\ell_j - x_0) = x_0^2$$

holds. On the other hand, if there exists a binary solution to the system of all the equations $x_j = \ell_j(1, x_1, \cdots, x_{n-m})$, then the left-hand polynomial vanishes at the binary solution. Therefore, an affirmative answer confirms that there is no binary solution to the system. Otherwise, the machine halts in the vague state.

The set $\{\lambda_k\}$ is a solution to an inhomogeneous system of linear equations in n unknowns $\lambda_1, \ldots, \lambda_n$. The system contains only one inhomogeneous equation. Let us denote by r the number of all the equations, that is, $r = \frac{1}{2}(n-m+1)(n-m+2) \leq n$. The sufficient condition for the solvability is the full rank of a $r \times n$ matrix. If $r = n$, then it is sufficient that the determinant does not vanish. If $r < n$, then it is sufficient that some $r \times r$ minor does not vanish. For example, let us pick up the leading principal minor. In any case, it is a polynomial of degree r in matrix entries. Every entry is a polynomial of degree at most two in coefficients of some ℓ_j. Thus, the minor is a polynomial of degree at most $2r \leq 2n$. To complete the proof, we need to show that this polynomial does not vanish identically. □

Remark 1. Over the field of rational numbers, not only the arithmetic complexity but also the bit complexity is polynomial because the rank can be easily computed [1]. So, there is a generic-case polynomial-time algorithm. Moreover, the rank can be computed in $O(\log^2 n)$ operations over an arbitrary field using a polynomial number of processors [17–18].

Remark 2. Our method can be generalized using higher degree forms. For example, let us consider a general straight line L in the projective plane. There exist four $(0,1)$-points with homogeneous coordinates $(1:0:0)$, $(1:0:1)$, $(1:1:0)$, and $(1:1:1)$, respectively. Our goal is a sufficient condition such that no $(0,1)$-point belongs to L. Every ternary quadratic form vanishing at every $(0,1)$-point is one of the type $\lambda_1 x_1(x_1 - x_0) + \lambda_2 x_2(x_2 - x_0)$. These forms span a linear space of dimension two. Ternary cubic forms vanishing at every $(0,1)$-point span a linear space of dimension six [19]. All binary cubic forms span a linear space of dimension four. The restriction of a ternary cubic form to the straight line L defines a linear map from the linear space of ternary cubic forms to the linear space of binary cubic forms. The kernel of the map is spanned by forms vanishing identically at whole L. Every such form is reducible and has a linear factor corresponding to L. Consequently, the dimension of the kernel equals the dimension of the space of some ternary quadratic forms.

Let the image of a ternary cubic form vanishing at every $(0,1)$-point be its restriction to the general straight line L. The dimension of the kernel of the linear map equals two. The dimension of the image of the linear map equals four and coincides with the dimension of the space of all binary cubic forms. Consequently, the map is surjective. Obviously, its surjectivity is a sufficient condition for the absence of any $(0,1)$-point belonging to L.

Conclusion

We have considered a decision problem. The binary search allows to find binary solutions to sufficiently large systems of linear equations when such a solution exists and some generality assumption holds. So, the proposed method can be used to solve some combinatorial optimization problems that can be reduced to Boolean programming. In particular, such problems arise in bioinformatics.

References

1. *Schrijver A.* Theory of linear and integer programming. John Wiley & Sons, New York, 1986.
2. *Seliverstov A.V.* Binary solutions to some systems of linear equations. In: Eremeev A., Khachay M., Kochetov Y., Pardalos P. (eds) Optimization Problems and Their Applications. OPTA 2018. Communications in Computer and Information Science. Vol. 871. Springer, Cham, 2018. P. 183–192.
3. *Seliverstov A.V.* On binary solutions to systems of equations. Prikladnaya Diskretnaya Matematika. 2019. No. 45. P. 26–32 (in Russian).
4. *Smolev V.V.* On an approach to the solution of a Boolean linear equation with positive integer coefficients. Discrete Mathematics and Applications. 1993. Vol. 3, No. 5. P. 523–530.

5. *Koiliaris K., Xu C.* Faster pseudopolynomial time algorithms for subset sum. ACM Transactions on Computation Theory. 2019. Vol. 15, No. 3. Article 40.

6. *Curtis V.V., Sanches C.A.A.* An improved balanced algorithm for the subset-sum problem. European Journal of Operational Research. 2019. Vol. 275. P. 460–466.

7. *Mucha M., Węgrzycki K., Włodarczyk M.* A subquadratic approximation scheme for partition. In: Chan N.M. (ed.) Proceedings of the 2019 Annual ACM-SIAM Symposium on Discrete Algorithms. 2019. P. 70–88.

8. *Horowitz E., Sahni S.* Computing partitions with applications to the knapsack problem. Journal of the Association for Computing Machinery. 1974. Vol. 21, No. 2. P. 277–292.

9. *Schroeppel R., Shamir A.* A $T = O(2^{n/2})$, $S = O(2^{n/4})$ algorithm for certain NP-complete problems. SIAM Journal on Computing. 1981. Vol. 10, No. 3. P. 456–464.

10. *Bansal N., Garg S., Nederlof J., Vyas N.* Faster space-efficient algorithms for subset sum, k-sum, and related problems. SIAM Journal on Computing. 2018. Vol. 47, No. 5. P. 1755–1777.

11. *Kuzyurin N.N.* An algorithm that is polynomial in the mean in integer linear programming. Sibirskii Zhurnal Issledovaniya Operatsii. 1994. Vol. 1, No. 3. P. 38–48. (In Russian)

12. *Neumann E., Pauly A.* A topological view on algebraic computation models. Journal of Complexity. 2018. Vol. 44. P. 1–22.

13. *Blum L., Shub M., Smale S.* On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. Bulletin of the American Mathematical Society (N.S.) 1989. Vol. 21, No. 1. P. 1–46.

14. *Seliverstov A.V.* Symmetric matrices whose entries are linear functions. Computational Mathematics and Mathematical Physics. 2020. Vol. 60, No. 1. P. 102–108.

15. *Miasnikov A., Ushakov A.* Generic case completeness. Journal of Computer and System Sciences. 2016. Vol. 82, No. 8. P. 1268–1282.

16. *Rybalov A.N.* On generic complexity of the subset sum problem for semigroups of integer matrices. Prikladnaya Diskretnaya Matematika. 2020. No. 50. P. 118–126. (In Russian)

17. *Chistov A.L.* Fast parallel calculation of the rank of matrices over a field of arbitrary characteristic. In: Budach L. (eds) Fundamentals of Computation Theory. FCT 1985. Lecture Notes in Computer Science, vol 199. Springer, Berlin, Heidelberg. 1985.

18. *Mulmuley K.* A fast parallel algorithm to compute the rank of a matrix over an arbitrary field. Combinatorica. 1987. Vol. 7, No. 1. P. 101–104.

19. *Seliverstov A.V., Lyubetsky V.A.* About forms equal to zero at each vertex of a cube. Journal of Communications Technology and Electronics. 2012. Vol. 57, No. 8. P. 892–895.

Научное издание

КОМПЬЮТЕРНАЯ АЛГЕБРА
Материалы 4-й международной конференции
Москва, 28–29 июня 2021 г.

Издательство «МАКС Пресс»
Главный редактор: *Е. М. Бугачева*

Напечатано с готового оригинал-макета
Подписано в печать 28.05.2021 г.
Формат 60x90 1/16. Усл.печ.л. 7,75.
Тираж 300 (1–80) экз. Заказ 86.

Издательство ООО “МАКС Пресс”
Лицензия ИД N 00510 от 01.12.99 г.
119992, ГСП-2, Москва, Ленинские горы, МГУ им. М.В. Ломоносова,
2-й учебный корпус, 527 к.
Тел. 8(495)939-3890/91. Тел./Факс 8(495)939-3891.

Отпечатано в полном соответствии с качеством
предоставленных материалов в ООО «Фотоэксперт»
115201, г. Москва, ул. Котляковская, д.3, стр. 13.