On Probabilistic Algorithm for Solving Almost All Instances of the Set Partition Problem

Alexandr V. Seliverstov(✉)

Institute for Information Transmission Problems of the Russian Academy of Sciences (Kharkevich Institute), Bolshoy Karetny per. 19, build. 1, Moscow 127051, Russia
slvstv@iitp.ru

Abstract. Earlier, I.V. Latkin and the author have shown the set partition problem can be reduced to the problem of finding singular points of a cubic hypersurface. The article focuses on the new link between two different research areas as well as on methods to look for singular points or to confirm the smoothness of the hypersurface. Our approach is based on the description of tangent lines to the hypersurface. The existence of at least one singular point imposes a restriction on the algebraic equation that determines the set of tangent lines passing through the selected point of the space. This equation is based on the formula for the discriminant of a univariate polynomial. We have proposed a probabilistic algorithm for some set of inputs of the set partition problem. The probabilistic algorithm is not proved to have polynomial complexity.

Keywords: Set partition · Cubic hypersurfaces · Smoothness · Tangent line · Polynomial · Discriminant · Computational complexity

1 Introduction

The set partition problem is NP-complete [1]. Let us recall its definition. Given a multiset of positive integers $\{\alpha_0, \ldots, \alpha_n\}$. Can it be partitioned into two subsets with equal sums of elements? Points with coordinates ± 1 are called $(-1, 1)$-points. Obviously, this problem is to recognize whether a $(-1, 1)$-point belongs to the hyperplane given by $\alpha_0 + \alpha_1 x_1 + \cdots + \alpha_n x_n = 0$. So, it is hard to find a $(-1, 1)$-point belonging to the hyperplane in high dimensions. The problem is to solve the system that consists of one linear equation and the set of quadratic equations $x_1^2 = 1, \ldots, x_n^2 = 1$. If there is no solution, then a direct proof of the unsolvability of the system by means of Hilbert's Nullstellensatz requires to produce polynomials of very high degree [2]. The informal explanation is that many $(-1, 1)$-points can lie on a hyperplane. In case $n = 2k$, the number of $(-1, 1)$-points belonging to the hyperplane given by $x_1 + \cdots + x_n = 0$ is equal to $n!/(k!)^2$. The full description of a large number of solutions requires polynomials

The research has been carried out at the expense of the Russian Science Foundation, project no. 14–50–00150.

P. Weil (Ed.): CSR 2017, LNCS 10304, pp. 285–293, 2017.
DOI: 10.1007/978-3-319-58747-9_25

of high degree. There are known randomized algorithms for solving some systems of algebraic equations [3]. But their applicability in this case is doubtful.

There are other methods for solving integer linear programming problems [1,4]. One can find $(-1,1)$-points belonging to the hyperplane given by a linear function with integer coefficients near zero, using dynamic programming [5,6]. There is also the related optimization problem. So, there are well known both fully polynomial time approximation scheme and pseudo-polynomial time algorithm for solving the problem. The obstacle for solving the optimization problem is a large number of values of the linear functional at different $(-1,1)$-points.

In this paper, we focus on an algorithm for solving all but an exponentially small fraction of inputs; these inputs are incorrectly accepted without any warning. In accordance with the Schwartz–Zippel lemma [7], if the stupid algorithm rejects all inputs, then it works correctly on a strongly generic set of inputs [8,9]. But our algorithm can make errors of another type only.

Our method is based on the reduction of the set partition problem to the recognition problem for hypersurface singularities [10,11]. Two viewpoints may clarify each other. Other geometric formulations of related problems have already appeared in the literature [12,13]. For example, maximization of cubic form over the Euclidean ball is NP-hard too. Of course, we consider a very special type of singularities. In general the problem is very hard [14]. Singular points on the variety corresponds to roots of a system of algebraic equations. The best methods for solving the system require at least exponential time in general case [3,15]. A solution to n algebraic equations in n variables can be obtained by a series of hypergeometric type [16]. Methods based on the computation of Gröbner bases are widely used in small dimensions [17–19], but the computational complexity quickly increases in high dimensions [20]. Some examples have been computed by means of the cloud service MathPartner [21].

2 Preliminaries

The binary representation of a positive integer n has the length $\lceil \log_2(n+1) \rceil$, where $\lceil t \rceil$ is the smallest integer not less than t. We denote by $\mathbb{C}$ and $\mathbb{Q}$ the fields of complex and rational numbers, respectively.

The discriminant Δ_d of a univariate polynomial of degree d is a homogeneous function of its coefficients. The discriminant vanishes if and only if the polynomial has a multiple root. For example, the discriminant Δ_3 of the cubic polynomial $at^3 + bt^2 + pt + q$ is equal to $b^2p^2 - 4ap^3 - 4b^3q - 27a^2q^2 + 18abpq$. Moreover, $\Delta_d(g_0, g_1, \ldots, g_{d-1}, g_d) = \Delta_d(g_d, g_{d-1}, \ldots, g_1, g_0)$. If the leading coefficient vanishes, then the value of the function Δ_d is equal to the discriminant of another polynomial without the constant term. If the degree is equal to $d-1$, then Δ_d vanishes if and only if the polynomial has a multiple root. If the degree is less than $d-1$, then $\Delta_d = 0$.

A square-free polynomial is a polynomial that does not have as a factor any square of a polynomial of positive degree. An affine hypersurface is the vanishing locus of a square-free polynomial over the field of complex numbers.

Let us consider an affine hypersurface given by a square-free polynomial f. A straight line passing through the selected point U in n-dimensional affine space is defined as the set of points with coordinates $((x_1-u_1)t+u_1,\ldots,(x_n-u_n)t+u_n)$, where $(u_1,\ldots,u_n)$ are coordinates at U, and t is a parameter. Let us denote by $r(t)$ a univariate polynomial that is the restriction of the polynomial f to the line, and by $D[f,U]$ the discriminant of $r(t)$. If $\deg r(t) < d$, then we use the formula for Δ_d by means of substitution the zero as the leading coefficient. At the general point U the degree of $D[f,U](x_1,\ldots,x_n)$ is equal to d^2-d. If the line is a tangent line to the hypersurface, then the discriminant of the polynomial $r(t)$ vanishes. If U is not a singular point of the hypersurface, then $D[f,U](x_1,\ldots,x_n)$ defines a cone. If U is a smooth point of the hypersurface, the cone is reducible and contains a tangent hyperplane at the point U. If U is singular, then $D[f,U]$ vanishes identically.

If the selected point U is a smooth point of the hypersurface, then let us denote by $B[f,U]$ the discriminant of $r(t)/t$. Since $r(0)=0$, $r(t)/t$ is a polynomial of degree at most $d-1$, where $d=\deg f$. If $\deg r(t) < d-1$, then we use the formula for degree $d-1$ by means of substitution the zero as the leading coefficient. Of course, the polynomial $B[f,U]$ is a divisor of the polynomial $D[f,U]$.

To study generic-case complexity of an algorithm, let us recall the definition of the generic set [8,9]. For every positive n, let B_n denote the set of all inputs of length at most n. Let us define the asymptotic density $\rho(S)$ for S as

$$\rho(S) = \lim_{n\to\infty} \rho_n(S),$$

where

$$\rho_n(S) = \frac{|S \cap B_n|}{|B_n|}.$$

If $\rho(S)=1$, then the subset S is called generic. If in addition $\rho_n(S)$ converges to 1 exponentially fast, then S is called strongly generic.

For example, hard inputs are rare for the simplex algorithm for linear programming [22,23].

3 Results

In this section let us denote

$$f = \alpha_0 + \alpha_1 x_1^3 + \cdots + \alpha_n x_n^3$$
$$h = \alpha_0 + \alpha_1 x_1 + \cdots + \alpha_n x_n,$$

where all coefficients $\alpha_0,\ldots,\alpha_n$ are nonzero. Of course, the hypersurface $f=0$ is smooth. The following theorem is a reformulation of the result from [11].

Theorem 1. *Given a multiset of positive integers $\{\alpha_0,\ldots,\alpha_n\}$, where $n \geq 2$. There exists a one-to-one correspondence between singular points of the affine variety given by two equations $f=h=0$ and $(-1,1)$-points belonging to the hyperplane given by the equation $h=0$.*

Proof. If both polynomials f and h vanish simultaneously at a $(-1,1)$-point, then the hyperplane $h=0$ is tangent to the hypersurface $f=0$ at this point. Thus, the hyperplane section is singular.

At a singular point of the section, the hyperplane $h=0$ coincides with the tangent hyperplane to the hypersurface $f=0$. Since all the coefficients α_k are nonzero, both gradients ∇f and ∇h can be collinear only at the points whose coordinates satisfy the system of the equations $x_k^2 = x_j^2$ for all indices k and j. All the points are $(-1,1)$-points. □

The polynomial $D[f,U]$ is equal to the discriminant of a univariate polynomial at^3+bt^2+pt+q. That is, $D[f,U] = b^2p^2 - 4ap^3 - 4b^3q - 27a^2q^2 + 18abpq$, where the coefficients are sums of univariate polynomials $a = a_1(x_1) + \cdots + a_n(x_n)$, $b = b_1(x_1) + \cdots + b_n(x_n)$, $p = p_0 + p_1x_1 + \cdots + p_nx_n$, and the constant term q. Each monomial from $D[f,U](x_1,\ldots,x_n)$ is dependent on at most four variables.

The polynomial $B[f,U]$ is equal to the discriminant of a univariate polynomial at^2+bt+c. That is, $B[f,U] = b^2 - 4ac$, where the coefficients are sums of univariate polynomials $a = a_1(x_1) + \cdots + a_n(x_n)$, $b = b_1(x_1) + \cdots + b_n(x_n)$, and $c = c_0 + c_1x_1 + \cdots + c_nx_n$. Each monomial from $B[f,U](x_1,\ldots,x_n)$ is dependent on at most two variables.

Let us consider the factor ring $\mathbb{C}[x_1,\ldots,x_n]/\langle x_1^2-1,\ldots,x_n^2-1\rangle$. It is referred to as the set of multilinear polynomials. In this way, we have a surjective map φ from the set of all polynomials onto the set of multilinear polynomials.

Let us denote by $M[f,U](x_1,\ldots,x_{n-1})$ a multilinear polynomial that is an image of the restriction to the hyperplane $h=0$ of the multilinear polynomial $\varphi(B[f,U])$. The restriction to the hyperplane $h=0$ means that we substitute $x_n = -(\alpha_0 + \alpha_1x_1 + \cdots + \alpha_{n-1}x_{n-1})/\alpha_n$. Unfortunately, it is hard to compute a Gröbner basis of the ideal $\langle h, x_1^2-1,\ldots,x_n^2-1\rangle$. Instead, we use computations over the set of multilinear polynomials.

Let us denote by L or $L_{\alpha_0,\ldots,\alpha_n}$ a linear space spanned by all multilinear polynomials $M[f,U](x_1,\ldots,x_{n-1})$, where U belongs to the section $f=h=0$.

A polynomial vanishes at a $(-1,1)$-point if and only if its multilinear image vanishes at this point. Thus, if the hyperplane section given by $f=h=0$ contains a $(-1,1)$-point, then all multilinear polynomials from L vanish at the point. Contrariwise, if L coincides with the linear space of all multilinear polynomials of degree at most two, then the section does not contain any $(-1,1)$-point. Of course, all such $(-1,1)$-points are singular.

Lemma 1. *If $n=2$ and $\alpha_0=1$, then there exist infinitely many values of two coefficients α_1 and α_2 such that the linear space L coincides with the linear space of all multilinear polynomials of degree at most two. In particular, the same is true for all algebraically independent numbers α_1 and α_2.*

Proof. Let us consider a plane curve defined by $f = 3x_1^3 + 2x_2^3 + 1$. The intersection of the line $3x_1 + 2x_2 + 1 = 0$ and the curve $f=0$ consist of two points $U(-1,1)$ and $V(\frac{1}{5},-\frac{4}{5})$. The union of all tangent lines passing through the point U is defined by the polynomial $B[f,U] = -3x_2^4 - 36x_2^3x_1 - 24x_2^3 -$

$54x_2^2x_1^2 + 36x_2^2 - 36x_2x_1^3 - 24x_2 - 27x_1^4 - 72x_1^3 - 108x_1^2 - 72x_1 - 12$. Its multilinear image is $\varphi(B[f,U]) = -72x_2x_1 - 48x_2 - 144x_1 - 168$. The substitution $x_2 = -\frac{3x_1+1}{2}$ yields a univariate polynomial $108x_1^2 - 36x_1 - 144$. Its multilinear image $M[f,U] = -36x_1 - 36$. At the second point V the multilinear polynomial

$$M[f,V] = \frac{26172}{3125}x_1 + \frac{428292}{15625}.$$

Two polynomials $M[f,U]$ and $M[f,V]$ together span the whole linear space of univariate linear polynomials. The same is true for almost all cubic curves because the first-order theory of the field of complex numbers admits quantifier elimination. □

Remark 1. Let us consider an affine plane curve defined by $f = x_1^3 + x_2^3 + 1$. The intersection of the curve and the line defined by $h = x_1 + x_2 + 1$ consists of two points $U(0,-1)$ and $V(-1,0)$. The third point does not belong to the affine plane. So, $B[f,U] = -12x_1x_2 - 24x_2 - 12x_1 - 24$; the multilinear polynomial $M[f,U] = 24x_1 + 12$. On the other hand, at the point V the polynomial $B[f,V] = -12x_1x_2 - 12x_2 - 24x_1 - 24$; the multilinear polynomial $M[f,V]$ vanishes identically. Thus, L is a proper subspace in the two-dimensional space of univariate linear polynomials.

Lemma 2. *For all $n \geq 2$, if there exist nonzero numbers $\beta_0,\ldots,\beta_n$ such that the linear space $L_{\beta_0,\ldots,\beta_n}$ coincides with the linear space of all multilinear polynomials of degree at most two, then for almost all nonzero integers $\alpha_0,\ldots,\alpha_n$, the linear space $L_{\alpha_0,\ldots,\alpha_n}$ coincides with the linear space of all multilinear polynomials of degree at most two. Moreover, if for all indices k the numbers $1 \leq \alpha_k \leq S$, then the upper bound on the fraction of the exception set of $(n+1)$-tuples $\{\alpha_0,\ldots,\alpha_n\}$ is equal to $2^{poly(n)}/S$.*

Proof. All coefficients from $M[f,U]$ are continuous functions on the open set $\alpha_0 \neq 0,\ldots,\alpha_n \neq 0$. The matrix determinant is continuous too. Let us consider a set of points $\{U^{(k)}\}$ on the hypersurface $f = 0$ for a set $\{\alpha_0,\ldots,\alpha_n\}$. If all polynomials $\{M[f,U^{(k)}]\}$ are linearly independent, then under a sufficiently small change of α_k there exists a set of points $\{V^{(k)}\}$, such that for all indices $V^{(k)}$ belongs to a small polydisk near $U^{(k)}$, $V^{(k)}$ belongs to the new hypersurface $\check{f} = 0$, and all polynomials $\{M[\check{f},V^{(k)}]\}$ are linearly independent. This property is satisfied on a nonempty open set of $(n+1)$-tuples $\{\alpha_0,\ldots,\alpha_n\}$ because the first-order theory of the field of complex numbers admits quantifier elimination. Thus, $\dim L$ is a lower semi-continuous function.

In accordance with our premise, the fraction of the exception set is less than one. In accordance with Lemma 1, in case $n = 2$, the premise holds.

There exists a nontrivial polynomial $g(\alpha_0,\ldots,\alpha_n)$ of degree at most $2^{poly(n)}$ such that if L does not coincide with the linear space of all multilinear polynomials of degree at most two, then g vanishes. (The converse implication is not necessary true.) Vanishing of the polynomial g is equivalent to inconsistency of a system of $O(n^2)$ algebraic equations, where the degree of each algebraic

equations is $poly(n)$. In accordance with [15], the polynomial g can be chosen so that its degree $\deg(g) \le 2^{poly(n)}$. Thus, in accordance with the Schwartz–Zippel lemma [7], the fraction is less than $2^{poly(n)}/S$. □

Let us denote by π the projection of the hyperplane section $f = h = 0$ that forgets two coordinates x_{n-1} and x_n. Let us define

$$\lambda(n) = \frac{n(n+1)}{2} + 1$$

that is the upper bound on $\dim L$ for all $n \ge 3$.

Lemma 3. *Given a multiset of positive integers $\alpha_0, \ldots, \alpha_n$, and a real $\varepsilon > 0$. Let us consider the multilinear polynomials $m_k = M[f, U^{(k)}]$ for random points $U^{(k)}$ of the hyperplane section given by $f = h = 0$, where the index k runs the segment $1 \le k \le \lambda(n)$. If all coordinates of their images $\pi(U^{(k)})$ are independent and uniformly distributed on the set of integers from one to $\lceil 2^{180n^4}/\varepsilon \rceil$, then the probability of spanning the whole linear space L is at least $1 - \varepsilon$.*

Proof. All polynomials $m_1, \ldots, m_{\lambda(n)}$ belong to L. If the polynomials are linearly dependent, then the determinant of the matrix, whose entries are coefficients, vanishes. The order of the matrix is equal to $\lambda(n)$. Each matrix entry is a polynomial of degree at most six. The determinant of the matrix is a polynomial of degree at most $6\lambda(n)$. Let us denote the polynomial by g. The resultant $\mathrm{res}_{x_{n-1}}(g, f(x_1, \ldots, x_{n-1}, -(\alpha_0 + \alpha_1 x_1 + \cdots + \alpha_{n-1} x_{n-1})/\alpha_n)$ vanishes with probability at most ε. Else it vanishes identically. The resultant degree is less than $(3 + \deg g)\deg g \le 9n^4 + 18n^3 + 54n^2 + 45n + 54 < 180n^4$. The upper bound on the probability of vanishing the resultant is calculated by the Schwartz–Zippel lemma [7]. □

Remark 2. The enormous integer $\lceil 2^{180n^4}/\varepsilon \rceil$ has a binary representation of polynomial length. But we assume it is only very rough upper bound. Another approach to prove Lemma 3 is briefly discussed in the next section.

Theorem 2. *There exists a function $S(n)$ of the type $2^{poly(n)}$ such that for any real $\varepsilon > 0$ there exists a probabilistic algorithm for solving the set partition problem in certain sense.*

- *The algorithm receives as the input a set of positive integers $\alpha_0, \ldots, \alpha_n$ from one to $S(n)$;*
- *The algorithm executes $O(n^6)$ arithmetic operations over algebraic numbers as well as square root or cube root extraction operations;*
- *If a solution exists, then the probability of accepting is at least $1 - \varepsilon$;*
- *Else if there exist nonzero numbers $\beta_0, \ldots, \beta_n$ such that the linear space $L_{\beta_0,\ldots,\beta_n}$ coincides with the linear space of all multilinear polynomials of degree at most two, then the probability of rejecting is at least $1 - \varepsilon$ except an exponentially small fraction of inputs, i.e., on a strongly generic set of inputs.*

Proof. Let us consider the cubic hypersurface given by $f = 0$. In accordance with Theorem 1, a singular point of its hyperplane section given by $f = h = 0$ corresponds to a solution to the set partition problem [10,11].

In case $n \leq 1$, the algorithm simply checks all $(-1, 1)$-points.

In case $n \geq 2$, the algorithm picks up $\lambda(n)$ random points on the section. In this way, it picks up a random point P from the coordinate subspace, whose $n - 2$ coordinates are independently and uniformly distributed on the set of integers from one to a large number as in Lemma 3. A preimage $U \in \pi^{-1}(P)$ belongs to the section. Both points P and U have the same $n - 2$ coordinates. Other two coordinates are calculated as a solution of the system of two equations $f = h = 0$. They can be irrational.

If a $(-1, 1)$-point is picked up, then the input is accepted. Else the algorithm calculates a spanning set of the linear space L in accordance with Lemma 3. If L does not coincide with the linear space of all multilinear polynomials of degree at most two, then the input is accepted because a solution gives a linear dependence of polynomials. Else the input is rejected.

The total number of random bits used by the algorithm is bounded by a polynomial in n and $1/\varepsilon$; it does not depend on the values $\alpha_0, \ldots, \alpha_n$. The total number of the arithmetic operations over algebraic numbers is bounded by a polynomial in n.

In accordance with Lemma 2, if there exist nonzero numbers $\alpha_0, \ldots, \alpha_n$ such that the linear space L coincides with the linear space of all multilinear polynomials of degree at most two, then the error probability is small for a generic set of inputs. □

Remark 3. Instead of computation $\dim L$ it is sufficient to check whether a nonzero constant belongs to the linear space L. Moreover, if the linear space L contains a linear polynomial, one can reduce the dimension of the initial task.

4 Discussion

In fact, the algorithm from Theorem 2 computes the determinant of a matrix with irrational entries. Its value is an algebraic number that is result of $poly(n)$ arithmetic operations over roots of cubic polynomials. Unfortunately, there are such algebraic numbers whose both length and degree can be large [24]. On the other hand, if the determinant does not belong to a very small polydisk near zero, then one can use Diophantine approximation to prove that it is nonzero. Thus, we have a sufficient condition over $\mathbb{Q}$ for the absence of any solution for the set partition problem.

In Lemma 3, we pick up a point from the preimage $\pi^{-1}(P)$ containing three points. But we need only one point. Instead, the point on the cubic hypersurface can be computed in more deterministic way using a rational parameterization of the variety. All cubic surfaces as well as hypersurfaces in higher dimensions are unirational over $\mathbb{C}$, although any smooth cubic curve is not unirational. Moreover, such a cubic hypersurface defined over $\mathbb{Q}$ is unirational over $\mathbb{Q}$ if and only if it has a $\mathbb{Q}$-point [25]. Obviously, the same result is true for the

hyperplane section $f = h = 0$ that is hypersurface inside the hyperplane. Thus, if the section contain a $\mathbb{Q}$-point, then we have not only a lot of rational points but also a rational map from the set of points with integer coordinates to the variety defined by both polynomials f and h. In this case, one can modify Lemma 3 as well as Theorem 2 to eliminate irrational numbers.

The number of arithmetic operations in the algorithm depends on the computational complexity of a method for solving systems of linear equations. We adopt Gaussian elimination. Some upper bounds can be improved by means of asymptotically more efficient methods [26].

The algorithm works correctly on a strongly generic set of inputs. Maybe the exception set is empty, but this hypothesis is not obvious. Although two smooth hypersurfaces are diffeomorphic each other, their algebraic properties can differ. For example, there exists an exotic smooth complex affine variety which is diffeomorphic to an affine space, but is not algebraically isomorphic to it [27]. In case $n = 2$, see also Remark 1. But in accordance with Lemma 1, the method can be used for smoothness recognition of almost all cubic curves.

In Theorem 2, all $\alpha_0, \ldots, \alpha_n$ are integers with binary representations of length $poly(n)$. One can consider the continuous version, where all $\alpha_0, \ldots, \alpha_n$ are nonzero complex numbers (or algebraic numbers having finite descriptions). In this case, the exception set has measure zero.

The same method can be applied to find additional algebraic equation that vanishes at all singular points of an arbitrary algebraic variety of degree d. In the case, a polynomial of the type $D[f, U]$ can be computed using finitely many tangent lines passing through the selected point U. The approach based on the description of tangent lines to the surface can be useful for solving some problems of machine vision and image recognition.

Acknowledgements. The author would like to thank Mark Spivakovsky, Sergei P. Tarasov, Mikhail N. Vyalyi, and the anonymous reviewers for useful comments.

References

1. Schrijver, A.: Theory of Linear and Integer Programming. Wiley, New York (1986)
2. Margulies, S., Onn, S., Pasechnik, D.V.: On the complexity of Hilbert refutations for partition. J. Symbolic Comput. **66**, 70–83 (2015). doi:10.1016/j.jsc.2013.06.005
3. Herrero, M.I., Jeronimo, G., Sabia, J.: Affine solution sets of sparse polynomial systems. J. Symbolic Comput. **51**, 34–54 (2013). doi:10.1016/j.jsc.2012.03.006
4. Bodur, M., Dash, S., Günlük, O.: Cutting planes from extended LP formulations. Math. Program. **161**(1), 159–192 (2017). doi:10.1007/s10107-016-1005-7
5. Tamir, A.: New pseudopolynomial complexity bounds for the bounded and other integer Knapsack related problems. Oper. Res. Lett. **37**(5), 303–306 (2009). doi:10.1016/j.orl.2009.05.003
6. Claßen, G., Koster, A.M.C.A., Schmeink, A.: The multi-band robust knapsack problem — a dynamic programming approach. Discrete Optimization. **18**, 123–149 (2015). doi:10.1016/j.disopt.2015.09.007
7. Schwartz, J.T.: Fast probabilistic algorithms for verification of polynomial identities. J. ACM **27**(4), 701–717 (1980). doi:10.1145/322217.322225

8. Kapovich, I., Myasnikov, A., Schupp, P., Shpilrain, V.: Generic-case complexity, decision problems in group theory, and random walks. J. Algebra **264**, 665–694 (2003). doi:10.1016/S0021-8693(03)00167-4
9. Rybalov, A.N.: A generic relation on recursively enumerable sets. Algebra Logic **55**(5), 387–393 (2016). doi:10.1007/s10469-016-9410-9
10. Latkin, I.V., Seliverstov, A.V.: Computational complexity of fragments of the theory of complex numbers. Bulletin of University of Karaganda. Ser. Mathematics, vol. 1, pp. 47–55 (2015). (in Russian)
11. Seliverstov, A.V.: On cubic hypersurfaces with involutions. In: Vassiliev, N.N. (ed.) International Conference Polynomial Computer Algebra 2016, St. Petersburg, 18–22 April 2016, pp. 74–77. VVM Publishing, Saint Petersburg (2016)
12. Nesterov, Y.: Random walk in a simplex and quadratic optimization over convex polytopes. CORE Discussion Paper 2003/71 (2003)
13. Hillar, C.J., Lim, L.H.: Most tensor problems are NP-hard. J. ACM **60**(6), 45 (2013). doi:10.1145/2512329
14. Gel'fand, I.M., Zelevinskii, A.V., Kapranov, M.M.: Discriminants of polynomials in several variables and triangulations of Newton polyhedra. Leningrad Math. J. **2**(3), 499–505 (1991)
15. Chistov, A.L.: An improvement of the complexity bound for solving systems of polynomial equations. J. Math. Sci. **181**(6), 921–924 (2012). doi:10.1007/s10958-012-0724-4
16. Kulikov, V.R., Stepanenko, V.A.: On solutions and Waring's formulae for the system of n algebraic equations with n unknowns. St. Petersburg Math. J. **26**(5), 839–848 (2015). doi:10.1090/spmj/1361
17. Bokut, L.A., Chen, Y.: Gröbner-Shirshov bases and their calculation. Bull. Math. Sci. **4**(3), 325–395 (2014). doi:10.1007/s13373-014-0054-6
18. Bardet, M., Faugère, J.-C., Salvy, B.: On the complexity of the F_5 Gröbner basis algorithm. J. Symbolic Comput. **70**, 49–70 (2015). doi:10.1016/j.jsc.2014.09.025
19. Eder, C., Faugère, J.-C.: A survey on signature-based algorithms for computing Gröbner bases. J. Symbolic Comput. **80**(3), 719–784 (2017). doi:10.1016/j.jsc.2016.07.031
20. Mayr, E.W., Ritscher, S.: Dimension-dependent bounds for Gröbner bases of polynomial ideals. J. Symbolic Comput. **49**, 78–94 (2013). doi:10.1016/j.jsc.2011.12.018
21. Malaschonok, G., Scherbinin, A.: Triangular decomposition of matrices in a domain. In: Gerdt, V.P., Koepf, W., Seiler, W.M., Vorozhtsov, E.V. (eds.) CASC 2015. LNCS, vol. 9301, pp. 292–306. Springer, Cham (2015). doi:10.1007/978-3-319-24021-3_22
22. Vershik, A.M., Sporyshev, P.V.: An estimate of the average number of steps in the simplex method, and problems in asymptotic integral geometry. Sov. Math. Dokl. **28**, 195–199 (1983)
23. Smale, S.: On the average number of steps of the simplex method of linear programming. Math. Program. **27**(3), 241–262 (1983). doi:10.1007/BF02591902
24. Dubickas, A., Smyth, C.J.: Length of the sum and product of algebraic numbers. Math. Notes. **77**, 787–793 (2005). doi:10.1007/s11006-005-0079-y
25. Kollár, J.: Unirationality of cubic hypersurfaces. J. Inst. Math. Jussieu. **1**(3), 467–476 (2002). doi:10.1017/S1474748002000117
26. Cenk, M., Hasan, M.A.: On the arithmetic complexity of Strassen-like matrix multiplications. J. Symbolic Comput. **80**(2), 484–501 (2017). doi:10.1016/j.jsc.2016.07.004
27. Hedén, I.: Russell's hypersurface from a geometric point of view. Osaka J. Math. **53**(3), 637–644 (2016)