

ON COMPLEXITY OF THE PROBLEM OF SOLVING SYSTEMS OF TROPICAL POLYNOMIAL EQUATIONS OF DEGREE TWO

I. M. BUCHINSKIY, M. V. KOTOV, AND A. V. TREIER

ABSTRACT. In this paper, we investigate the computational complexity of the problem of solving a one-sided system of equations of degree two of a special form over the max-plus algebra. Also, we consider the asymptotic density of solvable systems of this form. Such systems have appeared during the analysis of some tropical cryptography protocols that were recently suggested. We show how this problem is related to the integer linear programming problem and prove that this problem is NP-complete. We show that the asymptotic density of solvable systems of this form with some restrictions on the coefficients, the number of variables, and the number of equations is 0. As a corollary, we prove that this problem (with some restrictions on the coefficients, the number of variables, and the number of equations) is decidable generically in polynomial time.

This paper is dedicated to the memory of Prof. Vitaly Roman'kov (1948–2023).

1. INTRODUCTION

The subject of this paper lies at the intersection of tropical algebra and algebraic cryptography. Tropical algebra studies tropical semirings, i.e., semirings with the operations of addition and maximum (or minimum). These semirings have a lot of applications in combinatorial optimization, game theory, scheduling, algebraic geometry, etc. Optimization problems can be formulated and solved in terms of tropical mathematics. These problems arise in many real-world applications [20]. One of the advantages of tropical algebras is that operations can be computed efficiently. Algebraic cryptography is an area of cryptography in which different algebraic structures such as non-commutative groups, semigroups, rings, and so on are used as platforms for cryptographic protocols [23, 26, 28, 29].

Sidelnikov, Cherepnev, and Yaschenko [33] proposed the following key exchange method based on non-commutative semigroups:

- (1) Alice and Bob agree on a non-commutative semigroup G , two commutative subsemigroups H and R of G , and $W \in G$.
- (2) Alice chooses two elements $P_A \in H$ and $Q_A \in R$ as her secret key. She computes $K_A = P_A \cdot W \cdot Q_A$ and sends it to Bob.
- (3) Bob chooses two elements $P_B \in H$ and $Q_B \in R$ as his secret key. He computes $K_B = P_B \cdot W \cdot Q_B$ and sends it to Alice.
- (4) Alice computes the common secret key $K_{AB} = P_A \cdot K_B \cdot Q_A$.
- (5) Bob computes the common secret key $K_{BA} = P_B \cdot K_A \cdot Q_B$.

They share the same key because $P_A \cdot (P_B \cdot W \cdot Q_B) \cdot Q_A = P_B \cdot (P_A \cdot W \cdot Q_A) \cdot Q_B$. The success of this method is determined by the choice of G , H , and R .

Miasnikov and Roman'kov [24, 29] analyzed this protocol for the case when G is a group.

Grigoriev and Shpilrain [14] suggested using tropical semigroups: G is the tropical semiring of square matrices of order n over the min-plus semiring $\mathbb{Z}_{\min,+}$, $W = I_n$, $H = \{p(A) \mid p(x) \in \mathbb{Z}_{\min,+}[x]\}$, and $R = \{q(B) \mid q(x) \in \mathbb{Z}_{\min,+}[x]\}$, where A and B are two non-commuting matrices over $\mathbb{Z}_{\min,+}$. Kotov and Ushakov [19] analyzed this protocol and suggested an attack on it. Muanalifah and Sergeev [22] considered protocols with other G, H , and R and analyzed some attacks on them. In one of the protocols, they used the semiring of square matrices of order n over $\mathbb{R}_{\max,+}$ as G , and sets of quasi-polynomials of Jones matrices as H and R . In the other protocol, they used the same G and sets of Linde–De la Puente matrices as H and R . Durcheva [7] proposed a protocol where G is a matrix semiring over the max-plus semiring, $H = \{p(A)^m \mid p(x) \in \mathbb{R}_{\max,+}[x]\}$, and $R = \{p(A)^k \mid p(x) \in \mathbb{R}_{\max,+}[x]\}$. The matrix A and the integers m and k are public. Also, Durcheva and Trendafilov [9] used the same G , $H = \{A^n \mid n \in \mathbb{N}\}$, and $R = \{B^m \mid m \in \mathbb{N}\}$. Ahmed, Pal, and Mohan [1] showed that these protocols are insecure. Durcheva [8] offered a new key exchange protocol employing circulant matrices. Jiang, Huang, and Pan [16] demonstrated that this protocol is not secure. Huang, Li, and Deng [15] offered a key exchange protocol based on tropical upper- t -circulant matrices. Amutha and Perumal [3] proposed protocols based on tropical lower- t -circulant matrices and tropical anti- t - p -circulant matrices. Attacks on these protocols were offered by Buchinskiy, Treier, and Kotov [5] and Alhussaini, Collett, and Sergeev [2].

During the analysis of these protocols, the following equation arises:

$$X \otimes W \otimes Y = K_A,$$

where $X = \bigoplus_{i=1}^{d_1} x_i \otimes B_i$, $Y = \bigoplus_{j=1}^{d_2} y_j \otimes C_j$, B_i and C_j are known matrices and x_i, y_j are unknowns. Then we have

$$\left(\bigoplus_{i=1}^{d_1} x_i \otimes B_i \right) \otimes W \otimes \left(\bigoplus_{j=1}^{d_2} y_j \otimes C_j \right) = K_A.$$

Let $T^{ij} = B_i \otimes W \otimes C_j - K_A$, and E be the matrix of the corresponding size with all entries equal to 0. Then we obtain

$$\bigoplus_{\substack{i \in \{1, \dots, d_1\} \\ j \in \{1, \dots, d_2\}}} (x_i \otimes y_j) \otimes T^{ij} = E.$$

Therefore, we have the following system of equations:

$$\bigoplus_{\substack{i \in \{1, \dots, d_1\} \\ j \in \{1, \dots, d_2\}}} (x_i \otimes y_j \otimes T_{kl}^{ij}) = 0 \text{ for each } k, l \in \{1, \dots, n\},$$

or, using the max and + signs,

$$\max_{\substack{i \in \{1, \dots, d_1\} \\ j \in \{1, \dots, d_2\}}} (x_i + y_j + T_{kl}^{ij}) = 0 \text{ for each } k, l \in \{1, \dots, n\}.$$

Note that this is a system of polynomial one-sided equations, and each equation has degree two.

Several heuristic algorithms for solving this system were suggested [19, 5, 22, 2].

Here, we want to study the computational complexity of the problem to solve such systems of tropical equations.

We can ask the following questions:

Problem 1. *Given a system of equations. Decide if there is a solution to this system.*

Problem 2. *Given a system of equations. Find a solution to this system or say that this system has no solution.*

Problem 3. *Given a system of equations. Find all the solutions to this system or say that the system has no solution.*

In this paper, we forget how we get the numbers T_{kl}^{ij} and will consider only the first problem:

Problem 4. *Given numbers m, n, a_{kij} , $1 \leq k \leq m$, $1 \leq i, j \leq n$. Decide if there is a solution to the system of equations*

$$\bigoplus_{1 \leq i, j \leq n} a_{kij} \otimes x_i \otimes y_j = 0, \quad 1 \leq k \leq m. \quad (1)$$

In computational complexity theory, the generic-case complexity is a way of measuring the complexity of a computational problem by neglecting a small set of unrepresentative inputs and considering the worst-case complexity on the rest. This approach was introduced over twenty years ago as a way of estimating the difficulty of unsolvable problems in combinatorial group theory [18]. Some of the advantages of this approach are that it can be applied to undecidable problems, it is easier to employ than the average-case complexity, and it is a direct measure of the difficulty of a problem on most inputs [12]. Therefore, it is a helpful tool for analyzing problems in cryptography because good problems should be difficult for almost every input. We refer the reader to [25, 32, 31, 30], where some applications of this approach can be found.

We consider the worst-case complexity and the generic-case complexity of this problem here.

Gilman, Miasnikov, and Roman'kov studied the satisfiability of random equations in free groups [10] and in nilpotent groups [11]. Men'shov [21] studied the asymptotic probability that a random system of equations in the free abelian group \mathbb{Z}^m of rank m is solvable. In this paper, we study the asymptotic probability that a random system of equations of the form (1) is solvable.

The remainder of this paper is structured into four parts. In Section 2, we recall some definitions from tropical algebra. Section 3 shows that the problem is NP-complete. In Section 4, we demonstrate that the problem with some restrictions on the coefficients, the number of variables, and the number of equations is decidable generically in polynomial time. The final section offers a conclusion of the work.

2. TROPICAL ALGEBRAS

In this section, tropical algebras, tropical polynomials, and systems of tropical equations are defined.

The *max-plus algebra* $\mathbb{R}_{\max,+}$ is the set $\mathbb{R} \cup \{-\infty\}$ equipped with the operations $x \oplus y = \max(x, y)$ and $x \otimes y = x + y$. The *min-plus algebra* $\mathbb{R}_{\min,+}$ is the set $\mathbb{R} \cup \{\infty\}$ equipped with the operations $x \oplus y = \min(x, y)$ and $x \otimes y = x + y$. These

two structures are known as tropical algebras. These algebras are semirings, which means they are similar to rings but without the requirement that each element must have an additive inverse. Moreover, they are idempotent and commutative. We denote the unit for \oplus as o and the unit for \otimes as e : $o = \infty$ and $e = 0$ for the min-plus semiring and $o = -\infty$ and $e = 0$ for the max-plus semiring.

Sometimes \mathbb{Z} instead of \mathbb{R} is used. We denote the corresponding algebras as $\mathbb{Z}_{\max,+}$ and $\mathbb{Z}_{\min,+}$.

A *tropical monomial* is an expression of the form $a \otimes x_1^{\otimes k_1} \otimes \dots \otimes x_n^{\otimes k_n}$. A tropical sum of tropical monomials is called a *tropical polynomial*. The *degree* of a tropical monomial $a \otimes x_1^{\otimes k_1} \otimes \dots \otimes x_n^{\otimes k_n}$ is $k_1 + \dots + k_n$. The *degree* of a tropical polynomial is the maximal degree of its monomials.

We can consider two types of tropical polynomial equations: one-sided and two-sided. A *one-sided tropical polynomial equation* has the form $p(x) = c$, where $p(x)$ is a tropical polynomial. A *two-sided tropical polynomial equation* has the form $p(x) = q(x)$, where $p(x)$ and $q(x)$ are tropical polynomials. These cases are very different because the tropical algebras are semirings. The degree of a two-sided tropical polynomial equation is the maximum of the degrees of its parts.

A finite set of one-sided tropical polynomial equations is called a *one-sided system of tropical polynomial equations*. A finite set of two-sided tropical polynomial equations is called a *two-sided system of tropical polynomial equations*.

Using the matrix notation, we can write any one-sided system of tropical linear equations as

$$A \otimes X = B, \tag{2}$$

and any two-sided system of tropical linear equations as

$$A \otimes X + B = C \otimes X + D. \tag{3}$$

The min-plus and max-plus algebras have been widely studied and have many applications. For more information on tropical algebra and, in particular, on the theory of systems of tropical linear equations, we refer the reader to [6]. For more information on complexity results in tropical algebra, we refer the reader to [34] and the survey [13].

3. WORST-CASE COMPLEXITY

In this section, we recall some results about the worst-case complexity of the problem of solving a system of tropical polynomial equations, prove a technical theorem about solutions to systems of the form (1), and prove a theorem about the complexity of Problem 4.

In the remainder of this paper, we will consider the max-plus algebra $\mathbb{Z}_{\max,+}$ only.

It is easy to find a solution to a one-sided system of tropical linear equations (2). The vector

$$\bar{x} = \left(-\max_i (a_{ij} - b_i) \right)_j$$

is called the *principal solution* to the system (2). It is known [6] that this system has a solution if and only if \bar{x} is a solution. Moreover, let $M_j = \operatorname{argmax}(a_{ij} - b_i)$, then the system (2) has a solution if and only if $\bigcup_j M_j = \{1, \dots, m\}$, where m is the number of equations [6]. It is easy to see that these conditions can be checked

in $O(mnb)$, where $m \times n$ is the size of the matrix A , and b is the number of bits to store the elements of A and B .

It was proven by Bezem, Nieuwenhuis, and Rodríguez-Carbonell [4] that two-sided systems of tropical linear equations (3) are polynomially equivalent to mean payoff games, a well-known hard problem in $\text{NP} \cap \text{co-NP}$.

Some problems that are closely related to the problem of solving systems of tropical polynomial equations were studied by Theobald [34].

Grigoriev and Shpilrain proved the following theorem.

Theorem 1 ([14]). *The problem of determining if there exists a solution to a given system of tropical polynomial equations is NP-hard.*

Actually, if we take a look at their proof, we will see that they proved the following result.

Theorem 2 ([14]). *The problem of determining if there exists a solution to a given one-sided system of tropical polynomial equations of degree $d \leq 2$ is NP-hard.*

Here, we modify their proof in order to prove the following theorem.

Theorem 3. *Problem 4 is NP-complete.*

To prove this and the theorems in the next section, we need the following theorem.

Theorem 4. *Consider a system of equations (1). Let $c_{ij} = -\max_k(a_{kij})$ and $S_{ij} = \text{argmax}_k(a_{kij})$. Then x_i, y_i is a solution to the system if and only if there is a set $C \subseteq \{1, \dots, n\} \times \{1, \dots, n\}$ such that*

$$\bigcup_{(i,j) \in C} S_{ij} = \{1, \dots, m\} \quad (4)$$

and

$$\begin{aligned} x_i + y_j &= c_{ij} \text{ if } (i, j) \in C, \\ x_i + y_j &\leq c_{ij} \text{ otherwise.} \end{aligned} \quad (5)$$

Proof. Indeed, let x_i, y_j be a solution to the system. Then, in every equation, there is a term $a_{kij} \otimes x_i \otimes y_j$ equal to 0. Consider one of these terms $a_{k_0 i_0 j_0} \otimes x_{i_0} \otimes y_{j_0}$. Denote $-a_{k_0 i_0 j_0}$ by $c_{i_0 j_0}$. Then we have $x_{i_0} + y_{j_0} = c_{i_0 j_0}$. Note that $a_{k_0 i_0 j_0}$ must be equal to the maximum among all the $a_{k i_0 j_0}$. Otherwise, the corresponding equation will have no solution. Therefore, for all k , $x_{i_0} + y_{j_0} \leq c_{i_0 j_0}$. Let S_{ij} be the set of k such that $a_{kij} \otimes x_i \otimes y_j = 0$. We have that $\bigcup S_{ij} = \{1, \dots, m\}$ because we have a term equal to 0 in each equation.

Now, we prove the backward direction. Let us have x_i, y_j , and C such that the conditions (4) and (5) are true. It is easy to see that x_i, y_j is a solution because each equation has a term equal to 0, and all other terms are non-positive. \square

Now we are ready to prove Theorem 3.

Proof. We will show how to reduce the 3-SAT problem to the problem of determining if there is a solution to a given one-sided system of tropical polynomial equations of the form (1). Let us have a 3-CNF $\varphi(u_1, \dots, u_n)$ that has m clauses. We need to build in polynomial time in m a system of tropical polynomial equations that has a solution if and only if φ is satisfiable. In order to make the proof simpler, we will not write a term $a_{ijk} \otimes a_i \otimes b_j$ if $a_{ijk} = -\infty$. Also, we will consider

non-zero left-hand sides of the equations because it is easy to obtain equations of the form (1) from them. First, for every variable u_i , we include the following pair of equations:

$$(x_{2i-1} \otimes y_{2i-1}) \oplus (x_{2i} \otimes y_{2i}) = 2 \quad (6)$$

and

$$(x_{2i-1} \otimes y_{2i}) \oplus (x_{2i} \otimes y_{2i-1}) = 1. \quad (7)$$

From the equations of the form (6), we obtain the inequality $x_i \otimes y_i \leq 2$ for all $1 \leq i \leq 2n$.

Note that $x_{2i-1} \otimes y_{2i-1}$ and $x_{2i} \otimes y_{2i}$ cannot be equal to 2 at the same time. Indeed, let w.l.o.g. $x_1 + y_1 = 2$ and $x_2 + y_2 = 2$. Then from the equation (7), we have that $x_1 + y_2 \leq 1$ and $x_2 + y_1 \leq 1$. Adding these inequalities, we obtain $x_1 + x_2 + y_1 + y_2 \leq 2$. But it is impossible because $x_1 + x_2 + y_1 + y_2 = 4$.

Now suppose we have a clause with three literals $u_i^\alpha \vee u_j^\beta \vee u_k^\gamma$, where u_i^0 means $\neg u_i$, and u_i^1 means u_i .

For this clause, we include the following equation:

$$(x_{2i-\alpha} \otimes y_{2i-\alpha}) \oplus (x_{2j-\beta} \otimes y_{2j-\beta}) \oplus (x_{2k-\gamma} \otimes y_{2k-\gamma}) = 2. \quad (8)$$

Add such equations for all the clauses.

Now, we need to show that this system has a solution if and only if φ is satisfiable.

Let the formula φ be satisfiable, i.e., there are values of u_1, \dots, u_n such that $\varphi(u_1, \dots, u_n)$ is true. Consider the following solution to the built system. If $u_i = 1$, then let $x_{2i-1} = y_{2i-1} = 1$ and $x_{2i} = y_{2i} = 0$. If $u_i = 0$, then let $x_{2i} = y_{2i} = 1$ and $x_{2i-1} = y_{2i-1} = 0$. It is easy to see that they form a solution to the equations of the form (6) and (7). These values are also a solution to the equations of the form (8) because the corresponding clauses are true.

On the other hand, let the built system have a solution x_i, y_i , $1 \leq i \leq 2n$. Consider the equations of the form (8). If $x_{2i-1} \otimes y_{2i-1} = 2$, then let $u_i = 1$. If $x_{2i} \otimes y_{2i} = 2$, then let $u_i = 0$. From the way the equation (8) was built, we get that these u_i satisfy the formula φ .

Now we need to show that Problem 4 is in NP. Let the system have a solution. From Theorem 4, it is clear that we can obtain a solution to the system as a solution to a linear programming problem. The number of equations and the number of variables in this problem is polynomial in n . The size of the coefficients is polynomial in the size of the coefficients a_{kij} . From the proof that the integer programming problem is NP-complete [17, 27], we get that our problem has a polynomial-length certificate. It is easy to see that we can check in polynomial time that the certificate is a solution to the problem. \square

4. GENERIC-CASE COMPLEXITY

In this section, we recall the definitions of the asymptotic density and the generic-case complexity and prove a theorem about the generic-case complexity of Problem 4 and a theorem about the asymptotic density of solvability of a random system of equations (1).

Let I be a set. A *stratification* of I is a sequence $\{I_n\}_{n \in \mathbb{N}}$ of non-empty finite subsets I_n such that $\bigcup_n I_n = I$. Stratifications are often specified by length functions. A *length function* on I is a map $l: I \rightarrow \mathbb{N}$ such that the inverse image of every integer is finite. The corresponding spherical stratification is formed by

spheres $S_n = \{x \in I \mid l(x) = n\}$. For a subset $A \subseteq I$ and a stratification $\{I_n\}$, the limit

$$\rho(A) = \lim_{n \rightarrow \infty} \frac{|A \cap I_n|}{|I_n|}$$

(if it exists) is called the *asymptotic density* of A with respect to the stratification $\{I_n\}$. If $\rho(A) = 1$, we say that A is *generic*. If $\rho(A) = 0$, we say that A is *negligible*.

Sometimes, for a set A , we denote the set $A \cap I_n$ by A_n .

An algorithm $\mathcal{A}: I \rightarrow J \cup \{?\}$ is called *generic* if

- (1) \mathcal{A} stops on every input $x \in I$,
- (2) $\{x \in I \mid \mathcal{A}(x) \neq ?\}$ is a generic set.

Here, the answer ? means “don’t know”.

A decision problem $A \subseteq I$ is *decidable generically in polynomial time* if there is a polynomial generic algorithm computing the indicator function of A .

Let $Sys(m, n, M)$ be the set of all systems of m equations in the variables x_i, y_j , $1 \leq i \leq n$, $1 \leq j \leq n$, of the form (1), where all the coefficients a_{kij} are in M . Let S be a set of systems of equations. Denote by $Sat(S)$ the set of all the solvable systems in S .

Theorem 5. *Let $n = n(r)$, $m = m(r)$, $R = R(r)$, and $L = L(r)$ be functions of a positive integer r . Consider the union*

$$Sys = \bigcup_r Sys(m(r), n(r), [L(r), R(r)])$$

and its stratification

$$\{Sys(m(r), n(r), [L(r), R(r)])\}_r.$$

If $m(r) \leq n(r)^2$ and $R(r) - L(r) = \omega(m(r)^2 n(r)^2)$, then the asymptotic density of $Sat(Sys)$ is 0.

For example, let m and n be fixed, and $m \geq n^2$. Then $Sat(Sys(m, n, \mathbb{Z}_{\geq 0})) = 0$ with respect to the stratification $\{Sys(m, n, [0, r])\}_r$, and $Sat(Sys(m, n, \mathbb{Z})) = 0$ with respect to the stratification $\{Sys(m, n, [-r, r])\}_r$.

Proof. Note that the total number of systems for a fixed r is $(R(r) - L(r))^{n(r)^2 m(r)}$ because we can consider systems of the form (1) as matrices.

It follows from Theorem 4 that, to prove the theorem, we need to prove that the density of the set of systems such that

$$\bigcup_{i,j} S_{ij} \neq \{1, \dots, m\}, \tag{9}$$

holds is generic. Denote this set by A . Consider the set of systems such that (9) holds and all S_{ij} have only one element. Denote this set by B . It is easy to see that B is a subset of A . To prove the theorem, it is enough to show that B is generic. Let us count how often $|S_{ij}| = 1$. Let us select $m(r)$ integers $a_1, \dots, a_{m(r)}$ uniformly and independently from $[L(r), R(r)]$. We can assume that $m(r) < R(r) - L(r)$. The probability that all these numbers are different is

$$p(r) = \prod_{i=1}^{m(r)} \frac{R(r) - L(r) - i + 1}{R(r) - L(r)}.$$

It can easily be checked that

$$p(r) \geq \left(1 - \frac{m(r)}{R(r) - L(r)}\right)^{m(r)} \geq 1 - \frac{m(r)^2}{R(r) - L(r)}.$$

Compute for how many systems all the $|S_{ij}|$ are equal to 1. The density is

$$q(r) = p(r)^{n(r)^2} \geq \left(1 - \frac{m(r)^2}{R(r) - L(r)}\right)^{n(r)^2} \geq 1 - \frac{m(r)^2 n(r)^2}{R(r) - L(r)}.$$

Let $|S_{ij}| = 1$ for all S_{ij} . Then, the probability that (9) holds is equal to 1 if $m(r) > n(r)^2$, and is equal to $\left(1 - \frac{(n(r)^2)!}{(n(r)^2)^{n(r)^2}}\right)$ if $m(r) = n(r)^2$. Denote this probability by $s(r)$.

Therefore, the density of the set of equations such that $|S_{ij}| = 1$ and (9) holds is equal to

$$\rho(B_r) = s(r)q(r) \geq s(r) \left(1 - \frac{m(r)^2 n(r)^2}{R(r) - L(r)}\right).$$

It is easy to see that $\lim_{r \rightarrow \infty} \rho(B_r) = 1$ because $R(r) - L(r) = \omega(m(r)^2 n(r)^2)$. It means that the set B is generic. Therefore, the set A is also generic. It follows from Theorem 4 that the set of all inconsistent systems is generic. Therefore, the set $Sat(Sys)$ is negligible. \square

Theorem 6. *Consider the problem of determining if there is a solution to a system of equations (1), where all the coefficients are integers and $L \leq a_{kij} < R$. Let $n = n(r)$, $m = m(r)$, $R = R(r)$, and $L = L(r)$ be functions of a positive integer r . If*

- (1) $m = O(f(r))$ for some polynomial $f(r)$,
- (2) $n = O(g(r))$ for some polynomial $g(r)$,
- (3) $\log(\max(|R(r)|, |L(r)|)) = O(h(r))$ for some polynomial $h(r)$,
- (4) $m(r) \geq n(r)^2$,
- (5) $R(r) - L(r) = \omega(m(r)^2 n(r)^2)$,

then this problem is decidable generically in polynomial time in r .

Proof. Consider the following algorithm based on Theorem 4.

- (1) Compute $S_{ij} = \operatorname{argmax}_k(a_{kij})$.
- (2) If (9) is true, then return “no solution”, or else return “don’t know”.

Note that the complexity of the first step is $O(n(r)^2 m(r) \log(\max(|R(r)|, |L(r)|)))$ because we need $n(r)^2$ times to compute argmin of $m(r)$ numbers. The complexity of the second step is $O(n(r)^2 m(r))$. Since $m = O(f(r))$, $n = O(g(r))$, and $\log(\max(|R(r)|, |L(r)|)) = O(h(r))$ for some polynomials $f(r)$, $g(r)$, and $h(r)$, this algorithm is polynomial.

The fact that this algorithm is generic follows from Theorem 5. \square

5. CONCLUSION

In this paper, we have studied the worst-case complexity and the generic-case complexity of Problem 4. We have shown that this problem is NP-complete, but (with some restrictions on the coefficients, the number of variables, and the number of equations) it is decidable generically in polynomial time. Also, we have shown that the asymptotic density of solvable systems of the form (1) with some restrictions on the coefficients, the number of variables, and the number of equations is 0.

Our results and methods can be used to analyze some protocols based on tropical matrix algebras.

As a future work, it would be interesting to study the generic-complexity of the problem if we know that the system has a solution.

FUNDING

This research was supported in accordance with the state task of the IM SB RAS, project FWNF-2022-0003.


REFERENCES


- [1] K. Ahmed, S. Pal, and R. Mohan. “A review of the tropical approach in cryptography”. In: *Cryptologia* 47.1 (2023), pp. 63–87. DOI: 10.1080/01611194.2021.1994486.
- [2] S. Alhussaini, C. Collett, and S. Sergeev. *Generalized Kotov–Ushakov Attack on Tropical Stickel Protocol Based on Modified Circulants*. Cryptology ePrint Archive, Paper 2023/1904. 2023. URL: <https://eprint.iacr.org/2023/1904>.
- [3] B. Amutha and R. Perumal. “Public key exchange protocols based on tropical lower circulant and anti-circulant matrices”. In: *AIMS Math.* 8.7 (2023), pp. 17307–17334. DOI: 10.3934/math.2023885.
- [4] M. Bezem, R. Nieuwenhuis, and E. Rodríguez-Carbonell. “Hard problems in max-algebra, control theory, hypergraphs and other areas”. In: *Information processing letters* 110.4 (2010), pp. 133–138. DOI: 10.1016/j.ipl.2009.11.007.
- [5] I. Buchinskiy, M. Kotov, and A. Treier. *Analysis of four protocols based on tropical circulant matrices*. Cryptology ePrint Archive, Paper 2023/1707. 2023. URL: <https://eprint.iacr.org/2023/1707>.
- [6] P. Butkovič. *Max-linear systems: theory and algorithms*. London: Springer, 2010. ISBN: 978-1-84996-298-8. DOI: 10.1007/978-1-84996-299-5.
- [7] M. I. Durcheva. “Public key cryptography with max-plus matrices and polynomials”. In: *AIP Conf. Proc.* Vol. 1570. AIP. 2013, pp. 491–498. DOI: 10.1063/1.4854794.
- [8] M. I. Durcheva. “TrES: Tropical Encryption Scheme Based on Double Key Exchange”. In: *Eur. J. Inf. Tech. Comp. Sci.* 2.4 (2022), pp. 11–17. DOI: 10.24018/compute.2022.2.4.70.
- [9] M. I. Durcheva and I. D. Trendafilov. “Public key cryptosystem based on max-semirings”. In: *AIP Conf. Proc.* Vol. 1497. AIP. 2012, pp. 357–364. DOI: 10.1063/1.4766805.
- [10] R. Gilman, A. Myasnikov, and V. Roman’kov. “Random equations in free groups”. In: *Groups Complexity Cryptology* 3.2 (2011), pp. 257–284. DOI: 10.1515/gcc.2011.010.
- [11] R. Gilman, A. Myasnikov, and V. Roman’kov. “Random equations in nilpotent groups”. In: *Journal of Algebra* 352.1 (2012), pp. 192–214. DOI: 10.1016/j.jalgebra.2011.11.007.
- [12] R. Gilman et al. “Report on generic case complexity”. In: *Vestnik Omsk Univ. Combinatorial Methods of Algebra and Computational Complexity* (2008), pp. 103–110. DOI: 10.48550/arXiv.0707.1364.
- [13] D. Grigoriev. “Complexity in Tropical Algebra (Invited Talk)”. In: *Computer Algebra in Scientific Computing: 15th International Workshop*. Springer. 2013, pp. 148–154. DOI: <https://doi.org/10.1007/978-3-319-02297-0>.
- [14] D. Grigoriev and V. Shpilrain. “Tropical cryptography”. In: *Comm. Algebra* 42.6 (2014), pp. 2624–2632. DOI: 10.1080/00927872.2013.766827.

- [15] H. Huang, C. Li, and L. Deng. “Public-Key Cryptography Based on Tropical Circular Matrices”. In: *Appl. Sci.* 12.15 (2022), p. 7401. DOI: 10.3390/app12157401.
- [16] X. Jiang, H. Huang, and G. Pan. “Cryptanalysis of Tropical Encryption Scheme Based on Double Key Exchange”. In: *J. Cyber Secur. Mobil.* 12.02 (2023), pp. 205–220. DOI: 10.13052/jcsm2245-1439.1224.
- [17] R. Kannan and C. L. Monma. “On the computational complexity of integer programming problems”. In: *Optimization and Operations Research: Proceedings of a Workshop Held at the University of Bonn, October 2–8, 1977*. Springer, 1978, pp. 161–172. DOI: 0.1007/978-3-642-95322-4_17.
- [18] I. Kapovich et al. “Generic-case complexity, decision problems in group theory, and random walks”. In: *Journal of Algebra* 264.2 (2003), pp. 665–694. DOI: 10.1016/S0021-8693(03)00167-4.
- [19] M. Kotov and A. Ushakov. “Analysis of a key exchange protocol based on tropical matrix algebra”. In: *Journal of Mathematical Cryptology* 12.3 (2018), pp. 137–141. DOI: 10.1515/jmc-2016-0064.
- [20] N. Krivulin. “Tropical optimization problems”. In: *Advances in Economics and Optimization: Collected Scientific Studies Dedicated to the Memory of L. V. Kantorovich* (2014), pp. 195–214. DOI: 10.48550/arXiv.1408.0313.
- [21] A. Menshov. “Random systems of equations in free abelian groups”. In: *Siberian Mathematical Journal* 55.3 (2014), pp. 440–450. DOI: 10.1134/S0037446614030057.
- [22] A. Muanalifah and S. Sergeev. “Modifying the tropical version of Stickel’s key exchange protocol”. In: *Appl. Math.* 65.6 (2020), pp. 727–753. DOI: 10.21136/AM.2020.0325-19.
- [23] A. Myasnikov, V. Shpilrain, and A. Ushakov. *Group-based cryptography*. Basel: Birkhäuser, 2008. ISBN: 978-3-7643-8826-3. DOI: 10.1007/978-3-7643-8827-0.
- [24] A. G. Myasnikov and V. A. Roman’kov. “A linear decomposition attack”. In: *Groups Complexity Cryptology* 7.1 (2015), pp. 81–94. DOI: 10.1515/gcc-2015-0007.
- [25] A. G. Myasnikov and A. N. Rybalov. “Generic complexity of undecidable problems”. In: *Journal of Symbolic Logic* 73.2 (2008), pp. 656–673. DOI: 10.2178/jsl/1208359065.
- [26] A. G. Myasnikov, V. Shpilrain, and A. Ushakov. *Non-commutative cryptography and complexity of group-theoretic problems*. Vol. 177. Math. Surv. Monogr. Providence, RI: Amer. Math. Soc., 2011. ISBN: 978-0-8218-5360-3. DOI: 10.1090/surv/177.
- [27] C. H. Papadimitriou. “On the complexity of integer programming”. In: *Journal of the ACM (JACM)* 28.4 (1981), pp. 765–768.
- [28] V. A. Roman’kov. *Algebraic cryptography*. Omsk: Omsk State University Press, 2013. ISBN: 978-5-7779-1600-6.
- [29] V. A. Roman’kov. *Algebraic cryptology*. Omsk: Omsk State University Press, 2020. ISBN: 978-5-7779-2491-9.
- [30] A. Rybalov and A. Shevlyakov. “Generic complexity of solving of equations in finite groups, semigroups and fields”. In: *Journal of Physics: Conference Series*. Vol. 1901. IOP Publishing, 2021, p. 012047. DOI: 10.1088/1742-6596/1901/1/012047.
- [31] A. N. Rybalov. “Generic polynomial algorithms for the knapsack problem in some matrix semigroups”. In: *Siberian Electronic Mathematical Reports* 20.1 (2023), pp. 100–109. DOI: 10.33048/semi.2023.20.009.
- [32] A. N. Rybalov. “On generic complexity of the discrete logarithm problem”. In: *Prikladnaya Diskretnaya Matematika* 3(33) (2016), pp. 93–97. DOI: 10.17223/20710410/33/8.
- [33] V. M. Sidelnikov, M. A. Cherepnev, and V. V. Yashchenko. “Public key distribution systems based on noncommutative semigroups”. In: *Dokl. Akad. Nauk* 332.5 (1993). Transl. in: *Russian Acad. Sci. Dokl. Math.* 48.2 (1994), 384–386, pp. 566–567. URL: <http://mi.mathnet.ru/dan5041>.

- [34] T. Theobald. “On the frontiers of polynomial computations in tropical geometry”. In: *Journal of Symbolic Computation* 41.12 (2006), pp. 1360–1375. DOI: [10.1016/j.jsc.2005.11.006](https://doi.org/10.1016/j.jsc.2005.11.006).

I. M. BUCHINSKIY , SOBOLEV INSTITUTE OF MATHEMATICS OF SB RAS, OMSK, RUSSIA
Email address: buchvan@mail.ru

M. V. KOTOV , SOBOLEV INSTITUTE OF MATHEMATICS OF SB RAS, OMSK, RUSSIA
Email address: matvej.kotov@gmail.com

A. V. TREIER , SOBOLEV INSTITUTE OF MATHEMATICS OF SB RAS, OMSK, RUSSIA
Email address: alexander.treyer@gmail.com