PROBLEMS IN ALGEBRA INSPIRED BY TROPICAL CRYPTOGRAPHY

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

Abstract. In 2011, Grigoriev and Shpilrain proposed using tropical algebraic structures in cryptography. In recent years, numerous protocols based on tropical and related structures have been introduced, as well as many attacks on some of these protocols. This direction of research is now known as tropical cryptography. As a result of the efforts both to design secure schemes and to analyze their vulnerabilities, many purely algebraic and computational problems have emerged. In this paper, we give an overview of several results and open questions in this area. We discuss the complexity of solving certain classes of systems of equations over tropical and similar structures, as well as algorithms and approaches for solving such systems. We also present results on the asymptotic density of satisfiable systems of equations of special forms over tropical algebras. Furthermore, we discuss the discrete logarithm problem, the two-sided discrete logarithm problem, the knapsack problem, and the subset sum problem over tropical matrix structures. We consider a generalization of marginal sets for tropical semirings and semigroups. We also explore different classes of pairwise commuting matrices. This survey is based on a talk given at the Omsk Algebra Seminar in 2025.

1. Introduction

Algebraic cryptography is a branch of cryptography in which different algebraic structures such as groups, semigroups, rings, etc. are employed as platforms for cryptographic schemes [55, 58, 64, 66]. Sidelnikov et al. [74] proposed the following generalization of the well-known Diffie–Hellman key exchange method [19] based on non-commutative semigroups. A similar idea of using non-abelian groups was proposed by Stickel [75].

Protocol 1 ([74])**.** Let $\mathcal{G}$ be a non-commutative semigroup, H and R be subsets of pairwise commuting elements of $\mathcal{G}$, and $W \in \mathcal{G}$.

(1) Alice chooses two elements $P_1 \in H$ and $Q_1 \in R$ as her secret key. She computes $U = P_1 \cdot W \cdot Q_1$ and sends it to Bob.
(2) Bob chooses two elements $P_2 \in H$ and $Q_2 \in R$ as his secret key. He computes $V = P_2 \cdot W \cdot Q_2$ and sends it to Alice.
(3) Alice computes the common secret key $K = P_1 \cdot V \cdot Q_1$.
(4) Bob computes the common secret key $K = P_2 \cdot U \cdot Q_2$.

They share the same key because $P_1 \cdot (P_2 \cdot W \cdot Q_2) \cdot Q_1 = P_2 \cdot (P_1 \cdot W \cdot Q_1) \cdot Q_2$.

The success of this method is determined by the choice of $\mathcal{G}, H$, and R. Some examples of groups were analyzed by Sidelnikov et al. [74]. A general analysis in the case of groups was done by Miasnikov and Roman'kov [56, 66], where they proposed a quite general linear decomposition attack. Shpilrain [73] also showed that Stickel's schemes were vulnerable to linear algebra attacks.

In 2011, Grigoriev and Shpilrain [33] proposed a new key-exchange protocol based on tropical semirings. Two classical tropical semirings are the max-plus algebra $\mathcal{Z}_{\max,+} = \langle \mathbb{Z} \cup \{-\infty\}, \oplus, \otimes \rangle$, where $a \otimes b = a + b$ and $a \oplus b = \max(a, b)$, and the min-plus algebra $\mathcal{Z}_{\min,+} = \langle \mathbb{Z} \cup \{\infty\}, \oplus, \otimes \rangle$, where $a \otimes b = a + b$ and $a \oplus b = \min(a, b)$. Durcheva and Trendafilov [25] also proposed a series of key-exchange schemes based on the tropical algebras. There are two reasons for this choice. First, it helps avoid linear algebra attacks. Second, the tropical operations can be performed quickly and efficiently. This approach is now known as tropical cryptography.

The following $\mathcal{G}, H$, and R were proposed in [33]. $\mathcal{G}$ is the tropical semiring of square matrices of order k over the min-plus semiring $\mathcal{Z}_{\min,+}$, $w = I_k$, $H = \{p(A) : p(x) \in \mathcal{Z}_{\min,+}[x]\}$, and $R = \{q(B) : q(x) \in \mathcal{Z}_{\min,+}[x]\}$, where A and B are two non-commuting matrices over $\mathcal{Z}_{\min,+}$. Kotov and Ushakov [44] analyzed this protocol and suggested a successful attack on it. The key point of their method is the fact that sequences of powers of tropical matrices over the min-plus algebra often display some patterns.

Durcheva [22] used a matrix semiring over the max-plus semiring as $\mathcal{G}$, $H = \{p(A)^m : p(x) \in \mathcal{Z}_{\max,+}[x]\}$, and $R = \{p(A)^n : p(x) \in \mathcal{Z}_{\max,+}[x]\}$. Durcheva and Trendafilov [25] used the same $\mathcal{G}$, $H = \{A^n : n \in \mathbb{N}\}$, and $R = \{B^m : m \in \mathbb{N}\}$. Ahmed et al. [1] showed that these protocols are insecure.

The protocol and the attacks were also analyzed by Muanalifah and Sergeev [52]. They considered the protocol with the semiring of square tropical matrices of order k as $\mathcal{G}$, and sets of quasi-polynomials of Jones matrices [41] as H and R and the protocol with the same $\mathcal{G}$ and sets of Linde–De la Puente matrices [45] as H and R.

Another interesting class of pairwise commuting matrices is circulant matrices. Recently, a few protocols based on these matrices have been proposed. Durcheva [24] proposed a new key exchange protocol employing circulant matrices. Jiang et al. [40] demonstrated that this protocol is not secure. Huang et al. [38] proposed a key exchange protocol based on tropical upper-t-circulant matrices. Amutha and Perumal [9] proposed protocols based on tropical lower-t-circulant matrices and tropical anti-t-p-circulant matrices. Attacks on these protocols were proposed by Buchinskiy et al. [13] and Alhussaini et al. [3].

Alhussaini and Sergeev [5, 6, 7] analyzed various generalizations of this scheme, using mixed-integer linear programming and optimization heuristics. Recently, Otero Sánchez et al. [59] considered a new approach to analyze similar schemes.

As we can see, classes of pairwise commuting matrices over tropical semirings are important for tropical cryptography. In Section 3, we provide an overview of known classes and related theorems.

The analysis of tropical protocols often leads to different classes of systems of equations.

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

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

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

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

It can be rewritten as

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

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

Another way to attack this scheme is as follows. Suppose that we can find z_{ij} such that

$$\bigoplus_{i=1}^{d_1}\bigoplus_{j=1}^{d_2} z_{ij} \otimes (B_i \otimes W \otimes C_j) = U.$$

Then, we can compute the secret key in the following way:

$$\bigoplus_{i=1}^{d_1}\bigoplus_{j=1}^{d_2} z_{ij} \otimes B_i \otimes V \otimes C_j = K.$$

Indeed, this works because

$$\begin{aligned}\bigoplus_{i=1}^{d_1}\bigoplus_{j=1}^{d_2} z_{ij} \otimes B_i \otimes V \otimes C_j &= \bigoplus_{i=1}^{d_1}\bigoplus_{j=1}^{d_2} z_{ij} \otimes B_i \otimes P_2 \otimes W \otimes Q_2 \otimes C_j \\ &= P_2 \otimes \left(\bigoplus_{i=1}^{d_1}\bigoplus_{j=1}^{d_2} z_{ij} \otimes B_i \otimes W \otimes C_j\right) \otimes Q_2 = P_2 \otimes U \otimes Q_2 = K.\end{aligned}$$

Therefore, for this trick, we need to be able to solve a system of linear one-sided equations.

Thus, analyzing such schemes requires solving various systems of equations. For systems of equations, we can ask the following questions:

Problem 1. *Given a system of equations, decide whether it has a solution.*

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 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 [42]. 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 [30]. 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 [57, 71, 70], where some applications of this approach can be found.

In Section 4, we discuss the worst-case complexity and the generic complexity of the problem of the decidability of some classes of systems of equations over tropical algebras and

some tropical-like algebras. Also, we consider the asymptotic probability of solvable systems of equations of certain forms.

Grigoriev and Shpilrain in [34] proposed two new key-exchange protocols based on tropical matrix algebras. They suggested using semidirect products to destroy patterns of sequences of powers of matrices which were exploited in the attacks on their first protocol. Three different approaches to attack one of these protocols were proposed. Isaac and Kahrobaei [39] used the property of a sequence of matrices to be almost linear periodic. Rudy and Monico [68] exploited the fact that the sequences of matrices appearing in the protocol are monotonically decreasing. This made it possible to apply a binary search. The attack suggested by Muanalifah and Sergeev in [53] is based on the solution of the tropical discrete logarithm problem:

Problem 4 ([53]). *Given matrices V, W, and C over the max-plus algebra of appropriate dimensions, find $x \in \mathbb{Z}_{\geq 0}$ such that $V \otimes W^{\otimes x} = C$.*

Muanalifah [51] generalized this problem and considered the two-sided tropical discrete logarithm problem.

Problem 5 ([51]). *Given matrices W_1, W_2, V, and C over the max-plus algebra of appropriate dimensions, find $x_1, x_2 \in \mathbb{Z}_{\geq 0}$ such that $W_1^{\otimes x_1} \otimes V \otimes W_2^{\otimes x_2} = C$.*

In Section 6, we discuss these problems and their modifications with a shift.

The subset sum problem and the knapsack problem are well-known problems in combinatorial optimization. One can consider the decision versions of such problems.

Problem 6. *Given a number c and n items, each item i has weight w_i, decide if $x_1w_1 + \ldots + x_nw_n = c$ for some $x_1, \ldots, x_n \in \{0, 1\}$.*

Problem 7. *Given a number c and n items, each item i has weight w_i, decide if $x_1w_1 + \ldots + x_nw_n = c$ for some $x_1, \ldots, x_n \in \mathbb{Z}_{\geq 0}$.*

Miasnikov et al. [54] generalized Problem 6 and Problem 7 to arbitrary groups.

Problem 8 ([54]). *Let $\mathcal{G}$ be a group. Given $w_1, \ldots, w_n, c \in \mathcal{G}$, decide if $w_1^{x_1} \ldots w_k^{x_n} = c$ for some non-negative integers $x_1, \ldots, x_n$.*

Problem 9 ([54]). *Let $\mathcal{G}$ be a group. Given $w_1, \ldots, w_n, c \in \mathcal{G}$, decide if $w_1^{x_1} \ldots w_k^{x_n} = c$ for some $x_1, \ldots, x_n \in \{0, 1\}$.*

Problem 9 is called the *subset sum problem for* $\mathcal{G}$ and denoted by $\mathbf{SSP}(\mathcal{G})$. Problem 8 is called the *knapsack problem for* $\mathcal{G}$ and denoted by $\mathbf{KP}(\mathcal{G})$. These problems can be generalized to any semigroup.

Studying the knapsack problem and the subset sum problem for groups has become a very active area of research [46, 43, 49, 26, 47, 48, 50, 27, 10, 20]. Also, these problems have been studied for some matrix semigroups [71, 70, 69].

Therefore, it is natural to increase the number of matrices in Problems 4 and 5 and consider the tropical versions of the knapsack problem and the subset sum problem.

Problem 10 ([17]). *Given matrices $W_1, \ldots, W_n$, and C of size $k \times k$ over a tropical semiring, decide if $W_1^{\otimes x_1} \otimes \ldots \otimes W_n^{\otimes x_n} = C$ for some non-negative integers $x_1, \ldots, x_n$.*

Problem 11 ([17]). *Given matrices $W_1, \ldots, W_n$, and C of size $k \times k$ over a tropical semiring, decide if $W_1^{\otimes x_1} \otimes \ldots \otimes W_n^{\otimes x_n} = C$ for some $x_1, \ldots, x_n \in \{0, 1\}$.*

Buchinskiy et al. investigated the complexity of these tropical knapsack-type problems [17]. We give an overview of these results in Section 7.

The concept of marginal sets for groups, introduced by Roman'kov, was inspired by the classical notion of marginal subgroups. However, the generalization to marginal sets is very different from the original concept. For context, recall the classical definition of a marginal subgroup introduced by P. Hall [35].

Definition 1. Let $\mathcal{G}$ be a group and let $w(x_1, \dots, x_n)$ be a group word. A normal subgroup $\mathcal{N}$ is said to be *w-marginal* in $\mathcal{G}$ if

$$w(ag_1, g_2, \dots, g_n) = w(g_1, ag_2, \dots, g_n) = \dots w(g_1, g_2, \dots, ag_n) = w(g_1, g_2, \dots, g_n)$$

for all $a \in \mathcal{N}$, $g_i \in G$, $1 \leq i \leq n$.

V. Roman'kov introduced the following generalization of this definition [62, 65, 61, 63].

Definition 2. Let $\mathcal{G}$ be a group, $w(x_1, \dots, x_n)$ be a group word, and $g = (g_1, \dots, g_n)$ be a tuple of elements of $\mathcal{G}$. A tuple $c = (c_1, \dots, c_n)$ of elements of $\mathcal{G}$ is called a *marginal tuple* with respect to w and g if

$$w(c_1 g_1, \dots, c_n g_n) = w(g_1, \dots, g_n).$$

We denote this relation by $c \perp w(g)$. A set C of n-tuples of elements of $\mathcal{G}$ is said to be *marginal* with respect to w and g if $c \perp w(g)$ for every tuple $c \in C$. In this case, we write $C \perp w(g)$.

Note that a marginal set does not have to be a subgroup. Note that any solution $(c_1, \dots c_n)$ to the equation $w(x_1 g_1, \dots, x_n g_n) = w(g_1, \dots, g_n)$ is a marginal tuple with respect to w and g.

Roman'kov employed marginal sets to improve the Anshel–Anshel–Goldfeld protocol. Here, we present a simplified version of his protocol, focusing only on the use of marginal sets and omitting additional improvements such as permutations of published elements, virtual elements, and hidden elements.

Protocol 2. Suppose that two correspondents, Alice and Bob, want to exchange a key. They agree on a public group $\mathcal{G} = \langle G, \cdot, ^{-1}, e \rangle$.

(1) Alice fixes a positive integer k and chooses a public tuple of elements $a = (a_1, \dots, a_k)$. She selects a private group word $u = u(x_1, \dots, x_k)$ and computes $u(a) = u(a_1, \dots, a_n)$. She constructs a public marginal set $C \subseteq G^k$, $C \perp u(a)$. She publishes the tuple a and the set C.

(2) Bob fixes a positive integer l and chooses a public tuple of elements $b = (b_1, \dots, b_l)$. He selects a private group word $v = v(y_1, \dots, v_l)$ and computes $v(b) = v(b_1, \dots, b_l)$. He constructs a public marginal set $D \subseteq G^l$, $D \perp v(b)$. He publishes the tuple b and the set D.

(3) Alice selects a tuple $d \in D$ and computes $db = (d_1 b_1, \dots, d_l b_l)$. She sends Bob the tuple

$$(db)^{u(a)} = ((d_1 b_1)^{u(a)}, \dots, (d_l b_l)^{u(a)}).$$

(4) Bob selects a tuple $c \in C$ and computes $ca = (c_1 a_1, \dots, c_k a_k)$. He sends Alice the tuple

$$(ca)^{v(b)} = ((c_1 a_1)^{v(b)}, \dots, (c_k a_k)^{v(b)}).$$

(5) Alice computes $K = u(a)^{-1}u((ca)^{v(b)})$.
(6) Bob computes $K = (v((db)^{u(a)}))^{-1}v(b)$.

Note that they share the same key, since

$$u(a)^{-1}u((ca)^{v(b)}) = (v((db)^{u(a)}))^{-1}v(b) = [u(a), v(b)].$$

Also, Roman'kov extended the concept of marginal sets to associative algebras and used marginal sets to improve the Diffie–Hellman protocol in [63].

In Section 5, we extend his ideas and introduce the concept of marginal sets for semigroups and semirings. For tropical matrix semigroups and semirings, we describe how some marginal sets can be constructed. We apply marginal sets to improve some key exchange schemes over semigroups.

In addition to the classical tropical structures, other similar and close structures have been used. For example, the max-times algebra and the min-times algebra were considered in [23, 1, 15]. The digital semirings have been considered in [37, 60]. Alhussaini and Sergeev studied the max-min and max-t semirings [6] and the symmetrized and supertropical semirings [8]. We consider some of such semirings in Sections 4 and 7.

Buchinskiy in [16] proved some results on equationally Noetherian tropical semirings.

Recently, Grigoriev et al. published a new paper [32], which may open a new chapter in tropical cryptography.

Several dozen papers and preprints are now devoted to tropical cryptography. We refer the reader to two overview papers: [1] and [21]. For more information on non-commutative cryptography, we refer the reader to [58].

2. Preliminaries

In the first part of this section, we discuss tropical semirings, tropical polynomials, systems of tropical equations, and tropical matrix semirings. In the second, we discuss how the size of a matrix can be defined. In the final part, we recall the definition of the asymptotic density of a set and the definition of a generic algorithm.

Let S be a set, and a be a number. In this paper, we denote the set $\{x \in S : x \geq a\}$ by $S_{\geq a}$ and the set $\{x \in S : x > a\}$ by $S_{>a}$. For example, $\mathbb{Z}_{\geq 0}$ is the set of all non-negative integers, and $\mathbb{Z}_{\geq 1}$ is the set of all positive integers. Also, we denote $S \cup \{\infty\}$ by $\overline{S}$ and $S \cup \{-\infty\}$ by $\underline{S}$.

A *semiring* is a ring without the requirement that each element must have an additive inverse.

Two famous examples of semirings are the max-plus algebra and min-plus algebra. The *max-plus algebra* $\mathcal{R}_{\max,+}$ is the set $\underline{\mathbb{R}}$ equipped with the operations

$$x \oplus y = \max(x, y) \quad \text{and} \quad x \otimes y = x + y.$$

The *min-plus algebra* $\mathcal{R}_{\min,+}$ is the set $\overline{\mathbb{R}}$ equipped with the operations

$$x \oplus y = \min(x, y) \quad \text{and} \quad x \otimes y = x + y.$$

These semirings are idempotent and commutative. These two semirings are known as tropical algebras. They have been widely studied and have many applications in combinatorial optimization, algebraic geometry, auction theory, mechanism design, theory, scheduling etc.

Some researchers studied the min-times and max-times algebras, where one of the operations is the multiplication of numbers, and the other is either min or max [72, 76, 23, 28]. The domain of the *max-times* algebra $\mathcal{R}_{\max,\times}$ is $\mathbb{R}_{\geq 0}$, and the operations are

$$x \oplus y = \max(x, y) \quad \text{and} \quad x \otimes y = x \cdot y.$$

The domain of the *min-times* algebra $\mathcal{R}_{\min,\times}$ is $\overline{\mathbb{R}}_{>0}$ and the operations are

$$x \oplus y = \min(x, y) \quad \text{and} \quad x \otimes y = x \cdot y.$$

One can use other sets closed under $\oplus$ and $\otimes$ as domains to define similar structures. For example, in case of the max-plus algebra, one can consider $\mathbb{Z}$ or $\mathbb{Z}_{\geq 0}$ instead of $\underline{\mathbb{R}}$.

In this paper, we will use the following algebras: $\mathcal{N}_+ = \langle \mathbb{Z}_{\geq 0}, + \rangle$, $\mathcal{N}_\times = \langle \mathbb{Z}_{\geq 1}, \cdot \rangle$, $\mathcal{N}_{\max,+} = \langle \mathbb{Z}_{\geq 0}, \oplus, \otimes \rangle$, where $\oplus$ is max and $\otimes$ is $+$, and $\mathcal{N}_{\max,\times} = \langle \mathbb{Z}_{\geq 1}, \oplus, \otimes \rangle$, where $\oplus$ is max and $\otimes$ is $\cdot$, $\mathcal{Z}_{\max,+} = \langle \underline{\mathbb{Z}}, \oplus, \otimes \rangle$, where $\oplus$ is max and $\otimes$ is $\cdot$, and $\mathcal{Z}_{\min,+} = \langle \overline{\mathbb{Z}}, \oplus, \otimes \rangle$, where $\oplus$ is min and $\otimes$ is $\cdot$,.

Akian et al. [2], and Alhussaini and Sergeev [8] considered the following constructions.

Let $\mathcal{S} = \langle S, +, \cdot, 0, 1 \rangle$ be a semiring and let $\mathcal{R} = \langle R, \oplus, \otimes, \mathbf{0}, \mathbf{1} \rangle$ be a totally ordered additively idempotent semiring. Let us consider two following operations defined on $R \times S$:

$$(a, \alpha) \oplus (b, \beta) = \begin{cases} (a, \alpha) & \text{if } a > b, \\ (b, \beta) & \text{if } a < b, \\ (a, \alpha + \beta) & \text{if } a = b, \end{cases}$$

and

$$(a, \alpha) \otimes (b, \beta) = (a \otimes b, \alpha \cdot \beta).$$

The semiring $\mathcal{R} \bar{\ltimes} \mathcal{S}$ is defined as the set $R \times S$ endowed with the operations $\oplus$ and $\otimes$. The semiring $\mathcal{R} \underline{\ltimes} \mathcal{S}$ is defined as the set $(R \setminus \{\mathbf{0}\} \times S) \cup \{(\mathbf{0}, 0)\}$ endowed with the operations $\oplus$ and $\otimes$. If $\mathcal{S}$ is zero-sum free and without zero divisors, then $\mathcal{R} \ltimes \mathcal{S}$ is defined as the set $(R \setminus \{\mathbf{0}\} \times S \setminus \{0\}) \cup \{(\mathbf{0}, 0)\}$ endowed with operations $\oplus$ and $\otimes$.

The *supertropical semiring* [8] is $\mathcal{R}_{\max,+} \ltimes \mathbb{N}_2$, where $\mathbb{N}_2$ denotes the quotient of the semiring $\mathbb{Z}_{\geq 0}$ by the equivalence relation for which the equivalence classes are $\{0\}$, $\{1\}$, and $\mathbb{Z}_{\geq 2}$ (denoted by $\bar{0}$, $\bar{1}$ and $\bar{2}$ respectively). The addition table and the multiplication table for $\mathbb{N}_2$ are

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{2}$
$\bar{2}$	$\bar{2}$	$\bar{2}$	$\bar{2}$

and

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{2}$

.

The symmetrized semiring is $\mathcal{R}_{\max,+} \ltimes \mathbb{B}_s$ [8], where $\mathbb{B}_s$ is the four-element symmetrized Boolean semiring $\{\varepsilon, 0, \ominus 0, 0^\bullet\}$ with the following addition and multiplication tables:

$\oplus$	ε	0	$\ominus 0$	$0^\bullet$
ε	ε	0	$\ominus 0$	$0^\bullet$
0	0	0	$0^\bullet$	$0^\bullet$
$\ominus 0$	$\ominus 0$	$0^\bullet$	$\ominus 0$	$0^\bullet$
$0^\bullet$	$0^\bullet$	$0^\bullet$	$0^\bullet$	$0^\bullet$

and

$\odot$	ε	0	$\ominus 0$	$0^\bullet$
ε	ε	ε	ε	ε
0	ε	0	$\ominus 0$	$0^\bullet$
$\ominus 0$	ε	$\ominus 0$	0	$0^\bullet$
$0^\bullet$	ε	$0^\bullet$	$0^\bullet$	$0^\bullet$

.

Let q be a prime number. An *extended q-modular tropical semiring* [67] is $\mathbb{T}_{\text{ext}}(q) := \mathcal{Z}_{\max,+} \bar{\ltimes} \mathbb{Z}_q$, where $\mathbb{Z}_q$ is the ring of integers modulo q.

We denote the unit for $\oplus$ as o and the unit for $\otimes$ as e. For example, $o = \infty$ and $e = 0$ for the min-plus semiring and $o = -\infty$ and $e = 0$ for the max-plus semiring.

Let R be a set. We denote by $\mathrm{Mat}_{m\times n}(R)$ the set of $m \times n$ matrices with entries in R, and by $\mathrm{Mat}_n(R)$ the set of $n \times n$ matrices with entries in R.

Let $\mathcal{S} = \langle S, \oplus, \otimes\rangle$ be an algebra with two binary operations, and let k be a positive integer. The set of all $k \times k$ matrices $\mathrm{Mat}_k(S)$ can be equipped with addition $\oplus$ and multiplication $\otimes$ using the following formulae:

$$(A \oplus B)_{ij} = a_{ij} \oplus b_{ij},$$

$$(A \otimes B)_{ij} = a_{i1} \otimes b_{1j} \oplus \cdots \oplus a_{ik} \otimes b_{kj}.$$

If $\mathcal{S}$ is an idempotent semiring, then the obtained algebra is also an idempotent semiring.

In this paper, we use capital letters for matrices and the corresponding lowercase letters for elements of matrices: x_{ij} is an element of X.

We have a partial order on a set of $k \times k$ matrices defined by the following rule:

$$A \le B \text{ iff } a_{ij} \le b_{ij} \text{ for all } i, j \in \{1, \ldots, k\}.$$

Let $\mathcal{S} = \langle S, \otimes, \oplus\rangle$ be a tropical semiring. A *tropical polynomial* over $\mathcal{S}$ in one variable x is an expression of the form

$$p(x) = a_0 \oplus a_1 \otimes x \oplus a_2 \otimes x^{\otimes 2} \oplus \cdots \oplus a_k \otimes x^{\otimes k},$$

where $a_i \in S$, and $x^{\otimes i}$ denotes $\underbrace{x \otimes \cdots \otimes x}_{i \text{ times}}$.

Let $A \in \mathrm{Mat}(n, S)$ be a matrix and $p(x) \in \mathcal{S}[x]$ be a polynomial over $\mathcal{S}$. Define $p(A)$ as follows:

$$p(A) = a_0 \otimes I \oplus a_1 \otimes A \oplus a_2 \otimes A^{\otimes 2} \oplus \cdots \oplus a_k \otimes A^{\otimes k},$$

where I is the tropical identity matrix of size $n \times n$.

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

Now, let us define the size of an integer, a matrix, and an instance of a problem.

Let a be a non-negative number. We can consider two sizes of a. The first one is the number of bits that we need to write this number using the binary numeral system:

$$\mathrm{size}_2(a) = \begin{cases} \lfloor \log_2(a) \rfloor + 1 & \text{if } a > 0, \\ 0 & \text{otherwise.} \end{cases}$$

For $a \ge 1$, if $\mathrm{size}(a) = s$, then $2^{s-1} \le a < 2^s$.

The second size is the number of symbols that we need to write this number using the unary numeral system:

$$\mathrm{size}_1(a) = a.$$

Let A be a matrix of size $k \times k$. The matrix can be represented as a list of k^2 numbers separated with $k^2 - 1$ delimiters. Therefore,

$$\mathrm{size}_b(A) = \sum_{i=1}^{k} \sum_{j=1}^{k} \mathrm{size}_b(a_{ij}) + k^2 - 1.$$

Let U be a set. *A stratification* of U is a sequence $\{U_m\}_m$ of non-empty finite subsets $U_m \subseteq U$ such that $\bigcup_m U_m = U$. Stratifications are often specified by length functions. *A length function* on U is a map $l\colon U \to \mathbb{N}$ such that the inverse image of every integer is finite. The corresponding spherical stratification is formed by spheres $S_n = \{x \in U : l(x) = n\}$. Sometimes, for a set A, we denote the set $A \cap U_n$ by A_n. For a subset $A \subseteq U$ and a stratification $\{U_m\}_m$, the limit

$$\rho(A) = \lim_{m\to\infty} \frac{|A \cap U_m|}{|U_m|}$$

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

An algorithm $\mathcal{A}\colon U \to V \cup \{?\}$ is called *generic* if $\mathcal{A}$ stops on every input $I \in U$, and $\{I \in U : \mathcal{A}(I) \neq ?\}$ is a generic set. Here, the answer "?" means "don't know".

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

For more information on tropical algebra and, in particular, on the theory of systems of tropical linear equations, we refer the reader to [18]. For more information on complexity results in tropical algebra, we refer the reader to the survey [31].

3. Classes of pairwise commuting matrices

In this section, we discuss some classes of pairwise commuting matrices. Recall that *a set of pairwise commuting matrices* S is a set such that $A \otimes B = B \otimes A$ for all $A, B \in S$. As demonstrated in Introduction, sets of pairwise commuting matrices are important for building tropical key exchange protocols. In this section, we consider the following two matrix semirings: $\langle \mathrm{Mat}_k(\mathcal{R}_{\max,+}), \otimes, \oplus\rangle$ and $\langle \mathrm{Mat}_k(\mathcal{R}_{\min,+}), \otimes, \oplus\rangle$.

Let $\mathcal{S}$ be a tropical semiring. Let M be a matrix of size $k \times k$ over $\mathcal{S}$. It is easy to see that for any two polynomials $p(x)$ and $q(x)$, the matrices $p(M)$ and $q(M)$ commute.

Lemma 1. *Let M be a matrix of size $k \times k$ over $\mathcal{S}$, and let $p(x), q(x) \in \mathcal{S}[x]$. Then*

$$p(M) \otimes q(M) = q(M) \otimes p(M).$$

Let $\mathcal{P}_k(\mathcal{S}, M) = \{p(M) : p(x) \in \mathcal{S}[x]\}$. The following lemma follows immediately from Lemma 1.

Lemma 2. *For any $A, B \in \mathcal{P}_k(\mathcal{S}, M)$, $A \otimes B = B \otimes A$.*

A matrix of size $k \times k$ is called *circulant* if each row is a cyclic right shift of the previous row:

$$\begin{pmatrix} c_1 & c_2 & \cdots & c_k \\ c_k & c_1 & \cdots & c_{k-1} \\ \vdots & & \ddots & \vdots \\ c_2 & c_3 & \cdots & c_1 \end{pmatrix} \tag{1}$$

The matrix (1) is denoted by $C(c_1, \ldots, c_k)$. The set of all circulant matrices of size $k \times k$ is denoted by $\mathcal{C}_k(\mathcal{S})$.

The following lemma is well known.

Lemma 3. *For any $A, B \in \mathcal{C}_k(\mathcal{S})$, $A \otimes B = B \otimes A$.*

Proof. Any circulant matrix (1) can be presented as

$$c_1 \otimes I \oplus c_k \otimes P \oplus \cdots \oplus c_2 \otimes P^{\otimes k-1}, \tag{2}$$

where

$$P = \begin{pmatrix} o & o & o & \cdots & o & e \\ e & o & o & \cdots & o & o \\ o & e & o & \cdots & o & o \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ o & o & o & \cdots & e & o \end{pmatrix}.$$

This follows from the fact that

$$p_{lij} = \begin{cases} e \text{ if } i - j = l \text{ and } i \geq j, \\ e \text{ if } n + i - j = l \text{ and } i < j, \\ o \text{ otherwise,} \end{cases}$$

where p_{lij} are the elements of P^l, which can be proven by induction.

Since any circulant matrix is a matrix polynomial in the cyclic permutation matrix $C(o, \ldots, o, e)$, it follows from Lemma 1 that any two circulant matrices commute. □

A matrix of the form

$$\begin{pmatrix} c_1 & t \otimes c_2 & t \otimes c_3 & \cdots & t \otimes c_{k-1} & t \otimes c_k \\ c_k & c_1 & t \otimes c_2 & \cdots & t \otimes c_{k-2} & t \otimes c_{k-1} \\ c_{k-1} & c_n & c_1 & \cdots & t \otimes c_{k-3} & t \otimes c_{k-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ c_2 & c_3 & c_4 & \cdots & c_k & c_1 \end{pmatrix} \tag{3}$$

is called *upper-t-circulant*.

Analogously, a matrix of the form

$$\begin{pmatrix} c_1 & c_2 & c_3 & \cdots & c_{k-1} & c_k \\ s \otimes c_k & c_1 & c_2 & \cdots & c_{k-2} & c_{k-1} \\ s \otimes c_{k-1} & s \otimes c_k & c_1 & \cdots & c_{k-3} & c_{k-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ s \otimes c_2 & s \otimes c_3 & s \otimes c_4 & \cdots & s \otimes c_k & c_1 \end{pmatrix} \tag{4}$$

is called *lower-s-circulant*.

Let $\mathcal{UC}_k(\mathcal{S}, t)$ be the set of all upper-t-circulant matrices over $\mathcal{S}$ of size $k \times k$, and let $\mathcal{LC}_k(\mathcal{S}, s)$ be the set of all lower-s-circulant matrices of size $k \times k$.

The following lemmas can be found in [9, 38]. We provide proofs here based on Lemma 1, following the approach of [13].

Lemma 4 ([9, 38])**.** *For any $A, B \in \mathcal{UC}_k(\mathcal{S}, t)$, $A \otimes B = B \otimes A$.*

Proof. Any upper-t-circulant matrix (3) can be presented as (2), where

$$P = \begin{pmatrix} o & o & o & \cdots & o & t \\ e & o & o & \cdots & o & o \\ o & e & o & \cdots & o & o \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ o & o & o & \cdots & e & o \end{pmatrix}.$$

This follows from the fact that

$$p_{lij} = \begin{cases} e \text{ if } i - j = l \text{ and } i \geq j, \\ t \text{ if } n + i - j = l \text{ and } i < j, \\ o \text{ otherwise,} \end{cases}$$

where p_{lij} are the elements of P^l. Therefore, it follows from Lemma 1 that any two upper-t-circulant commute. □

Lemma 5 ([9, 38])**.** *For any $A, B \in \mathcal{LC}_k(\mathcal{S}, s)$, $A \otimes B = B \otimes A$.*

Proof. And any lower-s-circulant matrix (4) can be presented as (2), where

$$P = \begin{pmatrix} o & o & o & \cdots & o & e \\ s & o & o & \cdots & o & o \\ o & s & o & \cdots & o & o \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ o & o & o & \cdots & s & o \end{pmatrix}.$$

Similarly, this follows from the fact that

$$p_{lij} = \begin{cases} s \text{ if } j - i = l \text{ and } j > i, \\ e \text{ if } n + j - i = l \text{ and } j \leq i, \\ o \text{ otherwise,} \end{cases}$$

where p_{lij} are the elements of P^l. Analogically, it follows from Lemma 1 that any two lower-s-circulant commute. □

Let $r \geq 0$ and $m \leq 0$ be real numbers. A matrix $A \in \mathrm{Mat}_k(\mathcal{R}_{\min,+})$ such that $a_{ii} = m$ and $a_{ij} \in [r, 2r]$, $i \neq j$, is called a *Linde–de la Puente matrix* [45, 52]. The set of such matrices is denoted by $[r, 2r]_k^m$. The definition of Linde–de la Puente matrices in $\mathcal{R}_{\max,+}$ is similar.

The following result was proved by Muanalifah and Sergeev [52].

Lemma 6 ([52])**.** *Let $r, s \geq 0$ and $m_1, m_2 \leq 0$. For $A \in [r, 2r]_k^{m_1}$ and $B \in [s, 2s]_k^{m_2}$,*

$$A \otimes B = B \otimes A = m_2 \otimes A \oplus m_1 \otimes B.$$

Alhussaini and Sergeev [7] considered the centralizers of Linde–de la Puente matrices over tropical semirings. Recall that the *centralizer* of all Linde–de la Puente matrices of size $k \times k$ and negative integer values of r over the max-plus semiring is the set consisting of all matrices X such that $X \otimes A = A \otimes X$ for any such Linde–de la Puente matrix.

They proved [7] the following result.

Theorem 1 ([7]). *The centralizer of all Linde–de la Puente matrices of size* 2×2 *and negative integer values of* r *over the max-plus semiring is precisely the set of matrices appearing as tropical linear combinations of the matrices from the following set:*

$$\left\{ \begin{pmatrix} 0 & -\infty \\ -\infty & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -\infty & 0 \end{pmatrix}, \begin{pmatrix} 0 & -\infty \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & -2 \end{pmatrix} \right\}.$$

This generating set is minimal with respect to inclusion.

For higher dimensions, Alhussaini and Sergeev's experiments demonstrate that a finite generating set is unlikely to exist. They ask the following question [7].

Question 1 ([7]). Prove that the centralizer of all Linde–de la Puente matrices of fixed dimension k and arbitrary negative integer values of r does not admit a finite generating set for any $k \geq 3$.

Alhussaini and Sergeev [7] also extended the concept of Linde–de la Puente matrices beyond the tropical semiring, generalizing it to a broader class of semirings.

The following type of matrices was considered by D. Jones [41]. A matrix $A = (a_{ij}) \in \mathrm{Mat}_n(\mathcal{R}_{\max,+})$ is called a *Jones matrix* if it satisfies the following condition:

$$a_{ij} \otimes a_{jk} \leq a_{ik} \otimes a_{jj}, \quad \forall i, j, k \in \{1, \ldots, n\}.$$

Let $A = (a_{ij})$ be a Jones matrix and $\alpha \in \mathbb{R}$. The matrix $A^{(\alpha)} = (b_{ij})$ defined by

$$b_{ij} = a_{ij} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)}$$

is called a *deformation* of A.

Muanalifah and Sergeev proved [52] the following result.

Theorem 2 ([52]). *If* A *is a Jones matrix, then* $A^{(\alpha)}$ *is also a Jones matrix for any* $\alpha < 1$. *if* A *and* B *are Jones matrices, then*

$$A^{(\alpha)} \otimes B^{(\beta)} = A^{(\beta)} \otimes A^{(\alpha)} = A^{(\alpha+\beta)}$$

for any α *and* β *such that* $0 \leq \alpha \leq 1$ *and* $0 \leq \beta \leq 1$.

One can consider a quasi-polynomial of A: $B = \bigoplus_{\alpha \in R} a_\alpha \otimes A^{(\alpha)}$, where R is a finite set of rational numbers in $[0, 1]$ and $a_\alpha \in \mathcal{R}_{\max,+}$ for all $\alpha \in R$.

Let $\mathcal{J}_k(M)$ be a set of all quasi-polynomials of M. The following theorem follows from Theorem 2.

Theorem 3 ([52]). *For any* $A, B \in \mathcal{J}_k(M)$, $A \otimes B = B \otimes A$.

We conclude this section with the following question.

Question 2. Describe other classes of pairwise commuting matrices over tropical algebras.

4. Solving systems of tropical equations

In this section, we discuss questions related to the solving systems of equations over tropical and close structures.

Recall that the decidability of one-sided systems of tropical linear equations can be checked in polynomial time. Indeed, consider the max-plus algebra. We can write such a system as a matrix equation $A \otimes X = B$, where A is a matrix and B is a vector. Let us assume that $b_i \in \mathbb{R}$. The vector $X^* = (-\max_i(a_{ij} - b_i))_j$ is called the *principal solution* to this system. It is known [18] that this system has a solution if and only if X^* is a solution. Moreover, let $M_j = \operatorname{argmax}(a_{ij} - b_i)$, then the system has a solution if and only if $\bigcup_j M_j = \{1, \dots, m\}$, where m is the number of equations. 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.

The same approach can be applied for a matix equation

$$A \otimes X = B, \tag{5}$$

where A and B are matrices of size $k \times k$. Let us describe how to solve such equations over $\mathrm{Mat}_k(\mathcal{R}_{\max,+})$ or $\mathrm{Mat}_k(\mathcal{R}_{\max,\times})$. The matrix $X^* = X^*(A, B)$ such that $x^*_{ij} = \min\{b_{lj} \otimes a_{li}^{\otimes -1}\}_l$ is called the *principal solution* to the equation (5). Actually, the principal solution may not be a solution to (5). The following lemma is an adaptation of Theorem 3.1.1 in [18].

Lemma 7. *Let $\mathcal{S}$ be $\mathrm{Mat}_k(\mathcal{R}_{\max,+})$ or $\mathrm{Mat}_k(\mathcal{R}_{\max,\times})$. Let A, B, X be matrices of size $k \times k$. X is a solution to $A \otimes X = B$ over $\mathcal{S}$ if and only if $X \leq X^*(A, B)$ and*

$$\bigcup_{(i,j)\,:\,x_{ij} = x^*_{ij}} M_{ij}(A, B) = \{1, \dots, k\} \times \{1, \dots, k\},$$

where $M_{ij}(A, B) = \{(l, j) : x^*_{ij} = b_{lj} \otimes a_{li}^{\otimes -1}\}$.

Otero Sánchez et al. [59] considered generalized tropical semirings. Recall that a semiring $\mathcal{R} = \langle R, +, \cdot \rangle$ is called a *generalized tropical semiring* if for all $a, b \in \mathcal{R}$,

$$a + b = a \quad \text{or} \quad a + b = b.$$

Theorem 4 ([59])**.** *Let $\mathcal{R} = \langle R, +, \cdot \rangle$ be a generalized tropical semiring, and let $XA = Y$ be a system of equations with $Y = (y_i) \in \mathcal{R}^m$ and $A = (a_{ij}) \in \mathrm{Mat}_{n \times m}(\mathcal{R})$. $X = (x_1, \dots, x_n)$ is a solution to the system if and only if*

1. *$x_i \cdot a_{ij} + y_j = y_j$ for all $j \in \{1, \dots, m\}$,*
2. *for all $j \in \{1, \dots, m\}$, there exists $h \in \{1, \dots, n\}$ such that $x_j \cdot a_{hj} = y_h$.*

The following result follows from this theorem.

Theorem 5 ([59])**.** *Let $\mathcal{R} = \langle R, +, \cdot \rangle$ be a generalized tropical semiring such that $\langle R, \cdot \rangle$ is a group, and let $XA = Y$ be a system of equations with $Y \in \mathcal{R}^m$ and $A = (a_{ij}) \in \mathrm{Mat}_{n \times m}(\mathcal{R})$. Determining all of the solutions of the system has a computational cost of $O(mn)$.*

They applied this method to cryptanalyze two different key exchange protocols [59].

In [8], algorithms for solving one-sided linear systems of equations over the supertropical semiring and over the symmetrized semiring are considered.

In [67], the following two theorems were proved, which demonstrates that the supertropical semirings and the q-modular tropical semirings have very different complexity properties.

Theorem 6. *The problem of deciding whether a system of one-sided linear equations over $\mathcal{Z}_{\max,+} \ltimes \mathbb{N}_2$ has a solution is NP-complete.*

Theorem 7. *Let $A \in M_{m\times n}(\mathbb{T}_{\text{ext}}(q))$ and $b \in M_{m\times 1}(\mathbb{T}_{\text{ext}}(q))$. There is a polynomial algorithm to solve $A \otimes x = b$.*

It was proven by Bezem et al. [11] that two-sided systems of tropical linear equations

$$A \otimes X \oplus B = C \otimes X \oplus D.$$

are polynomially equivalent to mean payoff games, a well-known hard problem in NP∩co-NP.

Now consider systems of polynomial equations.

Grigoriev and Shpilrain proved [33] the following theorem.

Theorem 8 ([33])**.** *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 9. *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.*

It is possible to prove that this problem is actually NP-complete.

Theorem 10 ([67])**.** *The problem of determining if there exists a solution to a given system of tropical polynomial equations is NP-complete.*

For the semirings $\mathbb{T}_{\text{ext}}(q))$, it is possible to prove NP-hardness.

Theorem 11 ([67])**.** *The problem of deciding whether a finite system of polynomial equations over the extended q-modular tropical semiring $\mathbb{T}_{\text{ext}}(q)$ has a solution is NP-hard.*

Consider systems of equations of the following form:

$$\bigoplus_{1\leq i,j\leq n} a_{kij} \otimes x_i \otimes y_j = 0,\ 1 \leq k \leq m. \tag{6}$$

Problem 12. *Given numbers m, n, a_{kij}, $1 \leq k \leq m$, $1 \leq i, j \leq n$. Decide if there is a solution over $\mathbb{Z}_{\max,+}$ to the system of equations (6).*

Buchinskiy et al. [14] proved the following theorem.

Theorem 12 ([14])**.** *Problem 12 is NP-complete.*

Although, it is shown that this problem is NP-complete, with some restrictions on the coefficients, the number of variables, and the number of equations, it is decidable generically in polynomial time. Also, it can be shown that the asymptotic density of solvable systems of the form (6) with some restrictions on the coefficients, the number of variables, and the number of equations is 0.

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 (6), 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.

Buchinskiy et al. [14] proved the following two theorems.

Theorem 13 ([14]). *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 $m(r) \geq n(r)^2$ 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 $Sat(Sys(m, n, \mathbb{Z}_{\geq 0})) = 0$ w.r.t. $\{Sys(m, n, [0, r))\}_r$, and $Sat(Sys(m, n, \mathbb{Z})) = 0$ w.r.t. $\{Sys(m, n, [-r, r])\}_r$.

Theorem 14 ([14]). *Consider the problem of determining if there is a solution to a system of equations (6), 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.

In cryptanalysis, it is usually given that a system has a solution. It would be interesting to prove that there is a generic polynomial-time algorithm to solve systems of the form (6) if the system has a solution.

5. Marginal sets in semigroups and semirings

In the Introduction, we discussed the concept of Romankov's marginal sets in groups and their use in developing key exchange schemes. In this section, following [12], we define marginal sets for semigroups, give an example of marginal sets for tropical matrix algebras, and demonstrate how this concept can be used to improve some key exchange schemes. Note that these schemes based on semigroups differ from Roman'kov's because semigroups lack multiplicative inverses, and semirings lack both multiplicative and additive inverses. Also, note that for constructing marginal sets, we need to be able to solve systems of equations.

Definition 3. Let $\mathcal{S} = \langle S, \cdot, e \rangle$ be a semigroup with an identity element e, let $(a_1, \ldots, a_m) \in S^m$, and let $w(x_1, \ldots, x_m, \square_1, \ldots, \square_n)$ be a semigroup word. A tuple $(c_1, \ldots, c_n) \in S^n$ is called $w(a_1, \ldots, a_m, \square_1, \ldots, \square_n)$-*marginal* if

$$w(a_1, \ldots, a_m, c_1, \ldots, c_n) = w(a_1, \ldots, a_m, e, \ldots, e). \tag{7}$$

We denote this by writing $(c_1, \ldots, c_n) \perp w(a_1, \ldots, a_m, \square_1, \ldots, \square_n)$. Any subset $C \subseteq S^n$ of $w(a_1, \ldots, a_m, \square_1, \ldots, \square_n)$-marginal tuples is called a $w(a_1, \ldots, a_m, \square_1, \ldots, \square_n)$-*marginal* set. We also denote this by writing $C \perp w(a_1, \ldots, a_m, \square_1, \ldots, \square_n)$.

Note that marginal sets are subsets of the solution sets of the corresponding equations (7). For example, if $a \in S$, then $(c) \perp a \cdot \square$ for any solution c to the equation $a \cdot x = a$.

Example 15. Consider the semigroup of tropical matrices of size 3×3 over the min-plus algebra. Let $w(x, \Box) = x \otimes \Box$ and

$$A = \begin{pmatrix} 3 & 7 & 4 \\ 5 & 12 & 7 \\ 6 & 5 & 11 \end{pmatrix}.$$

It is easy to check that the set

$$C = \left\{ \begin{pmatrix} 0 & 7 & 5 \\ 1 & 0 & 6 \\ -1 & 5 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 7 & 5 \\ 1 & 0 & 6 \\ 0 & 5 & 0 \end{pmatrix} \right\}$$

is $(A \otimes \Box)$-marginal.

Marginal sets can be used for key exchange schemes. A few variations of the Sidelnikov–Cherepnev–Yaschenko protocol based on marginal sets were considered [12]. Here, we consider one of these variations.

Protocol 3. Alice and Bob agree on a public noncommutative semigroup $\mathcal{S} = \langle S, \cdot, e \rangle$, two public subsets of pairwise commuting elements $H \subseteq S$ and $R \subseteq S$, and a public element $w \in S$.

(1) Alice chooses two private elements $p_1 \in H$ and $q_1 \in R$, constructs a public $(p_1 \cdot \Box_1 \cdot w \cdot \Box_2 \cdot q_1)$-marginal set $M_1 \subseteq S^2$, and sends M_1 to Bob.
(2) Bob chooses two private elements $p_2 \in H$ and $q_2 \in R$, constructs a public $(p_2 \cdot \Box_1 \cdot w \cdot \Box_2 \cdot q_2)$-marginal set $M_2 \subseteq S^2$, and sends M_2 to Alice.
(3) Alice chooses a pair $(c_2, d_2) \in M_2$, computes $u = p_1 \cdot c_2 \cdot w \cdot d_2 \cdot q_1$, and sends it to Bob.
(4) Bob chooses a pair $(c_1, d_1) \in M_1$, computes $v = p_2 \cdot c_1 \cdot w \cdot d_1 \cdot q_2$ and sends it to Alice.
(5) Alice computes her shared key $k_A = p_1 \cdot v \cdot q_1$.
(6) Bob computes his shared key $k_B = p_2 \cdot u \cdot q_2$.

They share the same key because

$$k_A = p_1 \cdot v \cdot q_1 = p_1 \cdot (p_2 \cdot c_1 \cdot w \cdot d_1 \cdot q_2) \cdot q_1 = (p_1 \cdot p_2) \cdot c_1 \cdot w \cdot d_1 \cdot (q_2 \cdot q_1) = (p_2 \cdot p_1) \cdot c_1 \cdot w \cdot d_1 \cdot (q_1 \cdot q_2) = p_2 \cdot (p_1 \cdot c_1 \cdot w \cdot d_1 \cdot q_1) \cdot q_2 = p_2 \cdot (p_1 \cdot w \cdot q_1) \cdot q_2 = p_2 \cdot p_1 \cdot w \cdot q_1 \cdot q_2$$

and

$$k_B = p_2 \cdot u \cdot q_2 = p_2 \cdot (p_1 \cdot c_2 \cdot w \cdot d_2 \cdot q_1) \cdot q_2 = (p_2 \cdot p_1) \cdot c_2 \cdot w \cdot d_2 \cdot (q_1 \cdot q_2) = (p_1 \cdot p_2) \cdot c_2 \cdot w \cdot d_2 \cdot (q_2 \cdot q_1) = p_1 \cdot (p_2 \cdot c_2 \cdot w \cdot d_2 \cdot q_2) \cdot q_1 = p_1 \cdot (p_2 \cdot w \cdot q_2) \cdot q_1 = (p_1 \cdot p_2) \cdot w \cdot (q_2 \cdot q_1) = p_2 \cdot p_1 \cdot w \cdot q_1 \cdot q_2.$$

To use this scheme, we should be able to construct marginal sets. Let us consider how to construct $(A \otimes \Box_1 \otimes B \otimes \Box_2 \otimes C)$-marginal sets in the semigroup of $k \times k$ matrices over the min-plus algebra. The following lemma helps us to solve equations of the form $A \otimes X \otimes B \otimes Y \otimes C = A \otimes B \otimes C$. Note that it is known that in general the problem to solve a system of tropical equations of degree two is NP-hard [33, 14], but we will demonstrate that these systems of equations are simpler.

Lemma 8. *Let $A, B, C \in \mathrm{Mat}_k(\mathbb{R})$. A pair of matrices (X, Y), $X, Y \in \mathrm{Mat}_k(\mathbb{R})$, is a solution to*

$$A \otimes X \otimes B \otimes Y \otimes C = A \otimes B \otimes C$$

over $\mathcal{M}^k_{\min,+}$ if and only if $x_{pq} \otimes y_{rs} \geq x^*_{pqrs}(A, B, C)$ and

$$\bigcup_{(p,q,r,s)\,:\, x_{pq} \otimes y_{rs} = x^*_{pqrs}(A,B,C)} M_{pqrs}(A, B, C) = \{1, \ldots, k\} \times \{1, \ldots, k\},$$

where

$$x^*_{pqrs}(A, B, C) = \max\{d_{ij} \otimes a_{ip}^{\otimes -1} \otimes b_{qr}^{\otimes -1} \otimes c_{sj}^{\otimes -1}\}_{i,j},$$

$$d_{ij} = \bigoplus_{u=1}^{k} \bigoplus_{v=1}^{k} a_{iu} \otimes b_{uv} \otimes c_{vj},$$

and

$$M_{pqrs}(A, B, C) = \{(i, j) \ : \ x^*_{pqrs}(A) = d_{ij} \otimes a_{ip}^{\otimes -1} \otimes b_{qr}^{\otimes -1} \otimes c_{sj}^{\otimes -1}\}.$$

Now consider an algorithm to generate $(A \otimes \square_1 \otimes B \otimes \square_2 \otimes C)$-marginal sets, where $A, B, C \in \mathrm{Mat}_k(\mathbb{Z})$, based on this lemma.

Note that

$$\bigcup_{(p,r)\,:\, x^*_{pprr}(A,B,C)=0} M_{pprr}(A) = \{1, \ldots, k\} \times \{1, \ldots, k\}.$$

Therefore, consider the following linear programming problem. First, add the inequalities

$$x_{pq} \otimes y_{rs} \geq x^*_{pqrs}(A, B, C)$$

to the set of constraints. Second, let

$$\begin{aligned} P(A, B, C) &= \{(p, r) : x^*_{pprr}(A, B, C) = 0\}, \\ P_x(A, B, C) &= \{p : \exists\, r \text{ such that } x^*_{pprr}(A, B, C) = 0\}, \\ P_y(A, B, C) &= \{r : \exists\, p \text{ such that } x^*_{pprr}(A, B, C) = 0\}. \end{aligned}$$

For each $(p, r) \in P(A, B, C)$ add the equations

$$x_{pp} \otimes y_{rr} = 0$$

to the set of constraints. Third, to add more randomness, select a random integer h and integers r_{ij}, s_{ij}, such that

$$\begin{array}{ll} r_{ii} = h & \text{if } i \in P_x(A, B, C), \\ r_{ij} \text{ is a random integer} & \text{otherwise,} \end{array}$$

and

$$\begin{array}{ll} s_{jj} = -h & \text{if } j \in P_y(A, B, C), \\ s_{ij} \text{ is a random integer} & \text{otherwise,} \end{array}$$

and add inequalities

$$\begin{aligned} x_{ij} &\geq r_{ij}, 1 \leq i \leq k, 1 \leq j \leq k, \\ y_{ij} &\geq s_{ij}, 1 \leq i \leq k, 1 \leq j \leq k. \end{aligned}$$

to the set of constraints as well. To solve this problem, we can apply the simplex method or another method for linear programming. Note that it follows from Ghouila-Houri's Theorem [29] that the matrix of this linear programming problem is totally unimodular. Therefore, from the Hoffman–Kruskal Theorem [36] it follows that the problem is integral, i.e. it has an integral optimum whenever an optimum exists.

To generate an $(A \otimes \square_1 \otimes B \otimes \square_2 \otimes C)$-marginal set M of size n, we start with $M = \emptyset$ and repeatedly construct and solve the linear programming problem described above, adding each solution to M until it reaches size n.

The following marginal sets over the semigroup of matrices over the min-plus algebra were also considered in [12]: $M \perp A \otimes \square$, $M \perp \square \otimes A$, and $M \perp \square_1 \otimes A \otimes \square_2$.

Since it is interesting to study applications of marginal sets to cryptography, the following questions arise.

Question 3. What information does a $w(A_1, \ldots, A_m, \square_1, \ldots, \square_n)$-marginal set reveal about the matrices $A_1, \ldots, A_m$?

Question 4. Explore examples of marginal sets in other classes of semigroups.

6. Tropical discrete logarithm problems

In this section, we provide an overview of different variations of the tropical discrete logarithm problem, which was defined in the Introduction, following [53, 4, 51].

The following theorem describes a case in which the tropical discrete logarithm is well defined.

Theorem 16 ([53])**.** *Suppose that V has finite entries and F is irreducible. Then $V \otimes F^{\otimes t_1} \neq V \otimes F^{\otimes t_2}$ for any t_1 and t_2 if and only if $\lambda(F) \neq 0$.*

Muanalifah and Sergeev suggested a solution of Problem 4 based on the weak CSR expansion. Recall that $\mathcal{G}^c(F)$ is the critical graph of F, the subgraph of $\mathcal{G}(F)$ which consists of all nodes and arcs of the cycles where the maximum cycle mean $\lambda(F)$ is attained. Denote $U_Z = (\lambda^- \otimes F)^{\otimes l(Z)})^+$,

$$(C_Z)_{ij} = \begin{cases} (U_Z)_{ij} & j \text{ in } Z, \\ -\infty & \text{otherwise}, \end{cases} \tag{8}$$

$$(R_Z)_{ij} = \begin{cases} (U_Z)_{ij} & i \text{ in } Z, \\ -\infty & \text{otherwise}, \end{cases} \tag{9}$$

and

$$(S_Z)_{ij} = \begin{cases} \lambda^- \otimes F_{ij} & (i,j) \in Z, \\ -\infty & \text{otherwise}. \end{cases} \tag{10}$$

The following result is useful for solving the tropical discrete logarithm.

Theorem 17 ([53])**.** *Let $V \in \mathrm{Mat}_{m \times d}(\mathcal{R}_{\max,+})$ and $F \in \mathrm{Mat}_{d \times d}(\mathcal{R}_{\max,+})$ with $\lambda = \lambda(F) \neq -\infty$ and let Z be a cycle of $\mathcal{G}^c(F)$. Then for any $t \geq (d-1)^2 + 1$, the columns of $V \otimes F^{\otimes t}$ with indices in Z are equal to the corresponding columns in $\lambda^{\otimes t} \otimes V \otimes C_Z S_Z^{t(\mathrm{rem}\, l(Z))} R_Z[F]$.*

Algorithm 1

Input: $A, V \in \mathbb{R}_{\max}^{m\times d}$, $F \in \mathbb{R}_{\max}^{d\times d}$.
Output: t such that $A = V \otimes F^{\otimes t}$.
Find $\lambda = \lambda(F)$ and a critical cycle Z.
Compute C_Z and S_Z according to (8) and (10)
For $t = 0, 1, \ldots, (d-1)^2$, check if $A = V \otimes F^{\otimes t}$ and return t if it is found
For $k = 0, \ldots, l-1$, where $l = l(Z)$, check if $A_{\cdot i} - V \otimes (C_Z S_Z^k R_Z[F])_{\cdot i} = \mu + E_{\cdot i}$ for all $i \in Z$ and some μ such that $t = \mu/\lambda$ is a natural number and return the first such t that is found

Algorithm 1 finds t such that $A = V \otimes F^{\otimes t}$. The time complexity of this algorithm and the theorem about the conditions when it is applicable can be found in [53].

Subsequently, Alhussaini et al. [4] considered the tropical discrete logarithm problem with a shift and the tropical two-sided discrete logarithm problem with a shift.

Problem 13. *Given matrices V, W, and C of appropriate dimensions, find $s \in \mathbb{R}$ and $x \in \mathbb{Z}_{\geq 0}$ such that $s \otimes V \otimes W^{\otimes x} = C$.*

Problem 14. *Given matrices W_1, W_2, V, and C of appropriate dimensions, find $x_1, x_2 \in \mathbb{Z}_{\geq 0}$ and $s \in \mathbb{R}$ such that $s \otimes W_1^{\otimes x_1} \otimes V \otimes W_2^{\otimes x_2} = C$.*

Their approach to solving these problems is also based on the CSR expansion of tropical matrix powers and can be found in [4].

7. Tropical knapsack and subset sum problems

In this section, we discuss the computational complexity of the knapsack problem and subset sum problem for the following tropical algebraic structures. We consider the semigroup of square matrices of size $k \times k$ with non-negative entries over the max-plus algebra $\mathrm{Mat}_k(\mathcal{N}_{\max,+})$ and the semigroup square matrices of size $k \times k$ with positive entries over the max-times algebra $\mathrm{Mat}_k(\mathcal{N}_{\max,\times})$.

Let $I = (W_1, \ldots, W_n, C)$ be an input of $\mathbf{SSP}(\mathcal{S})$ or $\mathbf{KP}(\mathcal{S})$, where $\mathcal{S}$ is a matrix semigroup, Then the size of I is

$$\mathrm{size}_b(I) = \sum_{l=1}^{n}\sum_{j=1}^{k}\sum_{l=1}^{k} \mathrm{size}_b(w_{lij}) + \sum_{i=1}^{k}\sum_{j=1}^{k} \mathrm{size}_b(c_{ij}) + (n+1)k^2 - 1.$$

Note that we consider the number k as a parameter of a problem. Hence, k can occur in exponents in polynomials.

The following theorem shows that the knapsack problem and subset sum problem over these structures are NP-complete.

Theorem 18 ([17])**.** $\mathbf{SSP}(\mathrm{Mat}_k(\mathcal{N}_{\max,+}))$, $\mathbf{SSP}(\mathrm{Mat}_k(\mathcal{N}_{\max,\times}))$, $\mathbf{KP}(\mathrm{Mat}_k(\mathcal{N}_{\max,+}))$, *and* $\mathbf{KP}(\mathrm{Mat}_k(\mathcal{N}_{\max,\times}))$ *are* NP*-complete.*

Recall that an algorithm is pseudo-polynomial if its time complexity is polynomial in $\mathrm{size}_1(I)$. Using the dynamic programming approach, it is possible to demonstrate that there are pseudo-polynomial algorithms to solve these problems.

Theorem 19 ([17]). $\mathbf{SSP}(\mathrm{Mat}_k(\mathcal{N}_{\max,+}))$, $\mathbf{SSP}(\mathrm{Mat}_k(\mathcal{N}_{\max,\times}))$, $\mathbf{KP}(\mathrm{Mat}_k(\mathcal{N}_{\max,+}))$, *and* $\mathbf{KP}(\mathrm{Mat}_k(\mathcal{N}_{\max,\times}))$ *are weakly* NP*-complete.*

To consider generic case complexity of these problems, we need to define a stratification of U. Let U be the set of all tuples of the form $(W_1, \ldots, W_n, C)$, where $W_1, \ldots, W_n, C \in \mathrm{Mat}_k(\mathbb{Z}_{\geq 1})$ and $n \in \mathbb{Z}_{\geq 0}$. We consider the stratification $\{U_m\}_m$ of U, where $U_m = \{I \in U : \mathrm{size}_2(I) = m\}$.

For $\mathrm{Mat}_k(\mathcal{N}_{\max,\times})$, the following theorem was proved.

Theorem 20 ([17]). $\mathbf{SSP}(\mathrm{Mat}_k(\mathcal{N}_{\max,\times}))$ *and* $\mathbf{KP}(\mathrm{Mat}_k(\mathcal{N}_{\max,\times}))$ *are decidable generically in polynomial time.*

It would be interesting to know if there are such algorithms for $\mathrm{Mat}_k(\mathcal{N}_{\max,+})$.

Question 5. Does there exist polynomial generic algorithms to solve $\mathbf{SSP}(\mathrm{Mat}_k(\mathcal{N}_{\max,+}))$ and $\mathbf{KP}(\mathrm{Mat}_k(\mathcal{N}_{\max,+}))$?

The above theorems are proven for matrices without negative numbers and $-\infty$. It would be interesting to study the problems for the semigroup of matrices of size $k \times k$ over the max-plus algebra $\mathcal{Z}_{\max,+}$.

Question 6. Is $\mathbf{KP}(\mathrm{Mat}_k(\mathcal{Z}_{\max,+}))$ NP-complete? Are there pseudo-polynomial or polynomial generic algorithms to solve $\mathbf{SSP}(\mathrm{Mat}_k(\mathcal{Z}_{\max,+}))$ and $\mathbf{KP}(\mathrm{Mat}_k(\mathcal{Z}_{\max,+}))$?

Also, we can consider matrices over the min-plus algebra.

Question 7. Is $\mathbf{KP}(\mathrm{Mat}_k(\mathcal{Z}_{\min,+}))$ NP-complete? Are there pseudo-polynomial or polynomial generic algorithms to solve $\mathbf{SSP}(\mathrm{Mat}_k(\mathcal{Z}_{\min,+}))$ and $\mathbf{KP}(\mathrm{Mat}_k(\mathcal{Z}_{\min,+}))$?

Alhussaini et al. considered the tropical discrete logarithm problem with a shift and the tropical two-sided discrete logarithm problem with a shift [4]. It would be interesting to consider a shifted version of the knapsack problem.

Problem 15. *Given matrices $W_1, \ldots, W_n$, and C of size $k \times k$ over a tropical semiring, decide if $s \otimes W_1^{\otimes x_1} \otimes \ldots \otimes W_n^{\otimes x_n} = C$ for some nonnegative integers $x_1, \ldots, x_n$ and $s \in \mathbb{Z}$.*

Denote this problem $\mathbf{SKP}(\mathcal{S})$.

Question 8. Is $\mathbf{SKP}(\mathrm{Mat}_k(\mathcal{Z}_{\max,+}))$ NP-complete? Is there a polynomial or a polynomial generic algorithm to solve $\mathbf{SKP}(\mathrm{Mat}_k(\mathcal{Z}_{\max,+}))$?

8. Conclusion

In this paper, we presented several problems and questions in algebra inspired by tropical cryptography. We demonstrated that tropical cryptography is not only an applied field, but also a source of interesting problems in algebra.

Acknowledgments

The research of the first and third authors was supported by the Russian Science Foundation project No. 25-11-20023.

References

[1] K. Ahmed, S. Pal, and R. Mohan. A review of the tropical approach in cryptography. *Cryptologia*, 47(1):63–87, 2023.

[2] M. Akian, S. Gaubert, and A. Guterman. Tropical cramer determinants revisited. *Tropical and idempotent mathematics and applications*, 616:1–45, 2014.

[3] S. Alhussaini, C. Collett, and S. Sergeev. Generalized Kotov–Ushakov attack on tropical Stickel protocol based on modified tropical circulant matrices, 2024.

[4] S. Alhussaini, C. Collett, and S. Sergeev. On the tropical two-sided discrete logarithm and a key exchange protocol based on the tropical algebra of pairs. *Communications in Algebra*, 52(10):4115–4134, 2024.

[5] S. Alhussaini and S. Sergeev. Attacking tropical Stickel protocol by MILP and heuristic optimization techniques. *IACR Cryptol. ePrint Arch.*, 2024.

[6] S. Alhussaini and S. Sergeev. On implementation of Stickel's key exchange protocol over max-min and max-t semirings. *Journal of Mathematical Cryptology*, 18(1):20240014, 2024.

[7] S. Alhussaini and S. Sergeev. On the security of the initial tropical Stickel protocol and its modification based on Linde–de la Puente matrices. *Applicable Algebra in Engineering, Communication and Computing*, pages 1–30, 2025.

[8] S. Alhussaini and S. Sergeev. Solving one-sided linear systems over symmetrized and supertropical semirings. *Cryptology ePrint Archive*, 2025.

[9] B. Amutha and R. Perumal. Public key exchange protocols based on tropical lower circulant and anti-circulant matrices. *AIMS Math.*, 8(7):17307–17334, 2023.

[10] P. Bergsträßer, M. Ganardi, and G. Zetzsche. A characterization of wreath products where knapsack is decidable. In *38th International Symposium on Theoretical Aspects of Computer Science (STACS 2021)*, volume 187, pages 11:1–11:17, 2021.

[11] M. Bezem, R. Nieuwenhuis, and E. Rodríguez-Carbonell. Hard problems in max-algebra, control theory, hypergraphs and other areas. *Information processing letters*, 110(4):133–138, 2010.

[12] I. Buchinskiy, M. Kotov, A. Ponmaheshkumar, and R. Perumal. Marginal sets in semigroups and semirings. *arXiv preprint arXiv:2509.06562*, 2025.

[13] I. Buchinskiy, M. Kotov, and A. Treier. Analysis of four protocols based on tropical circulant matrices. *Indian Journal of Pure and Applied Mathematics*, 2024.

[14] I. Buchinskiy, M. Kotov, and A. Treier. On the complexity of the problem of solving systems of tropical polynomial equations of degree two. In *Mathematical Optimization Theory and Operations Research: Recent Trends*, volume 2239 of *Communications in Computer and Information Science*, pages 73–84, Cham, 2024. Springer.

[15] I. Buchinskiy, M. Kotov, and A. Treier. An attack on a key exchange protocol based on max-times and min-times algebras. *Indian Journal of Pure and Applied Mathematics*, 56(1):180–190, 2025.

[16] I. M. Buchinskiy. Tropical cryptography. In *Proceedings of the XII Regional Conference of Master's Students, PhD Students and Young Scientists in Physics, Mathematics and Chemistry*, pages 66–71, Omsk, Russia, 2024. Omsk State University Press. June 3–23, 2024.

[17] I. M. Buchinskiy, M. V. Kotov, and A. V. Treier. On tropical knapsack-type problems. *arXiv e-prints*, 2025.

[18] P. Butkovič. *Max-linear systems: theory and algorithms*. Springer, London, 2010.

[19] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[20] F. Dudkin and A. Treier. Knapsack problem for Baumslag–Solitair groups. *Siberian Journal of Pure and Applied Mathematics*, 18(4):43–55, 2018. In Russian.

[21] M. Durcheva. Tropical cryptography–the state of the art and future prospects. *Athens J. Sci.*, 12:189–204, 2025.

[22] M. I. Durcheva. Public key cryptography with max-plus matrices and polynomials. In *AIP Conf. Proc.*, volume 1570, pages 491–498. AIP, 2013.

[23] M. I. Durcheva. An application of different dioids in public key cryptography. In *AIP Conf. Proc.*, volume 1631, pages 336–343. AIP, 2014.

[24] M. I. Durcheva. TrES: Tropical encryption scheme based on double key exchange. *Eur. J. Inf. Tech. Comp. Sci.*, 2(4):11–17, 2022.
[25] M. I. Durcheva and I. D. Trendafilov. Public key cryptosystem based on max-semirings. In *AIP Conf. Proc.*, volume 1497, pages 357–364. AIP, 2012.
[26] E. Frenkel, A. Nikolaev, and A. Ushakov. Knapsack problems in products of groups. *Journal of Symbolic Computation*, 74:96–108, 2016.
[27] M. Ganardi, D. König, M. Lohrey, and G. Zetzsche. Knapsack problems for wreath products. In R. Niedermeier and B. Vallée, editors, *35th Symposium on Theoretical Aspects of Computer Science*, volume 96 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 32:1–32:13, 2018.
[28] S. Gaubert and S. Sergeev. Cyclic projectors and separation theorems in idempotent convex geometry. *Journal of Mathematical Sciences*, 155:815–829, 2008.
[29] A. Ghouila-Houri. Characterisation des matrices totalement unimodulaires. *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences*, 254:1192–1194, 1962.
[30] R. Gilman, A. G. Miasnikov, A. D. Myasnikov, and A. Ushakov. Report on generic case complexity. *Vestnik Omsk Univ.*, Combinatorial Methods of Algebra and Computational Complexity:103–110, 2008.
[31] D. Grigoriev. Complexity in tropical algebra (invited talk). In *Computer Algebra in Scientific Computing: 15th International Workshop*, pages 148–154. Springer, 2013.
[32] D. Grigoriev, C. Monico, and V. Shpilrain. Tropical cryptography IV: Digital signatures and secret sharing with arbitrary access structure. Cryptology ePrint Archive, Paper 2026/095, 2026.
[33] D. Grigoriev and V. Shpilrain. Tropical cryptography. *Comm. Algebra*, 42(6):2624–2632, 2014.
[34] D. Grigoriev and V. Shpilrain. Tropical cryptography II: extensions by homomorphisms. *Communications in Algebra*, 47(10):4224–4229, 2019.
[35] P. Hall. Verbal and marginal subgroups. *Journal für die reine und angewandte Mathematik*, 1940(182):156–157, 1940.
[36] A. J. Hoffman and J. B. Kruskal. Integral boundary points of convex polyhedra. In H. W. Kuhn and A. W. Tucker, editors, *Linear Inequalities and Related Systems*, volume 38 of *Annals of Mathematical Studies*, pages 223–246. Princeton University Press, Princeton, 1956.
[37] H. Huang, X. Jiang, C. Peng, and G. Pan. A new semiring and its cryptographic applications. *AIMS Mathematics*, 9(8):20677–20691, 2024.
[38] H. Huang, C. Li, and L. Deng. Public-key cryptography based on tropical circular matrices. *Appl. Sci.*, 12(15):7401, 2022.
[39] S. Isaac and D. Kahrobaei. A closer look at the tropical cryptography. *Int. J. Comput. Math.: Comput. Syst. Theory*, 6(2):137–142, 2021.
[40] X. Jiang, H. Huang, and G. Pan. Cryptanalysis of tropical encryption scheme based on double key exchange. *J. Cyber Secur. Mobil.*, 12(02):205–220, 2023.
[41] D. Jones. *Special and structured matrices in max-plus algebra*. PhD thesis, University of Birmingham, 2017.
[42] I. Kapovich, A. Myasnikov, P. Schupp, and V. Shpilrain. Generic-case complexity, decision problems in group theory, and random walks. *Journal of Algebra*, 264(2):665–694, 2003.
[43] D. König, M. Lohrey, and G. Zetzsche. Knapsack and subset sum problems in nilpotent, polycyclic, and co-context-free groups. *Algebra and Computer Science*, 677:138–153, 2016.
[44] M. Kotov and A. Ushakov. Analysis of a key exchange protocol based on tropical matrix algebra. *Journal of Mathematical Cryptology*, 12(3):137–141, 2018.
[45] J. Linde and M. de la Puente. Matrices commuting with a given normal tropical matrix. *Linear Algebra Appl.*, 482:101–121, 2015.
[46] M. Lohrey. Knapsack in hyperbolic groups. *Journal of Algebra*, 545:390–415, 2020.
[47] M. Lohrey and G. Zetzsche. Knapsack in graph groups, HNN-extensions and amalgamated products. In *33rd Symposium on Theoretical Aspects of Computer Science*, volume 47, pages 50:1–50:14, 2016.
[48] M. Lohrey and G. Zetzsche. The complexity of knapsack in graph groups. In *34th Symposium on Theoretical Aspects of Computer Science*, volume 66 of *Leibniz International Proceedings in Informatics*, pages 52:1–52:14, 2017.
[49] A. Mishchenko and A. Treier. Knapsack problem for nilpotent groups. *Groups Complexity Cryptology*, 9(1):87–98, 2017.

[50] A. Mishchenko and A. Treier. On NP-completeness of subset sum problem for lamplighter group. In *Journal of Physics: Conference Series*, volume 1050, page 012055. IOP Publishing, 2018.
[51] A. Muanalifah. *Public key cryptography based on tropical algebra*. Ph.d. thesis, University of Birmingham, 2023.
[52] A. Muanalifah and S. Sergeev. Modifying the tropical version of Stickel's key exchange protocol. *Appl. Math.*, 65(6):727–753, 2020.
[53] A. Muanalifah and S. Sergeev. On the tropical discrete logarithm problem and security of a protocol based on tropical semidirect product. *Communications in Algebra*, 50(2):861–879, 2022.
[54] A. Myasnikov, A. Nikolaev, and A. Ushakov. Knapsack problems in groups. *Mathematics of Computation*, 84(292):987–1016, 2015.
[55] A. Myasnikov, V. Shpilrain, and A. Ushakov. *Group-based cryptography*. Birkhäuser, Basel, 2008.
[56] A. G. Myasnikov and V. A. Roman'kov. A linear decomposition attack. *Groups Complexity Cryptology*, 7(1):81–94, 2015.
[57] A. G. Myasnikov and A. N. Rybalov. Generic complexity of undecidable problems. *Journal of Symbolic Logic*, 73(2):656–673, 2008.
[58] A. G. Myasnikov, V. Shpilrain, and A. Ushakov. *Non-commutative cryptography and complexity of group-theoretic problems*, volume 177 of *Math. Surv. Monogr.* Amer. Math. Soc., Providence, RI, 2011.
[59] Á. Otero Sánchez, D Camazón Portela, and J. A. López-Ramos. On the solutions of linear systems over additively idempotent semirings. *Mathematics*, 12(18):2904, 2024.
[60] A. Ponmaheshkumar, M. Kotov, and R. Perumal. Cryptanalysis of a key exchange protocol based on a digital semiring. *Communications in Algebra*, 2025.
[61] V. A. Roman'kov. An improvement of cryptographic schemes based on the conjugacy search problem. *Prikl. Diskr. Mat. Suppl.*, pages 114–118, 2021.
[62] V. Roman'kov. An improved version of the AAG cryptographic protocol. *Groups Complexity Cryptology*, 11(1):35–41, 2019.
[63] V. Roman'kov. An improvement of the Diffie–Hellman noncommutative protocol. *Designs, Codes and Cryptography*, 90(1):139–153, 2022.
[64] V. A. Roman'kov. *Algebraic cryptography*. Omsk State University Press, Omsk, 2013. (In Russian).
[65] V. A. Roman'kov. Efficient methods of algebraic cryptanalysis and protection against them. *Prikl. Diskr. Mat. Suppl.*, pages 117–125, 2019.
[66] V. A. Roman'kov. *Algebraic cryptology*. Omsk State University Press, Omsk, 2020. (In Russian).
[67] B. Roy, M. Kotov, S. K. Sardar, and A. Treier. On extended q-modular tropical semirings. Manuscript submitted for publication, 2026.
[68] D. Rudy and C. Monico. Remarks on a tropical key exchange system. *J. Math. Cryptol.*, 15(1):280–283, 2021.
[69] A. N. Rybalov. On generic complexity of the subset sum problem for monoids and groups of integer matrices of order 2. *Vestnik of Omsk University*, 25(4):10–15, 2020. In Russian.
[70] A. N. Rybalov. On generic complexity of the subset sum problem for semigroups of integer matrices. *Prikladnaya Diskretnaya Matematika*, 50:118–126, 2020. In Russian.
[71] A. N. Rybalov. Generic polynomial algorithms for the knapsack problem in some matrix semigroups. *Siberian Electronic Mathematical Reports*, 20(1):100–109, 2023.
[72] Y. Shitov. A note on square roots of nonnegative matrices. *Linear Algebra and Its Applications*, 497:62–65, 2016.
[73] V. Shpilrain. Cryptanalysis of Stickel's key exchange scheme. In *CSR 2008: Computer Science – Theory and Applications*, pages 283–288. Springer, 2008.
[74] V. M. Sidelnikov, M. A. Cherepnev, and V. V. Yashchenko. Public key distribution systems based on noncommutative semigroups. *Dokl. Akad. Nauk*, 332(5):566–567, 1993. Transl. in: Russian Acad. Sci. Dokl. Math. 48.2 (1994), 384–386.
[75] E. Stickel. A new method for exchanging secret keys. In *ICITA'05*, volume 2, pages 426–430. IEEE, 2005.
[76] I. M. Sulandra and A. N. Isnia. On square roots of matrices over the max-time semiring $\mathbb{R}_+$. In *Journal of Physics: Conference Series*, volume 1872, page 012014. IOP Publishing, 2021.

I. M. Buchinskiy, Sobolev Institute of Mathematics of SB RAS, Omsk, Russia
Email address: buchvan@mail.ru

M. V. Kotov, Independent Researcher
Email address: matvej.kotov@gmail.com

A. V. Treier, Sobolev Institute of Mathematics of SB RAS, Omsk, Russia
Email address: alexander.treyer@gmail.com