On complexity of the problem of solving systems of tropical polynomial equations of degree two

Matvei Kotov

(based on joint work with I. Buchinskiy and A. Treier)

Sobolev Institute of Mathematics of SB RAS

Conference “Combinatorial-computational methods of algebra and logic”, Omsk, July 19th, 2024

Tropical algebras

The extended set of real numbers $\mathbb{R} \cup \{\infty\}$ equipped with two binary operations $\oplus, \otimes$ defined by

$$\begin{aligned} x \oplus y &= \min(x, y), \\ x \otimes y &= x + y. \end{aligned}$$

is called the **min-plus algebra**.

If we consider $\mathbb{R} \cup \{-\infty\}$ and define $\oplus, \otimes$ as

$$\begin{aligned} x \oplus y &= \max(x, y), \\ x \otimes y &= x + y, \end{aligned}$$

we obtain the **max-plus algebra**.

Why is it called tropical?

The adjective *tropical* was coined by French mathematicians in honor of the Hungarian-born Brazilian computer scientist Imre Simon, who wrote on the field.

Tropical algebras

Since the max-plus and min-plus algebras are commutative idempotent semirings, then the following identities hold:

1. $(a \oplus b) \oplus c = a \oplus (b \oplus c)$,
2. $o \oplus a = a \oplus o = a$,
3. $a \oplus b = b \oplus a$,
4. $(a \otimes b) \otimes c = a \otimes (b \otimes c)$,
5. $e \otimes a = a \otimes e = a$,
6. $a \otimes b = b \otimes a$,
7. $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$,
8. $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$,
9. $o \otimes a = a \otimes o = o$,
10. $a \oplus a = a$,

where o is $-\infty$ for the max-plus algebra and is ∞ for the min-plus algebra, and e is 0.

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

Tropical algebras

For example, let's consider the max-plus algebra:

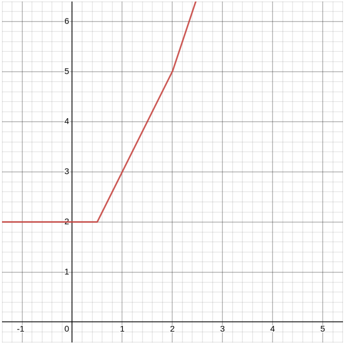
$$\begin{aligned} 4 \otimes (-6 \oplus -3) &= (4 \otimes -6) \oplus (4 \otimes -3) \\ &= -2 \oplus 1 \\ &= 1. \end{aligned}$$

Tropical polynomials

Consider, for example, the max-plus algebra. We can define a **tropical polynomial**:

$$p(x) = \bigoplus_{k=0}^{d} p_k \otimes x^{\oplus k} = \max_{1 \leq k \leq d} \{p_k + k \cdot x\}.$$

A max-plus polynomial is a convex, piecewise-linear function. For example, $p(x) = -1 \otimes x^{\otimes 3} \oplus 1 \otimes x^{\otimes 2} \oplus x \oplus 2$.



Tropical matrices

The set of all $n \times n$ matrices $\mathrm{Mat}_n(S)$ with entries from a semiring S can be equipped with operations $\oplus$ and $\otimes$ as defined below:

$$(a_{ij}) \oplus (b_{ij}) = (a_{ij} \oplus b_{ij})$$
$$(a_{ij}) \otimes (b_{ij}) = (a_{i1} \otimes b_{1j} \oplus \ldots \oplus a_{in} \otimes b_{nj}).$$

For example, let's consider two matrices over max-times algebra:

$$A = \begin{pmatrix} 1 & 2 \\ 0 & \infty \end{pmatrix}, B = \begin{pmatrix} 3 & 4 \\ 5 & 0 \end{pmatrix}.$$

Then

$$A \otimes B = \begin{pmatrix} 1 & 2 \\ 0 & \infty \end{pmatrix} \otimes \begin{pmatrix} 3 & 4 \\ 5 & 0 \end{pmatrix} =$$
$$\begin{pmatrix} 1 \otimes 3 \oplus 2 \otimes 5 & 1 \otimes 4 \oplus 2 \otimes 0 \\ 0 \otimes 3 \oplus \infty \otimes 5 & 0 \otimes 4 \oplus \infty \otimes 0 \end{pmatrix} =$$
$$\begin{pmatrix} 3 \oplus 10 & 4 \oplus 0 \\ 0 \oplus \infty & 0 \oplus 0 \end{pmatrix} = \begin{pmatrix} 10 & 4 \\ \infty & 0 \end{pmatrix}.$$

Tropical matrices

The obtained set of matrices also in an idempotent semiring. In other words, the following identities are true:

1. $(A \oplus B) \oplus C = A \oplus (B \oplus C)$,
2. $O \oplus A = A \oplus O = A$,
3. $A \oplus B = B \oplus A$,
4. $(A \otimes B) \otimes C = A \otimes (B \otimes C)$,
5. $E \otimes A = A \otimes E = A$,
6. $A \otimes (B \oplus C) = (A \otimes B) \oplus (A \otimes C)$,
7. $(A \oplus B) \otimes C = (A \otimes C) \oplus (B \otimes C)$,
8. $O \otimes A = A \otimes O = O$,
9. $A \oplus A = A$.

Let $A \in \mathrm{Mat}_n(\mathcal{S})$ and $p(x) = \bigoplus_{i=0}^{d} p_i \otimes x^{\otimes i}$, then we denote the matrix $\bigoplus_{i=0}^{d} p_i \otimes A^{\otimes i}$ by $p(A)$.

Applications

Tropical geometry has a lot of applications in combinatorial optimization, algebraic geometry, auction theory, mechanism design, game theory, scheduling etc.

In cryptography:

- Improved efficiency because the operations can be performed fast.
- Linear algebra attacks are not applicable.
- Systems of tropical equations are not easy to solve.

Also, there are ideas to add a tropical structure to neural networks:
[LANA:2021] Limonova, E., et al., Bipolar Morphological Neural Networks: Gate-Efficient Architecture for Computer Vision, IEEE Access 9 (2021): 97569–97581.
[PL:2023] Petrova A., Kazakevich, V., Application of the tropical mathematics apparatus in architecture of neural networks, Comp. Instr. Obraz. 3 (2023): 18–27.

Connection to optimization

Consider a weighted graph G. Let W be the weighted adjacency matrix.

Consider $W^{\otimes 2}$ in the min-plus algebra.

$$W^{\otimes 2} = (w_{ij}) \otimes (w_{ij}) = (w_{i1} \otimes w_{1j} \oplus \ldots \oplus w_{in} \otimes w_{nj})_{ij} =$$

$$= (\min(w_{i1} + w_{1j}, \ldots, w_{in} + w_{nj}))_{ij}$$

Therefore, we obtained the shortest distances among all the paths of length 2.

The third power gives as the shortest distances among all the paths of length 3, and so on.

The sum $W^{\otimes *} = I \oplus W \oplus W^{\otimes 2} \oplus W^{\otimes 2} \oplus \ldots$ gives as the shortest distances among all the paths.

Tropical Cryptography

Tropical cryptography is an area of cryptography in which different tropical algebraic structures are used as platforms for cryptographic protocols.

[GS:2014] Grigoriev, D., Shpilrain, V., Tropical cryptography, Comm. Algebra, 42(6), 2624–2632, 2014. (Preprint in 2011)
[GS:2019] Grigoriev, D., Shpilrain, V., Tropical cryptography II: extensions by homomorphisms, Comm. Algebra, 47(10), 4224–4229, 2019.
[CGS:2023] Chen J., Grigoriev D., Shpilrain V., Tropical cryptography III: digital signatures, Cryptology ePrint Archive, 2023.

Now, there are a few dozens papers and preprints devoted to tropical cryptography.

Sidelnikov, Cherepnev, and Yaschenko's key exchange

Sidelnikov, Cherepnev, and Yaschenko proposed the following key exchange method based on non-commutative semigroups.
Let G be a non-commutative semigroup, H and R be commutative subsemigroups of G, and $W \in G$.

1. Alice chooses as her secret key two elements $P_A \in H$ and $Q_A \in R$. She computes $K_A = P_A \cdot W \cdot Q_A$ and sends it to Bob.
2. Bob chooses as his secret key two elements $P_B \in H$ and $Q_B \in R$. He computes $K_B = P_B \cdot W \cdot Q_B$ and sends it to Alice.
3. Alice computes the common secret key $K_{AB} = P_A \cdot K_B \cdot Q_A$.
4. Bob computes the common secret key $K_{BA} = P_B \cdot K_A \cdot Q_B$.

They share the same key:
$P_A \cdot (P_B \cdot W \cdot Q_B) \cdot Q_A = P_B \cdot (P_A \cdot W \cdot Q_A) \cdot Q_B$.

[SCY:1993] V. Sidelnikov, M. Cherepnev, and V. Yashchenko, Systems of open distribution of keys on the basis of noncommutative semigroups, Dokl. RAN., 332.5, 566–567, 1993

Linear decomposition attack

[MR:2015] A. Myasnikov, V. Roman'kov, A linear decomposition attack, Groups, Complexity, Cryptology, 2015, 7, 81–94

In this paper, the authors offered a new attack on several known group-based cryptosystems. This attack gives a polynomial time deterministic algorithm that recovers the secret shared key from the public data in all the schemes under consideration. They showed show that in this case the typical computational security assumptions are not very relevant to the security of the schemes, i.e., one can break the schemes without solving the algorithmic problems on which the assumptions are based.

For more information:
[R:2020] V. Roman'kov Algebraic cryptology, Omsk, Omsk State University Press, 2020

Cryptanalysis

[KU:2018] M. Kotov, A. Ushakov, Analysis of a key exchange protocol based on tropical matrix algebra, J. Math. Cryptol., 12.3, 2018, 137–141

[MS:2020] A. Muanalifah, S. Sergeev, Modifying the tropical version of Stickel's key exchange protocol, Appl. Math., 65.6, 727–753, 2020.

[BKT:2023] I. Buchinskiy, M. Kotov, A. Treier, Analysis of four protocols based on tropical circulant matrices, Cryptology ePrint Archive, 2023, also submitted to IJPA

[ACS:2023] S. Alhussaini, C. Collett, S. Sergeev, Generalized Kotov-Ushakov Attack on Tropical Stickel Protocol Based on Modified Tropical Circulant Matrices, Cryptology ePrint Archive, 2023.

Problem 1

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

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

Problem 1

Therefore, we have the following system of equations:

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

or, using the max and $+$ signs,

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

To solve this system, heuristics algorithms are used. It is interesting to know the complexity of this problem.

Problem 1

Let us forget how we get the numbers T^{ij}_{kl}. We will consider the following problem:

Problem 1

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

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

Polynomials

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.

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.

Systems

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

$$A \otimes X = B,$$

and any two-sided system of tropical linear equations as

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

One-sided systems of linear equations

(We will consider the max-plus algebra $\mathbb{Z}_{\max,+}$.)

It is easy to find a solution to a one-sided system of tropical linear equations $A \otimes X = B$.

The vector

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

is called the **principal solution** to this system.

It is known that this system has a solution if and only if $\overline{x}$ is a solution.

Moreover, let $M_j = \operatorname{argmax}(a_{ij} - b_i)$, then the system has a solution if and only if $\bigcup_j M_j = \{1, \ldots, m\}$, where m is the number of equations.

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.

[B:2010] Butkovič, P.: Max-linear systems: theory and algorithms. Springer, London (2010).

Two-sided systems

It was proven by Bezem, Nieuwenhuis, and Rodríguez-Carbonell 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 $\cap$ co-NP.

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

Theorem 1

Grigoriev and Shpilrain proved the following theorem.

Theorem ([GS:2014])

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 ([GS:2014])

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 still not enough because this class of systems is wider than the class in Problem 1.

Theorem 1

We prove the following theorem.

Theorem (BKT, 2023)

Problem 1 is NP-complete.

Problem 1

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

$$\bigoplus_{1 \leq i,j \leq n} a_{kij} \otimes x_i \otimes y_j = 0, \ 1 \leq k \leq m. \tag{2}$$

Theorem 2

To prove this theorem, we need the following result.

Theorem

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

$$\bigcup_{(i,j)\in C} S_{ij} = \{1, \ldots, m\} \tag{3}$$

and

$$\begin{array}{l} x_i + y_j = c_{ij} \text{ if } (i,j) \in C, \\ x_i + y_j \leq c_{ij} \text{ otherwise.} \end{array} \tag{4}$$

This theorem shows that a solution can be obtained as a solution of linear programming problem.

The idea of the proof of Theorem 1

We will reduce the 3-SAT problem to this problem.
Let us have a 3-CNF $\varphi(u_1, \ldots, u_n)$ that has m clauses.
For every variable u_i, we include the following pair of equations:

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

and

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

Note that $x_{2i-1} \otimes y_{2i-1}$ and $x_{2i} \otimes y_{2i}$ cannot be equal to 2 at the same time.
For a clause with three literals $u_i^\alpha \vee u_j^\beta \vee u_k^\gamma$, we include the following equation:

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

Problem 1 is in NP becase we can obtain a solution to the system as a solution to a linear programming problem using Theorem 2.

Generic-case complexity

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 $l\colon I \to \mathbb{N}$ such that the inverse image of every integer is finite.
The corresponding spherical stratification is formed by spheres $S_n = \{x \in I \mid l(x) = n\}$. For a subset $A \subseteq I$ and a stratification $\{I_n\}$, the limit

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

(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**.

Generic-case complexity

An algorithm $\mathcal{A}\colon I \to J \cup \{?\}$ 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 3

Theorem (BKT, 2023)

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 $Sat(Sys(m, n, \mathbb{Z}_{\geq 0})) = 0$ 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 4

Theorem (BKT, 2023)

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.

[BKT:2024] Buchinskiy I., Kotov M., Treier A., On complexity of the problem of solving systems of tropical polynomial equations of degree two, Cryptology ePrint Archive, 2024.

Thank you!