令和2年度＜若手研究_再公募＞共同利用研究報告書

2021年05月09日

九州大学　マス・フォア・インダストリ研究所長 殿

所属・職名 筑波大学　システム情報系・研究員
Jo Hyungrok

下記の通り共同研究の報告をいたします。

記

		整理番号	20200030	
1.研究計画題目	トロピカル楕円曲線論における計算困難問題の探究と暗号技術への応用			
2.新規・継続	新規			
3.種別	若手研究			
4.種目	短期研究員			
5.研究代表者	氏名	Jo Hyungrok		
	所属 部局名	筑波大学　システム情報系	職名	研究員
6.研究実施期間	2021年03月23日(火曜日)～2021年03月26日(金曜日)			
7.キーワード	暗号理論、楕円曲線暗号、トロピカル幾何			
8.参加者人数	2人			

9.本研究で得られた成果の概要

楕円曲線理論では、有限体上の楕円曲線の点PとQが与えられたとき、離散対数log_P Q を求める問題を楕円曲線上の離散対数問題と呼ぶ。楕円曲線上の離散対数問題は暗号への応用があり、特に、公開鍵暗号技術によく使われている。しかし、楕円曲線上の離散対数問題を現実的な時間内で解ける量子アルゴリズムの発見から、量子アルゴリズムに耐性を持つ新しい暗号技術が要求されている。

本研究の目的は、トロピカル楕円曲線にも群構造があることに着目し、楕円曲線上の離散対数問題の代替として、トロピカル楕円曲線上の離散対数問題を設計し、その問題の困難性について調査することであった。

結論から言うと、トロピカル楕円曲線上の離散対数問題は定義可能であるが、暗号に使えるほどの強度を達成するものではないことがわかった。 群構造の側面から既存の楕円曲線と異なる大きな違いの一つは、トロピカル楕円曲線の群構造は、トロピカル楕円曲線内で唯一に存在するサイクル上で定義され、単位円と同型となる。つまり、トロピカル楕円曲線のサイクル上の点PとQが与えられたとき、離散対数log_P Q を求める問題は、ユークリッドノルム持つ実数上の単位円で距離を測定する問題に帰着し、問題は平易となる。難しい問題へ修正する一つの案として、有限体上のトロピカル楕円曲線を考えることが挙げられるが、今までの調査ではそのような研究は知られておらず、トロピカル幾何の構成から言うと不可能かもしれない。今回の研究は研究期間が短く、この問題についてはまだまだ様々な側面から再考する余地があると思われる。

一方、耐量子計算機暗号（Post-Quantum Cryptography）の中で同種写像暗号（Isogeny-based cryptography）という研究分野がある。それは超特異楕円曲線の同種写像関係における計算困難問題を安全性の根拠としている。最近では、超特異楕円曲線理論のトロピカルバージョンが研究され、トロピカル楕円曲線理論が精巧に具体化されている。このことから、同種写像暗号の類似研究から考えられる別のシードとしてトロピカル超特異楕円曲線理論を調査・研究することは興味深いことと思われ、今後の課題となる。

On computational hard problems and cryptographic applications based on tropical elliptic curve theory

Hyungrok Jo *

University of Tsukuba

Contents

*jo.hyungrok.gb@u.tsukuba.ac.jp

1 Introduction

This is a report of *"2020 IMI collaborative research program - young researcher - short period visiting scholar".*

This research mainly studies on computational hard problems of tropical elliptic curves, which have not been used for cryptographic applications in order to propose a new generation of cryptographic schemes. Since there is a view of "tropicalized" elliptic curves over a valuation ring in tropical geometry, it is a deep relationship with algebraic geometry. Especially, there are some variational approaches corresponding to the classical theory of elliptic curves over a projective plane, in recent, Riemann-Roch theorem is established in a way of tropical elliptic curves.

While, in an arithmetic of elliptic curves, Elliptic Curve Cryptography (ECC) is considered from a discrete logarithm problem based on the group structure of elliptic curves, which put to practical use especially for supporting a security in the era of IoT (Internet of Things). In fact, even though there are some cryptographic approaches of tropical algebra or tropical matrix algebra (which is considered as semirings) which is essentially a Diffie-Hellman-like key establishment mechanism based on the elementary tropicalized algebraic structures so far, it is not known that the study on a discrete logarithm problem over tropical elliptic curves. From these reasons, this research on the tropicalization of Elliptic Curve Discrete Logarithm Problem (ECDLP) is challenging and also has a potentiality which can be considered as a seed to propose a new hard computational problem for cryptographic applications. In addition, we investigate on the possibilities of usages for cryptographic applications, which come from the tropicalization of the existing hard computational problems over elliptic curves such as an isogeny path problem. We study on the possibilities of tropical elliptic curves which have not been suggested as cryptographic applications, so we expect to broaden a way of cryptography.

1.1 Related work

Tropical algebra. In 1988, Imre Simon, a Brazilian mathematician, introduced *min-plus* (or *max-plus*) *algebra*. In 1997, Jean-Eric Pin et al. named "*Tropical-*". It has been studied from the introduction of tropical algebra, especially on tropical geometry, it is well described in the textbook written by Maclagan and Sturmfels [11]. Please refer it if the readers get interested in. Essentially, it is developed by some purposes of solving problems in algebraic geometry and classifying curves using the theories of algebraic geometry and combinatorics.

Tropical elliptic curves. There are some tropicalized progress on a theory of elliptic curves along the classical theory of them. One of the main result on *tropical elliptic curve* is that there is a group law on tropical elliptic curve as a Jacobian of tropical elliptic curves by Vigeland [17]. Helmink [6] and Otter [14] described some preliminaries and improvements on the study of tropical elliptic curves, respectively. Chan and Stumpfels gave some graphic descriptions of tropical elliptic curve as a "honeycomb". Brandt and Helmink developed these theories to supersingular elliptic curves and in a moduli space.

Cryptographic applications of tropical algebra. Grigoriev et al. [4] suggested the Diffie-Hellman like key establishment mechanism based on [16] over non-commutative group. In 2019, Grigoriev et al. [5] added the operation which is called adjoint multiplication. About these progresses, Mach [10] (master's thesis) gave the introductory survey on cryptography based on semirings with some implementations by Python. In 2020, Muanalifah, Sergeev [13] showed the discrete logarithm problems over tropical semidirect product in IACR eprint.

2 The progress of program

This work is mainly discussed with Prof. Ikematsu Yasuhiko in IMI, Kyushu University. The work progress is appeared in the table as below:

Date	Summary
Online	
Feb. 18	Establish the research plan
Feb. 23	Learn preliminaries on tropical elliptic curves (I)
Mar. 4	Learn preliminaries on tropical elliptic curves (II)
Mar. 12	Explore the open source (SINGULAR) with tropical:geometry.lib
Mar. 19	Landscape : The group law of tropical elliptic curves (Vigeland [17])
Mar. 21	Landscape : The group law of tropical elliptic curves (Otter [14])
Mar. 22	Plan on-site research and preparing for a report
On-site (IMI, Kyushu University)	
Mar. 23	Tropical elliptic curve - Newton polytope, Subdivision
Mar. 24	Tropical elliptic curve - Divisor and explicit examples
Mar. 25	Checked the group law and its cryptographic promise
Mar. 26	Organizing contents in a report

3 Preliminaries

Tropical geometry is a variant of algebraic geometry whose "polynomial graphs" look like a piecewise linear polygonal nets, and whose based numbers in the "tropical semiring". Throughout the report, our ultimate purpose is to understand the group law of tropical elliptic curve which is mainly described in [14, 17] and estimate the hardness of a variant of discrete logarithm problem in a sense of tropical elliptic curve theory. Most contents of the computational results in this report are implemented by SINGULAR; a computer algebra system for polynomial computations. (Especially, tropical:geometry.lib is used.)

In this section, we give some basic notations of tropical geometry and its theories as in [17].

3.1 Tropical semiring: Max-plus algebra

For a usage through the report, we define the *tropical semiring*. Comparing to the classical study of polynomials, the differences are their own operations. i.e., addition is replaced with minimum (or maximum) and multiplication is replaced with ordinary addition. So tropical geometry has been mainly studied its geometric properties when the classical operations are replaced with.

In the majority of tropical related works, it seems to be prefer that addition is replaced with minimum, but in Vigeland's work [17], maximum is used. In this context, we consider that additive operation $\oplus$ is the maximum and multiplicative operation $\odot$ is ordinary addition on real numbers $\mathbb{R}$ with the negative infinity $-\infty$. It is called as the *max-plus algebra*. With minimum replaced by maximum we get the min-plus algebra on $\mathbb{R} \cup \{\infty\}$, which is isomorphic to the max-plus algebra.

In other words, the tropical semiring $(\mathbb{R} \cup \{-\infty\}, \oplus, \odot)$ simply can be defined by the basic arithmetic operations of addition and multiplication of real numbers as follows:

$$x \oplus y := \max(x, y) \quad \text{and} \quad x \odot y := x + y,$$
$$x \oplus -\infty := x \quad \text{and} \quad x \odot 0 := x.$$

We note that the negative infinity is the identity element for addition and zero is the identity element for multiplication. For example, the tropical sum of 5 and 13 is 13 ($5 \oplus 13 = \max(5, 13) = 13$) and the tropical product of 5 and 13 is 18 ($5 \odot 13 = 5 + 13 = 18$). Both addition and multiplication are commutative, associative, and distributive.

We also note that each identity acts as follows:

$$x \odot -\infty = -\infty \quad \text{and} \quad x \oplus 0 = \begin{cases} 0 & \text{if } x \leq 0, \\ x & \text{if } x > 0. \end{cases}$$

Tropical division can be defined to be classical subtraction, so $(\mathbb{R} \cup \{-\infty\}, \oplus, \odot)$ satisfies all ring axioms only except for the existence of an additive inverse.

A tropical polynomial f in n-variables $x_1, \ldots, x_n$ is a finite linear combination of tropical monomials:

$$f(x_1, \ldots, x_n) = a \odot {x_1}^{i_1} {x_2}^{i_2} \cdots {x_n}^{i_n} \oplus b \odot {x_1}^{j_1} {x_2}^{j_2} \cdots {x_n}^{j_n} \oplus \cdots .$$

Here the coefficients $a, b, \ldots$ are real numbers and the exponents $i_1, j_1, \ldots$ are integers.

When evaluating a tropical polynomial function $f : \mathbb{R}^n \to \mathbb{R}$, we have the maximum of a finite collection of linear functions,

$$f(x_1, \ldots, x_n) = \max(a + i_1 x_1 + i_2 x_2 + \cdots + i_n x_n, b + j_1 x_1 + j_2 x_2 + \cdots + j_n x_n, \cdots).$$

We define the *hypersurface* $V(f)$ of f to be the set of all points $w \in \mathbb{R}^n$ at which this maximum is attained at least twice. Namely,

$$\begin{aligned} V(f) = \{w \in \mathbb{R}^n \mid \exists k \neq j \text{ s.t. } ev(f)(w) \quad &= ev(\textstyle\bigoplus_k a_k \odot x_1^{k_1} \odot \cdots \odot x_n^{k_n})(w) \\ &= ev(\textstyle\bigoplus_j a_j \odot x_1^{j_1} \odot \cdots \odot x_n^{j_n})(w)\}, \end{aligned}$$

where ev is the usual evaluation map.

3.2 Newton Polytope and Subdivision

Through the report from this subsection, we consider a tropical polynomial f in two variables x, y:

$$f(x, y) = \bigoplus_{(i,j)} c_{ij} \odot x^i \odot y^j.$$

Definition 3.1. Let $f(x, y)$ be a tropical polynomial in two variables. Its Newton polytope Δ_f is defined as the convex hull of the set of points (i, j) in $\mathbb{R}^2$ such that $x^i y^j$ appears in the expansion of $f(x, y)$. The corresponding tropical hypersurface $V(f)$ is a *plane tropical curve.*

First, we consider a tropical polynomial as

$$f(x, y) = a \odot x \oplus b \odot y \oplus c, \quad \text{where } \ a, b, c \in \mathbb{R}.$$

Then the tropical hypersurface $V(f)$ is called a *tropical line* in the plane, and consists of all points (x, y) where the function

$$f : \mathbb{R}^2 \to \mathbb{R}, (x, y) \mapsto \max(a + x, b + y, c)$$

is not linear. It consists of three half-rays emanating from the point $(x, y) = (c - a, c - b)$ into the down, left, and upper-right directions.

Second, we consider a quadratic polynomial

$$f(x, y) = a \odot x^2 \oplus b \odot xy \oplus c \odot y^2 \oplus d \odot y \oplus g \odot x \oplus e.$$

We assume that the coefficients $a, b, c, d, e, g \in \mathbb{R}$ satisfy the inequalities

$$b + g > a + d, \quad d + g > b + e, \quad b + d > c + g.$$

Then, we have the graph of $f : \mathbb{R}^2 \to \mathbb{R}$ as an angled-dome shape in $\mathbb{R}^3$. Here, this angled-dome shape lies the tropical curve $V(f) \subset \mathbb{R}^2$ on xy-plane.

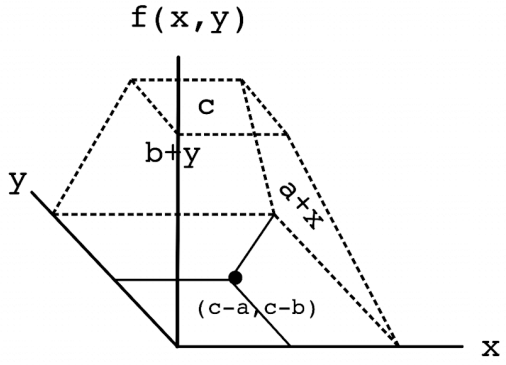


Figure 1: $f(x, y) = a \odot x \oplus b \odot y \oplus c$

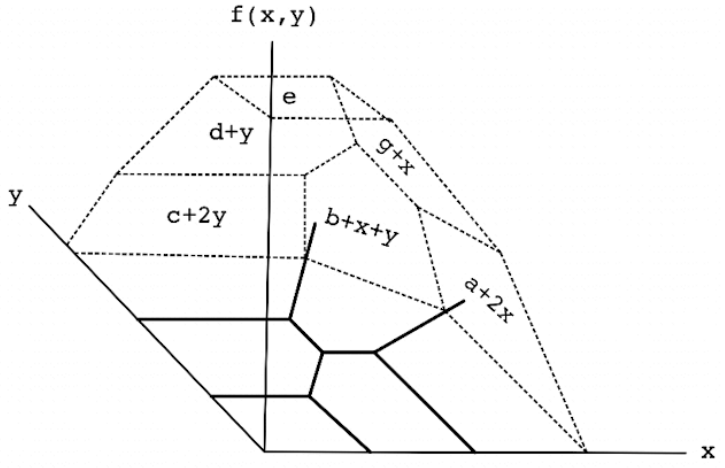


Figure 2: $f(x, y) = a \odot x^2 \oplus b \odot xy \oplus c \odot y^2 \oplus d \odot y \oplus g \odot x \oplus e$

In general, it is known that if $f(x, y)$ is a tropical polynomial, then its curve $V(f)$ can be constructed more easily from its Newton polytope Δ_f. The planar graph dual to $V(f)$ is a *subdivision* of Δ_f into smaller polytope. This subdivision is, of course, determined by the coefficients of f. The unbounded rays of a tropical curve $V(f)$ are perpendicular to the each edge of the Newton polytope.

For defining the degree of a tropical curve, we focus on tropical curves whose Newton polytopes are the standard triangles Γ_d with vertices $(0, 0), (0, d)$, and $(d, 0)$. We can refer to such a curve, obviously, as a curve of degree d.

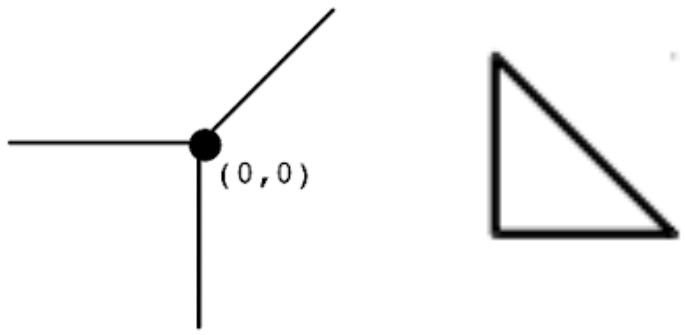
Definition 3.2. Let $C = V(f)$ be a tropical curve in $\mathbb{R}^2$, and let Δ_f be the Newton polytope of f. If Δ_f fits inside Γ_d, but not inside Γ_{d-1}, then C has *degree* d. If $\Delta_f = \Gamma_d$, we say that C has degree d with full support.

A vertex v of a tropical curve is called 3-*valent* if v has exactly 3 adjacent edges. If these edges have weights m_1, m_2, m_3 and *primitive integer direction vectors* $\mathrm{u} = (u_0, u_1), \mathrm{v} = (v_0, v_1), \mathrm{w} = (w_0, w_1)$ respectively, we define the *multiplicity* of V to be the absolute value of the number

$$m_1 m_2 \begin{vmatrix} u_0 & u_1 \\ v_0 & v_1 \end{vmatrix} = m_2 m_3 \begin{vmatrix} v_0 & v_1 \\ w_0 & w_1 \end{vmatrix} = m_1 m_3 \begin{vmatrix} w_0 & w_1 \\ u_0 & u_1 \end{vmatrix}.$$

From subsection 4.4, we consider the primitive integer direction vectors as standard as

Figure 3: Tropical line and its subdivision



(a) Tropical line $f = x \oplus y \oplus 1$. (b) Its subdivision Δ_f.

$\mathrm{u} = (-1, 0), \mathrm{v} = (0, -1), \mathrm{w} = (1, 1)$.

4 The group law on a tropical elliptic curve

In Vigeland's work [17], it is described that the group law of a tropical elliptic curve in the similar context from one of the classical elliptic curves. In Otter's thesis [14], it contains some improvements of Vigeland's work and more specific explanations about the group law of a tropical elliptic curve. Throughout this section, we refer to [14, 17].

A tropical curve is called *smooth* if every vertex is 3-valent and has multiplicity 1. Then, we can define the *genus* of a smooth tropical curve $C = V(f)$ is the number of vertices of Subdiv_f in the interior of the Newton polytope Δ_f.

4.1 The Z-metric

For a later usage, it is essential to define a metric on a tropical curve. Let $C \subseteq \mathbb{R}^2$ be a smooth tropical curve. If E is any edge of C, we define a metric on E called the **Z**-*metric*, in the following way. For any two points $\mathrm{x}, \mathrm{y} \in E$, we set their distance in the **Z**-metric to be the number $\frac{||\mathrm{x}-\mathrm{y}||}{||\mathrm{v}||}$, where $||\cdot||$ denotes the Euclidean norm, and v is a primitive integral direction vector of E. If E is a bounded edge, we define its *lattice length*, $\ell(E)$, to be the distance (in the **Z**-metric) between its endpoints.

4.2 Tropical Bezout's Theorem

In this subsection, we give some facts from [17] [14] . It is said that two tropical curves C and D intersect *transversally* if any vertex of C does not lie on D and vice versa. In the case of a transversal intersection, we define intersection multiplicities as follows: Let P be an intersection point of C and D, where the two edges meet with each weight m_1, m_2, and primitive direction vector (v_0, v_1), (w_0, w_1) respectively. Then the *intersection multiplicity* $\mathrm{mult}_P(C \cap D)$ is the absolute values of

$$m_1 m_2 \begin{vmatrix} v_0 & v_1 \\ w_0 & w_1 \end{vmatrix}.$$

In the case of non-transversal intersection, we define the intersection multiplicity differently as follows: For any intersecting tropical C and D, let C_ϵ and D_ϵ be nearby translations of C and D such that C_ϵ and D_ϵ intersect transversally.

Then we have a useful fact. We say the *stable intersection* of C and D, denoted $C \cap_{st} D$, be defined by

$$C \cap_{st} D = \lim_{\epsilon \to 0}(C_\epsilon \cap D_\epsilon),$$

where this limit is independent of the choice of perturbations, and is a well-defined subset of points with multiplicities in $C \cap D$. Then we know that if two tropical curves C and D of degrees c and d respectively having full supports, then their stable intersection are cd points, as counting multiplicities. This is a tropical variant of Bezout's theorem in algebraic geometry.

As a special case of this *tropical Bezout's theorem*, i.e., if at least one of the curves have full support, it holds. From this fact, we can have a useful result as its corollary if we consider that one of the curves is a tropical line C (,which is a tropical curve of degree 1) and the other is a tropical curve D of degree d, it still hold that they meets in exactly d points. Now, we can guarantee that our targeting group law is realized by the drawing tropical line over a tropical elliptic curve in conformity with their degrees.

4.3 Divisor

Let C be a smooth tropical curve in $\mathbb{R}^2$. For defining the Jacobian of curves, we first define the *group of divisors* on C, $\mathrm{Div}(C)$. It is the free abelian group generated by the points on C. A *divisor* D on C is an element of $\mathrm{Div}(C)$, which can be described as a finite formal sum of the form $\mathrm{D} = \sum \mu_P P$. In here, $\sum \mu_P$ is called the *degree* of D. The elements of degree 0 in $\mathrm{Div}(C)$ form a group, denoted by $\mathrm{Div}^0(C)$.

Given a tropical polynomial f, we now define the divisor $\mathrm{div}(f) \in \mathrm{Div}(C)$ as the formal sum of points in $C \cap_{st} V(f)$, which is counted with their respective intersection multiplicities $\mathrm{mult}_P(C \cap V(f))$. It is said to a *tropical rational function* $h : \mathbb{R}^2 \to \mathbb{R}$ of the form $h = f - g$, where f and g are tropical polynomials having same Newton polytopes. Here, if $h = f - g$ is a tropical rational function on $\mathbb{R}^2$, we set $\mathrm{div}(h) := \mathrm{div}(f) - \mathrm{div}(g)$. A divisor $\mathrm{D} \in \mathrm{Div}(C)$ is called a *principal divisor* if $\mathrm{D} = \mathrm{div}(h)$ for some tropical rational function h. It is said that two divisors D_1 and D_2 are *linearly equivalent*, denoted as $\mathrm{D}_1 \sim \mathrm{D}_2$, if $\mathrm{D}_1 - \mathrm{D}_2$ is principal.

Definition 4.1. The group $\mathrm{Div}^0(C)/\sim$ is called the *Jacobian* of C, $\mathrm{Jac}(C)$.

4.4 Tropical elliptic curve and its group law

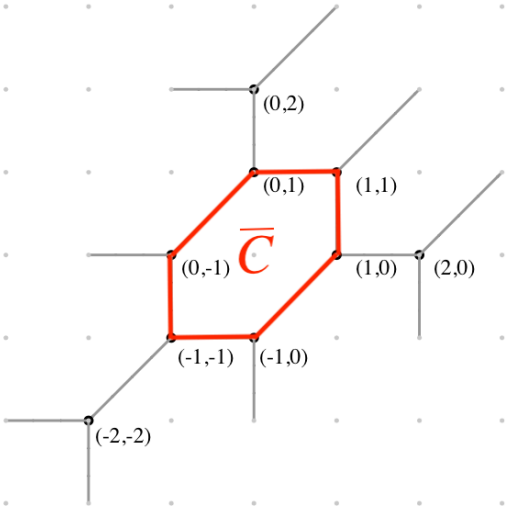
It is said to be a *tropical elliptic curve* C, if a tropical curve is smooth and of degree 3 with genus 1. We assume that $C = V(f)$, where $f(x, y)$ has Newton polytope $\Delta_f \subseteq \Gamma_3$. C contains a unique cycle, which we will denoted by $\overline{C}$. Each connected component of $C \setminus \overline{C}$ is called a *tentacle* of C. In Figure (4a), we can check the unique cycle $\overline{C}$ in $V(f)$ and subdivision Δ_f of a tropical curve $f = 3 \odot x^3 \oplus x^2y \oplus xy^2 \oplus y^3 \oplus x^2 \oplus xy \oplus y^2 \oplus x \oplus y \oplus 3$ as a toy-example. Now we have three important facts from [17] as belows:

1. The explicit homeomorphism $\mu : \overline{C} \to \mathbb{R}/\ell\mathbb{Z} \simeq S^1$.

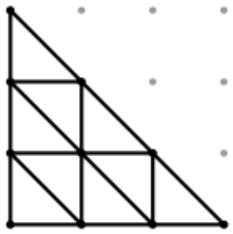
As a topological space, $\overline{C}$ is homeomorphic to the circle group S^1. We first choose any fixed point $O \in \overline{C}$. We put $V_1, \ldots, V_n$ as the vertices of $\overline{C}$ in counter-clockwise direction, such that if O is a vertex then $V_1 = O$, otherwise O lies between V_1 and V_n. We also put $E_1, \ldots, E_n$ as the edges of $\overline{C}$, such that $E_1 = V_1V_2$ and so on. Then we recall that for each i, $\ell(E_i)$ denotes the length of E_i in the $\mathbf{Z}$-metric on E_i. We say that ℓ is the *cycle length* of $\overline{C}$, i.e., $\ell = \ell(E_1) + \cdots + \ell(E_n)$.

Now we define a homeomorphism $\mu : \overline{C} \to \mathbb{R}/\ell\mathbb{Z} \approx S^1$, linear in the Euclidean metric of each edge E_i. It is then enough to specify the images in $\mathbb{R}/\ell\mathbb{Z}$ of the points $O, V_1, \ldots, V_n$, which we do recursively:

$$\begin{aligned} &\mu(O) = 0 \\ &\mu(V_1) = \ell(OV_1) \\ &\mu(V_{i+1}) = \mu(V_i) + \ell(E_i), \qquad\qquad i = 1, \ldots, n-1. \end{aligned}$$



(a) Tropical elliptic curve f.



(b) Its subdivision Δ_f.

We identify $\mathbb{R}/\ell\mathbb{Z}$ with the interval $[0, \ell)$, and we define the *displacement function* $d_C : \overline{C} \times \overline{C} \to \mathbb{R}$ by the formula

$$d_C(P, Q) = \mu(Q) - \mu(P).$$

Then, d_C is also satisfied with $d_C(Q, P) = -d_C(P, Q)$ for any $P, Q \in \overline{C}$. Furthermore, for any three points $P, Q, R \in \overline{C}$ we have

$$d_C(P, Q) + d_C(Q, R) = d_C(P, R).$$

2. Two points on C are linear equivalent?

The essential fact in here is that any two points on the same tentacle are linearly equivalent, while two distinct points on $\overline{C}$ are not linearly equivalent. In other words, there are facts that if P, Q are points on the same tentacle $C \setminus \overline{C}$, then $P \sim Q$ and if $P, Q \in \overline{C}$ and $P \sim Q$, then $P = Q$.

3. The group law

Set-theoretically, the Jacobian $\mathrm{Jac}(C)$ is equal to $\overline{C}$. So, we describe the resulting group structure on $\overline{C}$. The most important procedure is to determine when divisors of the $P + Q$ are linearly equivalent. Comparing to the classical case, we have the following problem: Given two points P and Q on $\overline{C}$, we cannot always find a tropical line L that intersects C stably in P and Q. If there exists such a tropical line, we call (P, Q) a *good pair*. If not, we call (P, Q) a *bad pair*.

Let P, Q, P', Q' be any points on $\overline{C}$. Then

$$P + Q \sim P' + Q' \iff d_C(P, P') = -d_C(Q, Q').$$

It means that even if we drag each point P and Q along $\overline{C}$ to P' and Q' in opposite directions, addition of P and Q is linearly equivalent to addition of P' and Q'. Furthermore, for any fixed point $O \in \overline{C}$, if we define the map $\tau_O : \overline{C} \to \mathrm{Jac}(C)$ given by $P \mapsto P - O$, τ_O is a bijection. Thus, $\overline{C}$ with a fixed point O consisting of points on $\overline{C}$ is naturally a group, which is induced from $\mathrm{Jac}(C)$ by an isomorphism τ_O. We denote the group above as $(\overline{C}, O)$.

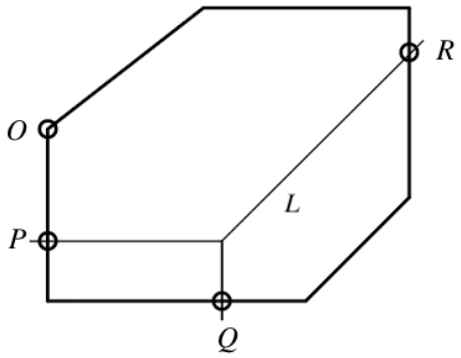
If P and Q are arbitrary points on $\overline{C}$, and $+$ denote addition in the group $(\overline{C}, O)$ in here, then the point $P + Q$ satisfies the relation

$$d_C(O, P + Q) = d_C(O, P) + d_C(O, Q).$$

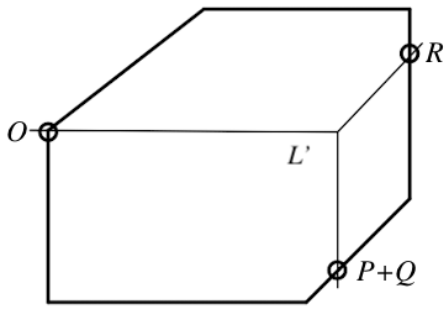
Since the definition of the displacement, we have $\mu(P) = d_C(O, P)$. It yields that

$$\mu(P+Q) = d_C(O, P+Q) = d_C(O, P) + d_C(O, Q) = \mu(P) + \mu(Q).$$

Thus, the map $\mu : (\overline{C}, O) \to \mathbb{R}/\ell\mathbb{Z} \approx S^1$ is actually a group isomorphism.



(a) P and Q :
Intersecting with a tropical line L.



(b) R and O :
Intersecting with a tropical line L'.

Geometrically, we can describe the group law. If (P, Q) is a good pair, consider the tropical line L through P and Q, and let R be the third intersection point of L and $\overline{C}$ as seen in Figure (5a). If (P, Q) is a bad pair, we move the two points equally with the **Z**-metric in opposite directions until they are a good pair. And we use this new pair (say, (P', Q')) to find the third intersection point of L and $\overline{C}$.

Now if (R, O) is a good pair, let L' be the through R and O. Then $P + Q$ is the third intersection point of L' and $\overline{C}$ as seen in Figure (5b). If (R, O) is a bad pair, in the same manner, we move the two points equally with the **Z**-metric in opposite directions until they are a good pair. And we use this new pair (say, (R', O')) to find the third intersection point of L' and $\overline{C}$, which is finally the point $P + Q$.

We note that the third point of intersection of tropical line L and L' on $\overline{C}$ does not depend on the distances that two points moved from the position of a bad pair. Refer to **Lemma 72.** in Otter's work [14].

5 Hardness of tropical elliptic curve discrete logarithm problem

We start from how to double a point P on $\overline{C}$. In order to add a point P to itself, apply the method to add two points are a bad pair (P, P). We move the point P along the cycle $\overline{C}$ to P' and P'' in opposite directions until two points (P', P'') form a good pair as described in Figure 6. Then, we use this pair (P', P'') to find the third intersection point R of L and $\overline{C}$. In a natural sense, we can find the doubling point $2 \cdot P$ in the same manner of Section 4.4.

If we iterate this procedure by n-times, we can calculate $n \cdot P$. However, as we studied so far, since $n \cdot P$ on $\overline{C}$ is equal to $n \cdot \mu(P)$ on $\mathbb{R}/\ell\mathbb{Z}$, it is possible to consider it on the interval $[0, \ell)$ with **Z**-metric, which means tropical ECDLP reduces to DLP on the $[0, \ell)$ with **Z**-metric.

Now, as a material of discrete logarithm problem, we can define a variant of elliptic curve discrete logarithm problem in tropical version as belows:

Definition 5.1 (Tropical Elliptic Curve Discrete Logarithm Problem)**.** Find $n \in \mathbb{Z}$ if P and Q in $\mathbb{R}/\ell\mathbb{Z}$ are given satisfying

$$Q = n \cdot P \text{ in } \mathbb{R}/\ell\mathbb{Z}.$$

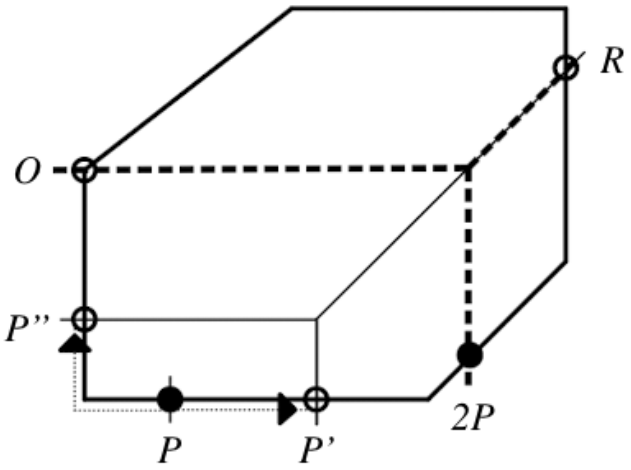


Figure 6: $2 \cdot P$: doubling the point P

It is obvious that $P/\ell, Q/\ell \in \mathbb{R}/\mathbb{Z}$. Thus, without loss of generality, we only consider when $\ell = 1$. If $P \in \mathbb{Q}$, it is easy to find such n. If $P \in \mathbb{R} \setminus \mathbb{Q}$, it can be solved in a similar way. For example, we can set $P := \sqrt{2} - 1$ then $n \cdot P$ can be described as $Q = n\sqrt{2} - m_n$ for some n, m_n. Then, it is also easy to find such n. Comparing with the case of classical elliptic curves, tropical ECDLP does not depend on its own equation except only its own cycle. This fact implies inferior security to the tropical elliptic curve discrete logarithm problem. It seems more vulnerable to the existing attack for DLP.

6 Results and after the collaborative research program

In a theory of classical elliptic curves, there is a problem finding $\log_P Q$ when two points P and Q are given from an elliptic curve over a finite field. We call it Elliptic Curve Discrete Logarithm Problem (ECDLP). Furthermore, ECDLP is applied to cryptography, nowadays we use it many crypto systems as standardized all over the world. However, since the practicality of quantum algorithms, which can solve ECDLP in realistic time, is getting increased, new crypto systems having anti quantum attacks are required. In this research, from the observation that the group law of tropical elliptic curves was existed (rarely known except tropical experts), as an alternate of the existed ECDLP threatened by quantum algorithms, we construct a tropical version of ECDLP and investigate on its difficulty.

As a result, at least in terms of our arguments, Tropical ECDLP appeared not to be hard enough than DLP or ECDLP. One of the main differences on the group law between the classical and the tropical version is coming from the Jacobian of each curve. In classical case, Jacobian ($\mathrm{Div}^0(C_o)$) of classical elliptic curves C_o is itself. In tropical case, Jacobian ($\mathrm{Div}^0(C)$) of tropical elliptic curve C is a subset of its curve, which is the cycle $\overline{C}$ in tropical curve. Additionally, there is a homeomorphism between $\overline{C}$ and a unit circle S^1. It means the tropical version of ECDLP turns out finding $\log_P Q$ when the point P and Q on a unit circle which is defined over a real number with a Euclidean norm. As far as we know, it has not been known that there is a tropical elliptic curve over a finite field or preserving a discreteness by base-field changes as a classical elliptic curve over a finite field. It seems not possible to have one based on the preliminaries of tropical geometry. However, the research period was not long enough, there are still several assignments we should consider about. (A combinatorial product of multiple tropical elliptic curves, base-field change, etc.)

While, there is a field of study, called Isogeny-based cryptography which is one of main

candidates in Post-Quantum Cryptography. Roughly speaking, the security of Isogeny-based cryptography is essentially based on the hardness of finding isogeny of a given degree between supersingular elliptic curve. In a sense of its far-reaching effects, it is an indispensable task to consider a tropical version of isogeny problems. In recent, several variants of supersingular elliptic curves as a version of tropical geometry are introduced, it becomes more elaborate and specific. Therefore, as a seed for next generation of crypto systems, it is necessary to keep eyes on theories of tropical geometry.

References

[1] Brandt, M., "Tropical Geometry of Curves." Dissertation of Ph.D. UC Berkeley (2020).

[2] Brandt, M., Helminck. P. A., "Tropical superelliptic curves." Advances in Geometry 20.4 (2020): 527-551.

[3] Gathmann, A., Kerber. M., "A Riemann–Roch theorem in tropical geometry." Mathematische Zeitschrift 259.1 (2008): 217-230.

[4] Grigoriev, D., Shpilrain, V., "Tropical cryptography." Communications in Algebra 42.6 (2014): 2624-2632.

[5] Grigoriev, D., Shpilrain, V., "Tropical cryptography II: extensions by homomorphisms." Communications in Algebra 47.10 (2019): 4224-4229.

[6] Helminck, P. A., "Tropical elliptic curves and j-invariants." Bachelor's thesis. Faculty of Science and Engineering, University of Groningen (2011).

[7] Steve, I., Kahrobaei, D., "A Closer Look at the Tropical Cryptography." International Journal of Computer Mathematics: Computer Systems Theory (2020): 1-7.

[8] Koblitz, N., "Elliptic curve cryptosystems." Mathematics of computation 48.177 (1987): 203-209.

[9] Koblitz, A. H., Koblitz, N., and Menezes, A., "Elliptic curve cryptography: The serpentine course of a paradigm shift." Journal of Number theory 131.5 (2011): 781-814.

[10] Mach, M., "Cryptography based on semirings." Master's Thesis, Charles University (2019).

[11] Maclagan, D., Sturmfels, D., "Introduction to tropical geometry." Vol. 161. American Mathematical Soc. (2015).

[12] Miller, V. S., "Use of elliptic curves in cryptography." Conference on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg, (1985).

[13] Muanalifah, A., Sergeev, S., "On the tropical discrete logarithm problem and security of a protocol based on tropical semidirect product." arXiv preprint arXiv:2101.02781 (2020).

[14] Otter, N., "The geometric group law on a tropical elliptic curve" Bachelor's thesis, ETH Zürich, (2012).

[15] Speyer, D., Sturmfels, D.,"Tropical mathematics." Mathematics Magazine 82.3 (2009): 163-173.

[16] Stickel, E., "A new method for exchanging secret keys." Third International Conference on Information Technology and Applications (ICITA'05). Vol. 2. IEEE, (2005).

[17] Vigeland, M. D., "The group law on a tropical elliptic curve." Mathematica scandinavica (2009): 188-204.