TIME COMPLEXITIES IN MAX-LINEAR SYSTEMS

by
JIAN LU

RALPH MORRISON, ADVISOR

A thesis submitted in partial fulfillment
of the requirements for the
Degree of Bachelor of Arts with Honors
in Mathematics

WILLIAMS COLLEGE
Williamstown, Massachusetts

June 13, 2019

ABSTRACT

In the current state of cryptography, one our most secure cryptographic systems is derived from incredibly simple curves defined by equations of the form $y^2 = x^3 + Ax + B$, also known as elliptic curves. Our thesis further explores the possibilities of cryptography within the system of tropical mathematics. Mainly we rewrite all operations of classical mathematics with the operations based on our max-plus semi-ring $(\mathbb{R} \cup \{-\infty\},\ \oplus,\ \otimes)$ where $x \oplus y = \max\{x, y\}$ and $x \otimes y = x + y$. Part 1 of this thesis will present some basic definitions, and properties of tropical geometry so that our readers will get a flavor for the mathematics which we are exploring. In addition, we will present some definitions and examples regarding metric graphs which will later be used to prove the main theorem. We will also introduce tropical linear algebra and how this could be used to define a cryptographic system similar to classic Diffie-Hellman cryptographic systems. Part 2 will introduce classic elliptic curve cryptography, and present a proof by Vigeland that defines a group law on tropical elliptic curves. We will also present a new different proof of the doubling map on tropical elliptic curves in $\mathbb{R}^2$. This section will also go into detail about how we construct a Diffie-Hellman key exchange algorithm based on the tropical elliptic curve. Part 3 presents and studies a new group law on tropical elliptic curves in $\mathbb{R}^3$.

ACKNOWLEDGEMENTS

I would like to thank Professor Ralph Morrison for the introduction in this field of mathematics and for his active and passive continued support throughout my senior year. His mere presence filled to the brim with passion for teaching and helping students, has been a guiding light and an inspiration to get my work done. I would also like to thank the Williams math department for creating such a perfect environment for students to grow and learn more about both themselves and the field of mathematics. In addition I want to thank my friends and family for their continued support throughout my schooling career.

CONTENTS

1. Introduction

1.1. **Notation and Definitions.** We present background on tropical geometry and will redefine some of the more traditional aspects of classical mathematics in search for some more optimal cryptographic schemes that could be better than the current standards in computer science. Since we are rebuilding our understanding of mathematics tropically, we must understand tropical linear algebra. In order to do so, we present results from Butkovič, which mainly focuses on max-linear algebra which is crucial for understanding the tropical linear algebra RSA method that is dicussed in Section 1.2 of this paper. Notably, many of the applications in max-linear boil down to some sort of NP-Complete problem in computer science such as scheduling problems, job assignment, optimization, and integer programming. Also, we will restate some definitions for tropical geometry from Diane Maclagan and Bernd Sturmfels' introductory book to tropical geometry Maclagan and Sturmfels. These definitions lay the groundwork towards understanding tropical polynomials, and the tropical curves that let us study the group law of tropical elliptic curve cryptography. As we delve into some of these basic definitions, we will begin to see that for almost every idea in classical mathematics, there likely exists some tropical variant. Lastly, we introduce the notion of metric graphs which is helpful with regards to observing properties of tropical elliptic curves since we will show that all such curves can be mapped to a similar metric graph.

Definition 1.1. *The tropical semiring* $(\mathbb{R} \cup \{-\infty\}, \oplus, \otimes)$ *is the foundation for our field of study. This set consists of the real numbers* $\mathbb{R}$ *union with an element which represents negative infinity. Our basic arithmetic operations of addition and multiplication are redefined as:*

$$x \oplus y := max\{x, y\} \qquad x \otimes y := x + y$$

For the remainder of this paper let us denote this semiring as S*.*

This means that the tropical sum of two numbers is their maximum, and the tropical product of two numbers is the usual sum. For example:

$$7 \oplus 13 = 13 \qquad \text{and} \qquad 7 \otimes 13 = 21.$$

Some other books such as Maclagan and Sturmfels use minimum instead of maximum. Note that these two arithmetic operations are both associative and commutative in this tropical arithmetic. We can also easily show that the distributive law holds for both tropical addition and multiplication. In this system, we have an identity element for both addition

and multiplication. The identity element for tropical addition is $\{-\infty\}$, and the identity element for tropical multiplication is 0, for example:

$$x \oplus -\infty = x \qquad \text{and} \qquad x \otimes 0 = x.$$

Example 1.2. *Tropical exponentiation is merely* $x^r = \underbrace{(x + x + ... + x)}_{r \text{ times}}$*, or in other words tropical exponentiation is equivalent to classical multiplication.*

Observation 1.3. *Note that in tropical arithmetic, the Freshman's Dream holds for all powers in tropical arithmetic. That is for any* $x, y \in \mathbb{R} \cup \{-\infty\}, (x \oplus y)^n = x^n \oplus y^n$.

1.2. **Tropical Linear Algebra and Tropical Linear Cryptography.** In classical mathematics, linear algebra is considered a core topic as it has applications branching into other fields of mathematics and applied mathematics such as probability, statistics, and computer science. Now a natural question would be to ask, what exactly does tropical linear algebra look like? This field of max-linear algebra was originally researched to find optimizations for computer algorithms.

Definition 1.4. *We define* $\overline{\mathbb{R}}$ *to be the set of extended reals by adjoining the elements* ∞ *and* $-\infty$ *to* $\mathbb{R}$.

Consider the tropical semiring S and the properties that we have stated in the previous chapter. For tropical linear algebra the, for some matrices $A, B \in \overline{\mathbb{R}}^{m \times n}$ we define $A \oplus B = M$ where the element m_{ij} of our result matrix is equal to $a_{ij} \oplus b_{ij}$. The $\otimes$ operation is the same as classical matrix multiplication, but every classical operation is tropicalized. That is the " $+$ " and " $\times$ " are replaced with $\oplus$ and $\otimes$ respectively.

Example 1.5. $\begin{pmatrix} 1 & 2 \\ 5 & -1 \end{pmatrix} \oplus \begin{pmatrix} 0 & 7 \\ 3 & 12 \end{pmatrix} = \begin{pmatrix} 1 & 7 \\ 5 & 12 \end{pmatrix}$.

Example 1.6. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} (a \otimes e) \oplus (b \otimes g) & (a \otimes f) \oplus (b \otimes h) \\ (c \otimes e) \oplus (d \otimes g) & (c \otimes f) \oplus (d \otimes h) \end{pmatrix}$

Definition 1.7. *The* $n \times n$ *tropical identity matrix* I *is the* $n \times n$ *matrix that has* "0" *'s along the diagonal from the top left to bottom right, and* $-\infty$ *everywhere else.*

Definition 1.8. *A scalar matrix is a square matrix with* $\lambda \in S$ *across the diagonal, and* $-\infty$ *elements filled into the matrix.*

In Grigoriev and Shpilrain, Dima Grigoriev and Vladimir Shpilrain explore the usage of tropical algebra as a platform for several cryptographic schemes that would be vulnerable to linear algebra attacks were they based on "usual" algebra as platforms. In the classical case, the powering of matrices is reversible, through the usage of brute force methods by testing all possible factors of the matrices in polynomial time which leads to the possibility that someone would be able to reverse engineer the original key. However in the tropical linear algebra, powering up a matrix involves permanently erasing information. Thus there is no algorithm that would allow someone to reverse engineer the key. We will first look at a classical protocol and adapt it into a tropical protocol. Note that the inspiration for the tropical protocol originated from Stickel's protocol Stickel. Let G be a public non-commutative semigroup, $a, b \in G$ public elements such that $ab \neq ba$. Then we have the following.

Protocol 1.9. *Stickel's Original Protocol.*

(1) *Alice picks two random natural numbers n, m and sends $u = a^n b^m$ to Bob.*
(2) *Bob picks two random natural numbers r, s and sends $v = a^r b^s$ to Alice.*
(3) *Alice computes $K_A = a^n v b^m = a^{n+r} b^{m+s}$.*
(4) *Bob computes $K_B = a^n u b^m = a^{n+r} b^{m+s}$*

Thus, Alice and Bob will share the same secret key $K = K_A = K_B$.

Protocol 1.10. *Let R be a public non-commutative ring $a, b \in R$ public elements $ab \neq ba$.*

(1) *Alice picks two random polynomials $p_1(x), p_2(x)$ (with positive integer coefficients) and sends $p_1(a) * p_2(b)$ to Bob.*
(2) *Bob picks two random polynomials $q_1(x), q_2(x)$ and sends $q_1(a) * q_2(b)$ to Alice.*
(3) *Alice computes $K_A = p_1(a) * (q_1(a) * q_2(b)) * p_2(b)$*
(4) *Bob computes $K_B = q_1(a) * (p_1(a) * p_2(b)) * q_2(b)$*

Thus, Alice and Bob end up with the same secret key $K = K_A = K_B$ because $p_1(a) * q_1(a) = q_1(a) * p_1(a)$ and $p_2(b) * q_2(b) = q_2(b) * p_2(b)$.

Protocol 1.11. *Tropical version. Let R be the tropical algebra of $n \times n$ matrices over the integers, and let $A, B \in R$ be the public matrices such that $A \otimes B \neq B \otimes A$.*

(1) *Alice picks two random tropical polynomials $p_1(x), p_2(x)$ with integer coefficients and sends $p_1(A) \otimes p_2(B)$ to Bob.*
(2) *Bob picks two random tropical polynomials $q_1(x), q_2(x)$ with integer coefficients and sends $q_1(A) \otimes q_2(B)$ to Alice.*

(3) *Alice computes* $K_A = p_1(A) \otimes (q_1(A) \otimes q_2(B)) \otimes p_2(B)$.
(4) *Bob computes* $K_B = q_1(A) \otimes (p_1(A) \otimes p_2(B)) \otimes q_2(B)$.

Thus, Alice and Bob end up with the same secret key $K = K_A = K_B$ *because* $p_1(A) \otimes q_1(A) = q_1(A) \otimes p_1(A)$ *and* $p_2(B) \otimes q_2(B) = q_2(B) \otimes p_2(B)$.

A natural question to ask is what is the purpose of attempting to tropicalize systems of cryptography that have already been developed in the world of classical mathematics. In Grigoriev and Shpilrain, the two authors point out that there is an "obvious advantage" in the improved efficiency of these systems because when multiplying tropical matrices, we actually are performing regular addition which can be completed in constant time, while multiplication is much more expensive.

Let us also compare the security of using the tropical linear algebra protocol over the normal linear algebra protocol. In Stickel's original method we have that G is a group of invertible matrices over a field. Then in order for someone to solve for a shared key K, it is sufficient to find matrices x and y such that $xa = ax$ and $yb = by$, and $xu = y$. (x corresponds to a^n, and y corresponds to b^m.) These conditions are equivalent to a system of $3k^2$ linear equations with $2k^2$ unknowns, where k is the size of matrices, and thus can be efficiently found. However, Grigoriev and Shpilrain proved the following result below, which shows that tropical linear algebra cryptography has equivalent security to some of the better cryptographic schemes in current existence.

Proposition 1.12 (Proposition 1 in Grigoriev and Shpilrain)**.** *The problem of solving systems of tropical polynomial equations is NP-hard.*

1.3. **Tropical Polynomials and Tropical Curves.**

Definition 1.13. *Let* $x_1, x_2, ..., x_n$ *be variables that can take on some values in* S*. A monomial is any product of these variables where repetition is allowed.*

Example 1.14. *A monomial.* $x_1 \otimes x_1 \otimes x_2 \otimes x_2 \otimes x_2 \otimes x_3 = x_1^2 x_2^3 x_3$.

In our max-linear algebra, a monomial defines a function from $\mathbb{R}^n$ to $\mathbb{R}$. Evaluation of the above function in a classical sense would yield the output below:

$$x_1 + x_1 + x_2 + x_2 + x_2 + x_3 = 2x_1 + 3x_2 + x_3$$

Definition 1.15. *Let* $\overline{x} = \begin{bmatrix} x_1 \\ x_2 \\ ... \\ x_n \end{bmatrix}$ *and* $\overline{v} = \begin{bmatrix} i_1 \\ i_2 \\ ... \\ i_n \end{bmatrix}$ *both be vectors where* $x_i's$ *are variables and* $i_i \in \mathbb{Z}_+$. *We write* $\overline{x}^{\overline{v}}$ *for a monomial of the form* $x_1^{i_1}x_2^{i_2}...x_n^{i_n}$ *where it is written as the vector of variables with a corresponding vector of exponents. If there is a coefficient, we write it as* $a_{\overline{v}}$. *We then tropically multiply the coefficient with the monomial vector:* $a_v x^v$.

A tropical polynomial is then a finite tropical linear combination of tropical monomials: $f(x_1, x_2, ..., x_n) = \bigoplus_{\overline{v} \in \mathbb{Z}_+^n} a_{\overline{v}}\overline{x}^{\overline{v}}$ *where the coefficients* $a \in \overline{\mathbb{R}}$ *and the exponents* $\overline{v} \in \mathbb{Z}_+^n$.

A tropical polynomial is just the maximum of a finite collection of tropical monomials. That is:

$$p(x_1, ..., x_n) \quad = \quad a_{\overline{v_1}} \otimes \overline{x}^{\overline{v_1}} \quad \oplus a_{\overline{v_2}} \otimes \overline{x}^{\overline{v_2}} \oplus ... \oplus \quad a_{\overline{v_n}} \otimes \overline{x}^{\overline{v_n}}$$ [Page 5, Maclagan and Sturmfels],

such that it is the max of a system of inequalities, namely: $\max\{a_{v_1} + x \cdot v_1, ..., a_{v_n} + x \cdot v_n\}$.

Observation 1.16. *Note that we can create two different polynomials that define the same function such as:*

$$x^2 \oplus 5 = x^2 \oplus (-100 \odot x) \oplus 5.$$

Theorem 1.17. *(The Fundamental Theorem of Tropical Algebra) Every tropical polynomial function in one-variable can be written uniquely as a function as a tropical product of tropical polynomials.*

Example 1.18. $x^2 \oplus 17 \otimes x \oplus 2 = x^2 \oplus 1 \otimes x \oplus 2 = (x \oplus 1)^2$.

Lemma 1.19 (Lemma 1.1.2 in Maclagan and Sturmfels)**.** *Functions defined by the tropical polynomials in* n *variables* $x_1, ..., x_n$ *are precisely the piece wise-linear convex functions on* $\mathbb{R}^n$ *with integer coefficients.*

Let us examine the case of the tropical polynomials with one variable. For example:

$$p(x) = a \otimes x^3 \oplus b \otimes x^2 \oplus c \otimes x \oplus d.$$

We can visualize this function with four lines on the (x, y) plane:

- $y = 3x + a$
- $y = 2x + b$
- $y = x + c$

- $y = d$

The value of $p(x)$ is the largest y such that (x, y) lies on one of these lines [1].

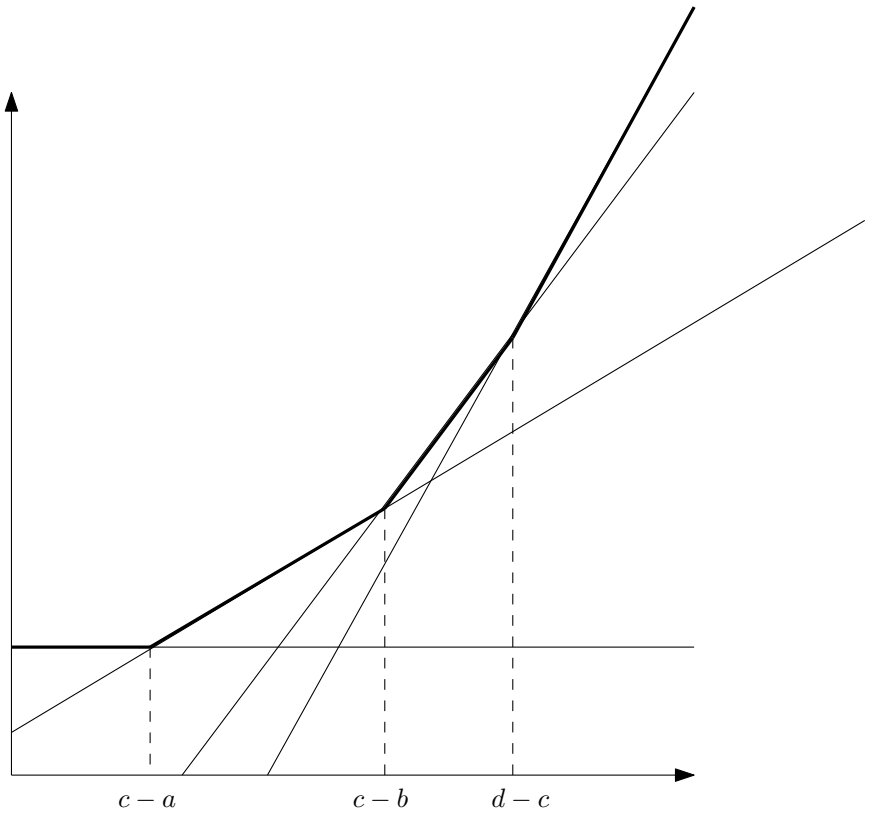


FIGURE 1. The graph of a cubic polynomial and its roots.

Definition 1.20. *A tropical root in one variable is defined as the breakpoints to where $p(x)$ changes slope. Visually, these are the changes from one segment to another line segment in the image below.*

Definition 1.21. *We say that a tropical polynomial vanishes at a point if the maximum is achieved at least twice.*

Example 1.22. *Where does $x \oplus y \oplus 0$ vanish tropically in $\mathbb{R}^2$?*

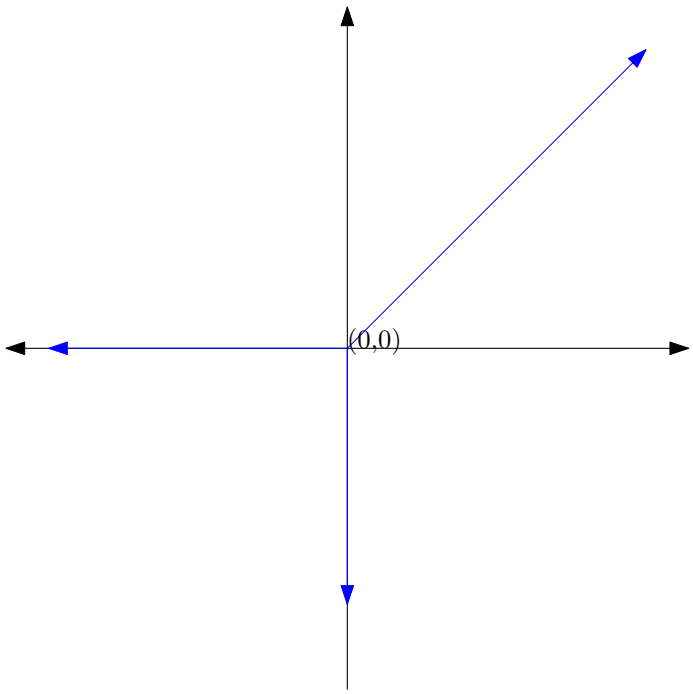


FIGURE 2. The tropical curve defined by $x \oplus y \oplus 0$

Note here we have rays extending towards infinity when we have two maxes tie. So the set of points where $x \oplus y \oplus 0$ *vanishes is the three rays* $x = 0 \geq y$, $y = 0 \geq x$, $x = y \geq 0$ *[This set is illustrated in Figure 2].*

The previous example motivates the following definition.

Definition 1.23 (1.3. Plane Curves Maclagan and Sturmfels)**.** *For some tropical polynomial function* $p : \mathbb{R}^n \to \mathbb{R}$*, the tropical hypersurface* $V(p)$ *of* p *is the set of all points* $w \in \mathbb{R}^n$ *at which the maximum is achieved at least twice. If* $n = 3$*, we call* $V(p)$ *a tropical surface. If* $n = 2$*, we call* $V(p)$ *a tropical curve.*

Then we have that tropical polynomials in two variables have the following form:

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

We will establish exactly how these tropical polynomials define geometric objects, or in other words how they can be graphed. It turns out that similar to how we can define a group law on elliptic curves in the realm of classic mathematics, we can also define group laws on the tropical curves defined by tropical polynomials. More specifically we will be looking at tropical elliptic curves of honeycomb form that have degree 3 and genus 1.

Definition 1.24. *Let $f(x, y)$ be a tropical polynomial in two variable. The Newton polygon, Newt(f), is defined as the convex hull in $\mathbb{R}^2$ of all the points (i, j) such that $x^i y^j$ appears with non-($-\infty$) coefficients in $f(x, y)$.*

Definition 1.25. *We define a lattice point to be a point in $\mathbb{R}^2$ with integer coordinates.*

Definition 1.26. *Let P be a polygon (2-dimensional, with vertices in $\mathbb{Z}^2$). Suppose $P_1, P_2, ..., P_m$ are polygons (also 2 dimensional, with vertices in $\mathbb{Z}^2$) satisfying the following:*

(1) $P_1 \cup P_2 \cup ... \cup P_m = P$

(2) *For $i \neq j, P_i \cap P_j$ is either (i) $\emptyset$, (ii) a vertex of $P_i \cup P_j$, or (iii) an edge of P_i and P_j.*

Then we say $P_1, ..., P_m$ form a subdivision of P.

We use Newt(f) help us visualize the tropical curve since we have that the tropical curve is actually dual to a subdivision of its Newt(f) [Definition 1.1.3., Maclagan and Sturmfels]. In order to get this induced subdivision of our Newt(f) we must lift the (x, y) coordinates of each lattice point of our Newt(f), take a convex hull, and project the upper faces of our shape to Newt(f) [3].

Thus we can obtain a subdivision of the Newt(f). The lattice points of the Newt(f) corresponds to each of the terms between each $\oplus$ in the polynomial. Let us examine the tropical polynomial

$$f(x, y) = -1 \otimes x^2 \oplus -1 \otimes y^2 \oplus x \otimes y \oplus x \oplus y \oplus -1.$$

For example the lattice point at $(0, 0)$ would correspond to the constant term, $c_{0,0}$, of our tropical polynomial if there existed a constant term in this polynomial. $(1, 0)$ would correspond to the $c_{1,0} \otimes x$ term, $(1, 1)$ would correspond with the $c_{1,1} \otimes x \otimes y$, and so on for $c_{i,j} \in \mathbb{R}$ and where (i, j) corresponds to the lattice point of the Newt(f). Newt(f) is the triangle illustrated in the upper left of Figure 3. Then based on the constant for each term, we can lift up the lattice points of our Newt(f) to a height given by the coefficient to find the subdivisions of the Newt(f), and the tropical curve $V(f)$ dual to the subdivision of Newt(f). We then solve for the coordinates of the vertices of our $V(f)$ by finding the solving the systems of equations given by our lattice points. In Figure [3], we have a set of six points $\{(0, 0, -1,), (0, 1, 0), (1, 0, 0), (1, 1, 0), (0, 2, -1,), (2, 0, -1)\}$ which we then take the convex hull in $\mathbb{R}^3$. When we lift up to find the upper convex hull, we find a set of 4 faces that induce the subdivision on the Newt(f) which gives us the necessary information to draw the tropical curve.

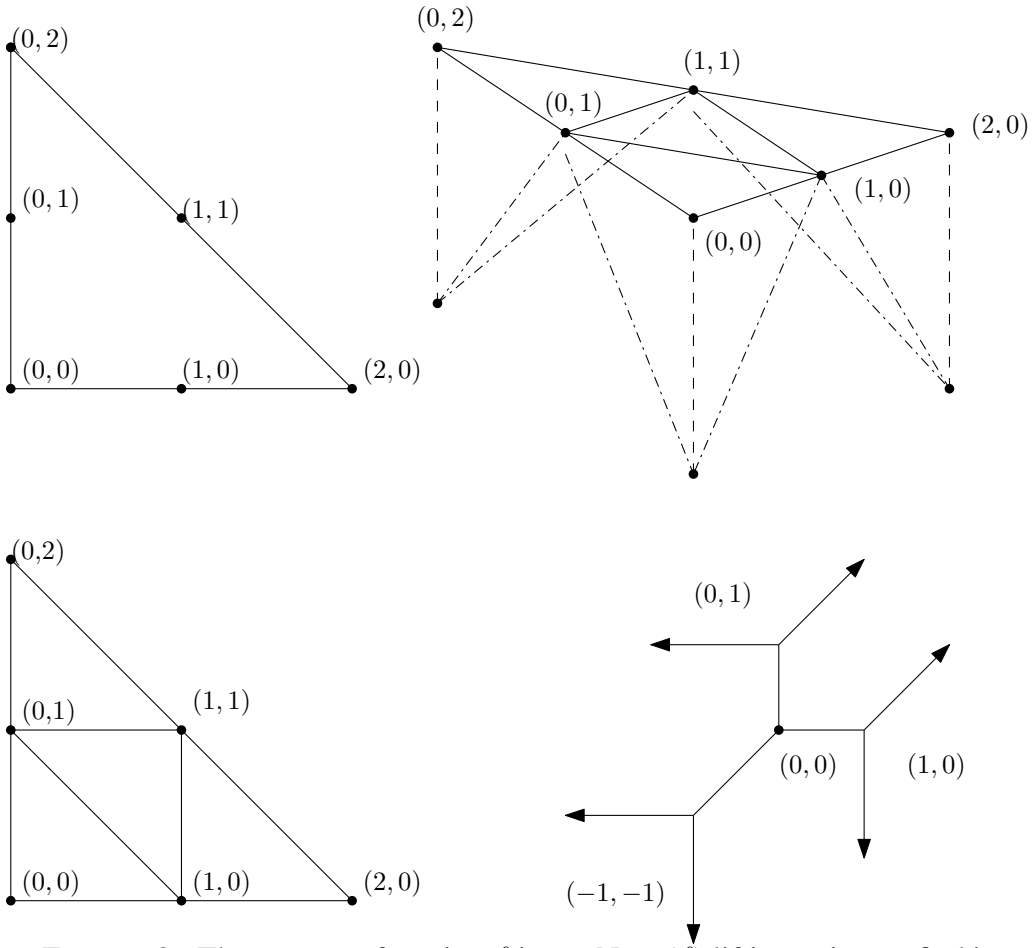


FIGURE 3. The process of turning f into a Newt(f) lifting points to find its subdivision and drawing the tropical curve $V(f)$.

Theorem 1.27. *(Duality Theorem, Page 13 Maclagan and Sturmfels) Let $p(x, y)$ be a tropical curve, and $P = Newt(f)$. Let S_p be the subdivision of P induced by $p(x, y)$. Then we have that $V(p)$ is dual to S_p. Respectively the polygons, internal edges, and external edges of S correspond to the vertices, edges, and rays of $V(p)$. Moreover, each line and ray in $V(p)$ is perpendicular to the dual edge in S_p.*

Definition 1.28 (Page 15, Maclagan and Sturmfels)**.** *We will focus on tropical curves whose Newt(f)s are the standard triangles with vertices $(0, 0), (0, d)$ and $(d, 0)$. Such a curve is said to be curve of degree d. Note that the curve in 3 is a curve of degree 2.*

Definition 1.29. *The genus of a tropical polynomial f is the number of interior lattice points within its Newt(f). We can also refer to this as the genus of the polygon.*

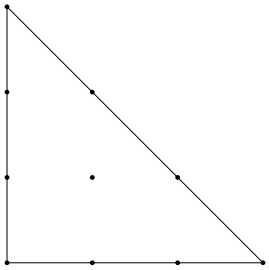


FIGURE 4. A Newt(f) with genus 1.

Definition 1.30. *A tropical polynomial $p(x, y)$ and its tropical curve $V(p)$ is called smooth if its Newt(f) subdivision is a unimodular triangulation; that is, when each lattice triangle in the subdivision has area $\frac{1}{2}$.*

In classical mathematics we denote the intersection of two curves as the shared common points between the two curves. Thus we are motivated to create a similar definition for tropical geometry, and we specifically will study the behavior of the intersection of two tropical curves which is also constituted of the set of shared points between the two curves. Since curves in tropical geometry are essentially piecewise-linear objects, we can see that many of these intersections will occur at a single point; however, we note that we can have some weird cases even in classic mathematics such as parallel lines, or lines on top of each other. Thus, we will describe the general behavior for tropical intersections, and establish rules for these "weird" edge cases.

Definition 1.31. *Let $V(f)$ be a tropical curve. Let E be an edge in $V(f)$ and Δ' be the corresponding edge in the subdivision of f. We define the weight of E as one more than the number of interior lattice points in Δ'.*

Definition 1.32 (Definition 49 Otter)**.** *Two tropical curve C and D are said to intersect transversally if no vertex of C lies on D or no vertex of D lies on C.*

Definition 1.33 (Definition 49 Otter)**.** *We define the intersection multiplicity of two tropical curves intersecting transversally at some point P as*

$$\mu(P) = w_1 \times w_2 \times \det \begin{vmatrix} v_{11} & v_{12} & v_{13} \\ v_{31} & v_{32} & v_{33} \\ 1 & 1 & 1 \end{vmatrix}$$

where, E_1 and E_2 are edges meeting at P with weights respectively w_1 and w_2, primitive integer direction vectors v_1 and v_2.

Theorem 1.34. *(Tropical Bezout's)[Theorem 1.3.2 Maclagan and Sturmfels] Consider two tropical curves C and D of degree $c, d \in \mathbb{R}^2$. If the two curves intersect transversally, then the number of intersection points, counted with multiplicities is equal to cd.*

Proof. The proof is found in Theorem 1.3.2 of Maclagan and Sturmfels □

Example 1.35. *Let us consider the polynomials $f(x, y) = -1 \otimes x^2 \oplus -1 \otimes y^2 \oplus x \otimes y \oplus x \oplus y \oplus -1$ and $g(x, y) = -1 \otimes x^2 \oplus -1 \otimes y^2 \oplus 1 \otimes x \otimes y \oplus x \oplus y \oplus 0$. As shown in Figure 5, we generate the Newton polygons of each curve, and we are able to graph their intersections.*

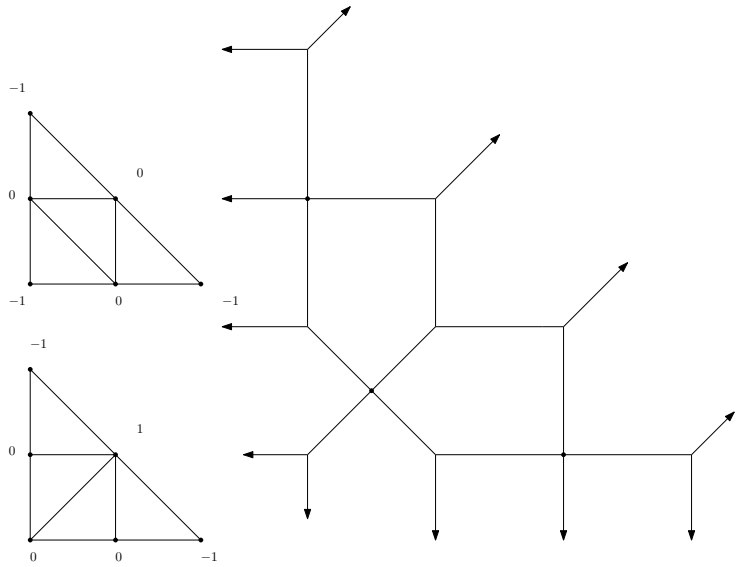
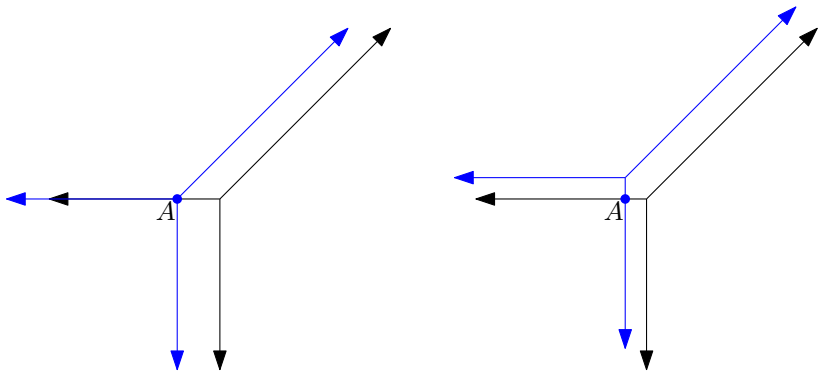


FIGURE 5. The subdivisions induced by f and g and the tropical curves.

When we consider Tropical Bezout's we must realize that there are some cases in which the curves C and D may intersect at infinitely many points. Although we can clearly see how this may hold for traditionally transversal intersections, we need not have "intersect transversally" in our theorem. Thus by defining stable intersections below, we are able to establish a Tropical Bezout's in the general case.

Theorem 1.36. *(Stable Intersection Principle) [Theorem 1.3.3 Maclagan and Sturmfels]. Let C, D be two tropical plane curves degree $c, d \in \mathbb{R}$ that do not intersect transversally. Let $\varepsilon > 0$, and let D_ε be the set obtained by translating D by $\epsilon\overline{V} = \langle \varepsilon V_1, V_2 \rangle$ where V_1, V_2 are both vectors that are not parallel to any rays of the curves. The limit of the point configuration $C_\varepsilon \cap D_\varepsilon$ is independent of the choice of perturbations. C_ε and D_ε can be thought of as the wiggling of the curves C and D by length ε such that they do intersect transversally. It is a well-defined multiset of cd points contained in the intersection $C \cap D$.*

As we can wiggle special case curves into stable intersections, we note that any two curves of degree c and d in $\mathbb{R}^2$, no matter how special they may be, will intersect stably in a well-defined multiset of cd points (Corollary 1.3.4 Maclagan and Sturmfels). As a result, we know that Tropical Bezout's will hold generally for any tropical curves in $\mathbb{R}^2$.



[b]

FIGURE 6. Stable Intersection of two tropical lines.

1.4. **Tropical Geometry in $\mathbb{R}^3$.** Since we have described tropical linear algebra and tropical polynomials in two variables, a natural extension would be to look at the tropical polynomials in three variables which have the following form:

$$p(x,y,z) = \bigoplus_{(i,j,k)} c_{ijk} \otimes x^i \otimes y^j \otimes z^k.$$

As we would consider the simplest tropical curve in $\mathbb{R}^2$ to be the tropical line, we naturally consider the building block in $\mathbb{R}^3$ to be the tropical plane. Typically we imagine a plane to be a flat surface, but a tropical plane looks quite different as described below.

Definition 1.37. *Let D be a tropical plane. This plane consists of 4 rays emanating from a point in the $-e_1 = \langle -1,0,0\rangle, -e_2 = \langle 0,-1,0\rangle, -e_3 = \langle 0,0,-1\rangle, e_1+e_2+e_3 = \langle 1,1,1\rangle$ directions. As well, it also consists of the 6 half-planes that are between every pair of these rays.*

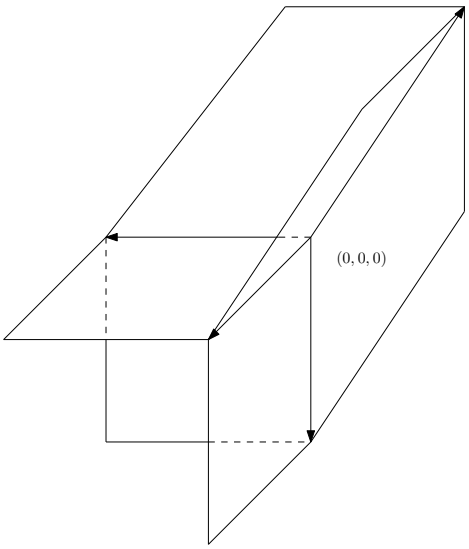


FIGURE 7. A tropical plane defined by $x \oplus y \oplus z \oplus 0$

Example 1.38.

During the presentation of our tropical curves in 2 dimensions, we noticed the existence of a duality theorem between Newt(f) and the curve $V(f)$ itself. Naturally, as we are expanding to one more dimension, we establish a similar duality theorem for tropical curves in $\mathbb{R}^3$; however our Newton polygons are also expanded in one dimension, and instead become Newton polytopes. For the rest of this paper whenever we reference Newf(f), we will assume that it is a Newton polytope that corresponds to the dimensions that are being discussed. As we have gone through a similar process in $\mathbb{R}^2$, in order to draw our surface, we still must lift one dimension higher and take the convex hull to induce the proper subdivisions in our Newt(f). Note that degree d follows the same notation as in the $\mathbb{R}^2$, but with some extra dimension.

Theorem 1.39 (Theorem 4.5.2 Maclagan and Sturmfels)**.** *A smooth tropical surface of degree d, we have:*

(1) d^3 *vertices,*
(2) $2d^2(d-1)$ *edges (bounded one-dimensional cells),*
(3) $4d^2$ *rays (unbounded one-dimensional cells),*
(4) $d(d-1)(6d-11)/6$ *bounded two-dimensional cells, and*
(5) $6d^2$ *unbounded two-dimensional cells.*

We move on to presenting the process of intersecting two different tropical polynomials in $\mathbb{R}^3$. In classic mathematics when we intersect a pair of two dimensional surfaces, we expect the intersection to be some one-dimensional curve. In tropical geometry, we can define some similar behavior assuming that the pieces of such surfaces will intersect stably.

Let us consider two tropical polynomials f and g such that $f, g \in \mathbb{R}^3$. Then we define $C = \text{newt}(f)$, $D = \text{newt}(g)$. In order to find the intersection between these two curves, we must find the Cayley polytope of these two curves which is built by overlaying the two Newton polytopes where without loss of generality D is at height 1, and C is at height 0. Note that the Cayley polytope would always be in the $(n+1)^{th}$ dimension, and in this case be in $\mathbb{R}^4$.

Definition 1.40. *A Cayley polytope of polynomials f, g with C, D as described above is written as Cay(C, D) and is the polytope in the $(n+1)$-dimension where f is at height 0, and g is set to height 1.*

Now that we have a Cay(C, D), we can lift into $\mathbb{R}^5$ in order to find the induced subdivision of Cay(C, D), which would subdivide our Cay(C, D) into 4-dimensional polytopes.

Definition 1.41. *A mixed cell is defined as a subdivision of some Cay(C, D) such that there are at least one vertex coming from both C and D.*

The mixed-cells in our subdivision would correspond directly to the vertices of the intersection curve meaning that the subdivisioned polytopes share vertices from from g and from f. If we have that all cells of the Cayley polytope happen to be composed of minimum volume (which is $\frac{1}{24}$), then we have that the tropical curve as a result of the intersection of two polynomials is considered smooth, and we can define the following special case for tropical intersections below.

Theorem 1.42 (Theorem 4.6.20 Maclagan and Sturmfels)**.** *Let $f(x, y, z)$ and $g(x, y, z)$ be polynomials of degree d and e with $C = Newt(f)$ and $D = Newt(g)$. Let us assume that $P = V(f) \cap V(g)$ is smooth, then P has*

- $d^2e + de^2$ *vertices,*
- $(3/2)d^2e + (3/2)de^2 - 2de$ *edges (bounded one-dimensional cells), and*
- $4de$ *rays (unbounded one-dimensional cells).*

1.5. **Metric Graphs and Rational Functions.** One of the first uses of metric graphs to compare different curves in tropical geometry came from Andreas Gathmann and Michael

Kerber Gathmann and Kerber. In their paper they considered the results of a Riemann-Roch theorem for finite graphs and extended this result into metric graphs and thus established a Riemann-Roch theorem for divisors on tropical curves. An astonishing result of these metric graphs on tropical curves is that we can consider tropical curves in $\mathbb{R}^n$ where n is different, and show that they have the same underlying metric graph. We will later utilize this result in order to establish a group law on tropical elliptic curves in $\mathbb{R}^3$, by expanding on some known results of tropical elliptic curves in $\mathbb{R}^2$.

Definition 1.43 (Gathmann and Kerber)**.** *A metric graph is a pair (Γ, l) consisting of a graph Γ together with its length function $l : E(\Gamma) \to \mathbb{R}_{>0}$. An edge e coincides with the real interval $[0, l(e)]$ leading to a "geometric representation" of the graph by gluing these intervals together at their boundary points according to the combinatorics of Γ.*

Observation 1.44 (Gathmann and Kerber)**.** *A tropical curve is simply a connected metric graph Γ possibly with infinite lengths on some edges and some "leaves" at infinity.*

Definition 1.45 (Gathmann and Kerber)**.** *A tropical rational function on Γ is a continuous piecewise-linear real-valued function f with integer slopes and only finitely many "pieces". For any point $P \in \Gamma$, the order $ord_p f$ of f in P is the sum of the slopes of f emanating from P. We define simple zeroes as the as the points of the rational function which have order 1, and simple poles as the points of the rational function that have order -1. (The order is merely the sum of the slopes outgoing on the points).*

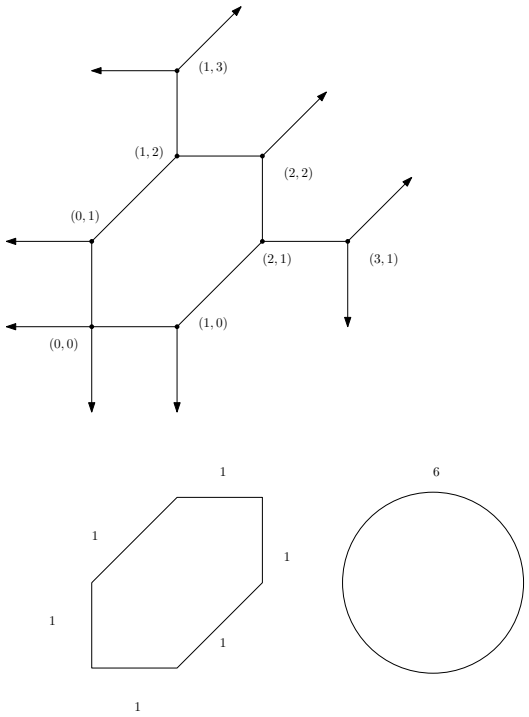


FIGURE 8. A tropical polynomial conversion to metric graph.

Example 1.46.

Since we have established that a tropical curve is simply a connected metric graph, we can utilize specific properties that have already been thoroughly established for these metric graphs in order to show properties of tropical curves.

Definition 1.47 (Definition 1.3 Gathmann and Kerber)**.** *A divisor on a tropical curve* Γ *is an element of the free abelian group group generated by the points of* Γ *in its geometric representation.*

A divisor on Γ is simply the formal $\mathbb{Z}$-linear combination of points of Γ as shown in 9. If the edge lengths of a metric graph Γ are integers we can call Γ a $\mathbb{Z}$-graph. Note that in the cases that we will be studying in tropical geometry, we will mostly be looking at rational points, which can be easily be scaled into integer coordinates.

Definition 1.48 (Definition 5.1 Dehli Vigeland)**.** *Let there a be a tropical rational function* $h : \Gamma \to R$ *of the form* $h = f - g$*, where* f *and* g *are tropical polynomials with with the same degree. A principle divisor on a smooth tropical curve* C *in* R^3*.*

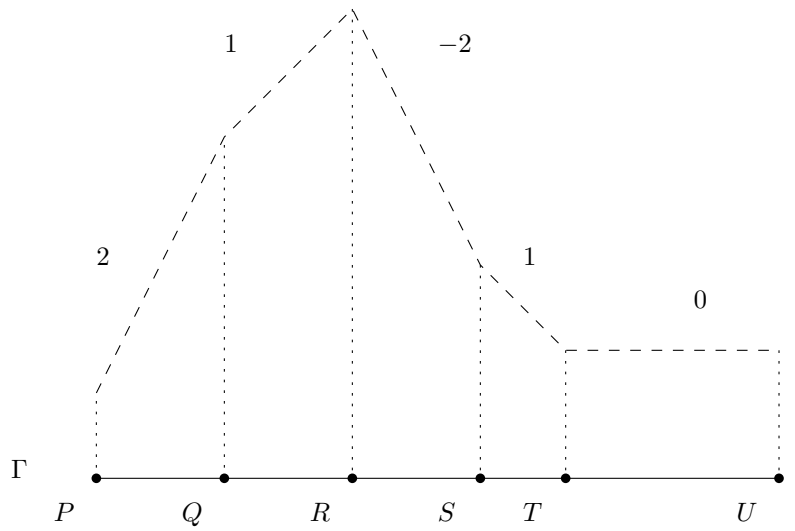


FIGURE 9. A tropical rational function with $\text{div}(f) = (2P + S + T) - (Q + 3R)$.

Example 1.49.

Observation 1.50. *Note that another form of divisor theory that may be more understandable to the reader is chip firing. In chip firing on graphs, we establish that different orientations of chips on graphs actually represent the same graph, and in fact any combination that can be fired is essentially the same graph. We will later utilize this exact intuition to show that certain lines and points on our tropical elliptic curve are essentially the same.*

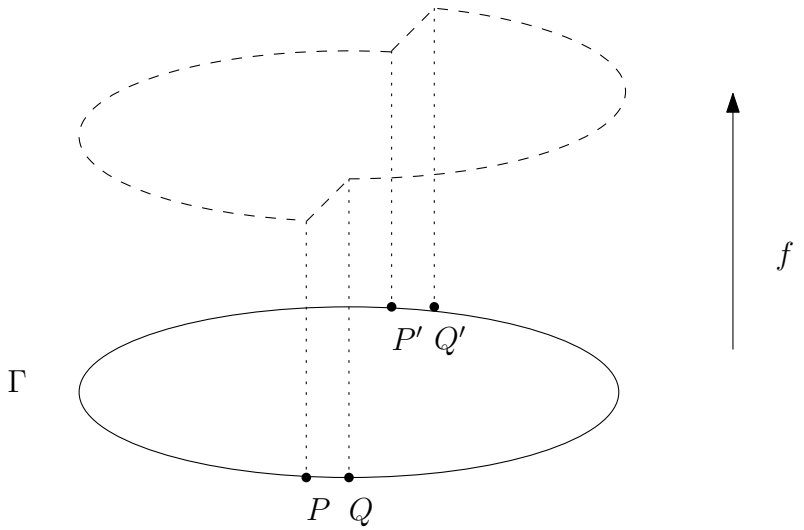


FIGURE 10. A tropical rational function with $\text{Div}(f) = (P + P') - (Q + Q')$ on a circle metric graph.

2. Tropical Elliptic Curve Cryptography

Directly following the recent research of Grigoriev and Shpilrain, a natural question to ask is are there any other encryption schemes that could become tropicalized? We note that one of the best encryption schemes in present day is elliptic curve cryptography, where one exponentiates a point based on the elliptic curve group law. There have been some results of looking at cryptographic schemes on the tropical elliptic curve group laws. Only the case of the Hessian pencil has been explored in Chauvet's paper Chauvet and Mahé; however, we can expand their research to the tropical curves of honeycomb structure. In this section we will first introduce classic elliptic curve cryptography, and then utilize the tropical group law developed by Vigeland in Dehli Vigeland and generalize the results by Chauvet to all tropical curves of degree 3 and genus 1 to introduce a new tropical elliptic curve cryptography.

Definition 2.1. *Weisstein An elliptic curve over a field K is a nonsingular cubic plane curve and the polynomial that defines it has two variables $f(x, y) = 0$.*

The field K is usually taken to be the complex numbers $\mathbb{C}$, reals $\mathbb{R}$, rationals $\mathbb{Q}$, algebraic extensions of $\mathbb{Q}$, p-adic numbers $\mathbb{Q}_P$, or a finite field. A general elliptic curve over any field has a defining polynomial that has the form

$$Ax^3 + Bx^2y + Cxy^2 + Dy^3 + Ex^2 + Fxy + Gy^2 + Hx + Iy + J = 0,$$

where $A, B, ... \in K$ with characteristic $\neq$ 2,3 can be written in the form

$$y^2 = x^3 + ax + b.$$

We usually consider the points on our elliptic curve C together with an extra point, called the point at infinity. We define it to have the property that every vertical line passes through it. Let us define the group law over elliptic curves as follows Corbellini:

(1) The elements of the group are the points of an elliptic curve, together with a "point at infinity".
(2) The identity element is the point at infinity.
(3) The inverse of a point P is its reflection about the x-axis.
(4) We define 0 to be the point at infinity. Addition is defined so that given three colinear, non-infinity points P, Q, R, $P + Q + R = 0$ if and only if P, Q, and R are collinear. Then as a result, we can define the addition of two points P, Q to be $P + Q = -R$.

To the unsuspecting reader, intuitively we could see that associativity for elliptic curves seems quite natural to prove; however, to show that $(P+Q)+R = P+(Q+R)$ requires a significant amount of algebra which can be found in the work of Kazuyuki Fujii1 and Hiroshi Oike who devoted an entire paper to proving associativity algebraically **elliptic**

As a result, we can provide a clear geometric method to compute the sum between two points P and Q. The intuition for this addition is given two points P, Q then we can draw a line passing through P and Q and then this will intersect a third point on the curve, R. The inverse of of this point $-R$ is equal to the addition of $P+Q$. Note that the property of associativity requires some significant algebra to prove. Note that the geometric addition of points are an abelian group as we can write $P+Q+R=0 \implies P+Q=Q+P=-R$.

Definition 2.2. *The identity element of our elliptic group law is referred to as the origin. Usually it is taken to be 0, the point at infinity.*

Since we have shown that this group is abelian, the encryption scheme for cryptography on the elliptic curve is similar to the protocols in the previous section. We have that some private key n is chosen, and both Alice and Bob choose some point on the elliptic curve to exponentiate according to this defined addition group law. Since the operation is commutative both Alice and Bob will share the same key afterwards.

Example 2.3. *Let us consider the elliptic curve, $y^2 = x^3 - x + 1$ shown in Figure 11.*

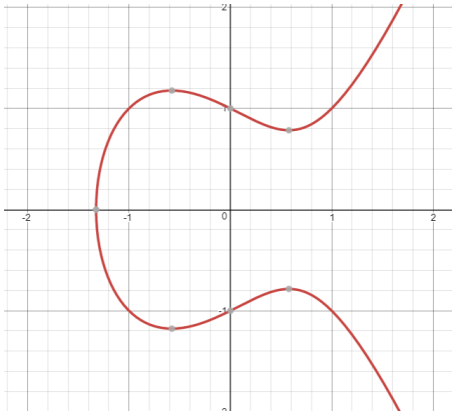


FIGURE 11. Elliptic curve defined by $y^2 = x^3 - x + 1$

Then we note that the geometric addition of the points P, Q is as follows in Figure 12.

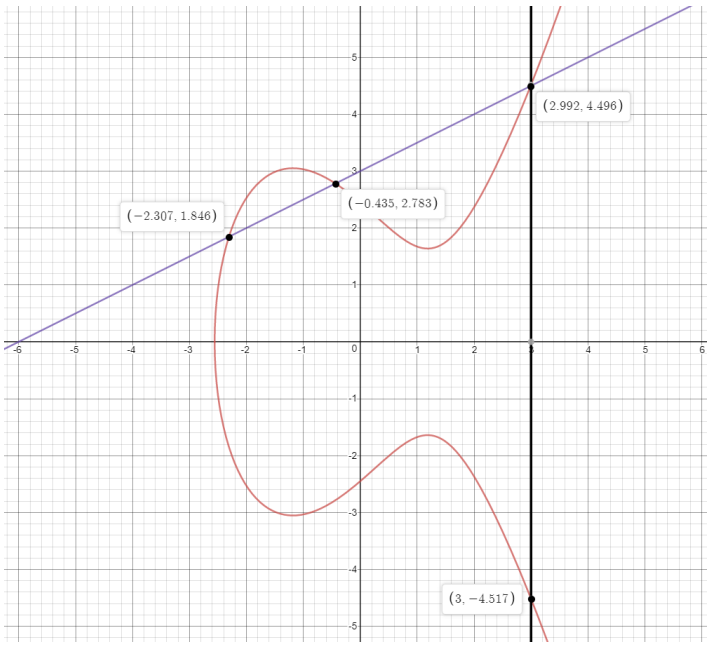


FIGURE 12. Addition of points P, Q in an elliptic curve.

2.1. **Algebraic Group Law on the Tropical Elliptic Curves.** Following the path of the two mathematicians before us, we tried to establish a new cryptographic system in tropical geometry that may prove more fruitful than only using tropical linear algebra. As a result of our curiosity we will present Vigeland's description of the group law on tropical elliptic curves [Remark 5.8, Dehli Vigeland] which he proves using divisor theory, and tropical rational functions.

Definition 2.4 (Definition 5.4 Dehli Vigeland)**.** *The Jac(C) or the Jacobian of C is the set of all degree zero divisors modulo equivalence.*

Definition 2.5. *A tropical elliptic curve is a smooth tropical plane curve of degree 3 and genus 1 as seen in Figure 13.*

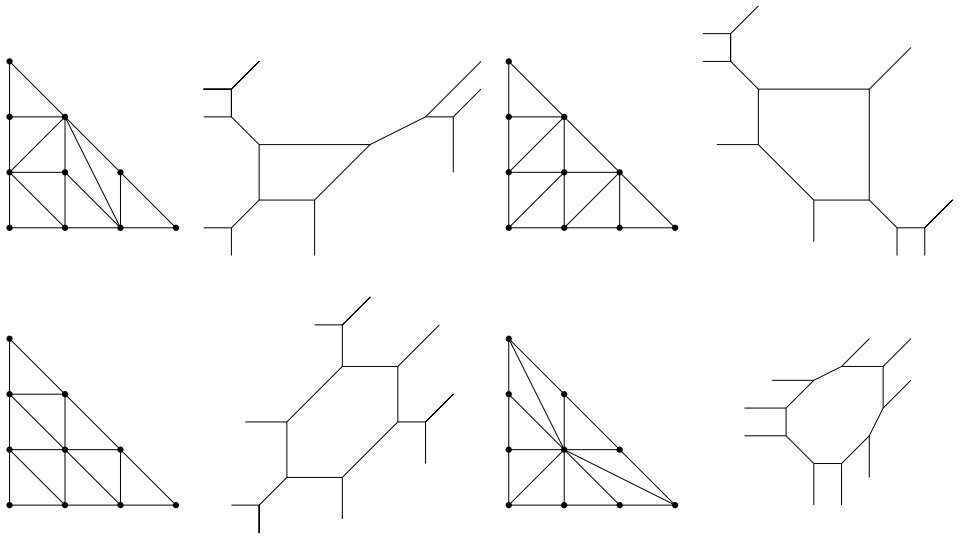


FIGURE 13. An assorted variety of tropical elliptic curves.

In our case, we will define for two points $P, Q \in C$, the distance $d_C(P, Q)$ to be the displacement from P to Q with respect to the $\mathbb{Z}$- metric on C Dehli Vigeland. Then, we are able to present the following theorem.

Theorem 2.6 (Theorem 1.1 Dehli Vigeland)**.** *Let C be a tropical elliptic curve, and $\overline{C}$ be its unique cycle. Let O be a point on C which we establish as its origin. Then we have that:*

(1) *We have a bijection of sets $\overline{C} \longrightarrow$ Jac(C), given by $P \mapsto P - O$.*
(2) *The induced group law on $\overline{C}$ satisfies the relation $d_C(O, P + Q) = d_C(O, P) + d_C(O, Q)$.*

(3) *As a group $\overline{C}$ is isomorphic to the circle.*

We will mainly focus on providing a brief overview of Vigeland's proof on the group law on tropical elliptic curves since we will be utilizing the fact that this group law will fit all the criteria such that a cryptographic system could possibly be created.

2.2. **Geometric Addition on Tropical Elliptic Curves.** As a result of Vigeland's group law we are able to describe a geometric addition on tropical elliptic curves similar to that of the geometric addition on classic elliptic curves. Let $C \subset \mathbb{R}^2$ be a tropical elliptic curve, and let $O \in \overline{C}$ be a fixed point. This fixed point will be considered the origin for our operation. Let $P, Q \in C$ and if (P, Q) is a good pair (the tropical line drawn from these two points do not intersect transversally with C), then we define R to be the third point of intersection between the tropical line that connects P and Q and C. Then we define $P + Q$ to be the third point of intersection between the tropical line that connects O and R given that (O, R) is a good pair.

For those points that are not in a good pair, the following algorithm will "fix" the bad pairs such that the tropical line drawn between the two points and C will not intersect transversally. Let $P, Q \in C$, and the pair (P, Q) be in a bad position. Then we define (P_t, Q_t) as the pair of points that are the result of $(P + t, Q + t)$, where t is some lattice length movement on C. That is to say that we shift the points following the curve C, an equal distance away from each other until the tropical line L_t formed by (P_t, Q_t) no longer intersect transversally with C. For the points R and O, we recreate this similar operation.

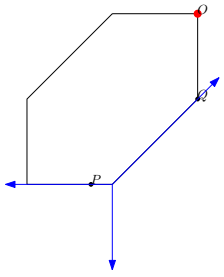


FIGURE 14. $P, Q \in C_K$ intersect transversally.

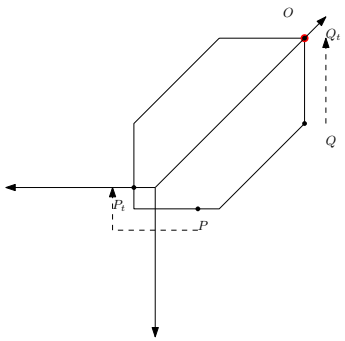


FIGURE 15. Moving the a bad pair P, Q.

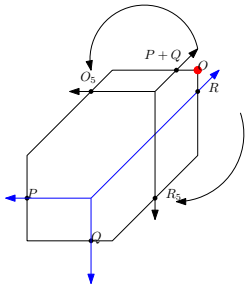


FIGURE 16. The geometric addition of two points $P, Q \in C_K$.

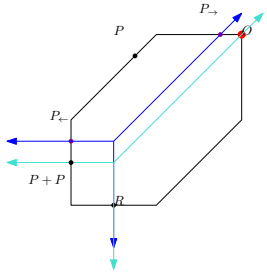


FIGURE 17. The geometric addition of the point $P + P \in C_K$.

Lemma 2.7 (Lemma 72 Otter)**.** *There exists some value of t such that translation by distance t results in a good pairing. That is to say that the third point of intersection with $\overline{C}$ does not depend on t, and produce the same intersection point.*

Proposition 2.8 (Proposition 6.1. Dehli Vigeland)**.** *Let P and Q be points on the same tentacle of C. Then $P \sim Q$.*

Preposition 2.7 implies that any two points lying on the same line of a tropical elliptic curve will be linearly equivalent, and that two points on distinct sections of the curve will not be linearly equivalent. The proof used in Vigeland's paper utilizes the idea that points on the same ray will have tropical rational functions passing through such that their some resulting divisors would show that the points are equivalent. He projects tropical elliptic curve to circular metric graphs which can give rise to divisors such as the one shown in Figure 10. Then he shows that this sort of process works for all points lying on the same line which we provide intuition for in Figure 19.

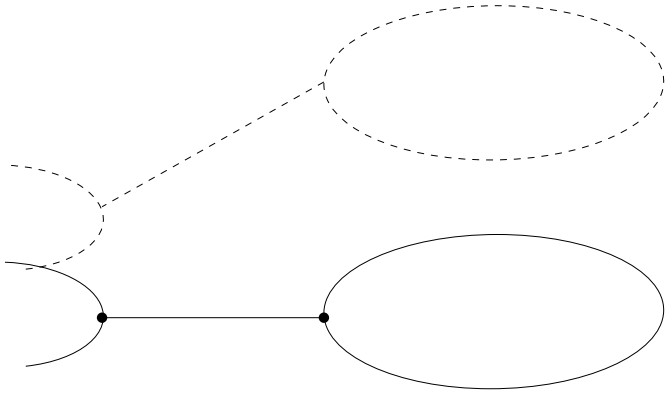


FIGURE 18. Points along the same tentacle have the same divisor.

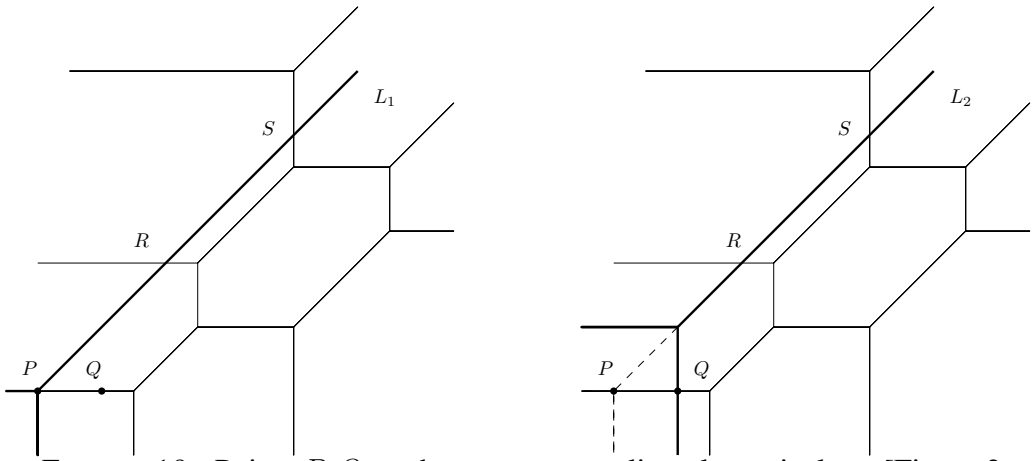


FIGURE 19. Points P, Q on the same ray are linearly equivalent. [Figure 2 Dehli Vigeland]

Example 2.9.

Proposition 2.10. *[Proposition 6.2. Dehli Vigeland] If $P, Q \in \overline{C}$ and $P \sim Q$, then $P = Q$.*

From the above two results, we are able to prove that a group law exists on the Jacobian of the elliptic curve. We were required to define when divisors of the form $P + Q$ were equivalent in order to distinguish between good and bad pair intersections. When $P, Q \in C$ has a tropical line L intersecting C stably we denote P, Q a good pair, otherwise we denote P, Q a bad pair. In order to show a complete group law, we must prove that addition works in both cases. For the sake of notation we will fix $p_1 = \langle -1, 0 \rangle, p_2 = \langle 0, -1 \rangle, p_3 = \langle 1, 1 \rangle$ for the primitive integer directions of a tropical line.

Lemma 2.11 (Lemma 6.3. Dehli Vigeland)**.** *Let P, Q, P', Q' be any points on C. Then $P + Q \sim P' + Q' \iff d_C(P, P') = -d_C(Q, Q')$.*

Proof. We will first show that the above lemma is true for good pairs (P, Q) and (P', Q'), and then generalize the result to bad pairs.

Assume that (P, Q) and (P', Q') are both good pairs and that $P + Q \sim P' + Q'$. Then there exist unique tropical lines L, L', and a point $R \in \overline{C}$ such that $L \cap_{st} C = P + Q + R$ and $L' \cap_{st} C = P' + Q' + R$ (the existence of R follows as a result of Proposition 2.9). Then we consider a translation L_t of the lines containing R such that $L_0 = L$ and $L_1 = L'$. We need only consider the cases where P and P' on the same edge and Q and Q' are on the same edge, since in any other case we can break down the translation into the parts with the above property.

Let v_P and v_Q be the primitive direction vectors of the edges of $\overline{C}$ containing P, P' and Q, Q' respectively, and assume that L' equals the shifting of $L \times \delta$ units in the direction of, say, p_1 (refer to Figure 20). Then based on the general formulas for non-orthogonal projection (see Figure 20), we derive the following formulas below:

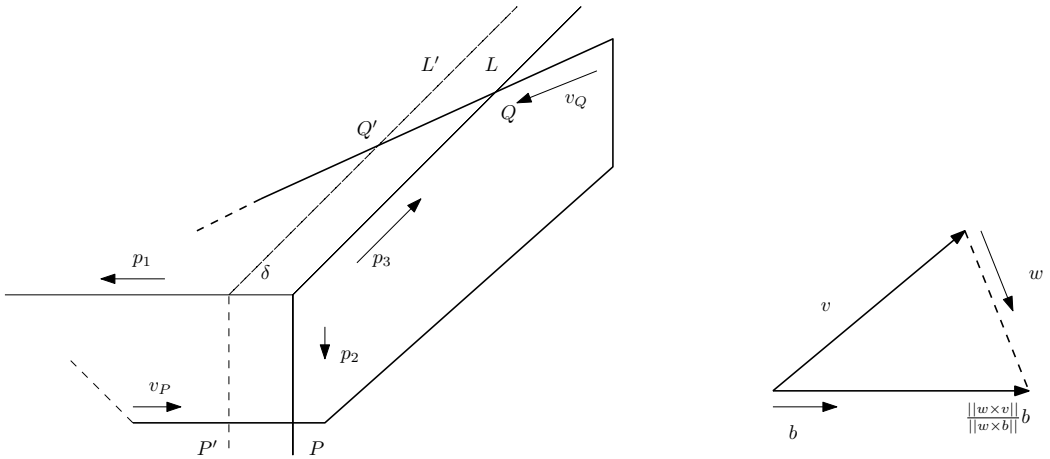


FIGURE 20. Illustrating Step 1 and Non-orthogonal projection [Figure 6, 7 Dehli Vigeland]

Example 2.12.

$$PP' = \frac{||p_2 \times \delta p_1||}{||p_2 \times v_P||} = \delta v_P \to |d_C(P, P')| = \frac{||\delta v_P||}{||v_P||} = \delta, \tag{2.1}$$

$$QQ' = \frac{||p_3 \times \delta p_1||}{||p_3 \times v_Q||} = \delta v_Q \to |d_C(Q, Q')| = \frac{||\delta v_Q||}{||v_Q||} = \delta. \tag{2.2}$$

Note that we have that $|\det(v_P, p_2)| = |\det(v_Q, p_3)| = 1$ since each of the intersections have multplicity 1. According to the orientation of $\overline{C}$, P and Q are moved in the opposite direction, and thus we have $d_C(P, P') = -d_C(Q, Q')$ for good pairs.

Now we will show that this also holds for bad pairs. Assume that (P, Q) is not a good pair. Let L_1 and L_2 be tropical lines that run through P and Q respectively, and let R_1, S_1, R_2, S_2 be the other intersection points. Then we move L_1 and L_2 into lines L_1' and L_2' such that R_1, S_1, R_2, S_2 is preserved, but P and Q will be different and move to points P' and Q'. By construction we have that $P' + Q' \sim P + Q$, so it will follow from the same steps used in proving good pairs that $d_C(P, P') = d_C(Q, Q')$. Since we choose L_1' and L_2' in a particular way, we have that (P', Q') will be a good pair so it follows that our lemma will hold for all pairs of points on $\overline{C}$. □

2.3. **Doubling Map on the Honeycomb Structures.** Now we will attempt to adapt protocols from classic elliptic curve cryptography into a new protocol for tropical elliptic curve cryptography. In Chauvet and Mahé, Chauvet defines a protocol on the tropical hessian pencil and studies the doubling map of the tropical hessian pencil in Figure 21.

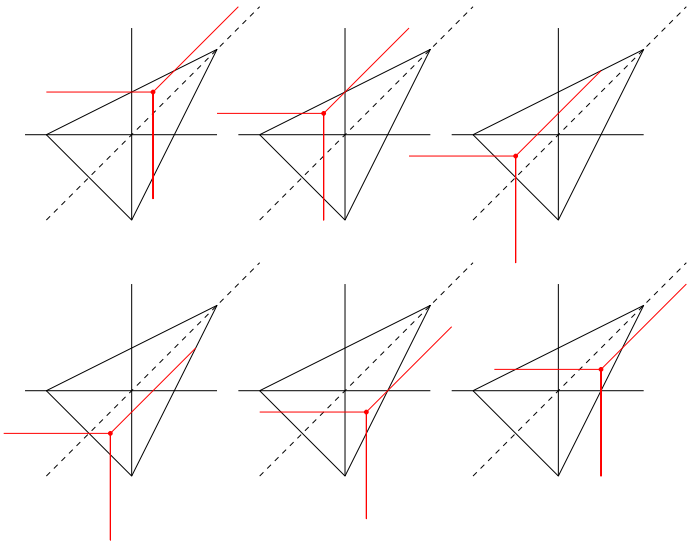


FIGURE 21. The doubling map of the Tropical Hessian pencil separated into 6 sides.

However, we will focus on studying the honeycomb structure variant of a tropical elliptic curve in . Although Chauvet proves in his paper that this cryptography system is not secure, we believe there are some interesting results regarding the behavior of the geometric group law on the honeycomb structures.

Although Vigeland also proves using divisor theory that the group law on tropical elliptic curves are isomorphic to the circle and therefore the doubling map, we present a different geometric approach. By considering the doubling map geometrically of where the resultant point R for each side of any tropical elliptic curve and it's origin point O, we can define mapping formulas for each side. In this section, we will go over the doubling map for one specific honeycomb- shaped tropical geometric curve.

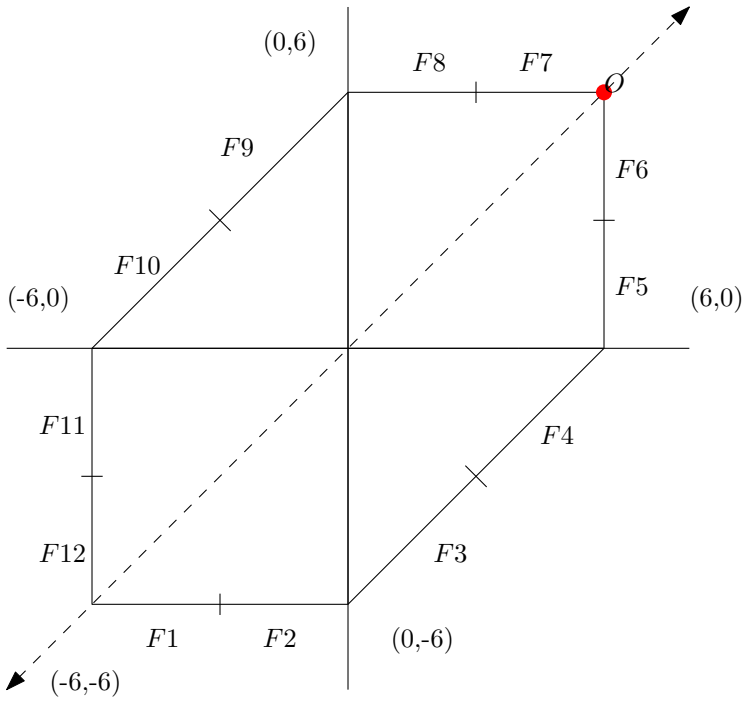


FIGURE 22. The 12 sides of the tropical honeycomb elliptic curve.

We utilize the origin in the top right corner since it is one of the easier origins to work with regards to the tropical line, and we have shown that placement of the origin on the curve C_K results in a rotation about the map. We also choose to study the regular honeycomb structure, since it feels the most natural to study. Moreover, we will choose $K = 6$, since it will allow for us to have enough lattice points to build up a strong intuition about this doubling map. We will divide the cycle C_K into 12 sections, respectively:

$$F_1 := \{X, Y \in \overline{C_K} : -K \geq X \geq -K/2, Y = -K\}, \qquad F_2 := \{X, Y \in \overline{C_K} : -K/2 \geq X \geq 0, Y = -K\},$$
$$F_3 := \{X, Y \in \overline{C_K} : 0 \geq X \geq K/2, -K \geq Y \geq -K/2\}, \qquad F_4 := \{X, Y \in \overline{C_K} : K/2 \geq X \geq K, -K/2 \geq Y \geq 0\},$$
$$F_5 := \{X, Y \in \overline{C_K} : X = K, 0 \geq Y \geq K/2\}, \qquad F_6 := \{X, Y \in \overline{C_K} : X = K, K/2 \geq Y \geq K\},$$
$$F_7 := \{X, Y \in \overline{C_K} : K/2 \geq X \geq K, Y = K\}, \qquad F_8 := \{X, Y \in \overline{C_K} : 0 \geq X \geq K/2, Y = K\},$$
$$F_9 := \{X, Y \in \overline{C_K} : -K/2 \geq X \geq 0, K/2 \geq Y \geq K\}, \qquad F_{10} := \{X, Y \in \overline{C_K} : -K \geq X \geq K/2, 0 \geq Y \geq K/2\},$$
$$F_{11} := \{X, Y \in \overline{C_K} : X = -K, -K/2 \geq Y \geq 0\}, \qquad F_{12} := \{X, Y \in \overline{C_K} : X = -K, -K \geq Y \geq -K/2\}.$$

We divide C_K in this way since the the doubling map of each edge of C_K corresponds directly to each one of these 12 sections. By taking some point $P \in C_K$, we can derive some natural doubling formulas based on its original position based on which section the point started in. As a result we can produce Table 1 below.

TABLE 1. Formulas for doubling of P and the alternate preimage Q of the double of P.

$2[P]$	
$P \in F_1:$	$2[P] = \binom{K+2x}{K}$
$P \in F_2:$	$2[P] = \binom{K+2x}{-2x}$
$P \in F_3:$	$2[P] = \binom{-K}{-2x}$
$P \in F_4:$	$2[P] = \binom{-2y}{-K}$
$P \in F_5:$	$2[P] = \binom{2y}{2y-k}$
$P \in F_6:$	$2[P] = \binom{K}{2y-k}$
$P \in F_7:$	$2[P] = \binom{2x-K}{K}$
$P \in F_8:$	$2[P] = \binom{K-2x}{2x-K}$
$P \in F_9:$	$2[P] = \binom{-K}{2x}$
$P \in F_{10}:$	$2[P] = \binom{-2y}{-K}$
$P \in F_{11}:$	$2[P] = \binom{2y}{K-2y}$
$P \in F_{12}:$	$2[P] = \binom{K}{-2y-K}$

In order to produce the doubling formulas, we consider the tropical line to be rooted to some point in C_k to be doubled, using the partitions of the curve above, we can derive these formulas.

Proof. Let us consider a regular honeycomb-shaped elliptic curve C_6 with $O = (12, 12)$, so such that we have lattice length 6 on each side. Our proof will show that the doubling map for the curve C_6 matches the formula above when $K = 6$. Our proof consists of 12 different cases for which some point $p \in C_6$ lies on one of the 12 faces $(F_1, ..., F_12)$. Note that this proof is sufficient since we can easily generalize the lattice length of 6 to a lattice length of K.

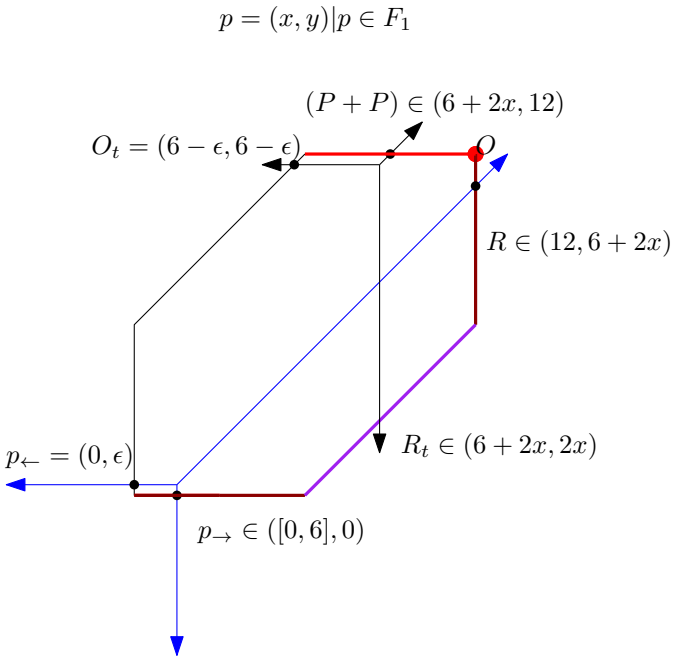


FIGURE 23. Doubling formula geometric proof for $p \in F_1$.

Case 1: For some $p \in C_6$ where $p = (x, y)$ such that $0 \leq x \leq 3, y = 0$. Note that this means $p \in F_1$. We have that currently $P + P$ is in bad position, so we move the points some equal lattice length apart such that they will be in a good position. We denote these points $P_{\rightarrow}$ and $P_{\leftarrow}$. We recall that a tropical line has consists of three rays stemming from one vertex in the $\langle -x \rangle, \langle -y \rangle, \langle x, y \rangle$ directions. From Lemma 1.38, we have that our shifting will not affect position of the third point R, so we only need to translate ϵ distance away from any corner so that we can have $P_{\rightarrow}$ and $P_{\leftarrow}$ will fit a tropical line. Then we can have that $P_{\leftarrow}$ can be fixed at $(0, \epsilon)$, and $P_{\rightarrow} \in ([0, 6], 0)$. Then R must lie in the interval $(12, [6, 12])$ since we know that the other ray of the tropical line has a slope of 1. Now we have that R, O are in bad position, so we can fix this by translating R, O away from each other until they are in a good position. We must use the same method and translate ϵ distance away from any corner so that we can have O_t and R_t fitting on a tropical line that does not intersect transversally with C_6. Let us fix O_t at $(6 - \epsilon, 12 - \epsilon)$. Since $R \in (12, [6, 12])$, then $R_t \in ([6, 12], [0, 6])$ since we must always translate by a lattice length of 6. Thus clearly from our tropical line rooted at these two points, then the third point must lie in $([6, 12], 6)$. The tropical line through these points is the tropical line with vertex at $(2x + \epsilon, \epsilon)$, which intersects our curve at the points $(2x, 0), (0, \epsilon), (6 + 2x, 12)$ Note

that this is equivalent to $(6 + 2x, 12)$, which is exactly the doubling formula for $p \in F_1$ (refer to Figure 10 for a visualization).

Case 2: For some $p \in C_6$ where $p = (x, y)|3 \leq x \leq 6, y = 0$. Note that this means $p \in F_2$. With the same reasoning given from Case 1, we have that $R \in ()$, which means that we have $P + P \in (6 + 2x, -2x)$.

Case 3: For some $p \in C_6$ where $p \in F_3$. With the same reasoning given from Case 1, we have that $R \in (6 - 2y, 0)$ (Note that this is an exact point given by the value of y on our honeycomb curve.), which means that we have $P + P \in (-6, -2x)$.

Case 4: For some $p \in C_6$ where $p \in F_4$. With the same reasoning given from Case 1, we have that $R \in (0, 12 - 2y)$, which means that we have $P + P \in (-2y, -6)$.

Case 5: For some $p \in C_6$ where $p \in F_5$. With the same reasoning given from Case 1, we have that $R \in ([0, 6], [6, 12])$, which means that we have $P + P \in (2y, 2y - 6)$.

Case 6: For some $p \in C_6$ where $p \in F_6$. With the same reasoning given from Case 1, we have that $R \in ([6, 12], 12)$, which means that we have $P + P \in (6, 2y - 6)$.

Case 7: For some $p \in C_6$ where $p \in F_7$. With the same reasoning given from Case 1, we have that $R \in (12, [6, 12])$, which means that we have $P + P \in (2x - 6, 6)$.

Case 8: For some $p \in C_6$ where $p \in F_8$. With the same reasoning given from Case 1, we have that $R \in ([6, 12], [0, 6])$, which means that we have $P + P \in (6 - 2x, 2x - K)$.

Case 9: For some $p \in C_6$ where $p \in F_9$. With the same reasoning given from Case 1, we have that $R \in ([0, 6], 0)$, which means that we have $P + P \in (-K, 2x)$.

Case 10: For some $p \in C_6$ where $p \in F_{10}$. With the same reasoning given from Case 1, we have that $R \in (0, [0, 6])$, which means that we have $P + P \in (-2y, -6)$.

Case 11: For some $p \in C_6$ where $p \in F_{11}$. With the same reasoning given from Case 1, we have that $R \in ([0, 6], [6, 12])$, which means that we have $P + P \in (2y, 6 - 2y)$.

Case 12: For some $p \in C_6$ where $p \in F_{12}$. With the same reasoning given from Case 1, we have that $R \in ([6, 12], 12)$, which means that we have $P + P \in (6, -2y - 6)$.

□

Observation 2.13 (Theorem c. Dehli Vigeland)**.** *We note that the doubling maps of tropical elliptic curves are isomorphic to the circle. Our proof shows geometrically, that these tropical line intersections actually result in a doubling map of some circle in both the cases of the placement of both* R *and* $2[P]$.

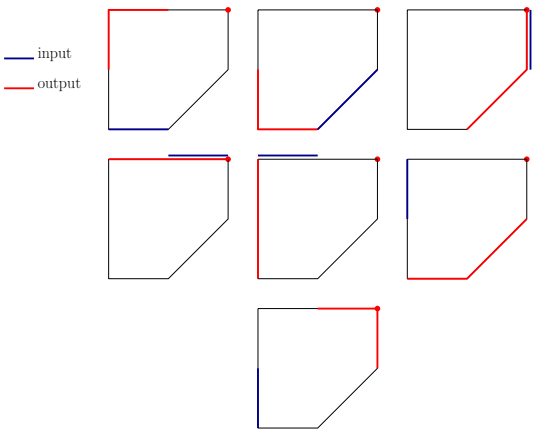


FIGURE 24. Pentagon Tropical Elliptic Doubling Map

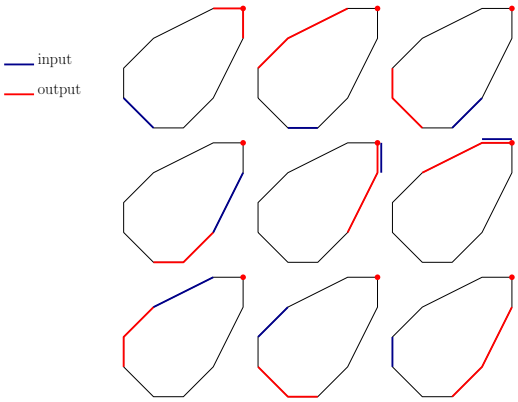


FIGURE 25. Nonagon Tropical Elliptic Doubling Map

Our work in researching the doubling map of tropical elliptic curves utilize the geometric addition that comes as a result of the group law which Vigeland had proved. We fix the point at infinity to the top right corner of tropical elliptic curves, and we studied the doubling map for tropical elliptic curves of n-sides. We noticed that the doubling map of these curves will rotate based on the position of our chosen point at infinity, and we also have that the doubling map is a continuous function for any point $p \in C$. In Figures 24,25 we have figures of the visual representations of the doubling maps for the pentagon and nonagon variants of the tropical elliptic curve.

3. Group Law on Tropical Elliptic Curves in 3D

At this point we have established the machinery required to study a group on tropical elliptic curves in 3D. Our research is motivated by the discovery that Vigeland made when he established the tropical elliptic curve in $\mathbb{R}^2$ does indeed have a group law. We would like to inquire to see if we can establish a group law for tropical elliptic curves of higher dimensions. We are able to get tropical elliptic curves in 3D by finding a tropical curve variant of genus 1, and in particular these curves arise as the intersection of two quadratic surfaces. In the classical case of elliptic curves in 3D, given two points $P, Q \in C_c$ and an origin point $O \in C_c$ where C_c is a classic elliptic curve, the plane $\mathcal{P}$ that is collinear with P, Q, O will result in some fourth point of intersection $R \in C_c$. Then we define $P + Q + R = 0$ which leads to $P + Q = -R$. We will show that there exists a similar tropical geometric addition in the tropical variant. We indeed discover that we can indeed establish a group law for three dimensions, and utilize the same machinery to prove this fact as Vigeland. The overview of our proof is that we utilize the fact that our tropical elliptic curve can be represented as a metric graph in classical geometry, and by establishing the same properties that Vigeland had established we are able to define this group law.

Definition 3.1. *Let C be a smooth, connected complete intersection of two tropical quadric surfaces in $\mathbb{R}^3$. We call C a tropical elliptic curve.*

Theorem 3.2. *Tropical Bernstein [Maclagan and Sturmfels Theorem 4.6.14]*

The number of solutions in $(K^*)^n$ to a generic system of n polynomial equations $f_1 = ... = f_n$ with given Newton polytopes $P_1, ..., P_n$ is equal to the mixed area of the Newton polytopes.

The formation of our tropical elliptic curve in 3D follows a similar algorithm from determining tropical intersections in 2D. We would overlay the Newton polytopes for each of the quadric surfaces, and then raise it to the next dimension at different heights to get out a Cayley polytope. Then we find all of the mixed cells in order to establish the subdivisions of this Cayley polytope. As with before we have a structure of genus 1 which implies we will have exactly one cycle, $\overline{C}$.

By Tropical Bernstein, we are able to ascertain that we indeed have the proper number of intersections within the cycle of a tropical elliptic curve in 3D and a tropical plane. Note that we must ensure that the tropical elliptic curve is smooth, meaning that we will have 32 4-simplices within our subdivision each of area $\frac{1}{24}$.

For this specific result, we know that this graph has genus 1, so we focus our efforts on the most interesting portion of the graph which is the cycle in 3D. Our cycle may have any number from 3 to 16 vertices. We will first define a homeomorphism of $\overline{C} \to S^1$. Note that S^1 is the circle group. As a result, we are able to utilize the tools established in section 1.5. regarding metric graphs, since we can transformed our tropical elliptic curve into some metric graph S' using the integer lattice lengths of each distinct edge in the cycle of $\overline{C}$ as in Figure 26. Let us fix a point $O \in \overline{C}$, and let label each vertex $v_1, v_2, ..., v_n$ counting clockwise from O. We will denote each edge between these vertices as $e_1, e_2, ..., e_n$ starting from the edge e_1, of v_1v_2 and rotating clockwise. Then we consider the lattice length l_i of each of the edges. We denote $L = \Sigma_{i=1}^{n} l_i$ which is also equivalent to the total lattice length of the cycle. We set L as the circumference of a circle in the $\mathbb{R}^2$. Then our mapping will pick some point $O \in S'$, and starting going clockwise we will project our lattice length proportion of each edge onto the euclidean length on the circumference of this circle.

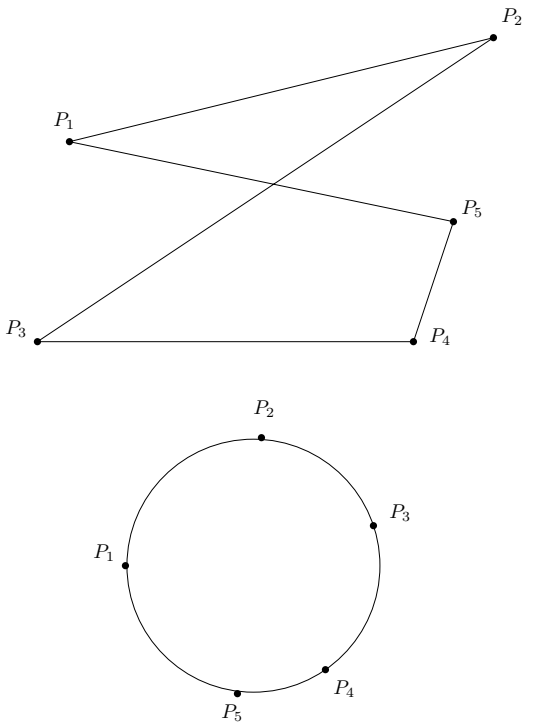


FIGURE 26. A contraction of some tropical elliptic curve in 3D to a metric graph.

Similar to Vigeland's proof of the group law on elliptic curves in 2D, we will show that the Jacobian, Jac(C) has a bijection to $\overline{C}$. One crucial step towards the proof in 3D is showing that divisors of the form $P + Q$ are linearly equivalent in the 3D case. The

idea comes from the limited degrees of freedom in our translation of the tropical plane that intersects with C. We note that in the 2D case, we can break down the translations of the tropical line to simple cases and it turns our that movements of the tropical plane can also be broken to down to translations in the 2D plane, which Vigeland has already proven to be linearly equivalent.

Note that by Bernstein's theorem, we are in fact guaranteed 4 points of stable intersection between the intersections of two tropical quadric surfaces and a tropical plane, since we have surfaces of degree 2,2 and 1 resulting in $2 \cdot 2 \cdot 1 = 4$ points of intersection. We imitate the technique of defining a good pair intersection and a bad pair intersection. That is, given two points P and Q on $\overline{C}$, we cannot always find a tropical plane D that intersects C stably in P, Q, and O. If there exists such a tropical plane, we label (P, Q) a good pair.

Lemma 3.3. *Let P, Q, P', Q' be any points on $\overline{C}$. Denote some point $O \in \overline{C}$ to be the origin of the curve. Then*

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

Proof. We will first show that this is true when (P, Q) and (P', Q') are each good pairs. Then we can there exists unique tropical planes $\mathcal{P}$ and $\mathcal{P}'$ that will connect (P, Q, O) and (P', Q', O) such that $\mathcal{P} \cap_{st} \overline{C} = P + Q + O + R$ and $\mathcal{P} \cap_{st} \overline{C} = P' + Q' + O + R$. We define the above connection as the phenomenon where points P, Q, O all lie on a tropical plane (since we are able to draw a tropical plane that connects any three points) that intersects stably with $\overline{C}$. It follows that O is obviously the same point, but we also know that existence and uniqueness of R follows from Preposition 1.56. We consider the case of these curves for which each of the points P and P' are on the same edge and Q and Q' are also on the same edge, since we have shown previously its linear equivalence. If these points were in different positions, we can show that the translation is broken into different pieces such that multiple linear transformations would lead to the same case just described. Thus it will be enough to consider the case where P and P are on the same edge and where Q and Q are on the same edge, and $\mathcal{P}$ is some parallel displacement of $\mathcal{P}$ along one of the axes.

Note that we only have 6 potential directions which we can move along since we fix two points (P, Q) and we try to slide onto the points (P', Q'). Since we have these two fixed points, we are only able to move along one of the directions along a tropical plane, or the tropical rays extending out from the tropical plane. Let us consider any tropical plane, then we have unbounded rays in the $-x, -y, -z$, $\langle x, y, z \rangle$ directions. Then we also have the 6 half planes that consisting of the planes in between each of these rays. Thus we have

that our tropical plane only has so many degrees of freedom, and we only need to consider movement along those 6 planes as we fix two points in each situation. Given that we only have movement of our curve along a 2D plane, this portion follows from Vigeland's proof of the group law on the xy-plane. Thus our proof for the good pair follows smoothly from the results of Vigeland once we fix points, and can only slide in the direction of some 2D plane.

Assume that P, Q is not a good pair. Let PL and PL' each be tropical planes through P and Q and let $S_p, O_p, R_p, S_q, O_q, R_q$ be the other points of intersection for these two points. So then we translate these planes PL and PL' such that those points are still preserved. Then since we have found new points P', Q' we can say that these points are now in a good pair.

□

We can consider the following example below of a tropical elliptic curve in 3D.

Example 3.4. *Let our smooth tropical elliptic curve in 3D be the intersection of $f(x, y, z)$ and $g(x, y, z)$ given below. We utilize Macaulay 2 in order to plot this intersection, and verify that it is indeed smooth using the cellDecompose function in Polymake.*

$f(x) = (-99 \otimes z^2) \oplus (77 \otimes x^2) \oplus (-72 \otimes y^2) \oplus (84 \otimes yz) \oplus (-92 \otimes xy) \oplus (23 \otimes xz) \oplus (-44 \otimes x) \oplus (72 \otimes y) \oplus (-20 \otimes z) \oplus -56.$

$g(x) = (44 \otimes z^2) \oplus (-75 \otimes x^2) \oplus (13 \otimes y^2) \oplus (-80 \otimes xy) \oplus (44 \otimes xz) \oplus (86 \otimes yz) \oplus (69 \otimes x) \oplus (27 \otimes y) \oplus (55 \otimes z) \oplus 86.$

WORKS CITED

Butkovič, Peter. *Max-linear systems: theory and algorithms*. Springer-Verlag London, Ltd., London, 2010. xviii+272. Web. Springer Monographs in Mathematics.

Chauvet, Jean-Marie and Eric Mahé. "Cryptography from the tropical Hessian pencil". *Groups Complex. Cryptol.* 9.1 (2017): 19–29. Web.

Corbellini, Andrew. "Elliptic Curve Cryptography: a gentle introduction" (). Web.

Dehli Vigeland, Magnus. "The group law on a tropical elliptic curve". *Math. Scand.* 104.2 (2009): 188–204. Web.

Gathmann, Andreas and Michael Kerber. "A Riemann-Roch theorem in tropical geometry". *Math. Z.* 259.1 (2008): 217–230. Web.

Grigoriev, Dima and Vladimir Shpilrain. "Tropical cryptography". *Comm. Algebra* 42.6 (2014): 2624–2632. Web.

Maclagan, Diane and Bernd Sturmfels. *Introduction to tropical geometry*. Vol. 161. American Mathematical Society, Providence, RI, 2015. xii+363. Print. Graduate Studies in Mathematics.

Otter, Nina. "The geometric group law on a tropical elliptic curve". 1 (2012): 1–29. Web.

Stickel, E. "A new Method for Exchanging Secret Keys". *Proc. of the Third International Conference on Information Technology and Applications* 1 (2005): 426fffdfffdfffd430. Print.

Weisstein, Eric W. "Elliptic Cruve". *MathWorld– A Wolfram Web Resource* (). Web.