Algorithm for Group Law on Tropical Elliptic Curve

Catie Lillja   Bora Olmez

Advisors: Matthew Baker, Griffin Edwards

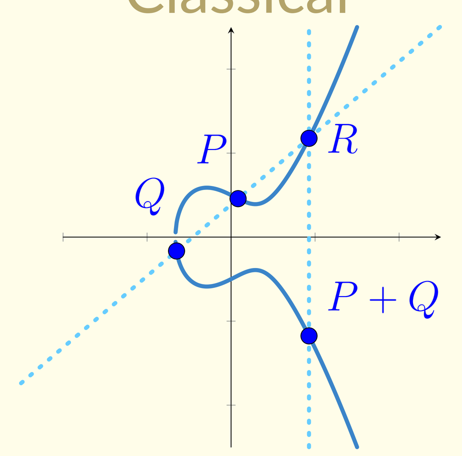
Georgia Institute of Technology

Georgia Tech College of Sciences
School of Mathematics

BACKGROUND

Group Law on Elliptic Curves

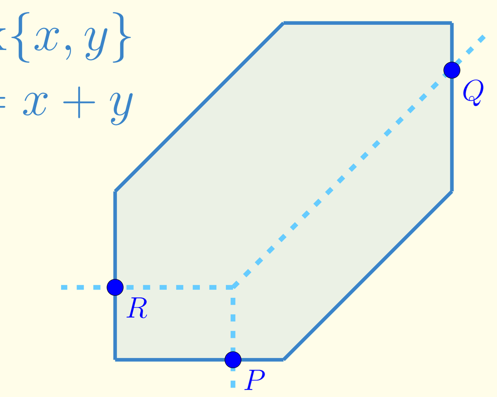
Classical



A genus 1 smooth algebraic curve over $\mathbb{R}$ with a choice of origin $\mathcal{O} = \infty$. R, P, Q lie on a Euclidean line.

Tropical (Standard Embedding)

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



A genus 1 smooth algebraic curve over the tropical semiring $\mathbb{T}$ (given by binary operations above) with an appropriate choice of origin $\mathcal{O}$. R, P, Q lie on a tropical line defined by $a \odot x \oplus b \odot y \oplus c$.

In both cases, **the group law is given by setting $\mathbf{R} + \mathbf{P} + \mathbf{Q} = \mathcal{O}$ for collinear triples $\mathbf{R}, \mathbf{P}$.**

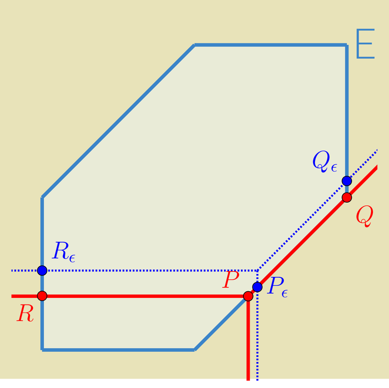
(Definition) Stable Intersection

Given a tropical line ℓ and a tropical elliptic curve E, their *stable intersection* is a set of three points:

$$\ell \cap_{st} E = \lim_{\epsilon \to 0} (\ell_\epsilon \cap E)$$

where ℓ_ϵ is any generic perturbation of ℓ. In this picture,

$$\ell \cap_{st} E = \{P, Q, R\}$$

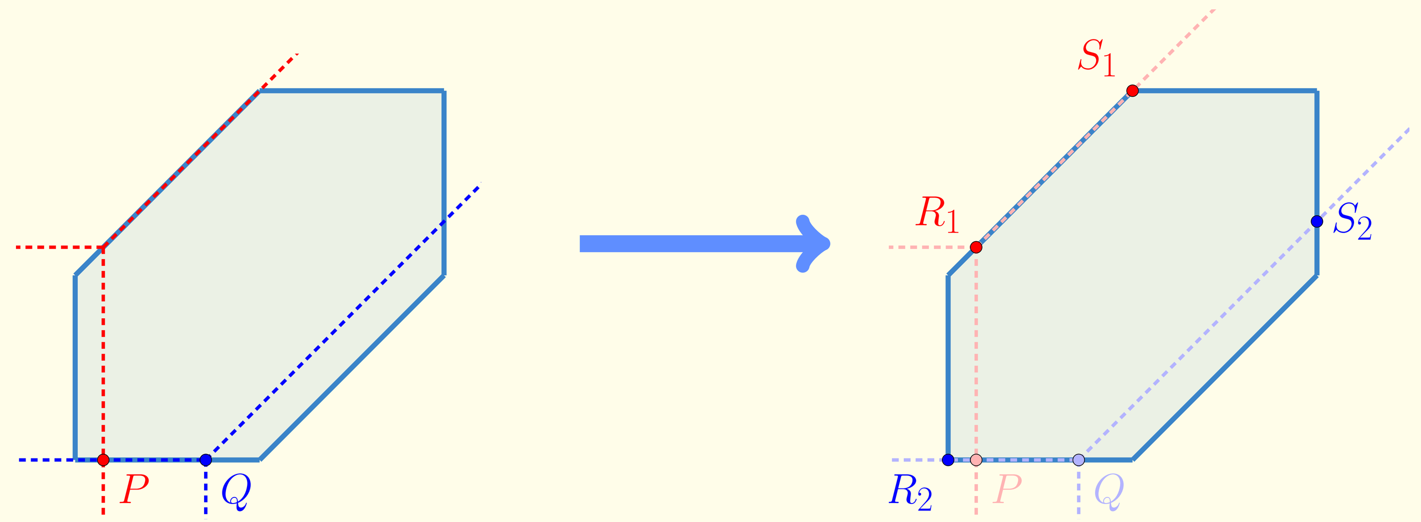


(Definition) Bad Pair

(P, Q) is a *bad pair* if $P, Q \in \ell \cap_{st} E$ for **NO** tropical line ℓ. Otherwise, (P, Q) is a *good pair*.

Problem: It is not possible to add P and Q if (P, Q) is a bad pair.

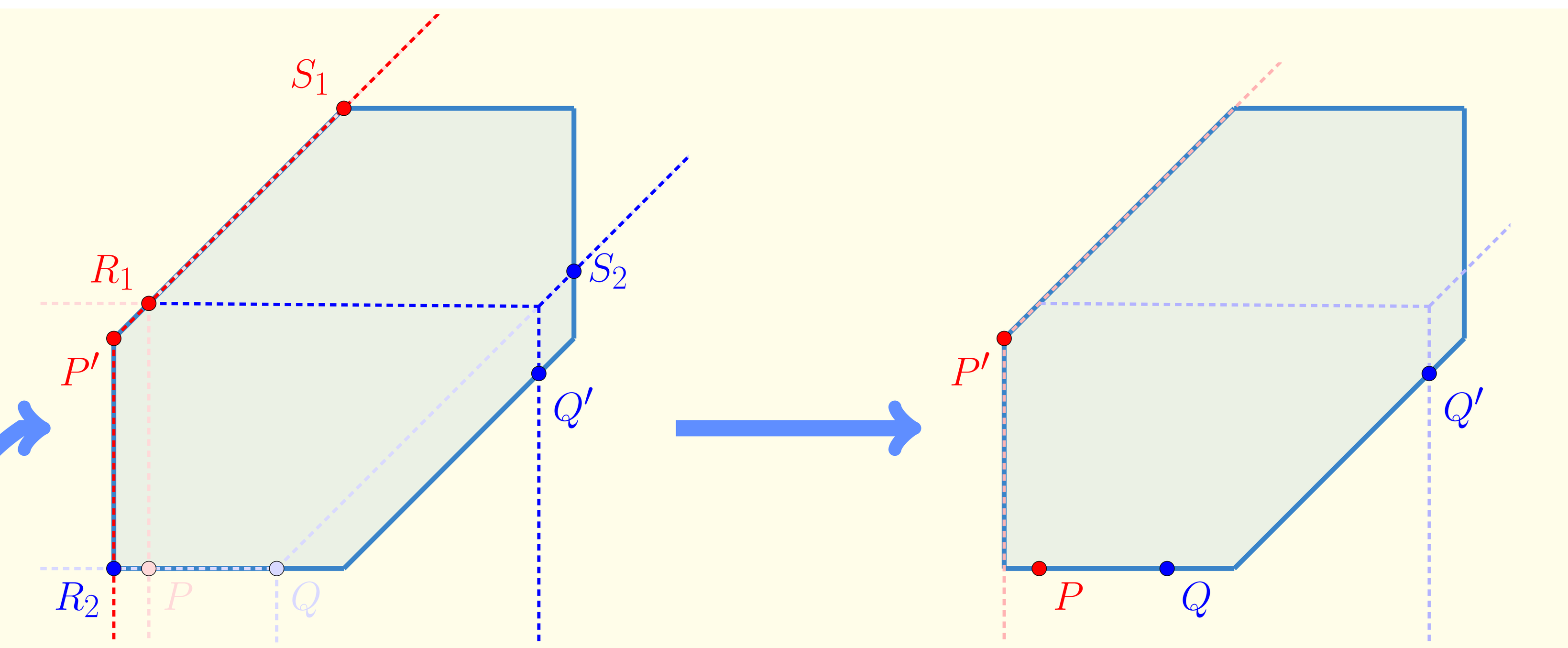
Proposed Solution: Vigeland's Moves



Step 1:
Suppose we have a bad pair (P, Q). Choose two tropical lines L_P and L_Q going through P and Q stably.

Step 2:
Label stable intersection points.

$$P + R_1 + S_1 = 0$$
$$Q + R_2 + S_2 = 0 \quad (1)$$



Step 3:
We get two new tropical lines such that

$$P' + R_2 + S_1 = 0$$
$$Q' + R_1 + S_2 = 0 \quad (2)$$

Step 4:
(P', Q') is the good pair we desired because $\exists$ a tropical line that goes through them stably and (1), (2) imply

$$P + Q = P' + Q'$$

MAIN RESULTS

Theorem: Sufficiency of a Single Move for Standard Embedding

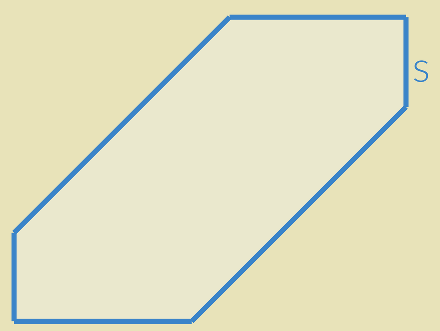
For the standard embedding, every bad pair (P, Q) can be moved to a good pair (P', Q') in exactly one move.

Proof Sketch

Exploit the symmetry of the standard embedding to fix P on the bottom edge and classify all $Q \in E$ such that (P, Q) is a bad pair. This reduces to 4 cases (one of them shown above).

General Embedding

The general embedding has a hexagonal cycle with vertical, horizontal and diagonal (of slope 1) sides. Let s be its smallest sidelength and j be its perimeter.

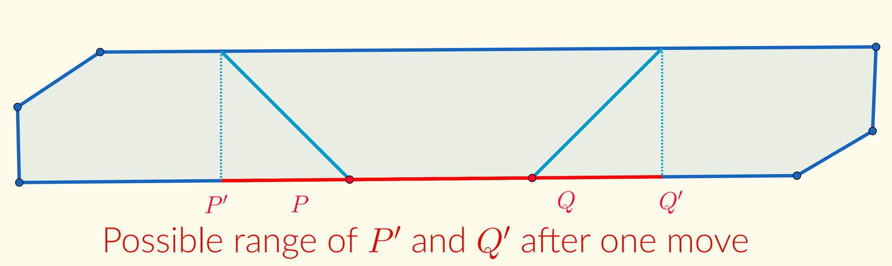


Intuition for General Embedding

The sum $P + Q$ is an invariant of any given move, it is natural to show that it is the only invariant. To this end, use local moves as motivated by the following:

Global Obstruction

Since P can only be moved at most $2s$ at a time, $\left\lceil \frac{j}{4s} \right\rceil - 1$ moves are required to get to a good pair (P', Q') such that $P + Q = P' + Q'$.

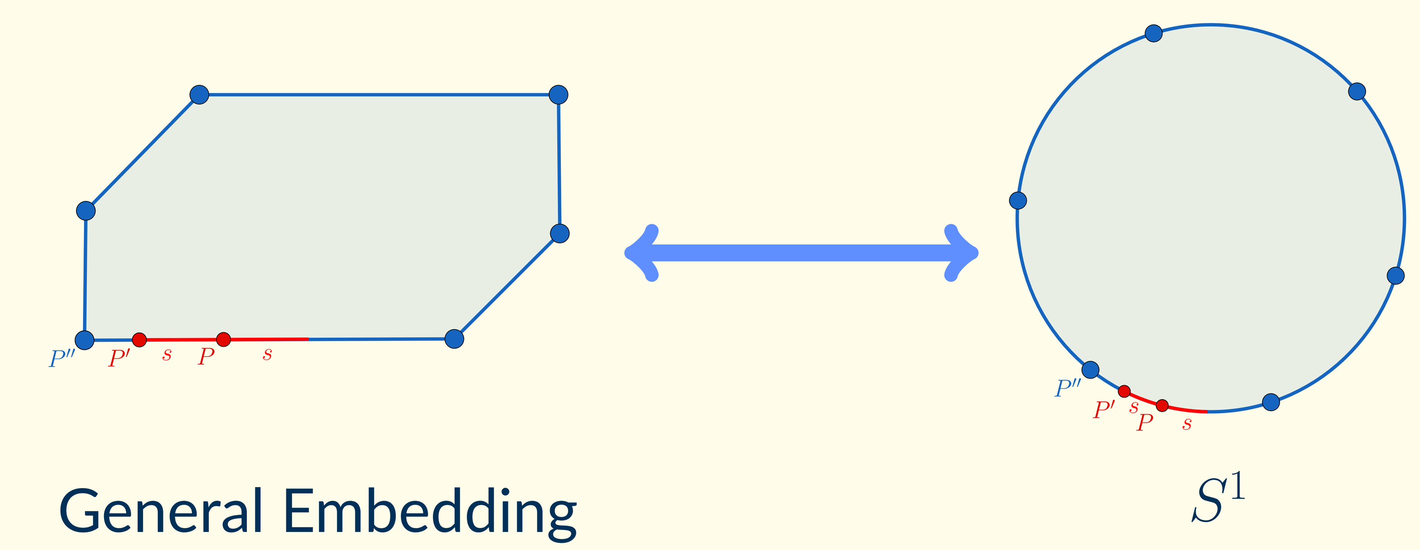


Possible range of P' and Q' after one move

Main Theorem for General Embedding

For any pair (P, Q), we can always perform two moves to shift P (in either direction), up to s away or until the next vertex, whichever is closest.

Implications for Possible Moves

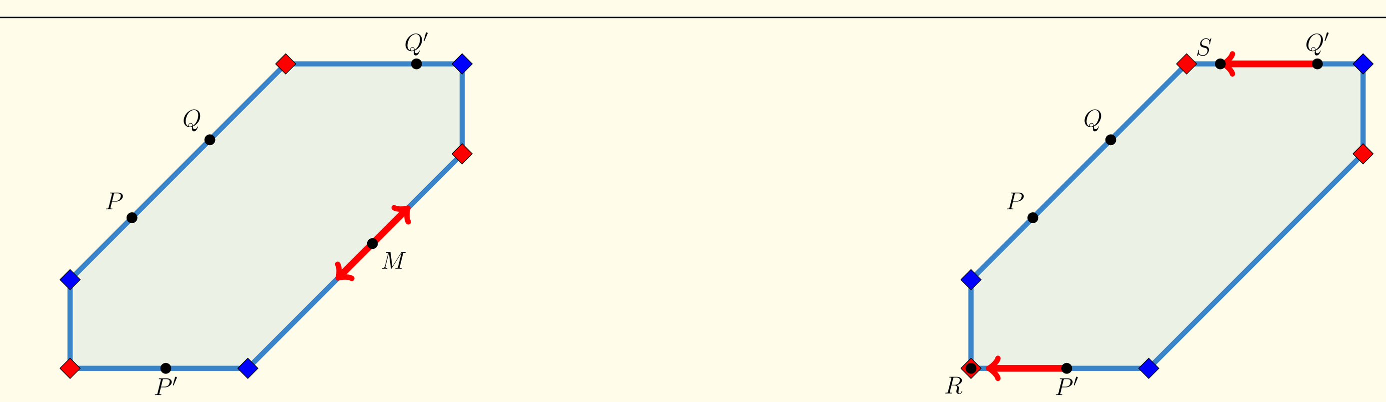


We can move P along a compact neighbourhood and thus around the whole cycle by repeatedly moving it clockwise (c.f. moving along closed arcs of positive length on S^1).

Theorem: Existence of Good Pair in Equivalence Class

If $P, Q \in E$, then $\exists R, S \in E$ such that (R, S) is a good pair and $P + Q = R + S$.

Proof Idea



Step 1:
Choose $M \in E$ such that $M + M = P + Q$. Move away from M at equal speeds (preserves sum) to find P', Q' lying on opposite edges of E with $P + Q = P' + Q'$.

Step 2:
Edges containing P', Q' both have red vertices. Moving to the closest red vertex in a similar fashion then gives a good pair (R, S).

Corollary: Complexity of Algorithm

We can move any pair (P, Q) of the general embedding to a good pair in $\left\lceil \frac{j}{s} \right\rceil + 4$ moves.

Additional Work: Elliptic Matroid

Using these ideas, we proved results about a certain matroid T_n, such as the fact that the partial valuation defined by the tropical determinant extends to a unique valuation on this matroid.

References

Chan, M. and Sturmfels, B. (2012). Elliptic curves in honeycomb form.

Vigeland, M. D. (2004). The group law on a tropical elliptic curve.

csmslillja@gmail.com (Catie Lillja, Johns Hopkins University), bo301@cam.ac.uk (Bora Olmez, University of Cambridge)