Max-Planck-Institut für Mathematik in den Naturwissenschaften Leipzig

Computing Unit Groups of Curves

by

Justin Chen, Sameera Vemulapalli, and Leon Zhang

Preprint no.: 62 2018

COMPUTING UNIT GROUPS OF CURVES

JUSTIN CHEN, SAMEERA VEMULAPALLI, AND LEON ZHANG

ABSTRACT. The group of units modulo constants of an affine variety over an algebraically closed field is free abelian of finite rank. Computing this group is difficult but of fundamental importance in tropical geometry, where it is desirable to realize intrinsic tropicalizations. We present practical algorithms for computing unit groups of smooth curves of low genus. Our approach is rooted in divisor theory, based on interpolation in the case of rational curves and on methods from algebraic number theory in the case of elliptic curves.

1. INTRODUCTION

Among the invariants of a commutative ring, the group of units is one of the most fundamental. However, explicit computation of this group is difficult, and even its structure remains mysterious in general [Fuc60]. To date, most progress has centered on rings of integers of algebraic number fields, or localizations thereof, driven by a need for practical algorithms in computational number theory [Coh93]. These results rely fundamentally on Dirichlet's unit theorem, which describes the group of units, modulo torsion, of a number field as a free abelian group of finite rank specified by simple invariants of the number field.

An analogous theorem of Samuel [Sam66] states that for a finitely generated domain over an algebraically closed field, the group of units, modulo scalars, is free abelian of finite rank. In contrast to the number field case, no formula for the rank is known. Given the coordinate ring of a very affine variety, a basis for its unit group yields an embedding of the variety into its so-called *intrinsic torus* [MS15]. In tropical geometry, this embedding of a very affine variety into its intrinsic torus realizes its *intrinsic tropicalization*, from which all other tropicalizations can be recovered. However, explicitly computing the intrinsic tropicalization is difficult, because one must first compute the unit group.

In this work we describe effective methods for computing unit groups of smooth very affine curves of low genus. Our methods rely on divisor theory for projective varieties: we embed the unit group of a very affine variety into the Weil divisor group of the projective closure, and study the cokernel of this embedding as a subgroup of the divisor class group. This allows us to give algorithms for computing unit groups of rational normal curves and elliptic curves:

Theorem 1.1. *Let $\overline{C} \subseteq \mathbb{P}^n_k$ be a rational normal curve over an algebraically closed field k, given parametrically as the image of a map $\mathbb{P}^1_k \hookrightarrow \mathbb{P}^n_k$. Let $C := \overline{C} \cap \mathbb{T}^n$ be the corresponding very affine curve, with coordinate ring R. Then Algorithm 5.4 correctly computes a $\mathbb{Z}$-basis of R^*/k^*.*

Theorem 1.2. *Let $k = \overline{\mathbb{Q}}$, let $\overline{E} \subseteq \mathbb{P}^2_k$ be an elliptic curve, and let $E := \overline{E} \cap \mathbb{T}^2$ be the corresponding very affine elliptic curve with coordinate ring R. Then Algorithm 6.13 correctly computes a $\mathbb{Z}$-basis of R^*/k^*.*

We briefly describe the structure of the paper. The basics of Samuel's theorem and intrinsic tropicalizations are discussed in Section 2. In Section 3 we develop the relationship between our problem and the geometry of boundary divisors, and describe a simple algorithm for interpolating divisors of rational functions in terms of Laurent polynomials, when possible. We consider the

Date: August 9, 2018.

families of Fermat curves and plane conics in Section 4, and rational normal curves in parametric form in Section 5. Finally, we discuss elliptic curves in Section 6.

Many of our algorithms have been implemented in Macaulay2 [GS], Singular [DGPS18], and Sage [The18]. Our code for the examples in this paper can be found at our supplementary materials website:

`https://math.berkeley.edu/~leonyz/code/`

1.3. **Acknowledgements.** Leon Zhang and Sameera Vemulapalli would like to thank the Max Planck Institute for Mathematics in the Sciences for its hospitality while working on this project. Leon Zhang was supported by a National Science Foundation Graduate Research Fellowship.

The authors thank Bernd Sturmfels for suggesting and advising this project. We would also like to thank Chris Eur and Martin Helmer for helpful discussions, Yue Ren for generous and thoughtful help in computing tropicalizations in Singular [DGPS18], and Bjorn Poonen and Ronald van Luijk for their expertise and guidance.

2. Background

We begin by stating the problem in a general setting. Let k be an algebraically closed field, and let R be a finitely generated k-algebra which is a domain. The inclusion $k \subseteq R$ induces a short exact sequence of multiplicative abelian groups

$$1 \longrightarrow k^* \longrightarrow R^* \longrightarrow R^*/k^* \longrightarrow 1 \tag{2.0.1}$$

Our goal is to compute, as explicitly as possible, the group R^*/k^*. Although this may seem to be a purely algebraic problem, the key to progress is to use insights from geometry, particularly divisor theory on projective varieties. Thus, writing $R = k[x_1, \dots, x_n]/I$ as a quotient of a polynomial ring by a prime ideal I, set $X := \operatorname{Spec} R \subseteq \mathbb{A}^n_k$, the affine variety corresponding to R, and let $\overline{X} \subseteq \mathbb{P}^n_k$ denote the projective closure of X in projective n-space. Write $\partial X := \overline{X} \setminus X = \overline{X} \cap V(x_0)$ for the boundary of $\overline{X}$, which is the intersection of $\overline{X}$ with the hyperplane at infinity in $\mathbb{P}^n_k$.

The main point is that a unit in R corresponds, via homogenization, exactly to a rational function on $\overline{X}$ which has zeros and poles only on ∂X. To be precise:

Lemma 2.1. *With notation as above, let $R \to \overline{R}$ be the homogenization map $f \mapsto \overline{f} := x_0^{\deg f} f(\frac{x_i}{x_0})$. Then:*
i) For any $f, g \in R$, $\overline{fg} = \overline{f}\,\overline{g}$, and
ii) $f \in R^*$ if and only if $V(\overline{f}) \cap \overline{X} \subseteq \partial X$.

Proof. First, note that dehomogenization is evaluation at $x_0 = 1$, hence is a ring map with kernel $(x_0 - 1)$. As the kernel contains no nonzero homogeneous elements, it follows that if f_1, f_2 are homogeneous of the same degree with the same dehomogenization, then $f_1 = f_2$.

i) Since $\overline{fg}$ and $\overline{f}\,\overline{g}$ are both homogeneous of the same degree and dehomogenize to fg, by the above reasoning they must be equal.

ii) Recall that $\partial X = \overline{X} \cap V(x_0)$, so it suffices to show that $f \in R^*$ if and only if $V(\overline{f}) \cap \overline{X} \subseteq V(x_0)$. If $g_1, \dots, g_r$ is a Gröbner basis for the defining ideal I of X, then $\overline{X}$ has defining ideal $(\overline{g_1}, \dots, \overline{g_r})$ [Eis95, Prop. 15.31]. It thus suffices to show $1 \in (f, g_1, \dots, g_r)$ if and only if $x_0 \in \sqrt{(\overline{f}, \overline{g_1}, \dots, \overline{g_r})}$. The "if" direction follows by dehomogenizing. For the "only if" direction, pick h with $1 - fh \in I$. Then $\overline{1 - fh} \in (\overline{g_1}, \dots, \overline{g_r})$. But $\overline{1 - fh} = x_0^d - \overline{fh}$, where $d = \deg(fh)$, as both sides are homogeneous and dehomogenize to $1 - fh$. By (i) therefore, $x_0^d \in (\overline{f}, \overline{g_1}, \dots, \overline{g_r})$ as desired. □

Suppose now that $\overline{X}$ is normal, and write $\operatorname{Div}(\overline{X})$ (resp. $\operatorname{Cl}(\overline{X})$) for the group of Weil divisors (resp. the divisor class group) on $\overline{X}$. Let $\operatorname{Div}^0(\overline{X})$ (resp. $\operatorname{Cl}^0(\overline{X})$) denote the subgroup of divisors (resp. divisor classes) of degree zero.

Definition 2.2. We define

$$\mathrm{Div}^0_\partial(\overline{X}) := \left\{ \sum_{\text{finite}} a_i P_i \;\middle|\; P_i \text{ component of } \partial X, a_i \in \mathbb{Z}, \sum a_i = 0 \right\} \subseteq \mathrm{Div}^0(\overline{X})$$

i.e. the subgroup of $\mathrm{Div}^0(\overline{X})$ supported on ∂X. This makes sense since ∂X has codimension 1 in $\overline{X}$.

Now, homogenization gives a natural map $R^* \hookrightarrow \mathrm{Frac}(\overline{R})^*$, which is a homomorphism of multiplicative groups by Lemma 2.1(i). Composing with the natural map $\mathrm{Frac}(\overline{R})^* \to \mathrm{Div}^0(\overline{X})$, $f \mapsto \mathrm{div}(f)$ gives a homomorphism $\widetilde{\phi} : R^* \to \mathrm{Div}^0(\overline{X})$ from a multiplicative abelian group to an additive abelian group. Since a unit is a rational function which is invertible on X, hence has zeros and poles only on ∂X by Lemma 2.1(ii), this shows that the image of $\widetilde{\phi}$ is contained in $\mathrm{Div}^0_\partial(\overline{X})$. Next, the kernel of $\widetilde{\phi}$ consists of units whose associated rational function has no zeros or poles anywhere on $\overline{X}$. Such an element must be a scalar, i.e. comes from k^*, so we have an induced map $\phi : R^*/k^* \hookrightarrow \mathrm{Div}^0_\partial(\overline{X})$.

Putting the above reasoning together yields a classical theorem of Samuel [Sam66] on the structure of the unit group:

Theorem 2.3 ([Sam66])**.** *Let k be an algebraically closed field, and let R be a finitely generated k-algebra that is a domain. Then R^*/k^* is a finitely generated free abelian group.*

Proof. Let $\overline{R}$ be the homogenization of R with respect to some new variable x_0. If $\overline{X} = \mathrm{Proj}(\overline{R})$ is normal, then the reasoning above shows that R^*/k^* embeds in the finitely generated free abelian group $\mathrm{Div}^0_\partial(\overline{X})$, and subgroups of finitely generated free abelian groups are again finitely generated free abelian.

If $\overline{X}$ is not normal, let $\widetilde{\overline{X}}$ be the normalization of $\overline{X}$. The normalization map $\widetilde{\overline{X}} \xrightarrow{\eta} \overline{X}$ identifies $\eta^{-1}(X)$ with $\mathrm{Spec}(\widetilde{R})$, where $\widetilde{R}$ is the integral closure of R in its fraction field. This gives an inclusion map $R^*/k^* \hookrightarrow (\widetilde{R})^*/k^*$. As $(\widetilde{R})^*/k^*$ is finitely generated free abelian by the previous case, R^*/k^* is as well. □

Remark 2.4. Note that the unit group of the coordinate ring of a projective variety is trivial to compute: indeed, in this case $\overline{R}^* = k^*$, as any positively graded domain has units concentrated in degree 0. Thus Theorem 2.3 is only interesting for rings which are not positively graded.

Remark 2.5. The assumptions in Theorem 2.3 are necessary: if k is not algebraically closed, then the unit group modulo scalar units may have torsion, i.e. roots of unity. If R is not a domain, then R^*/k^* need not be $\mathbb{Z}$-free: e.g. $R = k[x]/(x^2)$ has R^*/k^* isomorphic to the additive group of k.

Remark 2.6. In the setting of Theorem 2.3, the exact sequence (2.0.1) splits (since R^*/k^* is free abelian), i.e. $R^* \cong k^* \oplus R^*/k^*$. Thus we also understand R^* if we understand R^*/k^*.

2.7. **Intrinsic tropicalization.** We now discuss some motivation for computing unit groups coming from tropical geometry, following the presentation in [MS15]. Recall that a variety X is said to be *very affine* if X admits a closed embedding into an algebraic torus $\mathbb{T}$. Intuitively, a subvariety of $\mathbb{P}^m$ is affine if it misses a coordinate hyperplane, and very affine if it misses all coordinate hyperplanes. Algebraically, this means that the coordinate ring R of X is (isomorphic to) a quotient of a Laurent polynomial ring $k[x_1^{\pm}, \ldots, x_m^{\pm}]$. We note that given a very affine variety $X \subseteq \mathbb{T}^n$, one can take its projective closure $\overline{X} \subseteq \mathbb{P}^n$ with boundary $\partial X := \overline{X} \setminus X = \overline{X} \cap V(x_0 \cdots x_n)$, and the above discussion (cf. Lemma 2.1, Definition 2.2) carries over to this setting.

In general, there are many different closed embeddings of X into tori $\mathbb{T}^m$ for various m. To remove the dependence on the choice of embedding, one must choose a "natural" embedding of

X into a fixed torus. As it turns out, the right object to consider is the so-called *intrinsic torus* of X, which is by definition [MS15, Definition 6.4.2]

$$\mathbb{T}_{in} := \mathrm{Hom}_{\mathbb{Z}}(R^*/k^*, k^*).$$

Note that by Theorem 2.3, R^*/k^* is free abelian, so the Hom group is isomorphic to a product of copies of k^*, which is an algebraic torus over k. A $\mathbb{Z}$-basis $f_1, \ldots, f_n$ of R^*/k^* gives rise to an embedding $i : X \hookrightarrow T_{in}$, via $x \mapsto (f_1(x), \ldots, f_n(x))$. With such a choice of basis, the importance of the intrinsic torus is immediate from the following "pseudo-universal" property (cf. [MS15, Proposition 6.4.4]): for every closed embedding $j\colon X \hookrightarrow \mathbb{T}^m$ of X into a torus, there is a map of tori $\varphi : \mathbb{T}_{in} \to \mathbb{T}^m$ given by Laurent monomials (which need not be an embedding) such that the following diagram commutes:

$$\begin{array}{ccc} X & \xhookrightarrow{i} & \mathbb{T}_{in} \\ & \searrow^{j} & \downarrow{\scriptstyle \varphi} \\ & & \mathbb{T}^m \end{array}$$

It is a basic task in tropical geometry to tropicalize a very affine variety with respect to a particular embedding in a torus. From a foundational viewpoint, it is desirable to have an *intrinsic tropicalization*, with respect to the intrinsic torus, so that the tropicalization depends only on the very affine variety X and not the specific embedding $X \hookrightarrow \mathbb{T}^m$. Furthermore, in the setup of the commutative diagram above, the tropicalization of X embedded in $\mathbb{T}^m$ is given by the image of the intrinsic tropicalization under the affine map $\mathrm{Trop}(\varphi)$. Hence any other tropicalization of X can be recovered from the intrinsic tropicalization.

However, from a computational standpoint, the very affine variety is most often described by its ideal in a fixed embedding. To obtain an intrinsic tropicalization one must be able to compute the defining ideal of the very affine variety in its intrinsic torus; the key to doing so is to first compute a basis of R^*/k^*. Of course an embedding i into the intrinsic torus depends on our choice of basis for R^*/k^*, but we nevertheless often speak of *the* intrinsic embedding into the intrinsic torus.

3. General results on varieties

In this section we reinterpret our problem in the context of class groups. We retain the setup from the previous section: let X be a very affine variety over an algebraically closed field k, with coordinate ring R.

Definition 3.1. Define $\mathrm{Cl}^0_\partial(\overline{X})$ to be the cokernel of the group homomorphism $R^*/k^* \xrightarrow{\phi} \mathrm{Div}^0_\partial(\overline{X})$.

By definition, there is a short exact sequence of abelian groups

$$1 \longrightarrow R^*/k^* \xrightarrow{\phi} \mathrm{Div}^0_\partial(\overline{X}) \longrightarrow \mathrm{Cl}^0_\partial(\overline{X}) \longrightarrow 0 \tag{3.1.1}$$

Corollary 3.2. *Let r be the number of divisorial components of ∂X. Then $\operatorname{rank} R^*/k^* \leq r - 1$, with equality if and only if $Cl^0_\partial(\overline{X})$ is torsion.*

Proof. The subgroup $\mathrm{Div}_\partial(\overline{X})$ of $\mathrm{Div}(\overline{X})$ (consisting of Weil divisors supported on ∂X) is a free group of rank r, and the degree 0 condition implies $\mathrm{Div}^0_\partial(\overline{X})$ is a free subgroup of rank $r-1$. □

Corollary 3.3. *If C is a very affine curve over k with coordinate ring R, with projective closure $\overline{C} \subseteq \mathbb{P}^n_k$ of degree d, then $\operatorname{rank} R^*/k^* \leq (n+1)d - 1$.*

Proof. As C is a curve, the divisorial components of ∂C are just the (closed) points of ∂C. Since C is very affine, the boundary ∂C consists of the intersections of $\overline{C}$ with each of the $n+1$ coordinate hyperplanes in $\mathbb{P}^n_k$. Then $\deg \overline{C} = d$ implies ∂C consists of at most $(n+1)d$ points, and the result follows from Corollary 3.2. □

Samuel's Theorem 2.3 tells us that the structure of the unit group – as an *abstract* group – is as nice as possible. However, we need more information about the other groups in (3.1.1) to explicitly give generators for R^*/k^*. The following basic, but crucial, point states that all relations in $\mathrm{Cl}^0_\partial(\overline{X})$ are "geometric", in the sense that they come from the class group of $\overline{X}$.

Proposition 3.4. *$Cl^0_\partial(\overline{X})$ is a subgroup of $Cl^0(\overline{X})$.*

Proof. Consider the composition

$$\mathrm{Cl}^0_\partial(\overline{X}) \cong \mathrm{Div}^0_\partial(\overline{X})/(R^*/k^*) \xhookrightarrow{\alpha} \mathrm{Div}^0(\overline{X})/(R^*/k^*) \xrightarrow{\beta} \mathrm{Cl}^0(\overline{X}).$$

To show that the composite is an injection, it suffices to show that $\mathrm{Im}(\alpha) \cap \ker(\beta) = \{0\}$. But this follows since $\ker(\beta) = \mathrm{Frac}(\overline{R})^*/(R^*/k^*)$, and $\mathrm{Frac}(\overline{R})^* \cap \mathrm{Div}^0_\partial(\overline{X}) = R^*/k^*$, as a rational function on $\overline{X}$ supported only on ∂X is a unit on X. □

Remark 3.5. Recall that the class group of the ring of integers of a number field is finite. If a similar result held in our setting, Corollary 3.2 would give an explicit description for the rank of R^*/k^*. Unfortunately, of course, $\mathrm{Cl}(\overline{X})$ need not be so well-behaved in general.

In general, our approach to computing R^*/k^* via (3.1.1) proceeds in three parts:

Question 1. What are the generators of the image of R^*/k^* in $\mathrm{Div}^0_\partial(\overline{X})$?

Question 2. Given $D \in \mathrm{Div}^0_\partial(\overline{X})$ that is in the image of R^*/k^*, can we find polynomials f, g such that $f/g \in R^*/k^*$ is mapped to D (under the inclusion $R^* \subseteq \mathrm{Frac}(\overline{R})$)?

Question 3. Given an element of R^*/k^* expressed as a rational function as in Question 2, can we find a representative for it in R?

Note that Proposition 3.4 suggests a path towards progress on Question 1, as the image of R^*/k^* in $\mathrm{Div}^0_\partial(\overline{X})$ equals $\ker(\mathrm{Div}^0_\partial(\overline{X}) \to \mathrm{Cl}^0_\partial(\overline{X}))$, and by Proposition 3.4 this is the same as $\ker(\mathrm{Div}^0_\partial(\overline{X}) \to \mathrm{Cl}^0(\overline{X}))$. Ultimately though, one needs control over $\mathrm{Cl}^0(\overline{X})$ to solve Questions 1 and 2, and this will require methods particular to the varieties under consideration.

On the other hand, Question 3 can be solved with relatively basic Gröbner basis algorithms, which we use repeatedly in the remainder of the paper. We note that ordinary Gröbner basis arguments over polynomial rings can be adapted to Laurent polynomial rings by identifying the rings $k[x_1^{\pm}, \ldots, x_n^{\pm}] \cong k[x_1, \ldots, x_n, t]/(tx_1 \ldots x_n - 1)$.

Algorithm 3.6 (Clearing denominators)**.**
INPUT: $f, g \in k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$, $I = (\phi_1, \ldots, \phi_m) \subseteq k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ with a fixed monomial order
OUTPUT: $h \in k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ with $f - gh \in I$ if such an h exists, or **false** otherwise

```
J ← I + (g)
G ← GröbnerBasis(J)
if f ∉ ideal(G) then
    return false
end if
C = (C_0, ..., C_m) ← a vector with entries in R such that f = C_0 g + C_1 φ_1 + ... + C_m φ_m
return C_0
```

Lemma 3.7. *For $f, g \in R = k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]/I$, Algorithm 3.6 correctly determines whether there exists $h \in R$ such that $f = gh$, and returns such an h if it exists.*

Proof. A standard Gröbner basis argument checks whether $f \in J$ and, if so, finds such a vector C as above. Note that $f \in J$ if and only if there exists h such that $f - gh \in I$, so that $f = gh \in R$. □

Algorithm 3.8 (Testing units).
INPUT: $h \in k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$, $I = (\phi_1, \ldots, \phi_m) \subseteq k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ with a fixed monomial order
OUTPUT: **true** if $h \in (k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]/I)^*$, or **false** otherwise

```
J ← I + (h)
G ← GröbnerBasis(J)
if 1 ∈ ideal(G) then
    return true
end if
return false
```

Lemma 3.9. *For $h \in R = k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]/I$, Algorithm 3.8 correctly tests if h is a unit in R.*

Proof. A standard Gröbner basis argument checks whether $1 \in J$. Note that $1 \in J = I + (h) \subseteq k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ if and only if $h \in (k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]/I)^*$. □

Algorithm 3.10 (Computing preimages of $R^* \to \mathrm{Frac}(\overline{R})^*$).
INPUT: $\overline{f}, \overline{g} \in k[x_0, \ldots, x_n]$ homogeneous, $\frac{\overline{f}}{\overline{g}} \in \mathrm{Frac}(\overline{R})^*$ and $I = (\phi_1, \ldots, \phi_m) \subseteq k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ with a fixed monomial order
OUTPUT: $h \in k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ such that $h = \frac{\overline{f}}{\overline{g}}$ in $\mathrm{Frac}(\overline{R})^*$ (via the inclusion $R^* \subseteq \mathrm{Frac}(\overline{R})^*$) if such an h exists, or **false** otherwise

```
f ← f̄(1, x_1, ..., x_n)
g ← ḡ(1, x_1, ..., x_n)
if Algorithm 3.6(f, g, I) = false then
    return false
else
    h ← Algorithm 3.6(f, g, I)
    if Algorithm 3.8(h, I) = true then
        return h
    else
        return false
    end if
end if
```

Lemma 3.11. *Let X be a very affine variety over k with coordinate ring $R = k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]/(\phi_1, \ldots, \phi_m)$. Let $\overline{f}$ and $\overline{g}$ be homogeneous polynomials in $k[x_0, \ldots, x_n]$, and $f, g \in k[x_1, \ldots, x_n]$ their dehomogenizations with respect to x_0. Given a rational function $\frac{\overline{f}}{\overline{g}} \in \mathrm{Frac}(\overline{R})^*$, Algorithm 3.10 correctly decides whether $\frac{f}{g} \in R^*$ (via the inclusion $R^* \subseteq \mathrm{Frac}(\overline{R})^*$), and if so, computes a representative $h \in k[x_1^{\pm 1}, \ldots, x_n^{\pm}]$ for $\frac{f}{g}$.*

Proof. If $\overline{f}/\overline{g} \in R^*$ then there must exist a Laurent polynomial $h \in R^*$ such that $\frac{\overline{f}}{\overline{g}} = \overline{h}$ in $\mathrm{Frac}(\overline{R})^*$, where $\overline{h}$ is the homogenization of h with respect to x_0. Thus $\overline{f} - \overline{g}\overline{h} = 0$ in $\mathrm{Frac}(\overline{R})^*$, so $f - gh \in I$. Since $h \in R^*$, Algorithm 3.8 will verify that h is a unit, and Algorithm 3.10 will return h.

Now assume that $\overline{f}/\overline{g} \notin R^*$. The algorithm will return false unless Algorithm 3.6 returns some $h \in R^*$ such that $f - gh$. Suppose this occurs. By homogenizing, we see that $\overline{f} = \overline{g}\overline{h}$ in $\overline{R}$ and $\frac{\overline{f}}{\overline{g}} = \overline{h}$ in $\mathrm{Frac}(\overline{R})^*$, which is a contradiction. □

4. Fermat curves and plane conics

We now consider two simple families of curves, Fermat curves and plane conics. These serve as our first two classes of examples for our general problem of computing unit groups.

4.1. **Fermat curves.** We first approach the problem of constructing unit groups in a purely elementary, algebraic way:

Lemma 4.2. *Let* $T := k[x_1^{\pm 1}, \dots, x_d^{\pm 1}]$ *be a Laurent polynomial ring,* $I \subseteq T$ *an ideal,* $u \in T$ *a monomial,* $a \in k^*$*, and* $f \in I$*. If there exist* $g, h \in T$ *with* $f + au = gh$*, then* $\overline{g}, \overline{h}$ *are units in* $R := T/I$*.*

Proof. Note that u is a unit in T (being monomial), so $a\overline{u}$ is a unit in R. Since $\overline{g}\overline{h} = a\overline{u} \in R^*$, we have that $\overline{g}$ and $\overline{h}$ are also units in R. □

Example 4.3 (Fermat curves)**.** Consider the family of Fermat curves, which are plane curves in $\mathbb{P}^2 = \mathrm{Proj}(k[x, y, z])$ defined by equations of the form $x^d + y^d = z^d$, for $d \in \mathbb{N}$. For a fixed degree d, we have $\overline{C} := V(x^d + y^d - z^d) \subseteq \mathbb{P}^2$ with homogeneous coordinate ring $\overline{R} := \mathbb{C}[x, y, z]/(x^d + y^d - z^d)$. Dehomogenizing with respect to z and intersecting with the torus in $\mathbb{A}^2$ gives a very affine Fermat curve C with coordinate ring $R = \mathbb{C}[x^{\pm 1}, y^{\pm 1}]/(x^d + y^d - 1)$.

We will use (3.1.1) and Lemma 4.2 to show that the unit group R^*/k^* has $3d - 1$ independent elements. By Corollary 3.3, $\operatorname{rank} R^*/k^* \leq (n+1)d - 1 = 3d - 1$, so this bound is tight.

Consider the relation

$$-x^d = y^d - 1 = \prod_{i=0}^{d-1} (y - \zeta_d^i)$$

which holds in R, where ζ_d is a primitive d-th root of unity. From Lemma 4.2, we conclude that $(y - \zeta_d^i)$ is a unit in R, for all $0 \leq i \leq d-1$. Interpreting the above relation as a dependency among $x, y - \zeta_d, \dots, y - \zeta_d^{d-1}$ in R^*/k^*, we can write any $y - \zeta_d^i$ multiplicatively in terms of x and $y - \zeta_d^j$ for $j \neq i$. Thus we can choose – for instance – to treat $y - \zeta_d^{d-1}$ as redundant, and we obtain new units $y - \zeta_d^i$ for $0 \leq i \leq d-2$. Note that the relation above does not give a way to express x in terms of $y - \zeta_d^i$, since x appears with multiplicity d.

In an analogous way, we may also rearrange the defining equation of R to obtain

$$-y^d = x^d - 1 = \prod_{i=0}^{d-1} (x - \zeta_d^i)$$

which gives new units $x - \zeta_d^i$ for $0 \leq i \leq d-2$. Finally, the rearrangement

$$1 = x^d + y^d = \prod_{i=0}^{d-1} (x - \zeta_{2d}^{2i+1} y)$$

gives new units $x - \zeta_{2d}^{2i+1} y$ for $0 \leq i \leq d-2$.

We thus have the units $x - \zeta_d^i$, $y - \zeta_d^i$, $x - \zeta_{2d}^{2i+1}$ where $0 \leq i \leq d-2$. In addition to the two units x, y, this gives a total of $3(d-1) + 2 = 3d - 1$ units. Note that although we have accounted for obvious redundancies by removing $x - \zeta_d^{d-1}, y - \zeta_d^{d-1}$, and $x + \zeta_{2d}^{2d-1} y$, we have not yet shown that these $3d - 1$ units are independent. Algebraically, this would entail showing that there are no nontrivial multiplicative relations between these $3d - 1$ elements, a fairly nontrivial task. We instead adopt a geometric approach, whose utility will become evident already in this case.

First, the divisors of these units (viewed as rational functions) are supported on the boundary ∂C of the Fermat curve, which consists of the following $3d$ points:

(1) $P_i := [\zeta_{2d}^{2i+1} : 1 : 0]$ for $0 \leq i \leq d-1$

(2) $Q_i \coloneqq [\zeta_d^i : 0 : 1]$ for $0 \le i \le d-1$
(3) $T_i \coloneqq [0 : \zeta_d^i : 1]$ for $0 \le i \le d-1$

As before, let $\phi : R^*/k^* \to \mathrm{Div}_\partial^0(\overline{X})$ be the injection in Equation (3.1.1). We have

(1) $\phi(x) = \sum T_i - \sum P_i$
(2) $\phi(y) = \sum Q_i - \sum P_i$
(3) $\phi(y - \zeta_d^j) = dT_j - \sum P_i$ for $0 \le j \le d-2$
(4) $\phi(x - \zeta_d^j) = dQ_j - \sum P_i$ for $0 \le j \le d-2$
(5) $\phi(x - \zeta_{2d}^{2j+1} y) = (d-1)P_j - \sum_{i \ne j} P_i$ for $0 \le j \le d-2$

Under the identification $\mathrm{Div}_\partial(\overline{C}) = \mathbb{Z}\langle P_1, \dots, P_d, Q_1, \dots, Q_d, T_1, \dots, T_d\rangle \cong \mathbb{Z}^{3d}$, we obtain the following $3d \times (3d-1)$ matrix whose columns represent the divisors of our given units.

A straightforward check shows that this matrix has full rank $3d-1$, and therefore our units have no relations. It is natural at this point to ask whether these units form a basis for the unit group. It turns out that this need not be the case, as shown in Example 4.8.

Remark 4.4. We observe several things about this computation. First, we did not necessarily compute generators of R^*/k^*. Instead, we found enough mutually independent elements to confirm a rank statement on R^*/k^*. Next, this technique was only effective for the Fermat curve because of special features of its defining equation. With more variables or nearly any perturbation of the defining equation, the method of obtaining units above fails. Finally, the argument above can only prove lower bounds on the rank of the unit group. We want to compute generators of the unit group, so in general we will need more tools than Lemma 4.2.

4.5. **Plane conics.** Let $\overline{C} \subseteq \mathbb{P}_k^2$ be a smooth projective plane conic defined by a homogeneous quadric $f(x,y,z)$, and C the corresponding very affine curve (obtained by dehomogenizing with respect to z and intersecting with the 2-torus $\mathbb{T}^2 \coloneqq \mathbb{A}^2 \setminus V(xy)$), with coordinate ring R. We describe methods for answering Question 1 and Question 2 in this case. Combined with Lemma 3.11, this gives an algorithm to compute a basis of C^*/k^*.

Algorithm 4.6 (Computing unit groups of conics)**.**
INPUT: A homogeneous quadric $f(x,y,z)$ defining a plane conic $\overline{C} \subseteq \mathbb{P}^2$
OUTPUT: A basis of R^*/k^*

```
P_1, ..., P_n ← boundary points of C̄
P ← any other point of C̄
for all i ∈ {1, ..., n} do
    L_i ← defining equation of line between P_i and P
end for
for all i ∈ {1, ..., n − 1} do
    Compute f_i ∈ k[x^{±1}, y^{±1}] equivalent to L_i/L_{i+1} in R using Algorithm 3.10
end for
return f_1, ..., f_{n−1}
```

Theorem 4.7. *Algorithm 4.6 computes a basis for* R^*/k^*.

Proof. Observe that $\mathrm{Cl}^0(\overline{C}) = 0$ (as $\overline{C} \cong \mathbb{P}^1$). (3.1.1) then implies that the injection $R^*/k^* \hookrightarrow \mathrm{Div}_\partial^0(\overline{C})$ is an isomorphism. Then, note that $P_1 - P_2, \cdots, P_{n-1} - P_n$ forms a basis for $\mathrm{Div}_\partial^0(\overline{C})$, and L_i/L_{i+1} corresponds to the divisor $P_i - P_{i+1}$. Applying Algorithm 3.10 finishes the proof. □

Note that the choice of basis $\{P_i - P_{i+1}\}$ in the above proof was arbitrary; any basis of $\mathrm{Div}_\partial^0(\overline{C})$ would suffice. On the other hand, this basis gives the very simple rational functions L_i/L_{i+1}.

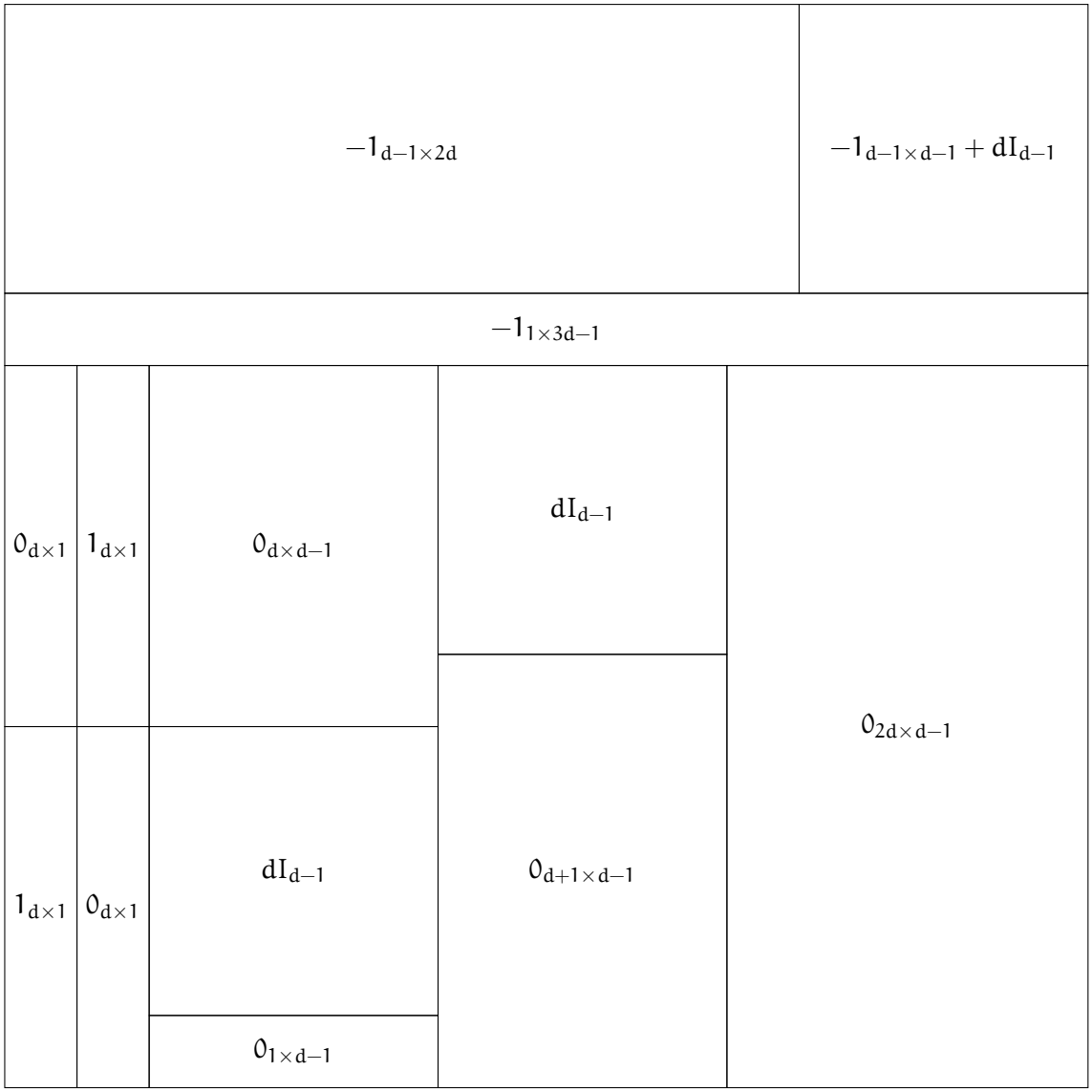

FIGURE 1. The block matrix whose columns are divisors of the units described in Example 4.3 for the Fermat curve $x^d + y^d = z^d$. Here $a_{m\times n}$ is an $m \times n$ matrix whose elements are all a, and I_n is the $n \times n$ identity matrix.

Example 4.8. Consider the degree 2 Fermat curve $\overline{C}$ defined by $x^2 + y^2 = z^2$. We show that the units produced in Example 4.3 are not generators of R^*/k^*. As in Example 4.3, we have the following boundary points:

(1) $P_0 \coloneqq [i\colon 1\colon 0]$
(2) $P_1 \coloneqq [-i\colon 1\colon 0]$
(3) $Q_0 \coloneqq [1\colon 0\colon 1]$
(4) $Q_1 \coloneqq [-1\colon 0\colon 1]$
(5) $T_0 \coloneqq [0\colon 1\colon 1]$
(6) $T_1 \coloneqq [0\colon -1\colon 1]$

Example 4.3 gives the following units and divisors (with $R^*/k^* \overset{\phi}{\hookrightarrow} \mathrm{Div}^0_\partial(\overline{C})$ as in Equation (3.1.1)):

(1) $\phi(x) = T_0 + T_1 - P_0 - P_1$
(2) $\phi(y) = Q_0 + Q_1 - P_0 - P_1$
(3) $\phi(y-1) = 2T_0 - P_0 - P_1$
(4) $\phi(x-1) = 2Q_0 - P_0 - P_1$
(5) $\phi(x - iy) = P_0 - P_1$

The subgroup of $\mathrm{Div}^0_\partial(\overline{C})$ generated by these divisors is given by the integer column span of the matrix, which is exactly Figure 1 for $d = 2$:

$$\begin{bmatrix} -1 & -1 & -1 & -1 & 1 \\ -1 & -1 & -1 & -1 & -1 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

As noted in Algorithm 4.6, one basis for $\mathrm{Div}^0_\partial(\overline{C})$ is $\{P_i - P_{i+1} \mid 1 \le i \le n-1\} = P_1 - P_2, P_2 - P_3, \ldots, P_{n-1} - P_n$. From this basis we obtain the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$

The first lattice has index 4 in the second. It follows that the units given in Example 4.3 are not generators in this case.

Example 4.9. Let $\overline{C}$ be the conic defined by $f = (1+t)x^2 + (1+t)y^2 + (1+t)z^2 - (2+2t+t^2)xy - (2+2t+t^2)yz - (2+2t+t^2)xz$, where k is the field of Puiseux series in t over $\mathbb{C}$. Consider the very affine curve C given by intersecting with the canonical torus. Its boundary points are

(1) $P_1 := [0 : 1 : t+1]$
(2) $P_2 := [0 : t+1 : 1]$
(3) $P_3 := [1 : 0 : t+1]$
(4) $P_4 := [t+1 : 0 : 1]$
(5) $P_5 := [1 : t+1 : 0]$
(6) $P_6 := [t+1 : 1 : 0]$

As described above, we can take a basis of $\mathrm{Div}^0_\partial(\overline{C})$ to be differences of these boundary points, e.g. $P_3 - P_1$, $P_3 - P_2$, $P_5 - P_3$, $P_5 - P_4$, and $P_6 - P_1$. Algorithm 4.6 gives the following particularly nice generators of the unit group:

(1) $P_3 - P_1$ gives $f_1 :=$ (line between P_3 and P_2)/(line between P_1 and P_2) $= \frac{(t+1)^2x+y-(t+1)}{x} = (t+1)^2 + yx^{-1} - (t+1)x^{-1}$
(2) $P_3 - P_2$ gives $f_2 :=$ (line between P_1 and P_3)/(line between P_1 and P_2) $= \frac{(t+1)x+(t+1)y-1}{x} = (t+1) + (t+1)yx^{-1} - x^{-1}$
(3) $P_5 - P_3$ gives $f_3 :=$ (line between P_5 and P_4)/(line between P_3 and P_4) $= \frac{(t+1)x-y-(t+1)^2}{y} = (t+1)xy^{-1} - 1 - (t+1)^2y^{-1}$
(4) $P_5 - P_4$ gives $f_4 :=$ (line between P_5 and P_3)/(line between P_3 and P_4) $= \frac{(t+1)x-y-1}{y} = (t+1)xy^{-1} - 1 - y^{-1}$

(5) $P_6 - P_1$ gives $f_5 :=$ (line between P_6 and P_2)/(line between P_1 and P_2) $= \frac{x-(t+1)y+(t+1)^2}{x} = 1-(t+1)yx^{-1}+(t+1)^2x^{-1}$

So the intrinsic torus has dimension 5, and these generators specify a map into the intrinsic torus, corresponding to the ring map $\varphi\colon k[x_1^{\pm 1},\dots,x_5^{\pm 1}] \to k[x^{\pm 1},y^{\pm 1}]/(f)$ sending $x_i \mapsto f_i$.

We note that the tropicalization of f is simply the tropical line $0 \oplus x \oplus y$ shown in Figure 2:

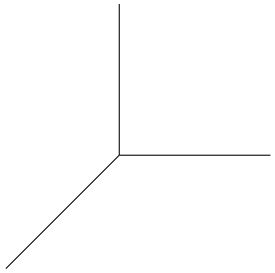

FIGURE 2. The tropicalization of the conic in Example 4.9.

We used Singular [DGPS18] to compute the tropicalization of f in its intrinsic torus with basis equal to $\{x, y, f_1, f_2, f_3\}$. The intrinsic tropicalization has the following snowflake structure typical of a generic tropical conic as in Figure 3:

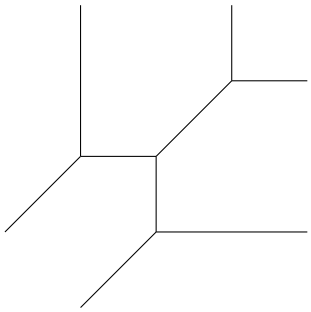

FIGURE 3. The intrinsic tropicalization of the conic in Example 4.9.

Remark 4.10. Consider the complete graph whose nodes are the elements of ∂C. Choose a spanning tree of this graph, and pick an edge for each direction. Each edge of this tree gives a divisor; namely an edge from P to Q gives the divisor $P - Q$. This gives a basis of $\mathrm{Div}_\partial(\overline{C})$.

For instance, in Example 4.8, the basis

$$P_0 - Q_0, P_1 - Q_0, Q_1 - P_0, T_0 - P_0, T_1 - P_0$$

corresponds to the directed tree in Figure 4:

Similarly, the basis

$$Q_0 - P_0, Q_0 - P_1, Q_0 - Q_1, Q_0 - T_0, Q_0 - T_1$$

corresponds to the tree in Figure 5 (rooted at Q_0):

5. Rational Normal Curves

We next turn our attention to rational normal curves in parametric form. Recall that for any n, a rational normal curve $\overline{C}$ of degree n is the image of $\mathbb{P}^1$ under an embedding $\nu\colon \mathbb{P}^1 \hookrightarrow \mathbb{P}^n$ given by $\nu([S\colon T]) = [f_0(S,T) : \cdots : f_n(S,T)]$, where $f_0,\dots,f_n$ are k-linearly independent homogeneous

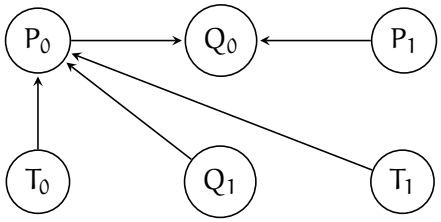

FIGURE 4. A directed tree describing a basis for the intrinsic torus of Example 4.8.

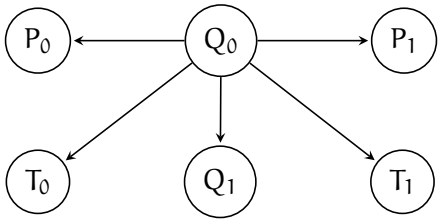

FIGURE 5. Another directed tree describing a basis for the intrinsic torus of Example 4.8.

polynomials of degree n. Let $C := \overline{C} \cap \mathbb{T}^n$ be the corresponding very affine curve, with coordinate ring R. Our goal in this section is to give an algorithm for computing a basis of R^*/k^*.

Remark 5.1. Plane conics are precisely the rational normal curves of degree 2, so the following discussion generalizes part of Section 4 in some sense. Note though that the presentation of the curves in question has changed: here we do not begin with the implicit equations of the rational normal curve in $\mathbb{P}^n$.

The following is a modification of the polynomial subalgebra membership algorithm given in [CLO15, 7.3.7].

Algorithm 5.2 (Subalgebra membership)**.**
INPUT: $f_0, \dots, f_n$ degree n homogeneous polynomials in $k[S,T]$ defining a rational normal curve, and a rational function $\frac{f}{g} \in k(S,T)$
OUTPUT: $\gamma \in k[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ such that its homogenization $\overline{\gamma} \in k[x_0^{\pm 1}, \dots, x_n^{\pm 1}]$ satisfies $\frac{f(S,T)}{g(S,T)} = \overline{\gamma}\big(f_0(S,T), \dots, f_n(S,T)\big)$ if such a γ exists, or **false** otherwise

```
I ← ideal(y_0 − f_0, ..., y_n − f_n, z_0 − s_0, ..., z_n − s_n, f_0 s_0 − 1, ..., f_n s_n − 1, gs − 1) in the polynomial ring k[y_0, ..., y_n, z_0, ..., z_n, s_0, ..., s_n, s, S, T]
G ← GröbnerBasis(I) in a monomial ordering where any monomial involving one of the S, T, s, s_0, ..., s_n is greater than any monomial in k[y_0, ..., y_n, z_0 ..., z_n]
h ← the remainder of dividing fs by G
if h ∈ k[y_0, ..., y_n, z_0, ..., z_n] then
    return h(1, x_1, ..., x_n, 1, x_1^{-1}, ..., x_{n-1}^{-1}, x_n^{-1})
else
    return false
end if
```

Lemma 5.3. *Let $\overline{C}$ be a rational normal curve with parametrization $\psi\colon \mathbb{P}^1 \hookrightarrow \mathbb{P}^n$ given by $f_0, \dots, f_n$. Algorithm 5.2 correctly returns the pushforward γ of a rational function $\frac{f(S,T)}{g(S,T)}$ on $\psi^{-1}(C)$ along the map given by $\psi^{-1}(C) \hookrightarrow C$, if such a γ exists and is regular.*

Proof. There exists $\overline{\gamma} \in k[x_0^{\pm 1}, \dots, x_n^{\pm 1}]$ such that

$$\frac{f}{g} = \overline{\gamma}(f_0, \dots, f_n)$$

if and only if there exists $\chi \in k[y_0, \dots, y_n, z_0, \dots, z_n]$ such that

$$\frac{f}{g} = \chi(f_0, \dots, f_n, f_0^{-1}, \dots, f_n^{-1}).$$

Setting the s_i to be the inverse of the f_i and setting s to be the inverse of g, this is equivalent to the statement that fs is in the k-algebra generated by $\{f_0, \dots, f_n, s_0, \dots, s_n\}$ in the quotient ring

$$k[y_0, \dots, y_n, z_0, \dots, z_n, s_0, \dots, s_n, s, S, T]/(f_0 s_0 - 1, \dots, f_n s_n - 1, gs - 1).$$

By [CLO15, 7.3.7], the previous statement is true if and only if h, the remainder upon dividing fs by the Gröbner basis G, is in the polynomial ring $k[y_1, \dots, y_n, z_1, \dots, z_n]$. Suppose γ exists, and let $\overline{\gamma}$ be its homogenization. By [CLO15, 7.3.7], $fs = h(f_0, \dots, f_n, s_0, \dots, s_n)$ and $\overline{\gamma} = h(x_0, \dots, x_n, x_0^{-1}, \dots, x_n^{-1})$. Dehomogenizing, we get $\gamma = h(1, x_1, \dots, x_n, 1, x_1^{-1}, \dots, x_n^{-1})$ as the pushforward of f/g. Because h is a Laurent polynomial, γ is regular on C. □

Algorithm 5.4 (Computing unit groups of rational normal curves)**.**

INPUT: A rational normal curve $\overline{C}$ given parametrically by $f_0(T, S), \dots, f_n(T, S) \in k[S, T]$ and a corresponding very affine curve given by setting $f_0 = 1$

OUTPUT: A basis of R^*/k^*

$D \leftarrow \emptyset$
$[a_1 : b_1], \dots, [a_m : b_m] \leftarrow$ preimages of ∂C under the parametrization map $\mathbb{P}^1 \hookrightarrow \mathbb{P}^n$.
Choose any basis of $\mathrm{Div}^0_\partial(\overline{C})$
for all basis elements $\sum_i c_i[a_{k_i} : b_{k_i}] - \sum_j d_j[a_{l_j} : b_{l_j}]$ **do**
  $f \leftarrow \prod_i (b_{k_i} S - a_{k_i} T)^{c_i}$
  $g \leftarrow \prod_j (b_{l_j} S - a_{l_j} T)^{d_j}$
  $\overline{\gamma} \leftarrow$ Algorithm 5.2$(f, g, f_0, \dots, f_n)$
  $\gamma \leftarrow \overline{\gamma}(1, x_1, \dots, x_n)$
  $D \leftarrow D \cup \{\gamma\}$
end for
return D

Theorem 1.1. *Let $\overline{C} \subseteq \mathbb{P}^n_k$ be a rational normal curve over an algebraically closed field k, given parametrically as the image of a map $\mathbb{P}^1_k \hookrightarrow \mathbb{P}^n_k$. Let $C := \overline{C} \cap \mathbb{T}^n$ be the corresponding very affine curve, with coordinate ring R. Then Algorithm 5.4 correctly computes a $\mathbb{Z}$-basis of R^*/k^*.*

Proof. Let C be parametrized by polynomials $f_0(S, T), \dots, f_n(S, T) \in k[S, T]$. As $\overline{C} \cong \mathbb{P}^1$, $\mathrm{Cl}^0_\partial(\overline{C}) = 0$, so the injection $R^*/k^* \hookrightarrow \mathrm{Div}^0_\partial(\overline{C})$ is an isomorphism. For each basis element $\sum_i c_i[a_{k_i} : b_{k_i}] - \sum_j d_j[a_{l_j} : b_{l_j}]$, Algorithm 5.2 will produce a rational function $\overline{\gamma}$ on the projective curve which has zeros of order c_i at the points $[f_0(a_{k_i}, b_{k_i}) : \dots, f_n(a_{k_i} : b_{k_i})]$ and poles of order d_j at the points $[f_0(a_{l_j} : b_{l_j}), \cdots : f_n(a_{l_j}, b_{l_j})]$. By dehomogenizing to arrive at γ, we get exactly the element of R^* corresponding to our divisor. □

Example 5.5. Consider the degree 3 rational normal curve $\overline{C} \subseteq \mathbb{P}^3$ given by the parametrization

$$[S^3 - 4ST^2 : S^2T - 9T^3 : (S - 3T)T^2 : (S + 3T)T^2]$$

We compute the following boundary points:

(1) $P_1 = [0 : 1]$
(2) $P_2 = [1 : 0]$

(3) $P_3 = [3:1]$
(4) $P_4 = [-3:1]$
(5) $P_5 = [2:1]$
(6) $P_6 = [-2:1]$

We choose the following basis of $\mathrm{Div}^0_\partial(\overline{C})$:

$$P_1 - 2P_2 - P_4 + P_5 + P_6, P_2 - P_3, P_3 - P_4, P_4 - P_5, P_5 - P_6$$

Choose coordinates x, y, z, w on $\mathbb{P}^3$. We run Algorithm 5.2 to obtain preimages under $\overline{\phi}$ of our basis of $\mathrm{Div}^0_\partial(\overline{C})$ in $\mathrm{Frac}(\overline{R})^*$. Their corresponding dehomogenizations with respect to w give a basis of R^*/k^*:

(1) $x \rightsquigarrow x$
(2) $y \rightsquigarrow y$
(3) $z \rightsquigarrow z$
(4) $\dfrac{x + 5y + \frac{45}{6}(w - z) + 10(w + z)}{x} \rightsquigarrow \dfrac{x + 5y + \frac{45}{6}(1 - z) + 10(1 + z)}{x}$
(5) $\dfrac{x - 4y + 6(w - z) + 4(w + z)}{x} \rightsquigarrow \dfrac{x - 4y + 6(1 - z) + 4(1 + z)}{x}$

Remark 5.6. Although we do not do so here, one could consider various generalizations of the results presented thus far. For example, one can essentially perform the same procedure with "pinched" rational curves, i.e. smooth rational curves of degree $> n$ in $\mathbb{P}^n$. However, once higher-dimensional varieties or curves with singularities are considered, the situation becomes more complicated; even computing the boundary is no longer a simple task.

6. Elliptic Curves

Fix $k = \overline{\mathbb{Q}}$, let $\overline{E} \subseteq \mathbb{P}^2_k$ be an elliptic curve with a given base point O, and set $E := \overline{E} \cap \mathbb{T}^2$. Due to Equation (3.1.1), computing the image of R^*/k^* in $\mathrm{Div}^0_\partial(\overline{E})$ is equivalent to computing the relations between the closed points of $\partial E =: \{P_1, \ldots, P_n\}$ in $\mathrm{Cl}^0_\partial(\overline{E})$. As the group law on the elliptic curve coincides with the group law in the class group, it suffices to compute relations between the corresponding points on the elliptic curve, which can be done via canonical Néron–Tate heights.

6.1. The Canonical Néron–Tate Height Pairing.

We briefly define canonical Néron–Tate heights, following the exposition from [Sil09]. Speaking broadly, height functions measure the "arithmetic complexity" of points on abelian varieties. For any field F and variety X, let $X(F)$ denote the F-rational points of X.

Theorem 6.2 (Néron–Tate)**.** *Let $\overline{E}$ be an elliptic curve defined over a number field. There exists a function $\hat{h}\colon \overline{E}(\overline{\mathbb{Q}}) \to \mathbb{R}$ called the* canonical Néron–Tate height *satisfying the following properties:*

(1) For all $P, Q \in \overline{E}(\overline{\mathbb{Q}})$, the parallelogram law holds, i.e.

$$\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q).$$

(2) For all $P \in E(\overline{\mathbb{Q}})$ and $m \in \mathbb{Z}$,

$$\hat{h}(mP) = m^2\hat{h}(P).$$

(3) $\hat{h}$ is an even function, and the pairing

$$\langle \quad , \quad \rangle\colon E(\overline{\mathbb{Q}}) \times E(\overline{\mathbb{Q}}) \to \mathbb{R}$$
$$\langle P, Q\rangle = \hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q)$$

is bilinear. This is equivalent to saying that $\hat{h}$ is a quadratic form on $E(\overline{\mathbb{Q}})$. We call this the canonical Néron–Tate height pairing.

(4) For all $P \in \overline{E}(\overline{\mathbb{Q}})$, one has $\hat{h}(P) \geq 0$, and $\hat{h}(P) = 0$ if and only if P is torsion.

For any number field K, we can obtain a bilinear form on $\overline{E}(K)$ by restricting the bilinear form on $\overline{E}(\overline{\mathbb{Q}})$ in Theorem 6.2(3). This can be extended to a bilinear form on the finite-dimensional real vector space $\overline{E}(K) \otimes \mathbb{R}$.

Proposition 6.3 ([Sil09, VIII.9.9.6])**.** *The Néron–Tate height induces a positive definite inner product on $\overline{E}(K) \otimes \mathbb{R}$.*

One can compute heights on elliptic curves efficiently with Algorithm 6.1 in [MS16].

6.4. **Computing Generators of the Unit Group.** We now detail algorithms to solve Questions 1 and 2 for elliptic curves. First we treat Question 1. In addition to the above theory on Néron–Tate heights, we will need the following theorem and subroutines.

Theorem 6.5 ([Mah38], [Wey40, Theorem 4])**.** *Suppose L is a sublattice in $\mathbb{Z}^n$ of rank m. Fix some topological vector space norm on $\mathbb{R}^n$. For all $1 \leq k \leq m$, let M_k denote the minimum size ball centered at the origin that contains k linearly independent vectors in L. Then there exists a basis $\{x_1, \ldots, x_n\}$ of L such that for all $1 \leq k \leq m$, $|x_k| \leq (\frac{3}{2})^{k-1} M_k$.*

Subroutine 6.6. INPUT: A set of torsion points $T_1, \ldots, T_r$ on an elliptic curve and torsion orders $m_1, \ldots, m_n$
OUTPUT: Generators for the lattice of relations among $T_1, \ldots, T_r$ in $\mathbb{Z}^r$

```
D ← ∅
for all (n_1, ..., n_r) where 0 ≤ n_i ≤ m_i do
    if n_1 T_1 + ··· + n_r T_r = 0 then
        add (n_1, ..., n_r) to D
    end if
end for
return D
```

Subroutine 6.6 correctly computes all relations among a set of torsion points, as it simply manually checks all possible relations.

Subroutine 6.7. INPUT: A set of torsion-free points $Q_1, \ldots, Q_n$ on an elliptic curve
OUTPUT: Generators in $\mathbb{Z}^n$ for the lattice of relations among the Q_i in $\overline{E}(\overline{\mathbb{Q}})/\text{tors}$

```
Compute the n × n matrix A such that the A_{i,j} ← ⟨Q_i, Q_j⟩ = ĥ(Q_i + Q_j) − ĥ(Q_i) − ĥ(Q_j)
return generators of ker A ∩ Z^n
```

Lemma 6.8. *Subroutine 6.7 correctly computes the lattice of relations among the nontorsion points $Q_1, \ldots, Q_n$ in $\overline{E}(\overline{\mathbb{Q}})/\text{tors}$.*

Proof. Choose some number field K large enough such that $\{Q_1, \ldots, Q_n\} \subseteq \overline{E}(K)$. Note that $\overline{E}(K)$ modulo torsion embeds into $\overline{E}(K) \otimes \mathbb{R}$. By Theorem 6.2 (3), A is the inner product matrix of a nondegenerate inner product, and thus $\ker A \cap \mathbb{Z}^n$ comprises the relations among the Q_i up to torsion. □

We are now ready to solve Question 1 for elliptic curves.

Algorithm 6.9 (Answering Question 1 for elliptic curves)**.**
INPUT: An elliptic curve over $\overline{\mathbb{Q}}$ with a nonempty finite set of distinguished points $S \subseteq \overline{E}(\overline{\mathbb{Q}})$ and a base point O
OUTPUT: A minimal generating set of $\ker(\mathrm{Div}^0_S(\overline{E}) \to \mathrm{Cl}^0(\overline{E}))$

1: Determine the torsion points of S using heights. Let $Q_1, \ldots, Q_n$ refer to torsion-free points, and let $T_1, \ldots, T_r$ refer to torsion points with orders $m_1, \ldots, m_r$ respectively.

$D \leftarrow \emptyset \subseteq \mathbb{Z}^{n+r}$
$G \leftarrow$ finite subgroup generated by $(T_1, \ldots, T_r) \subseteq \overline{E}(\overline{\mathbb{Q}})$
$D_T \leftarrow$ relations between $T_1, \ldots, T_r$ as given by Subroutine 6.6
for all $(n_1, \ldots, n_r) \in D_T$ **do**
  add $(0, \ldots, 0, n_1, \ldots, n_r)$ to D
end for
$D_Q \leftarrow$ relations modulo torsion between $Q_1, \ldots, Q_n$ as given by Subroutine 6.7
$\ell \leftarrow \operatorname{rank}(span_{\mathbb{Z}}(D_Q))$
$\lambda \leftarrow 0$, $S_\lambda \leftarrow \emptyset \subset \mathbb{Z}^n$
while $\operatorname{rank}(span_{\mathbb{Z}}(S_\lambda)) \neq \ell$ **do**
  $\lambda \leftarrow \lambda + 1$
  $S_\lambda \leftarrow \{(m_1, \ldots, m_n) \in span_{\mathbb{Z}}(D_Q) \mid \sqrt{\sum m_i^2} \leq \lambda \quad \text{and} \quad m_1 Q_1 + \cdots + m_n Q_n \in G\}$
end while
$\Lambda \leftarrow \{(m_1, \ldots, m_n) \in span_{\mathbb{Z}}(D_Q) \mid \sqrt{\sum m_i^2} \leq (\frac{3}{2})^{k-1}\lambda \quad \text{and} \quad m_1 Q_1 + \cdots + m_n Q_n \in G\}$
for $(m_1, \ldots, m_n) \in \Lambda$ **do**
  Choose $(n_1, \ldots, n_r)$ such that $m_1 Q_1 + \cdots + m_n Q_n + n_1 T_1 + \cdots + n_r T_r = 0$
  add $(m_1, ..., m_n, n_1, \ldots, n_r)$ to D
end for
$L \leftarrow \{(m_1, \ldots, m_n, n_1, \ldots, n_r) \in \mathbb{Z}^{n+r} \mid \sum m_i + \sum n_j = 0\}$
return a minimal set of generators for $span_{\mathbb{Z}}(D) \cap L$

Lemma 6.10. *For a distinguished set S of $\overline{\mathbb{Q}}$-points on the elliptic curve E, Algorithm 6.9 correctly computes a minimal generating set of the kernel of the map $\operatorname{Div}_S^0(\overline{E}) \to Cl^0(\overline{E})$.*

Proof. We first prove that the algorithm terminates. Let ψ denote the map $\operatorname{Div}_S(\overline{E}) \to \operatorname{Cl}_S(\overline{E})$, and let ψ_0 denote the restriction $\operatorname{Div}_S^0(\overline{E}) \to \operatorname{Cl}_S^0(\overline{E})$. Identify $\operatorname{Div}_S^0(\overline{E}) \cong \mathbb{Z}\langle Q_1, \ldots, Q_n, T_1, \ldots, T_r\rangle$ with $\mathbb{Z}^{n+r}$ using this ordering of elements in S. For any subset $M \subseteq \{1, \ldots, n+r\}$, let π_M denote the projection onto those coordinates.

Note that $\pi_{\{1,\ldots,n\}}(\ker\psi) \subseteq span_{\mathbb{Z}}(D_Q)$. In fact $\pi_{\{1,\ldots,n\}}(\ker\psi)$ has the same rank as $span_{\mathbb{Z}}(D_Q)$; if $(m_1, \ldots, m_n) \in span_{\mathbb{Z}}(D_Q)$, then $m_1 Q_1 + \cdots + m_n Q_n \in G$ and thus is torsion. It follows that there exists some $m \in \mathbb{Z}$ such that $mm_1 Q_1 + \cdots + mm_n Q_n = 0$, so that $(mm_1, \ldots, mm_n) \in \pi_{\{1,\ldots,n\}}(\ker\psi)$. Hence there exists a λ large enough to exit the while loop, and the algorithm terminates.

We now show the correctness of the algorithm. We claim that $\pi_{\{1,\ldots,n\}}(\ker\psi) = span_{\mathbb{Z}}(\Lambda)$. Note by definition that $\Lambda \subseteq \pi_{\{1,\ldots,n\}}(\ker\psi)$ so $span_{\mathbb{Z}}(\Lambda) \subseteq \pi_{\{1,\ldots,n\}}(\ker\psi)$. By Theorem 6.5, as S_λ contains at least ℓ linearly independent elements, Λ will contain a lattice basis of $\pi_{\{1,\ldots,n\}}(\ker\psi)$. Thus $\pi_{\{1,\ldots,n\}}(\ker\psi) = span_{\mathbb{Z}}(S)$.

Next we show that $span(D) = \ker\psi$. Clearly $span(D) \subseteq \ker\psi$ by construction. Suppose $(m_1, \ldots, m_n, n_1, \ldots, n_r) \in \ker\psi$. Then $(m_1, \ldots, m_n) \in \pi_{\{1,\ldots,n\}}(\ker\psi) = span_{\mathbb{Z}}(\Lambda)$, so there exist $n_1', \ldots, n_r'$ such that $(m_1, \ldots, m_n, n_1', \ldots, n_r') \in span(D) \subseteq \ker\psi$. Thus, $(0, \ldots, 0, n_1 - n_1', \ldots, n_r - n_r') \in \ker\psi$. However, $(0, \ldots, 0, n_1 - n_1', \ldots, n_r - n_r') \in span(D)$ because of Subroutine 6.6, so

$$(m_1, \ldots, m_n, n_1', \ldots, n_r') + (0, \ldots, 0, n_1 - n_1', \ldots, n_r - n_r') = (m_1, \ldots, m_n, n_1, \ldots, n_r) \in span(D).$$

To conclude, we note that $\ker\psi_0 = \ker\psi \cap L = span_{\mathbb{Z}}(D) \cap L$. □

We now turn our attention to answering Question 2. The following is an explicit version of Miller's algorithm, specialized to genus 1 [Mil86].

Algorithm 6.11 (Answering Question 2 for elliptic curves)**.**
INPUT: An elliptic curve $\overline{E}$ with basepoint O and a divisor $D \in \operatorname{Div}^0(\overline{E})$

OUTPUT: Whether D is in the image R^*/k^*, and an element of $\mathrm{Frac}(\overline{R})^*$ mapping to D if it is

1: $f \leftarrow 1$
2: **while** $|D| \neq 0$ **do**
3: **if** $\exists P, Q$ such that $n_P, n_Q > 0$ **and** $P \neq -Q$ **then**
4: $D \leftarrow D - (P + Q + (-P + Q) - 3O)$
5: $f \leftarrow fL$ where L is the line through P and Q
6: **else if** $\exists P, Q$ such that $n_P, n_Q > 0$ **and** $P = -Q$ **then**
7: $D \leftarrow D - (P + Q - 2O)$
8: $f \leftarrow fL$ where L is the line through P and Q
9: **else if** $\exists P, Q$ such that $n_P, n_Q < 0$ **and** $P \neq -Q$ **then**
10: $D \leftarrow D + (P + Q + (-P + Q) - 3O)$
11: $f \leftarrow f/L$ where L is the line through P and Q
12: **else if** $\exists P, Q$ such that $n_P, n_Q < 0$ **and** $P = -Q$ **then**
13: $D \leftarrow D + (P + Q - 2O)$
14: $f \leftarrow f/L$ where L is the line through P and Q
15: **else if** D is of the form $mP - nQ + oO$ for $m, n \geq 0$ **then**
16: **if** $m \geq 2$ **and** P has order 3 **then**
17: $D \leftarrow D - (3P - 3O)$
18: $f \leftarrow fL$ where L is the tangent line at P
19: **else if** $m \geq 2$ **and** P does not have order 2 **then**
20: $D \leftarrow D - (2P + (-2P) - 3O)$
21: $f \leftarrow fL$ where L is the tangent line at P
22: **else if** $m \geq 2$ **and** P has order 2 **then**
23: $D \leftarrow D - (2P - 2O)$
24: $f \leftarrow fL$ where L is the tangent line at P
25: **else if** $n \geq 2$ **and** Q has order 3 **then**
26: $D \leftarrow D + (3Q - 3O)$
27: $f \leftarrow f/L$ where L is the tangent line at Q
28: **else if** $n \geq 2$ **and** Q does not have order 2 **then**
29: $D \leftarrow D + (2Q + (-2Q) - 3O)$
30: $f \leftarrow f/L$ where L is the tangent line at Q
31: **else if** $n \geq 2$ **and** Q has order 2 **then**
32: $D \leftarrow D - (2Q - 2O)$
33: $f \leftarrow f/L$ where L is the tangent line at Q
34: **else if** $m = 1$ **and** $n = 1$ **then**
35: $D \leftarrow D + (Q + (-Q) - 2O)$
36: $f \leftarrow f/L$ where L is the line through Q and $-Q$
37: **else if** ($m = 1$ **and** $n = 0$) **or** ($m = 0$ **and** $n = 1$) **then**
38: **return** this divisor is not in the image of R^*/k^*
39: **end if**
40: **end if**
41: **end while**
42: **return** f

Lemma 6.12. *Algorithm 6.11 correctly determines whether a divisor D is in the image of R^*/k^* and computes an element f of $\mathrm{Frac}(\overline{R})^*$ mapping to D if so.*

Proof. Let ϕ denote the map $R^*/k^* \hookrightarrow \mathrm{Div}_0(\overline{E})$. Note that the quantity $D - \phi(f)$ is a loop invariant. Note additionally that during every execution of the loop, exactly one of the conditionals is satisfied; if line 3, 6, 9, and 12 are not satisfied, then D must be of the form $mP - nQ + oO$ for

$m, n \geq 0$. If $D = mP - nQ + oO$ then exactly one of line 16, 19, 22, 25, 28, 31, 34, or 37 must be satisfied. $|D|$ is strictly reduced during each iteration unless line 34 or line 37 are satisfied. Line 37 terminates the program. Line 34 cannot be satisfied in two consecutive loops. Thus the algorithm will terminate.

Assume $D \in \phi(R^*/k^*)$. If at some point in execution $|D| = 0$, then as D is degree 0, $D = 0$ and so $D = \phi(f)$. If, during the execution of the algorithm, line 37 is satisfied, then some point is linearly equivalent to the origin, which is a contradiction. Hence the algorithm outputs an element f with the desired property.

Now assume $D \notin \phi(R^*/k^*)$. Because of the loop invariant $D - \phi(f)$, we will never have $|D| = 0$. Because the algorithm terminates, it must terminate at line 37, as desired. □

Putting together Lemmas 6.10 and 6.12 and 3.11, we obtain the following result:

Algorithm 6.13 (Computing unit groups of elliptic curves)**.**
INPUT: An elliptic curve over $\overline{\mathbb{Q}}$ with boundary points ∂ and a base point O
OUTPUT: A basis of R^*/k^*
  $V \leftarrow$ a generating set of the image of $R^*/k^* \hookrightarrow \mathrm{Div}^0_\partial(\overline{E})$ by Algorithm 6.9
  $B \leftarrow \emptyset$
  for all $v \in V$ **do**
    $f/g \leftarrow$ rational function with divisor v using Algorithm 6.11
    $B \leftarrow B \cup \{h\}$, where h is a Laurent polynomial with the same divisor as f/g by Algorithm 3.10
  end for
  return B

Theorem 1.2. *Let $k = \overline{\mathbb{Q}}$, let $\overline{E} \subseteq \mathbb{P}^2_k$ be an elliptic curve, and let $E := \overline{E} \cap \mathbb{T}^2$ be the corresponding very affine elliptic curve with coordinate ring R. Then Algorithm 6.13 correctly computes a $\mathbb{Z}$-basis of R^*/k^*.*

Remark 6.14. Many of the algorithms presented in this section are most easily implemented (e.g. in Sage [The18]) for elliptic curves in Weierstrass form. Given a projective isomorphism of $\overline{E}$ to a Weierstrass form $\overline{W}$ as $\varphi\colon \overline{E} \to \overline{W}$, we can compute relations among the points in $\varphi(\partial E)$ using Algorithm 6.9. These relations can be pulled back by φ^{-1} to all relations among the points in ∂E, because φ induces an isomorphism $\mathrm{Div}^0_\partial(\overline{E}) \cong \mathrm{Div}^0_S(\overline{W})$.

Example 6.15. Let E be the very affine elliptic curve $E = \mathrm{Spec}(\overline{\mathbb{Q}_5}[x^{\pm 1}, y^{\pm 1}]/(y^2 - (x-1)(x+1)(x-4))$ with basepoint $[0:1:0]$. We compute the following six boundary points of $\overline{E} \subseteq \mathbb{P}^2$:

(1) $Q_1 := [0:2:1]$
(2) $Q_2 := [0:-2:1]$
(3) $T_1 := [0:1:0]$
(4) $T_2 := [1:0:1]$
(5) $T_3 := [-1:0:1]$
(6) $T_4 := [4:0:1]$

T_1 is the identity on E and has torsion order 1; T_2, T_3, and T_4 have torsion order 2; and Q_1 and Q_2 are nontorsion. Algorithm 6.13 yields the following generating set for the lattice of relations, with corresponding units:

(1) $[1,1,1,1,-2,-2] \rightsquigarrow -y/x^2$
(2) $[0,2,0,0,-1,-1] \rightsquigarrow (x-1)/x$
(3) $[0,0,2,0,-1,-1] \rightsquigarrow (x+1)/x$
(4) $[0,0,0,2,-1,-1] \rightsquigarrow (x-4)/x$

Note that it is easy to find these units by inspection, but to check that these form a basis of R^*/k^*, we rely on the algorithms given in this section.

We can easily compute the tropicalization of the elliptic curve $E \subseteq \mathbb{T}^2$ defined by the equation $y^2 = (x-1)(x+1)(x-4)$ to be three rays emerging from the origin, as seen in Figure 6:

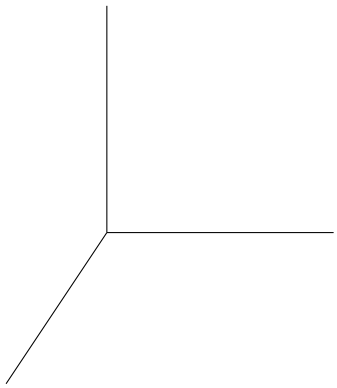

FIGURE 6. The tropicalization of the elliptic curve in Example 6.15.

Using the unit group basis $\{x, y, x-1, x+1\}$, we compute the intrinsic tropicalization of E in $\mathbb{T}^4$ with Singular, shown in Figure 7:

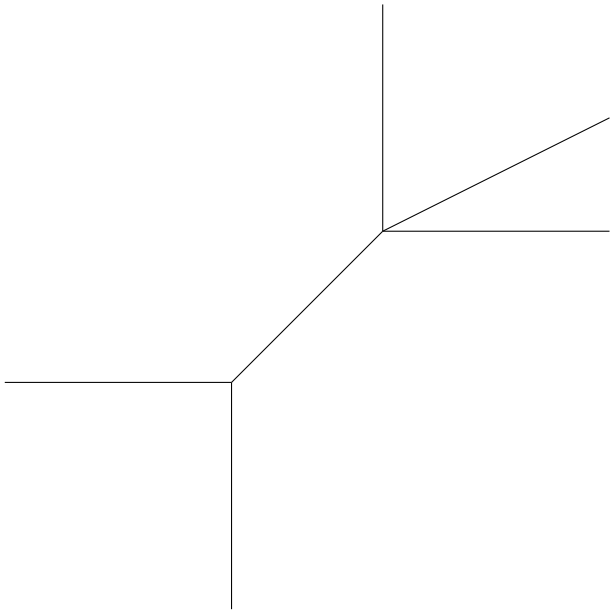

FIGURE 7. The intrinsic tropicalization of the elliptic curve in Example 6.15.

In particular, the intrinsic tropicalization is larger than the original. On the other hand, the j-invariant can be computed to be $j(E) = 438976/225$, so that its 5-adic valuation is -2. It follows from Chan and Sturmfels [CS13] that $\overline{E}$ can be projectively re-embedded so that its tropicalization is in honeycomb form. The intrinsic tropicalization of E does not retain this information, as this projective re-embedding of $\overline{E}$ does not preserve our dehomogenization procedure. In particular, intrinsic tropicalizations need not be faithful.

6.16. **Hyperelliptic curves.** The Néron–Tate canonical height can more generally be defined on any abelian variety defined over any number field. Fix some curve X defined over $\overline{\mathbb{Q}}$. Choose a number field K such that $\partial X \subseteq X(K)$. Letting J denote the Jacobian of X, the Néron–Tate canonical height pairing on $J(\overline{\mathbb{Q}})$ induces a positive definite inner product on $J(K) \otimes \mathbb{R}$. For curves of genus 2, Cassels, Flynn, and Smart provide an algorithm to compute the canonical height in [CF96] and [FS97], which has since been implemented in Magma. For hyperelliptic curves of genus 3, Stoll [Sto17] describes such an algorithm with a corresponding Magma implementation. Additionally, Holmes [Hol12] has provided a height algorithm for all hyperelliptic curves. Another algorithm to compute heights for all hyperelliptic curves has been provided by Müller [Mül13]. However, a hyperelliptic curve of the form $y^2 = f(x)$ in $\mathbb{P}^2$ with $\deg f \geq 4$ has a singularity at infinity, and thus the methods used for elliptic curves do not immediately generalize.

REFERENCES

[CF96] J.W.S. Cassels and E.V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Mathematical Society Lecture Note Series, Cambridge University Press, 1996.

[CLO15] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, fourth ed., Undergraduate Texts in Mathematics, Springer-Verlag, Switzerland, 2015.

[Coh93] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, Springer-Verlag, 1993.

[CS13] M. Chan and B. Sturmfels, *Elliptic Curves in Honeycomb Form,* in *Algebraic and Combinatorial Aspects of Tropical Geometry*, Contemp. Math. **589** (2013), 87–107.

[DGPS18] W. Decker, G-M Greuel, G. Pfister, and H. Schönemann, SINGULAR *4-1-1 — A computer algebra system for polynomial computations*, `http://www.singular.uni-kl.de`, 2018.

[Eis95] D. Eisenbud, *Commutative algebra with a view towards algebraic geometry*, first ed., Graduate Texts in Mathematics, Springer-Verlag, New York, 1995.

[FS97] E.V. Flynn and N.P. Smart, *Canonical heights on the jacobians of curves of genus 2 and the infinite descent*, Acta Arith. **79** (1997), 333–352.

[Fuc60] L. Fuchs, *Abelian groups*, International Series of Monographs on Pure and Applied Mathematics, Pergamon Press, 1960.

[GS] Daniel R. Grayson and Michael E. Stillman, *Macaulay2, a software system for research in algebraic geometry*, Available at `http://www.math.uiuc.edu/Macaulay2/`.

[Hol12] D. Holmes, *Computing Néron–Tate heights of points on hyperelliptic jacobians*, J. Number Theory **132** (2012), 1295–1305.

[Mah38] K. Mahler, *On Minkowski's theory of reduction of positive definite quadratic forms*, Q. J. Math. **9** (1938), 259–262.

[Mil86] V. Miller, *Short programs for functions on curves*, `https://crypto.stanford.edu/miller/miller.pdf`, unpublished.

[MS15] D. Maclagan and B. Sturmfels, *Introduction to tropical geometry*, Graduate Studies in Mathematics, vol. 161, American Mathematical Society, 2015.

[MS16] J.S. Müller and M. Stoll, *Computing canonical heights on elliptic curves in quasi-linear time*, LMS J. Comput. Math. **19** (2016), 391–405.

[Mül13] J.S. Müller, *Computing canonical heights using arithmetic intersection theory*, Math. Comp. **83** (2013), no. 285, 311–336.

[Sam66] P. Samuel, *A propos du théoreme des unités*, Bulletin des Sciences Mathématiques **90** (1966), 89–96.

[Sil09] J. H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, Springer-Verlag, 2009.

[Sto17] M. Stoll, *An explicit theory of heights for hyperelliptic Jacobians of genus three*, Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory (G. Böckle, W. Decker, and G. Malle, eds.), Springer-Verlag, 2017, pp. 665–715.

[The18] The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 8.2)*, 2018, `http://www.sagemath.org`.

[Wey40] H. Weyl, *Theory of reduction for arithmetical equivalence*, Trans. Amer. Math. Soc. **48** (1940), 126–164.

E-mail address: jchen@math.berkeley.edu

E-mail address: sameerav@princeton.edu

E-mail address: leonyz@math.berkeley.edu