J. reine angew. Math., Ahead of Print
DOI 10.1515/crelle-2023-0022

Journal für die reine und angewandte Mathematik

Blown-up toric surfaces with non-polyhedral effective cone

By *Ana-Maria Castravet* at Versailles, *Antonio Laface* at Concepción,
Jenia Tevelev at Amherst and *Luca Ugaglia* at Palermo

Abstract. We construct projective toric surfaces whose blow-up at a general point has a non-polyhedral pseudo-effective cone. As a consequence, we prove that the pseudo-effective cone of the Grothendieck–Knudsen moduli space $\overline{M}_{0,n}$ of stable rational curves is not polyhedral for $n \geq 10$. These results hold both in characteristic 0 and in characteristic p, for all primes p. Many of these toric surfaces are related to an interesting class of arithmetic threefolds that we call arithmetic elliptic pairs of infinite order. Our analysis relies on tools of arithmetic geometry and Galois representations in the spirit of the Lang–Trotter conjecture, producing toric surfaces whose blow-up at a general point has a non-polyhedral pseudo-effective cone in characteristic 0 and in characteristic p, for an infinite set of primes p of positive density.

Contents

1. Introduction
2. Polyhedrality of effective cones
3. Elliptic pairs: General theory
4. Lang–Trotter polygons and toric elliptic pairs
5. Arithmetic toric elliptic pairs of infinite order
6. Halphen polygons
7. On the effective cone of $\overline{M}_{0,n}$
8. Databases

References

The corresponding author is Antonio Laface.

Ana-Maria Castravet has been partially supported by the ANR-20-CE40-0023 grant. Antonio Laface has been partially supported by Proyecto FONDECYT Regular n. 1190777 and Proyecto FONDECYT Regular n. 1230287. Jenia Tevelev has been partially supported by the NSF grants DMS-1701704, DMS-2101726 and the Simons Fellowship. Luca Ugaglia is member of INdAM – GNSAGA.

1. Introduction

An effective cone of a projective variety X and its closure, the pseudo-effective cone $\overline{\mathrm{Eff}}(X)$, contain an impressive amount of information about the birational geometry of X. An even finer invariant is the Cox ring $\mathrm{Cox}(X)$, at least when the class group $\mathrm{Cl}(X)$ is finitely generated. If X is a Mori Dream Space (MDS), then $\mathrm{Cox}(X)$ is finitely generated, which in turn implies that $\overline{\mathrm{Eff}}(X)$ is polyhedral. A basic example of an MDS is a projective toric variety [20]. Its effective cone is generated by classes of toric boundary divisors. For a toric variety $\mathbb{P}$, we denote by $\mathrm{Bl}_e\,\mathbb{P}$ its blow-up at the identity element of the torus. Our main result contributes to the growing body of evidence that this is a very intriguing class of varieties.

Theorem 1.1. *In every characteristic, there exist projective toric surfaces* $\mathbb{P}$ *such that the pseudo-effective cone* $\overline{\mathrm{Eff}}(\mathrm{Bl}_e\,\mathbb{P})$ *is not polyhedral.*

In order to prove Theorem 1.1, we introduce two types of lattice polygons, Lang–Trotter polygons and Halphen polygons. The blow-ups $X = \mathrm{Bl}_e\,\mathbb{P}$ of toric surfaces associated to these polygons are examples of elliptic pairs studied in Section 3. An *elliptic pair* (C, X) is a projective rational surface X, with log terminal singularities, and a curve C contained in the smooth locus of X such that $p_a(C) = 1$ and $C^2 = 0$. Much of the geometry is encoded in the restriction map $\mathrm{res}\colon C^\perp \to \mathrm{Pic}^0(C)$, where $C^\perp \subseteq \mathrm{Cl}(X)$ is the orthogonal complement. The order of an elliptic pair is the order of $\mathrm{res}(C)$. A familiar example of an elliptic pair of infinite order in any characteristic is the blow-up of $\mathbb{P}^2$ in 9 general points. By contrast, elliptic pairs $X = \mathrm{Bl}_e\,\mathbb{P}$ associated with a toric surface are defined over the base field. In particular, their order is automatically finite in characteristic p.

If the order of an elliptic pair (C, X) is infinite and $\rho(X) \geq 3$, then $\overline{\mathrm{Eff}}(X)$ is not polyhedral (Lemma 3.3). By contrast, polyhedrality of $\overline{\mathrm{Eff}}(X)$ is harder to control if the order is finite unless the pair is *minimal* (Definition 3.5) and has Du Val singularities, in which case there is a simple criterion for polyhedrality (Corollary 3.18) in terms of the restriction map and the root sublattice $T \subset \mathbb{E}_8$. Every elliptic pair (C, X) has a $(K + C)$-minimal model (C, Y), and if $\overline{\mathrm{Eff}}(Y)$ is not polyhedral, then $\overline{\mathrm{Eff}}(X)$ is also not polyhedral. Remarkably, the minimal model (C, Y) has Du Val singularities if the order is *infinite* (Corollary 3.12).

We introduce the notion of an *arithmetic elliptic pair of infinite order*, a flat pair of schemes $(\mathcal{C}, \mathcal{X})$ over the spectrum of a ring of algebraic integers with elliptic pairs as geometric fibers, such that the generic fiber has infinite order. While closed fibers have finite order, their minimal models automatically have Du Val singularities (after removing finitely many primes). We call a prime p polyhedral if $\overline{\mathrm{Eff}}(Y)$ is polyhedral, where (C, Y) is the minimal model of the geometric fiber (C, X) in characteristic p. In Section 5, we study distribution of polyhedral primes using tools of arithmetic geometry in the spirit of the Lang–Trotter analysis [46].

We found many examples of *Lang–Trotter polygons* that give rise to arithmetic elliptic pairs of infinite order; see the list of 135 polygons displayed in Database 8.1. For some of them, $\overline{\mathrm{Eff}}(\mathrm{Bl}_e\,\mathbb{P})$ is not polyhedral in characteristic p for an infinite set of primes p of positive density. On the other hand, every prime $p < 2000$ is non-polyhedral for some Lang–Trotter polygon (see Database 8.2). This is probably true for every prime number p, but seems out of reach with our methods. While most of the Lang–Trotter polygons that we found are not smooth, in Remark 5.16, we describe a smooth toric elliptic pair (C, X) with a large Picard

number $\rho = 18$. The Mordell–Weil rank of C is equal to 9. We do not know if there is an upper bound on the Picard number (or the Mordell–Weil rank) of a toric elliptic pair.

The image $\Gamma \subset \mathbb{P}$ of the curve C has large multiplicity at $e \in \mathbb{P}$. In practice, we start by finding an equation of Γ, which would be difficult without a computer. We use a MAGMA package, which can be downloaded from https://github.com/alaface/non-polyhedral and contains descriptions of all functions. Throughout the paper, we often refer to [15, § 10], where we perform many computer-aided calculations, for example, to check that a given polygon is a Lang–Trotter polygon. This *implicit method* has obvious disadvantages; for example, it is not clear how to apply it to construct an infinite sequence of examples. By contrast, we also found infinite sequences of Lang–Trotter polygons using a *parametric method* (see Remark 5.14). We start with an infinite sequence of elliptic curves $\{C_k\}$, which are members of an elliptic fibration (rational or K3) with parameter k. We describe maps $C_k \to \mathbb{P}_k$ to an infinite sequence of toric surfaces that fold an arbitrarily large number of points of C_k onto one point $e \in \Gamma_k \subset \mathbb{P}_k$. We hope that this new method may help with other problems related to the Nagata approximation conjecture, where it is desirable to geometrically construct curves with points of high multiplicity.

We observe a different behavior in *Halphen polygons*, which give rise to elliptic pairs of finite order with Du Val singularities both in characteristic 0 and in prime characteristic. Here the condition on singularities of the minimal model is not guaranteed by a general theory and needs to be checked by hand. We exhibit an example in Theorem 6.5 of a Halphen polygon such that $\overline{\mathrm{Eff}}(\mathrm{Bl}_e \mathbb{P})$ is not polyhedral in characteristic 0 and in characteristic p for all but a finite set of primes p. Empirically, Halphen polygons seem to be harder to find than Lang–Trotter polygons.

Our main application of Theorem 1.1 is to the birational geometry of the Grothendieck–Knudsen moduli space $\overline{M}_{0,n}$ of stable rational curves with n marked points. The study of effective cones of moduli spaces has a long history, starting with the pioneering work of Harris and Mumford [40], who used computations of effective divisors to show that $\overline{M}_g$ is not unirational for $g \gg 0$.

While the moduli space $\overline{M}_{0,n}$ is a rational variety, its birational geometry is far from understood, in spite of numerous efforts; see for example [1,8,17,18,23,25,26,31–35,44]. The Picard number of $\overline{M}_{0,n}$ grows exponentially, and it is not a Fano variety for $n \geq 6$; in fact, its anticanonical class is not pseudo-effective if $n \geq 8$. In this regard, $\overline{M}_{0,n}$ looks similar to the blow-up of $\mathbb{P}^2$ in n points (a connection was found in [16]).

A question attributed to Fulton, which received a lot of attention, is whether, similarly to the case of toric varieties, any subvariety of $\overline{M}_{0,n}$ is numerically equivalent to a sum of strata. For the case of curves, the statement is known as the F-conjecture. A result of Gibney, Keel and Morrison [34] proves that the F-conjecture, if known for all n, implies the similar statement for $\overline{M}_{g,n}$, for all genera g and number of marked points n, thus giving an explicit combinatorial description to the ample cone of $\overline{M}_{g,n}$. The conjecture holds for $n \leq 7$ and is open for $n \geq 8$.

For the case of divisors, Fulton's question is whether the class of every effective divisor on $\overline{M}_{0,n}$ is a sum of boundary divisors. Every boundary divisor is an extremal ray of $\overline{\mathrm{Eff}}(\overline{M}_{0,n})$; in fact, these divisors are exceptional, i.e., they can be contracted by birational contractions. For example, $\overline{M}_{0,5}$ is a degree 4 del Pezzo surface, and its boundary divisors form the Petersen graph of ten (-1)-curves, which generate $\mathrm{Eff}(\overline{M}_{0,5})$. Extremal rays of a different type for $\overline{M}_{0,6}$ were found by Keel and Vermeire [67], thus giving a negative answer to Fulton's question for

divisors when $n \geq 6$.[1)] However, Hassett and Tschinkel proved in [41] that $\overline{\mathrm{Eff}}(\overline{M}_{0,6})$ is still fairly simple, namely it is a polyhedral cone, generated by the boundary and the Keel–Vermeire divisors (only one up to S_6 symmetry).

A large class of exceptional divisors on $\overline{M}_{0,n}$ was discovered by Castravet and Tevelev [17]. They are parametrized by irreducible hypertrees, which can be obtained, for example, from bi-colored triangulations of the 2-sphere. Up to the action of the symmetric group S_n, this gives $1, 2, 11, 93, 1027, \ldots$ new types of exceptional divisors on $\overline{M}_{0,n}$, $n = 7, 8, 9, 10, 11, \ldots$. Equations of these divisors appear as numerators of leading singularities scattering amplitude forms for n particles in $N = 4$ super-symmetric Yang–Mills theory [2, 65].

New extremal rays of $\overline{\mathrm{Eff}}(\overline{M}_{0,n})$ were found by Opie [58] disproving an over-optimistic conjecture from [17]. Further extremal rays were found by Doran, Giansiracusa and Jensen in [23]. Our second result explains this complexity.

Theorem 1.2. *The cone* $\overline{\mathrm{Eff}}(\overline{M}_{0,n})$ *is not polyhedral for* $n \geq 10$*, both in characteristic* 0 *and in characteristic* p*, for all primes* p*.*

The moduli space $\overline{M}_{0,n}$ is related to blown-up toric varieties via the notion of a *rational contraction*, a dominant rational map $X \dashrightarrow Y$ of projective varieties that can be decomposed into a sequence of small $\mathbb{Q}$-factorial modifications [43] and surjective morphisms. By [18], there exist rational contractions $\mathrm{Bl}_e \overline{\mathrm{LM}}_{n+1} \dashrightarrow \overline{M}_{0,n} \dashrightarrow \mathrm{Bl}_e \overline{\mathrm{LM}}_n$, where $\overline{\mathrm{LM}}_n$ is the Losev–Manin moduli space of chains of rational curves; see [19, 50]. This is a toric variety associated with the permutohedron. A feature of $\overline{\mathrm{LM}}_n$, noticed in [18] and proved in Theorem 7.1, is its "universality" among all projective toric varieties $\mathbb{P}$. Specifically, for any projective toric variety $\mathbb{P}$, there exist rational contractions $\overline{\mathrm{LM}}_n \dashrightarrow \mathbb{P}$ and $\mathrm{Bl}_e \overline{\mathrm{LM}}_n \dashrightarrow \mathrm{Bl}_e \mathbb{P}$ for n sufficiently large. Thus, $\overline{M}_{0,n}$ has worse birational geometry than $\mathrm{Bl}_e \mathbb{P}$. For example, given a rational contraction, if $\overline{\mathrm{Eff}}(X)$ is a (rational) polyhedral cone, then $\overline{\mathrm{Eff}}(Y)$ is also (rational) polyhedral (Lemma 2.2). In particular, if the cone $\overline{\mathrm{Eff}}(\mathrm{Bl}_e \mathbb{P})$ is not polyhedral for some toric variety $\mathbb{P}$, then $\overline{\mathrm{Eff}}(\mathrm{Bl}_e \overline{\mathrm{LM}}_n)$, and therefore $\overline{\mathrm{Eff}}(\overline{M}_{0,n})$, are not polyhedral either, for n sufficiently large.

A similar strategy was used in [18] to show that $\overline{M}_{0,n}$ is not an MDS in characteristic 0 for $n \geq 134$, answering a question of Hu and Keel [43]. The bound was lowered to 13 by Gonzalez and Karu [36] and then to 10 by Hausen, Keicher and Laface [42]. Theorem 1.2 gives the same bound $n \geq 10$, but it exhibits an even wilder behavior than previously expected, as effective cones are a rougher invariant than Cox rings (the Cox ring is graded and the effective cone is the semigroup of possible weights of the grading). For instance, the toric surfaces used in [18] were the weighted projective planes $\mathbb{P}(a, b, c)$. Of course, $\mathrm{Bl}_e \mathbb{P}(a, b, c)$ has Picard number 2 and its effective cone is polyhedral. Nevertheless, Goto, Nishida and Watanabe [37] proved that $\mathrm{Bl}_e \mathbb{P}(a, b, c)$ is not an MDS in characteristic 0 for certain values of a, b, c, by exhibiting a nef but not semi-ample line bundle. However, in characteristic $p > 0$, this line bundle is semi-ample, and therefore this space is an MDS, by Artin's criterion [3]. Hence, this technique cannot be used for blown-up toric surfaces and $\overline{M}_{0,n}$. So the following corollary of Theorem 1.2 is new.

Corollary 1.3. *If* $n \geq 10$*, the moduli space* $\overline{M}_{0,n}$ *is not an MDS in characteristic* p*, for all primes* p*.*

[1)] Using forgetful maps, one has a negative answer for all cycles of dimension at least 2 when $n \geq 6$.

By contrast, $\overline{M}_{0,n}$ is an MDS in all characteristics if $n \leq 6$ (see [14, 43]). This leaves open only the cases $n = 7, 8, 9$.

2. Polyhedrality of effective cones

Let k be an algebraically closed field of arbitrary characteristic. We recall some definitions (see for example [47, 48]). If X is a normal projective irreducible variety over k, let $\mathrm{Cl}(X)$ be the divisor class group and let $\mathrm{Pic}(X)$ be the Picard group of X. As usual, we denote by $\sim$ the linear equivalence of divisors and by $\equiv$ the numerical equivalence. For Cartier divisors D_1, D_2, we have $D_1 \equiv D_2$ if and only if $D_1 \cdot C = D_2 \cdot C$, for any curve $C \subseteq X$. We let $\mathrm{Num}^1(X) := \mathrm{Pic}(X)/\equiv$ be the group of numerical equivalence classes of Cartier divisors on X. We denote $\mathrm{Num}^1(X)_{\mathbb{R}} = \mathrm{Num}^1(X) \otimes_{\mathbb{Z}} \mathbb{R}$, $\mathrm{Num}^1(X)_{\mathbb{Q}} = \mathrm{Num}^1(X) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Sometimes, we extend $\sim$ to the linear equivalence of $\mathbb{Q}$-divisors in a usual way (for $\mathbb{Q}$-divisors, $A \sim B$ if $kA \sim kB$ as Cartier divisors for some $k > 0$), but mostly, we use numerical equivalence of $\mathbb{Q}$-divisors to avoid confusion.

Similarly, we define $\mathrm{Z}_1(X)_{\mathbb{R}}$ to be the group of $\mathbb{R}$-linear combinations of irreducible curves in X, i.e., formal sums $\gamma = \sum a_i C_i$, $a_i \in \mathbb{R}$, with all $C_i \subseteq X$ irreducible curves. As in [47, Definition 1.4.25], we let $\mathrm{Num}_1(X)_{\mathbb{R}} = \mathrm{Z}_1(X)_{\mathbb{R}}/\equiv$, where for two one-cycle classes $\gamma_1, \gamma_2 \in \mathrm{Z}_1(X)_{\mathbb{R}}$, we have numerical equivalence $\gamma_1 \equiv \gamma_2$ if and only if $D \cdot \gamma_1 = D \cdot \gamma_2$ for all Cartier divisors D on X. It follows from the definitions that $\mathrm{Num}^1(X)_{\mathbb{R}} \otimes \mathrm{Num}_1(X) \to \mathbb{R}$, $(\delta, \gamma) \mapsto \delta \cdot \gamma$ is a perfect pairing, so $\mathrm{Num}^1(X)_{\mathbb{R}}$ and $\mathrm{Num}_1(X)_{\mathbb{R}}$ are dual finite-dimensional real vector spaces.

We define the pseudo-effective cone $\overline{\mathrm{Eff}}(X) \subseteq \mathrm{Num}^1(X)_{\mathbb{R}}$ as the closure of the effective cone $\mathrm{Eff}(X)$, i.e., the convex cone generated by numerical classes of effective Cartier divisors [48, Definition 2.2.25]. We let $\mathrm{Nef}(X) \subseteq \mathrm{Num}^1(X)_{\mathbb{R}}$ be the cone generated by the classes of *nef divisors*. We define $\overline{\mathrm{Mov}}_1(X) \subseteq \mathrm{Num}_1(X)_{\mathbb{R}}$ as the closure of the cone generated by numerical classes of *movable* 1-cycles; see [48, Definition 11.4.16]. The cones $\overline{\mathrm{Eff}}(X)$ and $\overline{\mathrm{Mov}}_1(X)$ are dual to each other. This was proved first in [12] for the case when X is a smooth projective variety in characteristic 0, but it holds in general. For X an irreducible projective variety over a field k of characteristic 0, this is proved in [47, Theorem 11.4.19]. For the case of arbitrary characteristic, the same proof holds; see for example [29, Remark 2.1].

Definition 2.1. A convex cone $\mathcal{C} \subseteq \mathbb{R}^s$ is called *polyhedral* if there are finitely many vectors $v_1, \ldots, v_s \in \mathbb{R}^s$ such that $\mathcal{C} = \mathbb{R}_{\geq 0} v_1 + \cdots + \mathbb{R}_{\geq 0} v_s$. The cone is said to be *rational polyhedral* if one can choose the v_i's in $\mathbb{Q}^s$.

Lemma 2.2. *Let $f\colon X \to Y$ be a surjective morphism of normal projective irreducible varieties. If $\overline{\mathrm{Eff}}(X)$ is (rational) polyhedral, then the same is true for $\overline{\mathrm{Eff}}(Y)$.*

Proof. Suppose $\overline{\mathrm{Eff}}(X)$ is a (rational) polyhedral cone. By the duality between the cones $\overline{\mathrm{Eff}}(X)$ and $\overline{\mathrm{Mov}}_1(X)$, it follows that $\overline{\mathrm{Mov}}_1(X)$ is also a (rational) polyhedral cone. The proper push-forward of 1-cycles induces a map of $\mathbb{R}$-vector spaces

$$f_*\colon \mathrm{Num}_1(X)_{\mathbb{R}} \to \mathrm{Num}_1(Y)_{\mathbb{R}}.$$

By [30, Corollary 3.12], $f_*(\overline{\mathrm{Mov}}_1(X)) = \overline{\mathrm{Mov}}_1(Y)$. The definitions of $\mathrm{Num}_1(X)$ and $\overline{\mathrm{Mov}}_1(X)$ given in [30] coincide with the ones given above; see [30, Section 2.1, Example 3.3]. It follows that $\overline{\mathrm{Mov}}_1(Y)$ is a (rational) polyhedral cone. Again by the duality between the cones $\overline{\mathrm{Eff}}(Y)$ and $\overline{\mathrm{Mov}}_1(Y)$, it follows that $\overline{\mathrm{Eff}}(Y)$ is a (rational) polyhedral cone. □

We concentrate on the case of surfaces. The cone and contraction theorems hold in any characteristic with very mild assumptions; see [27, 28, 45, 64]. Our main reference for smooth algebraic surfaces is [53], while we refer to [52] for intersection theory on normal singular surfaces.

Proposition 2.3. *Let X be a normal projective $\mathbb{Q}$-factorial surface with Picard number at least 3 and such that the cone $\overline{\mathrm{Eff}}(X)$ is polyhedral. Then*

(1) *every class $C \in \mathrm{Num}^1(X)$ of self-intersection 0 (or its opposite $-C$) is in the relative interior of either the cone $\overline{\mathrm{Eff}}(X)$ or its codimension one facet.*

(2) *The effective cone $\mathrm{Eff}(X)$ is generated by finitely many negative curves.*[2] *In particular, $\overline{\mathrm{Eff}}(X) = \mathrm{Eff}(X)$ is a rational polyhedral cone.*

Part (2) of Proposition 2.3 appears also in [54].

Proof. (1) Fix h an ample divisor. Let

$$Q := \{\omega \mid \omega^2 \geq 0,\ \omega \cdot h \geq 0\} \subseteq \mathrm{Num}^1(X)_{\mathbb{R}}$$

be the non-negative part of the light cone. Then either C or its opposite $-C$ lies on the boundary ∂Q. By Riemann–Roch, the cone Q is contained in $\overline{\mathrm{Eff}}(X)$. Since the Picard number of X is at least 3, the cone Q is round. In particular, ∂Q can intersect only a facet of $\overline{\mathrm{Eff}}(X)$ of codimension 1 and only in its relative interior.

(2) By (1), any $\omega \in \mathrm{Num}^1(X)$ generating an extremal ray of $\overline{\mathrm{Eff}}(X)$ has $\omega^2 < 0$. By [22, Lemma 6.2 (e)][3], for any such ω, there exists an irreducible curve E such that ω is a positive multiple of the class of E. □

Remark 2.4. In the settings of Proposition 2.3, if the class C admits a positive integer multiple nC such that $|nC|$ is a base point free pencil, then C is not big. Thus, it lies in the relative interior of a maximal facet τ of $\overline{\mathrm{Eff}}(X)$, and by the Hodge Index Theorem, the supporting hyperplane of τ is $C^{\perp}$. In particular, any class of an irreducible curve R which generates an extremal ray of τ satisfies $R \cdot C = 0$ so that R is an irreducible component of a fiber of the fibration $\pi\colon X \to \mathbb{P}^1$ induced by $|nC|$. Since the contribution of the components of a fiber to the "vertical" rank of the Picard group is the number of components minus one, it follows that, in order for $\overline{\mathrm{Eff}}(X)$ to be polyhedral, it must be

$$1 + \sum_{b \in \mathbb{P}^1} (|\text{Comp. of } f^{-1}(b)| - 1) = \mathrm{rk}(\mathrm{Pic}(X)) - 1.$$

[2] A negative curve is an irreducible curve B with $B^2 < 0$.

[3] The proof in [22] is for smooth surfaces, but the argument works verbatim in our case.

Proposition 2.5. *Let X be a normal projective $\mathbb{Q}$-factorial surface with Picard number at least 3. Assume that $C \subseteq X$ is an irreducible curve with $C^2 = 0$ and $C \equiv -\alpha K_X$ with $\alpha \in \mathbb{Q}_{>0}$. Then the following are equivalent.*

(1) *There exist irreducible negative curves $B_1, \dots, B_s$ that generate $C^\perp \subseteq \mathrm{Num}^1(X)_\mathbb{Q}$ and such that*

$$C \equiv a_1 B_1 + \cdots + a_s B_s \quad \text{with } a_1, \dots, a_s \in \mathbb{Q}_{>0}. \tag{2.1}$$

(2) $\overline{\mathrm{Eff}}(X)$ *is a rational polyhedral cone generated by negative curves.*

Proof. Proposition 2.3 gives (2) $\Rightarrow$ (1). We prove (1) $\Rightarrow$ (2) under our additional assumptions. Note that C (hence $-K$) is nef. Recall that any $\omega \in \mathrm{Num}^1(X)_\mathbb{R}$ generating an extremal ray must have $\omega^2 \leq 0$, and if $\omega^2 < 0$, then ω is the class of a multiple of a curve [22, Lemma 6.2] (see footnote 3). The same is true when $\omega^2 = 0$, as if $\omega \cdot C = 0$, by the Hodge Index Theorem, ω and C generate the same ray, while if $\omega \cdot C > 0$, then $\omega \cdot K < 0$ and ω is generated by the class of a curve by the cone theorem. Hence, it suffices to prove that X contains finitely many irreducible curves E with $E^2 \leq 0$ such that E is not numerically equivalent to a rational multiple of C. We can also assume that $E \neq B_i$ for all i.

We consider two cases. If $E \cdot C = 0$, then $E \cdot B_i = 0$ for all i by (2.1) and by our assumption that $E \neq B_i$ for all i. Since $B_1 \dots, B_s$ generate $C^\perp$ over $\mathbb{Q}$, E must be numerically equivalent to a rational multiple of C, which we have also ruled out.

Suppose $E \cdot C > 0$. Since $B_1 \dots, B_s$ generate $C^\perp$ over $\mathbb{Q}$, the classes which have fixed intersections with the B_i's form an affine subspace of dimension one in $\mathrm{Num}^1(X)_\mathbb{Q}$, differing one from another by a multiple of the class of C. Since $E \cdot C > 0$ and $C \cdot C = 0$, there is at most one such class with E^2 also fixed. Hence, it suffices to prove that $E \cdot B_i$ and E^2 belong to a finite set. By assumption (1) and adjunction, we have

$$\frac{1}{\alpha} \sum a_i (E \cdot B_i) = E \cdot (-K) \leq E^2 + 2 \leq 2.$$

Hence, $0 \leq E \cdot B_i \leq 2\alpha / a_i$. As there exists $l \in \mathbb{Z}_{>0}$ (the index of $\mathrm{Pic}(X)$ in $\mathrm{Cl}(X)$) such that the lD is Cartier for any curve D (hence, $l(D \cdot E)$ is an integer), it follows that $E \cdot B_i$ belongs to a finite set. We have $-2 \leq E^2$ by adjunction and nefness of $-K$. As $E^2 \leq 0$, it follows similarly that E^2 must belong to a finite set. □

3. Elliptic pairs: General theory

As in Section 2, we work over an algebraically closed field k of arbitrary characteristic. While Propositions 2.3 and 2.5 address polyhedrality of $\overline{\mathrm{Eff}}(X)$ for a general surface X, in this section, we study polyhedrality further for a rational surface in the presence of a curve C with self-intersection 0 under some additional assumptions.

Definition 3.1. An *elliptic pair* (C, X) consists of a projective rational surface X with log terminal singularities and an irreducible curve $C \subseteq X$, of arithmetic genus one, disjoint from the singular locus of X and such that $C^2 = 0$. Let $C^\perp \subseteq \mathrm{Cl}(X)$ be the orthogonal

complement to C. We define the *restriction map*

$$\mathrm{res}\colon C^{\perp} \to \mathrm{Pic}^0(C), \quad D \mapsto \mathcal{O}(D)|_C.$$

Since $K \cdot C = 0$ by adjunction, we can also define the *reduced restriction map*

$$\overline{\mathrm{res}}\colon \mathrm{Cl}_0(X) := C^{\perp}/\langle K\rangle \to \mathrm{Pic}^0(C)/\langle \mathrm{res}(K)\rangle.$$

We will often study a birational morphism $X \to Y$, which is an isomorphism in a neighborhood of C. We will then use notation C_X, C_Y, etc., to avoid confusion.

The most familiar elliptic pairs are rational elliptic fibrations $X \to \mathbb{P}^1$ with a fiber C (which can be the support of a multiple fiber). However, we do not make this assumption. Note that, as X is rational, $h^1(X, \mathcal{O}_X) = 0$, and hence $\mathrm{Pic}(X)_{\mathbb{Q}} = \mathrm{Num}^1(X)_{\mathbb{Q}}$.

Lemma–Definition 3.2. *We define the order $e = e(C, X)$ of the elliptic pair (C, X) to be the positive integer satisfying any of the following equivalent conditions (or ∞ if none of them are met).*

(1) $\mathrm{res}(C) \in \mathrm{Pic}^0(C)$ *is a torsion line bundle of order e.*

(2) *e is the smallest positive integer such that $h^0(C, \mathrm{res}(eC)) = 1$.*

(3) *e is the smallest positive integer such that $h^0(X, eC) = 2$.*

(4) *e is the smallest positive integer such that $h^0(X, eC) > 1$.*

The order $e(C, X)$ only depends on a Zariski neighborhood of C in X.

Proof. The equivalence of (1) and (2) is clear. We use this as a definition of e. In particular, $e(C, X)$ only depends on a Zariski neighborhood of C in X. Since log terminal singularities are rational and C is disjoint from the singular locus of X, if $\widetilde{X}$ is a resolution of singularities of X, then $h^0(\widetilde{X}, nC_{\widetilde{X}}) = h^0(X, nC_X)$ for any integer n. Hence, to prove the remaining equivalences, we may assume that X is smooth. For any $n \geq 0$, we have

$$h^2(X, nC) = h^0(X, K_X - nC) = 0,$$

as otherwise K_X would be effective. Moreover, by Riemann–Roch, we have $\chi(\mathcal{O}_X(nC)) = 1$ for all n. Thus, either $h^0(X, nC) = 1$ and $h^0(C, \mathrm{res}(nC)) = 0$ for every $n > 0$, or for some $n > 0$, we have $h^0(X, nC) = 2$, $h^0(C, \mathrm{res}(nC)) = 1$ and $h^0(X, lC) = 1$, $h^0(C, \mathrm{res}(lC)) = 0$ for $1 \leq l < n$. □

Lemma 3.3. *Suppose (C, X) is an elliptic pair. Let $e = e(C, X)$. Then*

(1) *$e < \infty$ if and only if C is the support of a (multiple) fiber of a (quasi-)elliptic fibration.*[4)]

(2) *If $e = \infty$, then C is rigid, which means that $h^0(nC) = 1$ for all $n > 0$. In this case, $\overline{\mathrm{Eff}}(X)$ is not polyhedral if the Picard number $\rho(X) \geq 3$.*

[4)] If C is smooth or if $\mathrm{char}\, k \neq 2, 3$, then the fibration is automatically elliptic [9]. If not, it can be quasi-elliptic, i.e., have cuspidal generic fiber.

Proof. Suppose $e < \infty$. Then $eC \sim \sum D_i$ for some irreducible curves $D_i \neq C$ by Lemma 3.2 (3). As $C^2 = 0$, it follows that the D_i's are disjoint from C and $|eC|$ is a base-point-free pencil. Since $C^2 = K \cdot C = 0$ by adjunction, $\varphi_{|eC|}\colon X \to \mathbb{P}^1$ is a (quasi-)elliptic fibration. Suppose $e = \infty$. Then C is rigid by Lemma 3.2 (4). By Proposition 2.3, if $\overline{\mathrm{Eff}}(X)$ is polyhedral and the Picard number of X is at least 3, then $\overline{\mathrm{Eff}}(X)$ is generated by negative curves and C is contained in the interior of a facet. Thus, $h^0(X, kC) > 1$ for some k, and therefore $e(C, X) < \infty$ by Lemma 3.2 (4). □

Lemma 3.4. *If (C, X) is an elliptic pair, then $K_X + C$ is an effective divisor.*

Proof. As C is contained in the smooth locus of X, we can pass to a resolution of singularities and prove for a smooth surface X that $h^2(-C) = h^0(K + C) > 0$. By adjunction, $\mathcal{O}_X(K + C)|_C \simeq \omega_C \simeq \mathcal{O}_C$, so there is an exact sequence[5)]

$$0 \to \mathcal{O}_X(K) \to \mathcal{O}_X(K + C) \to \mathcal{O}_C \to 0.$$

The statement follows from the vanishing $h^0(X, K) = h^1(X, K) = 0$. □

Definition 3.5. We say that (C, X) is a *minimal* elliptic pair if it does not contain irreducible curves E such that $K \cdot E < 0$ and $C \cdot E = 0$.

Remark 3.6. A curve E as in the definition must have $E^2 < 0$. Indeed, $E^2 \leq 0$ by the Hodge Index Theorem, with equality if and only if the classes of C and E are multiples of each other. But since $E \cdot K < 0$ and $C \cdot K = 0$, the latter is not possible. Moreover, E is a rational curve [27, Theorem 5.6]. By the contraction theorem, there exists a morphism $\phi\colon X \to Y$ contracting only E. As ϕ is an isomorphism in a Zariski neighborhood of C and Y is log terminal, (C, Y) is an elliptic pair. Moreover, $K_X \equiv \phi^* K_Y + aE$ for some $a \in \mathbb{Q}$. Since $E \cdot K_X < 0$ and $E^2 < 0$, it follows that $a > 0$. Furthermore, $K_X^2 < K_Y^2$.

Lemma 3.7. *Let (C, X) be an elliptic pair. The following conditions are equivalent:*

(1) *(C, X) is minimal;*

(2) *$K + C$ is nef;*

(3) *$C \sim \alpha(-K)$ for some $\alpha \in \mathbb{Q}_{>0}$, a linear equivalence of $\mathbb{Q}$-divisors;*

(4) *$K^2 = 0$.*

Proof. To prove (1) $\Rightarrow$ (2), assume that $K + C$ is not nef. By the cone theorem[6)], for a log surface (X, C) (see [27, 64]), there is an irreducible curve E such that $(K + C) \cdot E < 0$ and $E^2 < 0$. As $K + C$ is effective, E must be one of its components. Since $C \cdot (K + C) = 0$ and C is nef, we must have $C \cdot E = 0$, and hence $K \cdot E < 0$. This contradicts the minimality of (C, X).

Next we prove (2) $\Rightarrow$ (3). Since $(K + C) \cdot C = 0$, by the Hodge Index Theorem, we must have $(K + C)^2 \leq 0$. But since $K + C$ is nef, $(K + C)^2 \geq 0$. Thus, $(K + C)^2 = 0$, and it must be that $K + C \equiv \lambda C$ for some $\lambda \in \mathbb{Q}$. As no multiple of K is effective, it follows that

[5)] This trick is from the proof of the canonical bundle formula for elliptic fibrations in [10].

[6)] Note that there are no singularity assumptions on $K + C$ in the cone theorem for surfaces.

$C \equiv \alpha(-K)$ for some $\alpha \in \mathbb{Q}_{>0}$. Since X is rational, in fact, $C \sim \alpha(-K)$, a linear equivalence of $\mathbb{Q}$-divisors.

The implication (3) $\Rightarrow$ (4) is clear. To see (4) $\Rightarrow$ (1), suppose (X, C) is not minimal. By Remark 3.6, there is a contraction $\phi\colon X \to Y$ of a curve E such that $K \cdot E < 0$, $E^2 < 0$ and $C \cdot E = 0$. Moreover, $K_Y^2 > K_X^2 = 0$. But (C, Y) is an elliptic pair, and so $K_Y^2 \leq 0$ by the Hodge Index Theorem, which gives a contradiction. □

Theorem 3.8. *Let (C, Z) be an elliptic pair with smooth Z. Then (C, Z) is minimal if and only if $\rho(Z) = 10$ or, equivalently, $K^2 = 0$. If (C, Z) is minimal, then*

(i) *$C \sim n(-K)$ for some positive integer n;*

(ii) *Z is a blow-up of $\mathbb{P}^2$ at 9 points (possibly infinitely near) and the intersection pairing on Z makes $\mathrm{Cl}_0(Z)$ isomorphic to the negative definite lattice $\mathbb{E}_8$.*

Suppose that (C, Z) is minimal and $e(C, Z) < \infty$. The following are equivalent.

(1) *$\overline{\mathrm{Eff}}(Z)$ is polyhedral and generated by (-2) and (-1)-curves.*

(2) *$\overline{\mathrm{Eff}}(Z)$ is polyhedral.*

(3) *$\mathrm{Ker}(\overline{\mathrm{res}}) \subseteq \mathbb{E}_8$ contains 8 linearly independent roots of $\mathbb{E}_8$.*

Proof. By Lemma 3.7, the elliptic pair (C, Z) is minimal if and only if $K^2 = 0$. Since Z is a smooth rational surface, it is an iterated blow-up of $\mathbb{P}^2$ or a Hirzebruch surface $\mathbb{F}_e$. As K^2 goes down by one and the Picard number goes up by one when blowing-up a smooth point, $K^2 = 0$ if and only if $\rho(Z) = 10$. We claim that Z is the blow-up of $\mathbb{P}^2$ at 9 points. Assume not. Then Z is the iterated blow-up of a Hirzebruch surface $\mathbb{F}_e$ ($e = 0$ or $e \geq 2$) at 8 points. A negative curve B on $\mathbb{F}_e$ has $B^2 = -e$ and B^2 goes down by blow-up. By adjunction and since $-K_Z$ is nef, the only negative curves on Z are (-1) and (-2)-curves, so we must have $e = 0$, or $e = 2$ and none of the blown up (possibly infinitely near) points on $\mathbb{F}_2$ lie on the negative section. If $e = 0$, we are done, as $\mathrm{Bl}_p\mathbb{P}^1 \times \mathbb{P}^1$ is isomorphic to the blow-up of $\mathbb{P}^2$ at two points. If $e = 2$, we are also done, as a blow-up of $\mathbb{F}_2$ at a point not lying on the negative section is isomorphic, via an elementary transformation, to a blow-up of $\mathbb{F}_1$ at one point. This proves the claim. It follows that $\mathrm{Cl}_0(Z) \cong \mathbb{E}_8$. Since $-K$ is a primitive vector of $\mathrm{Pic}(Z)$, it follows by Lemma 3.7 (3) that $C \sim n(-K)$ for some integer $n > 0$.

Suppose that (C, Z) is minimal and $e = e(C, Z) < \infty$. By Lemma 3.3, $|eC|$ gives a (quasi-)elliptic fibration $Z \to \mathbb{P}^1$. Clearly, (1) $\Rightarrow$ (2) and Proposition 2.3 (2) implies (2) $\Rightarrow$ (1), as the only negative curves are (-1) and (-2)-curves. Assume (1). By Proposition 2.5, we have $C \equiv \sum a_i B_i$ for $a_i \in \mathbb{Q}_{>0}$, with irreducible negative curves B_i generating $C^\perp$ over $\mathbb{Q}$. Since B_i is irreducible, $\mathrm{res}(B_i) = 0$. Since $B_i \cdot K = 0$, each B_i is a (-2)-curve. Since the curves B_i generate $C^\perp$ over $\mathbb{Q}$, eight of them are linearly independent modulo K. This proves (3).

Assume (3). Let $\beta_1, \ldots, \beta_8$ be (-2)-classes in $C^\perp$, linearly independent modulo K and such that $\overline{\mathrm{res}}(\beta_i) = 0$. Adding to each β_i an integer multiple of K, we may assume that each β_i restricts trivially to C. We claim that, for each i, either β_i or $(K + C) - \beta_i$ is effective. Indeed, for each $\beta := \beta_i$, we have a short exact sequence

$$0 \to \mathcal{O}(\beta - C) \to \mathcal{O}(\beta) \to \mathcal{O}_C \to 0.$$

If β is not effective, then $\beta - C$ is not effective either. Hence, we have $h^1(Z, \mathcal{O}(\beta - C)) > 0$. But $\chi(\mathcal{O}(\beta - C)) = 0$ by Riemann–Roch. Thus, $h^2(Z, \mathcal{O}(\beta - C)) > 0$, and so $(K + C) - \beta$

is effective. We have found 8 effective divisors $D_1, \dots, D_8$ with $\operatorname{res}(D_i) = 0$, $D_i^2 = -2$ and linearly independent modulo K. Each of the divisors D_i is supported on a union of the fibers of the (quasi-)elliptic fibration (and no D_i is a rational multiple of C). Since the irreducible components of reducible fibers are (-2)-curves, it follows that (-2)-curves generate $C^\perp$ over $\mathbb{Q}$. Clearly, for some integer $l \gg 0$, lC is an effective combination of (-2)-curves. Then Proposition 2.5 (1) implies (2). □

Remark 3.9. Smooth projective rational surfaces Z for which there is an integer $m > 0$ such that the linear system $|-mK_Z|$ is base-point free and of dimension 1 are called Halphen surfaces of *index m* and have been studied from many different points of view; see for example [4,13,38]. If (C, Z) is an elliptic pair as in the second half of Theorem 3.8, then Z is a Halphen surface with index $n \cdot e$, where $e := e(C, Z)$ and n is a positive integer such that $C \sim -nK_Z$. Let N be the sublattice of $\mathbb{E}_8$ that is generated by roots contained in $\operatorname{Ker}(\overline{\operatorname{res}})$, i.e., N is generated by the classes of all the (-2)-curves on Z (see the proof of Theorem 3.8). By the Hodge Index Theorem, the (-2)-curves on Z are precisely the irreducible components of reducible fibers of the fibration induced by the linear system $|eC| = |-n \cdot eK_Z|$; call them $S_1, \dots, S_\lambda$. If μ_j denotes the number of irreducible components of S_j, the rank of N (i.e., the maximum number of linearly independent roots of $\mathbb{E}_8$ contained in $\operatorname{Ker}(\overline{\operatorname{res}})$ or, equivalently, the maximum number of (-2)-curves that are linearly independent modulo K_Z) equals $\sum_{i=1}^{\lambda}(\mu_i - 1)$. By a result of Gizatullin, $\sum_{i=1}^{\lambda}(\mu_i - 1) < 8$ if and only if the automorphism group $\operatorname{Aut}(Z)$ is infinite; in this case, there exists a free abelian group G of rank $8 - \sum_{i=1}^{\lambda}(\mu_i - 1)$, of finite index in $\operatorname{Aut}(Z)$, such that any non-zero element in G is an automorphism that acts by translation on each fiber of the elliptic fibration [38, Theorem 7.11, Corollary 7.12], i.e., $\overline{\operatorname{Eff}}(Z)$ is not polyhedral if and only if $\operatorname{Aut}(Z)$ is infinite.

Theorem 3.10. *For any elliptic pair (C, X), there exist a minimal elliptic pair (C, Y) and a morphism $\pi\colon X \to Y$, which is an isomorphism over a neighborhood of C. Consider the Zariski decomposition on X of $K + C$,*

$$K + C \sim N + P, \quad N = a_1C_1 + \cdots + a_sC_s, \quad a_i \in \mathbb{Q}_{>0},$$

the linear equivalence of $\mathbb{Q}$-divisors.[7] *Then*

(1) *Y is obtained by contracting curves $C_1, \dots, C_s$ on X.*

(2) *$P \equiv 0$ if and only if $-K_Y \sim C_Y$; then N is an integral combination of $C_1, \dots, C_s$ and Y has Du Val singularities.*

Definition 3.11. We call an elliptic pair (C, Y) a *minimal model* of (C, X).

Corollary 3.12. *Let (C, Y) be a minimal model of an elliptic pair (C, X) such that $e(C, X) = \infty$. Then Y has Du Val singularities. Consider the Zariski decomposition*

$$K + C \sim N + P$$

on X. Then $P \sim 0$ and $K + C \sim N$ is an integral *effective combination of irreducible curves $C_1, \dots, C_s$ with a negative-definite intersection matrix. The minimal model Y is obtained by contracting curves $C_1, \dots, C_s$ and $C_Y \sim -K_Y$.*

[7] Recall that the C_i's are irreducible curves with a negative-definite intersection matrix and P is a nef effective $\mathbb{Q}$-divisor such that $P \cdot C_i = 0$ for all i. The $\mathbb{Q}$-divisor N is determined uniquely.

Proof. We first prove the theorem and then its corollary. We obtain a minimal model $\pi\colon X \to Y$ by running a $(K+C)$-MMP [27,64]. Equivalently (by Lemma 3.7), π is a composition of contractions of the form $\phi\colon X \to Y$, where each ϕ is the contraction of a K-negative curve E such that $E \cdot C = 0$. On each step,

$$K_X + C_X \sim \phi^*(K_Y + C_Y) + aE, \quad \text{with } a \in \mathbb{Q}_{>0},$$

a linear equivalence of $\mathbb{Q}$-divisors. At the end, we obtain that $K_Y + C_Y$ is nef, i.e., (C, Y) is minimal. If the curves contracted by π are $C_1, \dots, C_s \subseteq X$, then $K_X + C_X \sim N + P$, with

$$P = \pi^*(K_Y + C_Y), \quad N = \sum_{i=1}^{s} a_i C_i, \quad a_i \in \mathbb{Q}_{>0},$$

a linear equivalence of $\mathbb{Q}$-divisors. The divisor P is nef and effective (Lemma 3.4) and we have $P \cdot C_i = 0$ for all i. Hence, this is the Zariski decomposition of $K + C$. Moreover, $P \equiv 0$ if and only if $K_Y + C_Y \sim 0$.

Assume now $P \equiv 0$. Recall an algorithm for computing the Zariski decomposition [7]. Write $K + C \sim b_1 B_1 + \cdots + b_t B_t$ as an integral, effective sum of irreducible curves B_i. Let $N' := \sum x_i B_i$, where $0 \le x_i \le b_i$ are maximal such that $P' := \sum (b_i - x_i) B_i$ intersects all C_i non-negatively. Then N' and P' give a Zariski decomposition of $K + C$. Since $N = N'$ is unique and $P' \equiv P \equiv 0$, the Zariski decomposition is $K + C \sim b_1 B_1 + \cdots + b_t B_t$. To prove the singularity statement, note that $-K_Y \sim C_Y$ implies that K_Y is Cartier. Thus, Y has Du Val singularities.

Finally, we prove the corollary. Suppose that $e(C, X) = e(C_Y, Y) = \infty$. If $P \not\equiv 0$, we have $C_Y \sim \alpha(-K_Y)$ for some $\alpha \in \mathbb{Q}$, $\alpha \neq 1$. Then $C_Y \sim \frac{\alpha}{\alpha - 1}(K_Y + C_Y)$, a linear equivalence of $\mathbb{Q}$-divisors. But $K_Y + C_Y$ restricts trivially to C_Y by adjunction, and therefore $\operatorname{res}(C)$ is torsion, which is a contradiction. So we must have $P \equiv 0$, and this finishes the proof of the corollary by (1)–(2) of the theorem. □

Remark 3.13. We give an example of a minimal rational elliptic fibration that does not satisfy $C \sim -K$. Let W be a minimal smooth rational elliptic fibration with a nodal fiber I_0. Blow up the node of the fiber and contract the proper transform of the fiber (which has self-intersection -4). This produces a minimal rational elliptic fibration Y with a $\frac{1}{4}(1,1)$ singularity, which is log terminal. The fiber C_0 through the singularity is a nodal multiple fiber of multiplicity 2. We have $C \sim 2C_0 \sim -2K$.

Lemma 3.14. *Let (C, Y) be an elliptic pair such that Y has Du Val singularities. Let $\pi\colon Z \to Y$ be its minimal resolution.*

(1) *(C, Y) is minimal if and only if (C, Z) is minimal. Equivalently, $\rho(Y) = 10 - R$, where R is the rank of the root system of the singularities of Y.*

(2) *Assume (C, Y) is a minimal elliptic pair. Then the following are equivalent:*

- *$\overline{\operatorname{Eff}}(Y)$ is a polyhedral cone;*
- *$\overline{\operatorname{Eff}}(Y)$ is a rational polyhedral cone;*
- *$\overline{\operatorname{Eff}}(Z)$ is a polyhedral cone.*

When $\rho(Y) = 2$, all the above statements hold.

Proof. As $K_Z = \pi^* K_Y$, the pair (C, Z) is minimal if and only if (C, Y) is minimal by Lemma 3.7. As $\rho(Y) = \rho(Z) - R$, the first statement follows. If $\overline{\mathrm{Eff}}(Z)$ is (rational) polyhedral, then $\overline{\mathrm{Eff}}(Y)$ is (rational) polyhedral by Lemma 2.2. Assume now $\overline{\mathrm{Eff}}(Y)$ is polyhedral. If $\rho(Y) \geq 3$, then $e(C, Y) < \infty$ by Lemma 3.3, and by Proposition 2.3 (1), $\overline{\mathrm{Eff}}(Y)$ is a rational polyhedral cone with C_Y contained in the interior of a maximal facet. If $\rho(Y) = 2$ (the smallest possible), then $\mathrm{Eff}(Y)$ is a rational polyhedral cone by the cone theorem (it is spanned by the class of C and by the class of the unique negative curve). Note that this does not provide any information about $e(C, Y)$. In both cases, it follows that $C_Y^\perp$ contains $\rho(Y) - 2$ effective divisors which are linearly independent modulo K_Y and restrict trivially to C. As $\mathrm{Cl}(Z)_\mathbb{Q}$ decomposes as $\pi^* \mathrm{Cl}(Y)_\mathbb{Q} \oplus T_\mathbb{Q}$, where T is a sublattice spanned by classes of (-2)-curves over singularities of Y, we have

$$(C_Z^\perp)_\mathbb{Q} = (\pi^* C_Y^\perp)_\mathbb{Q} \oplus T_\mathbb{Q}.$$

It follows that $C_Z^\perp$ contains $\rho(Y) - 2 + R = 8$ effective divisors which are linearly independent modulo K_Z and restrict trivially to C. As in the proof of Theorem 3.8, it follows that $\overline{\mathrm{Eff}}(Z)$ is a polyhedral cone. □

Remark 3.15. In the set-up of Lemma 3.14, if (C, Y) has Du Val singularities and $C_Y \sim -K_Y$, where $\pi\colon Z \to Y$ is its minimal resolution, then Z is a Halphen surface of index $e(C, Z)$, as $C_Z \sim -K_Z$. Indeed, this follows from $\pi^* K_Y = K_Z$, $\pi^* C_Y = C_Z$.

Definition 3.16. Let (C, X) be an elliptic pair such that the minimal model (C, Y) has Du Val singularities. Let $\pi\colon Z \to Y$ be the minimal resolution of Y. Let

$$T \subseteq \mathbb{E}_8 = \mathrm{Cl}_0(Z)$$

be a root sublattice spanned by classes of (-2)-curves over singularities of Y. We call T the *root lattice of* (C, X), and we denote by $\widehat{T}$ its saturation $\mathbb{E}_8 \cap (T \otimes \mathbb{Q})$.

The push-forward $\pi_*\colon \mathrm{Cl}(Z) \to \mathrm{Cl}(Y)$ induces a map $\mathrm{Cl}_0(Z) \to \mathrm{Cl}_0(Y)$ with kernel T, i.e., $\mathrm{Cl}_0(Y) \simeq \mathbb{E}_8/T$ and the map $\overline{\mathrm{res}}_Z$ factors through $\overline{\mathrm{res}}_Y$. Moreover,

$$\mathrm{Cl}_0(Y)/\mathrm{torsion} \simeq \mathbb{E}_8/\widehat{T}.$$

The intersection pairing on Y and pull-back of $\mathbb{Q}$-divisors realizes $\mathbb{E}_8/\widehat{T}$ as a sublattice of the vector space $(T \otimes \mathbb{Q})^\perp \subseteq \mathbb{E}_8 \otimes \mathbb{Q}$ with the intersection pairing on Z.

Remark 3.17. Root lattices $T \subset \mathbb{E}_8$ were classified by Dynkin [24, Table 11]. The quotient group $\mathrm{Cl}_0(Y) \simeq \mathbb{E}_8/T$ was computed, e.g., in [57].

Corollary 3.18. *Let (C, Y) be a minimal elliptic pair with Du Val singularities and $\rho(Y) \geq 3$. Let R be the rank of the root lattice of (C, Y) and suppose $e(C, Y) < \infty$. Then $\overline{\mathrm{Eff}}(Y)$ is polyhedral if and only if there are roots $\beta_1, \ldots, \beta_{8-R} \in \mathbb{E}_8 \setminus \widehat{T}$, linearly independent modulo $\widehat{T}$ and such that $\overline{\mathrm{res}}(\beta_i) = 0$. In particular, if $R = 7$, then $\overline{\mathrm{Eff}}(Y)$ is polyhedral if and only if $\overline{\mathrm{res}}(\beta) = 0$ for some root $\beta \in \mathbb{E}_8 \setminus \widehat{T}$.*

Corollary 3.18 provides an effective criterion of polyhedrality for minimal elliptic pairs (C, Y) with Du Val singularities and $e(C, Y) < \infty$, while Corollary 3.12 shows that a minimal model (C, Y) of an elliptic pair (C, X) with $e(C, X) = \infty$ has Du Val singularities. These disjoint scenarios are reconciled in the following definition.

Definition 3.19. Let (C, X) be an elliptic pair with $e(C, X) = \infty$ defined over K, a finite extension of $\mathbb{Q}$. Let $R \subset K$ be the corresponding ring of algebraic integers. There exist an open subset $U \subset \operatorname{Spec} R$ and a pair of schemes $(\mathcal{C}, \mathcal{X})$ flat over U, which we call an *arithmetic elliptic pair of infinite order*, such that the following holds.

- Each geometric fiber (C, X) of $(\mathcal{C}, \mathcal{X})$ is an elliptic pair of order e_b which depends only on the corresponding point $b \in U$. We have $e_b < \infty$ for $b \neq 0$.
- The contraction morphism $X \to Y$ to the minimal model extends to the contraction of schemes $\mathcal{X} \to \mathcal{Y}$ flat over U.
- All geometric fibers (C, Y) of $(\mathcal{C}, \mathcal{Y})$ over U are minimal elliptic pairs with Du Val singularities and the same root lattice $T \subset \mathbb{E}_8$.

Let X, Y be geometric fibers over a place $b \in U, b \neq 0$. We call b a *polyhedral prime* if $\overline{\operatorname{Eff}}(Y)$ is polyhedral. If b is not polyhedral, then $\overline{\operatorname{Eff}}(X)$ is also not polyhedral.

Distribution of polyhedral primes is an intriguing question in arithmetic geometry that we will start to address for arithmetic toric elliptic pairs.

4. Lang–Trotter polygons and toric elliptic pairs

At the beginning, we work over an algebraically closed field k of any characteristic. We recall that a polygon $\Delta \subseteq \mathbb{R}^2$ is called a lattice polygon if its vertices are in $\mathbb{Z}^2$. If Δ is a lattice polygon, we will denote by $\operatorname{Vol}(\Delta)$ its *normalized volume*, i.e., twice its euclidean area (so that $\operatorname{Vol}(\Delta)$ is always a non-negative integer). We recall that, given any Laurent polynomial

$$f = \sum_{u \in \mathbb{Z}^2} \alpha_u x^u \in k[x_1^{\pm 1}, x_2^{\pm 2}], \tag{4.1}$$

where $x^u := x_1^{u_1} x_2^{u_2}$, we can construct a lattice polygon $\operatorname{NP}(f)$, called the *Newton polygon* of f, by taking the convex hull of the points $u \in \mathbb{Z}^2$ such that $\alpha_u \neq 0$.

A lattice polygon Δ defines a morphism

$$g_\Delta \colon \mathbb{G}_m^2 \to \mathbb{P}^{|\Delta \cap \mathbb{Z}^2| - 1}, \quad x \mapsto [x^u : u \in \Delta \cap \mathbb{Z}^2],$$

where $x = (x_1, x_2) \in (k^*)^2$. We will denote by $\mathbb{P}_\Delta$ the projective toric surface defined by Δ, i.e., the closure of the image of g_Δ, and by $e \in \mathbb{P}_\Delta$ the image $g_\Delta(1, 1)$. A hyperplane section is denoted by H_Δ. The linear system $|H_\Delta|$ is denoted by $\mathcal{L}_\Delta$, and given a positive integer m, we let $\mathcal{L}_\Delta(m)$ be the subsystem of $\mathcal{L}_\Delta$ consisting of the curves having multiplicity at least m at e. We will denote by $\pi_\Delta \colon X_\Delta \to \mathbb{P}_\Delta$ the blow-up at $e \in \mathbb{P}_\Delta$ and by E the exceptional divisor of π_Δ.

Notation 4.1. Given a triple (Δ, m, Γ), where Δ is a lattice polygon, m a positive integer and $\Gamma \in \mathcal{L}_\Delta(m)$, the curve Γ is given by a Laurent polynomial (4.1), and the curve $V(f) = \Gamma \cap \mathbb{G}_m^2$ will also be denoted by Γ. We denote by C the proper transform of Γ in X_Δ. In this section, we will investigate properties of pairs (C, X_Δ). We drop the subscript Δ from notation $\mathbb{P}_\Delta, X_\Delta$ if no confusion arises.

Proposition 4.2. *Consider a triple* (Δ, m, Γ) *as in Notation* 4.1. *Suppose* Γ *is irreducible and its Newton polygon is* Δ. *The following hold.*

(i) *The arithmetic genus of* C *is*

$$p_a(C) = \frac{1}{2}\big(\mathrm{Vol}(\Delta) - m^2 + m - |\partial\Delta \cap \mathbb{Z}^2|\big) + 1.$$

(ii) *Any edge* F *of* Δ *of lattice length* 1 *gives a smooth point* $p_F \in C$ *defined as the intersection of* C *with the toric boundary divisor corresponding to* F. *This point is defined over the field of definition of* Γ.

Proof. Since Δ is the Newton polygon of Γ, $\Gamma \subseteq \mathbb{P}$ does not contain any torus-invariant point of $\mathbb{P}$. In particular, Γ is contained in the smooth locus of $\mathbb{P}$, and hence C is contained in the smooth locus of X. By adjunction formula,

$$p_a(C) = \frac{1}{2}(C^2 + C \cdot K_X) + 1 = \frac{1}{2}(\mathrm{Vol}(\Delta) - m^2 + C \cdot K_X) + 1,$$

where the second equality follows from [21, Proposition 10.5.6]. But $C \cdot K_X = \Gamma \cdot K_{\mathbb{P}} + m$ so that, in order to prove (i), we only need to show that

$$\Gamma \cdot K_{\mathbb{P}} = -|\partial\Delta \cap \mathbb{Z}^2|. \tag{4.2}$$

Observe that $-K_{\mathbb{P}}$ is the sum of all the prime-invariant divisors of $\mathbb{P}$ and each prime-invariant divisor $D \subseteq \mathbb{P}$ corresponds to an edge F of Δ; see [21, Proposition 10.5.6]. Let us fix such an edge F. By a monomial change of variables, we can assume that F lies on the x_2 axis. The inclusion of algebras $k[x_1, x_2^{\pm 1}] \to k[x_1^{\pm 1}, x_2^{\pm 1}]$ gives the inclusion $\mathbb{G}_m^2 \to \mathbb{G}_m \times \mathbb{A}^1$, and $V(x_1) \subseteq \mathbb{G}_m \times \mathbb{A}^1$ is an affine open subset of D. Since Γ does not contain any torus-invariant points of $\mathbb{P}$, $\Gamma \cap D = \Gamma \cap V(x_1)$, and the latter intersection has equation

$$f|_F := \sum_{u \in F \cap \mathbb{Z}^2} \alpha_u x^u = f(0, x_2) = 0. \tag{4.3}$$

The degree of this Laurent polynomial is the lattice length of F so that (4.2) holds.

Moreover, if F has length 1, equation (4.3) has degree 1, which means that Γ intersects the prime divisor D transversally at a smooth point $p_F \in \Gamma$. Since D is defined over the base field, if Γ is defined over a subfield $k_0 \subset k$, then so is p_F. □

Definition 4.3. Let $\Delta \subseteq \mathbb{R}^2$ be a lattice polygon with at least four vertices (so that $\rho(X_\Delta) \geq 3$). We say that Δ is *good* if, for some integer m, the following hold:

(i) $\mathrm{Vol}(\Delta) = m^2$;

(ii) $|\partial\Delta \cap \mathbb{Z}^2| = m$;

(iii) $\dim \mathcal{L}_\Delta(m) = 0$, and the only curve $\Gamma \in \mathcal{L}_\Delta(m)$ is irreducible;

(iv) the Newton polygon of Γ coincides with Δ;

A good polygon is said to be

- a *Halphen polygon* if $\mathrm{res}(C) = \mathcal{O}_X(C)|_C$ is torsion;
- a *Lang–Trotter polygon* if $\mathrm{res}(C) = \mathcal{O}_X(C)|_C$ is not torsion.

Theorem 4.4. *If Δ is a good polygon, then (C, X_Δ) is an elliptic pair (we call it a* toric elliptic pair*), $e(C, X_\Delta) > 1$ and C is defined over the base field. If Δ is Lang–Trotter, then* $\operatorname{char} k = 0$*, $e(C, X_\Delta) = \infty$ and $\overline{\operatorname{Eff}}(X_\Delta)$ is not polyhedral.*

Proof. Let Δ be a good lattice polygon. The curve Γ is irreducible by Definition 4.3 (iii) and does not pass through the torus-invariant points of $\mathbb{P}_\Delta$ by Definition 4.3 (iv). It follows that C is contained in the smooth locus of X_Δ. Toric surface singularities, i.e., cyclic quotient singularities, are log terminal. By Definition 4.3 (iv) and [21, Proposition 10.5.6], $\Gamma^2 = \operatorname{Vol}(\Delta)$ so that Definition 4.3 (i) is equivalent to $C^2 = 0$. Finally, conditions (i) and (ii) of Definition 4.3, together with Proposition 4.2, imply that $p_a(C) = 1$. Thus, (C, X_Δ) is an elliptic pair. Observe that $\mathcal{O}_X(C)|_C = \operatorname{res}(C) \in \operatorname{Pic}^0(C)$ (see Definition 3.1) so that being Lang–Trotter is equivalent to $e(C, X_\Delta) = \infty$. Suppose this is the case. Since $\dim \mathcal{L}_\Delta(m) = 0$, the curve Γ, and thus also the curve C, and thus also the line bundle $\mathcal{O}_X(C)|_C$ are all defined over the base field. In characteristic p, the group $(\operatorname{Pic}^0 C)(\mathbb{F}_p)$ is torsion, which contradicts $e(C, X_\Delta) = \infty$. Thus, $\operatorname{char} k = 0$. Since Δ has at least 4 vertices, $\rho(X_\Delta) \geq 3$ and $\overline{\operatorname{Eff}}(X)$ is not polyhedral by Lemma 3.3. □

Database 8.1 contains all Lang–Trotter polygons with $m \leq 7$.

Example 4.5 (Polygon 111). This is the polygon Δ with 7 vertices

$$\begin{bmatrix} 6 & 5 & 1 & 8 & 0 & 0 & 3 \\ 1 & 4 & 3 & 2 & 6 & 7 & 0 \end{bmatrix}$$

which appears in Table 4 for $m = 7$ (where it corresponds to the blue matrix), and we will use it later in the proof of Theorem 1.2. We claim that Δ is Lang–Trotter.

First of all, $\operatorname{Vol}(\Delta) = 49$ and $|\partial\Delta \cap \mathbb{Z}| = 7$ (see [15, Computation 10.3]). By [15, Computation 10.4], $\mathcal{L}_\Delta(7)$ has dimension 0, and the unique curve $\Gamma \in \mathcal{L}_\Delta(7)$ has equation

$$\begin{aligned} &-u^8v^2 + 4u^7v^2 + 8u^6v^3 - 5u^6v^2 - 3u^6v - 5u^5v^4 - 50u^5v^3 + 21u^5v^2 \\ &\quad + 6u^5v + 40u^4v^4 + 85u^4v^3 - 55u^4v^2 - 6u^3v^5 - 85u^3v^4 - 40u^3v^3 \\ &\quad + 56u^3v^2 - 10u^3v + u^3 + 15u^2v^5 + 80u^2v^4 - 40u^2v^3 + u^2v^2 \\ &\quad + 3uv^6 - 30uv^5 + 5uv^4 + 2uv^3 - v^7 + 4v^6 = 0. \end{aligned}$$

The exponents of the red monomials are the vertices of Δ so that the Newton polygon of Γ is Δ. By [15, Computation 10.5], the curve Γ is geometrically irreducible and its strict transform $C \subseteq X_\Delta$ is a smooth elliptic curve. It has the minimal equation

$$y^2 + xy = x^3 - x^2 - 4x + 4$$

by [15, Computation 10.8]. This is the curve labeled 446.a1 in the LMFDB database [49]. Since $e(C, X) > 1$, $\operatorname{res}(C) \in \operatorname{Pic}^0(C)$ is not trivial. Since the Mordell–Weil group is $\mathbb{Z}^2$, $\operatorname{res}(C)$ is not torsion, and therefore Δ is Lang–Trotter.

Proposition 4.6. *There are no Lang–Trotter quadrilaterals Δ with $m = \operatorname{width}(\Delta)$.*

Proof. Assume Δ is a good quadrilateral, and let (C, X_Δ) be the corresponding elliptic pair. The divisor $K + C$ is linearly equivalent to an effective one whose components in the

support are in $C^\perp$. In particular, if $C^\perp$ contains the classes of two negative curves R_1, R_2, then, this space being two-dimensional, there are integers a_i, with $a_0 \neq 0$, such that

$$a_0 C + a_1 R_1 + a_2 R_2 \sim 0.$$

Taking restriction to C, one deduces that Δ is not Lang–Trotter. If $K + C \sim \alpha R + \beta C$, with $\alpha, \beta \in \mathbb{Q}_{>0}$ and $R \in C^\perp$ effective and not containing C in its support, then, after cleaning denominators and restricting to C, one again concludes that Δ is not Lang–Trotter. If $K + C \sim 0$, then, by considering multiplicities at e, we must have $m = 1$, which is impossible since $m = |\partial\Delta \cap \mathbb{Z}^2| \geq 4$. It remains to analyze the case $K + C \sim nR$, with $n > 0$ and R is an irreducible curve in $C^\perp$. Since we are assuming that $m = \text{width}(\Delta)$, the class of the one-parameter subgroup defined by one width direction lies in $C^\perp$ so that R must be this class, and in particular, its Newton polygon is a segment of lattice length 1. Moreover, by considering multiplicities at e, it must be that $n = m - 1$ so that Δ has m interior lattice points, lying on a line. If Δ were Lang–Trotter, Pick's formula would give $m^2 = 3m - 2$, which has integer solutions $m = 1, 2$, but this is impossible. □

Remark 4.7. We do not know examples of Lang–Trotter quadrilaterals. While in all the examples of Lang–Trotter polygons in Section 8 the condition $m = \text{width}(\Delta)$ is satisfied, there are examples in which m is smaller. For instance, one can check as in Example 4.5 that the pentagon with vertices

$$\begin{bmatrix} 0 & 12 & 11 & 9 & 8 \\ 0 & 4 & 7 & 12 & 12 \end{bmatrix}$$

is Lang–Trotter and it has $m = 11$ and $\text{width}(\Delta) = 12$. On the other hand, the quadrilateral with vertices

$$\begin{bmatrix} 0 & 12 & 14 & 9 \\ 10 & 4 & 5 & 15 \end{bmatrix}$$

satisfies the conditions $\text{Vol}(\Delta) = 169$, $|\partial\Delta \cap \mathbb{Z}^2| = 13$ and $\mathscr{L}_\Delta(13)$ contains only one curve Γ, irreducible. Moreover, $13 = m < \text{width}(\Delta) = 14$ so that Proposition 4.6 does not apply. However, in this case, Δ is not Lang–Trotter since $e(C, X_\Delta) = 6$.

Remark 4.8. If, in Definition 4.3, we substitute condition (ii) with $|\partial\Delta \cap \mathbb{Z}^2| < m$, the curve C will have arithmetic genus $p_a(C) > 1$ so that (C, X_Δ) is no longer an elliptic pair. However, if $\text{res}(C)$ is not torsion, we can still conclude that $\overline{\text{Eff}}(X_\Delta)$ is not polyhedral by Proposition 2.3. In the database [5], there are only two polygons satisfying $|\partial\Delta \cap \mathbb{Z}^2| < m$ together with (i), (iii) and (iv). Both polygons have volume 49 and 5 boundary points so that, by Proposition 4.2, the corresponding curve C has genus 2. In the first case, we verified that $2C$ moves [15, Computation 10.4], so $\text{res}(C)$ is torsion. The second polygon has the following vertices:

$$\begin{bmatrix} 0 & 5 & 7 & 3 & 1 \\ 0 & 2 & 3 & 8 & 3 \end{bmatrix},$$

and we claim that, in this case, $\text{res}(C)$ is not torsion. Indeed, the curve C is isomorphic to a hyperelliptic curve with equation

$$y^2 + (x^2 + x + 1)y = x^5 - 3x^4 + x^3 - x.$$

This is the curve labeled 1415.a.1415.1 in the LMFDB database [49], and the Mordell–Weil group of the corresponding jacobian surface is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By [15, Computation 10.4], $\dim|2C| = 0$, and we conclude that $\operatorname{res}(C)$ is non-torsion.

5. Arithmetic toric elliptic pairs of infinite order

Notation 5.1. Given a lattice polygon $\Delta \subseteq \mathbb{Z}^2$, let $\mathcal{P}$ be the projective toric scheme over $\operatorname{Spec}\mathbb{Z}$ given by the normal fan of Δ, with a relatively ample invertible sheaf $\mathcal{L}$ given by the polygon Δ. Let $\mathcal{X}$ be the blow-up of $\mathcal{P}$ along the identity section of the torus group scheme. Let $\mathcal{E} \simeq \mathbb{P}^1_{\mathbb{Z}}$ be the exceptional divisor. For any field k, we denote by $\mathbb{P}_k, L_k, X_k, E_k$ the corresponding base change (or simply by $\mathbb{P}, L, X, E$ if k is clear from the context). We will assume that Δ is a Lang–Trotter polygon, i.e., $(C_{\mathbb{C}}, X_{\mathbb{C}})$ is an elliptic pair of order $e(C_{\mathbb{C}}, X_{\mathbb{C}}) = \infty$. Then $(C_{\mathbb{C}}, X_{\mathbb{C}})$ is a geometric fiber of an arithmetic elliptic pair $(\mathcal{C}, \mathcal{X})$ of infinite order flat over an open subset $U \subset \operatorname{Spec}\mathbb{Z}$; see Definition 3.19. We assume that $C_{\mathbb{C}}$ is a *smooth elliptic curve*. A geometric fiber (C, X) of $(\mathcal{C}, \mathcal{X})$ over a prime $p \in U$ is an elliptic pair of finite order e_p. There is a morphism of schemes $\mathcal{X} \to \mathcal{Y}$ flat over U, inducing a morphism $X \to Y$ to the minimal model for any geometric fiber. Geometric fibers (C, Y) of $(\mathcal{C}, \mathcal{Y})$ over U are minimal elliptic pairs with Du Val singularities and the same root lattice T, which we call the *root lattice of* Δ. Recall that we call p a polyhedral prime of Δ if $\overline{\operatorname{Eff}}(Y)$ is a polyhedral cone in characteristic p. We are interested in the distribution of polyhedral and non-polyhedral primes. Recall that polyhedrality is governed by Corollary 3.18: p is polyhedral if and only if there are roots $\beta_1, \dots, \beta_{8-R} \in \mathbb{E}_8 \setminus \widehat{T}$, linearly independent modulo $\widehat{T}$ and such that $\overline{\operatorname{res}}(\beta_i) = 0$ in $C(\mathbb{F}_p)/\operatorname{res}(C)$. Here R is the rank of T.

We will need a lemma on arithmetic geometry of elliptic curves.

Lemma 5.2. *Let C be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication over $\bar{\mathbb{Q}}$. Fix points $x_0, \dots, x_r \in C(\mathbb{Q})$ of infinite order, and suppose that the subgroup $\langle x_1, \dots, x_r\rangle \subset C(\mathbb{Q})$ generated by $x_1, \dots, x_r$ is free abelian and does not contain a multiple of x_0. Then the reductions $\bar{x}_1, \dots, \bar{x}_r$ modulo p are not contained in the cyclic subgroup generated by the reduction $\bar{x}_0$ for a set of primes of positive density.*

Remark 5.3. Note that $x_1, \dots, x_r \in C(\mathbb{Q})$ are not assumed linearly independent.

Proof. For a fixed integer q, let $C[q] \subset C(\bar{\mathbb{Q}})$ be the set of q-torsion points so that $C[q] \simeq (\mathbb{Z}/q\mathbb{Z})^2$ as a group. Let K be the field $\mathbb{Q}(C[q])$. Since C does not have complex multiplication,

$$\operatorname{Gal}(K/\mathbb{Q}) \simeq \operatorname{GL}_2(\mathbb{Z}/q\mathbb{Z})$$

for almost all primes q by Serre's theorem [59]. Choose a basis $y_1, \dots, y_s$ of $\langle x_1, \dots, x_r\rangle$. Since x_0 has infinite order, $y_0 = x_0, y_1, \dots, y_s$ is a basis of the free abelian group $\langle x_0, \dots, x_r\rangle$. Choose points $y_0/q, \dots, y_s/q \in C(\bar{\mathbb{Q}})$. Let $K_{y_0,\dots,y_s}$ be a field extension of K generated by $y_0/q, \dots, y_s/q$ (any choice of quotients gives the same field). By Bashmakov's theorem [6], for almost all primes q, we have

$$\operatorname{Gal}(K_{y_0,\dots,y_s}/\mathbb{Q}) \simeq \operatorname{GL}_2(\mathbb{Z}/q\mathbb{Z}) \ltimes ((\mathbb{Z}/q\mathbb{Z})^2)^{s+1}.$$

For any $x \in C(\mathbb{Q})$, let $i(\bar{x})$ denote the index of the subgroup $\langle \bar{x} \rangle \subset C(\mathbb{F}_p)$. It suffices to prove that $i(\bar{x}_1), \dots, i(\bar{x}_r)$ are not divisible by q but $i(\bar{x}_0)$ is divisible by q for a set of primes p of positive density. By [46], $i(\bar{x})$ is divisible by q if and only if the Frobenius element (defined up to conjugacy)

$$\sigma_p = (\gamma_p, \tau_p) \in \mathrm{Gal}(K_x/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z}) \ltimes (\mathbb{Z}/q\mathbb{Z})^2$$

belongs to one of the following conjugacy classes: either $\gamma_p = 1$ or γ_p has eigenvalue 1 and $\tau_p \in \mathrm{Im}(\gamma_p - 1)$. We express

$$x_i = \sum_{j=1}^{s} a_{ij} y_j \quad \text{for } i = 1, \dots, r,\ a_{ij} \in \mathbb{Z}.$$

To apply the Chebotarev density theorem [66], it remains to note that the subset of tuples

$$(\gamma, \tau_0, \dots, \tau_s) \in \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z}) \ltimes ((\mathbb{Z}/q\mathbb{Z})^2)^{s+1}$$

such that γ has eigenvalue 1, $\tau_0 \in \mathrm{Im}(\gamma - 1)$ and $\sum_{j=1}^{s} a_{ij}\tau_j \notin \mathrm{Im}(\gamma - 1)$ for $i = 1, \dots, r$ is non-empty for $q \gg 0$. □

Remark 5.4. We were inspired by the following theorem of Tom Weston [68]. Suppose we are given an abelian variety A over a number field F such that $\mathrm{End}_F A$ is commutative, an element $x \in A(F)$ and a subgroup $\Sigma \subset A(F)$. If $\mathrm{red}_v x \in \mathrm{red}_v \Sigma$ for almost all places v of F, then $x \in \Sigma + A(F)_{\mathrm{tors}}$.

Here is another variation on the same theme.

Lemma 5.5. *Let C be an elliptic curve defined over $\mathbb{Q}$ with points $x, y \in C(\mathbb{Q})$ of infinite order such that $y = dx$ for a square-free integer d. Suppose there exists a prime p of good reduction and coprime to d such that the index of $\langle \bar{x} \rangle$ is coprime to d but the index of $\langle \bar{y} \rangle$ is divisible by d. Then $\bar{x}, 2\bar{x}, \dots, (d-1)\bar{x} \notin \langle \bar{y} \rangle$ for a set of primes of positive density.*

Proof. We need to prove positive density of primes such that the index of the subgroup $\langle \bar{y} \rangle$ in $\langle \bar{x} \rangle$ is equal to d. It is enough to prove positive density for the set of primes such that the index of $\langle \bar{x} \rangle$ in $C(\mathbb{F}_p)$ is coprime to d but the index of $\langle \bar{y} \rangle$ is divisible by d. Arguing as in the proof of Lemma 5.2, we can express this condition as a condition that the Frobenius element σ_p is contained in the union of certain conjugacy classes in the Galois group $\mathrm{Gal}\, L/\mathbb{Q}$, where L is obtained by adjoining the d-torsion $C[d]$ and the point x/d. To apply the Chebotarev density theorem, we need to know that this conjugacy class is non-empty. Arguing in reverse, it suffices to find a specific p such that the condition holds. □

Theorem 5.6. *Consider Lang–Trotter polygons from Table* 1 *(numbered as in Table* 4*). We list the root lattice T, the minimal equation of the elliptic curve C, its Mordell–Weil group $C(\mathbb{Q})$ and* $\mathrm{res}(C)$. *The set of non-polyhedral primes is infinite of positive density and includes primes under* 2000 *from Table* 2.

Proof. We first explain an outline of the argument and then proceed case by case. We compute the normal fan of Δ and the fan of the minimal resolution $\widetilde{\mathbb{P}}_\Delta$ of $\mathbb{P}_\Delta$ using [15, Compu-

N	T	C	MW	res(C)
19	A_7	$y^2+y=x^3-x^2-24x+54$	$\mathbb{Z}^2$	$-(1,5)$
24	$A_6\oplus A_1$	$y^2+y=x^3+x^2$	$\mathbb{Z}$	$6(0,0)$
111	$A_6\oplus A_1$	$y^2+xy=x^3-x^2-4x+4$	$\mathbb{Z}^2$	$(-1,-2)$
128	$A_3\oplus A_3$	$y^2+y=x^3+x^2-240x+1190$	$\mathbb{Z}^3$	$(15,34)$

Table 1

N	Primes
19	11, 41, 67, 173, 307, 317, 347, 467, 503, 523, 571, 593, 631, 677, 733, 797, 809, 811, 827, 907, 937, 1019, 1021, 1087, 1097, 1109, 1213, 1231, 1237, 1259, 1409, 1433, 1439, 1471, 1483, 1493, 1567, 1601, 1619, 1669, 1709, 1801, 1811, 1823, 1867, 1877, 1933, 1951, 1993
24	29, 59, 73, 137, 157, 163, 223, 257, 389, 421, 449, 461, 607, 641, 647, 673, 691, 743, 797, 929, 937, 983, 991, 1049, 1087, 1097, 1103, 1151, 1171, 1217, 1223, 1259, 1279, 1319, 1367, 1399, 1427, 1487, 1549, 1567, 1609, 1667, 1697, 1747, 1861, 1867, 1871, 1913
111	47, 71, 103, 197, 233, 239, 277, 313, 367, 379, 409, 503, 563, 599, 647, 677, 683, 691, 719, 727, 761, 829, 911, 997, 1103, 1123, 1151, 1171, 1187, 1231, 1283, 1327, 1481, 1493, 1709, 1723, 1861, 1907, 1997
128	13, 17, 23, 71, 101, 103, 109, 191, 233, 277, 281, 283, 311, 349, 379, 397, 419, 433, 439, 443, 449, 457, 479, 509, 547, 557, 571, 631, 647, 653, 691, 701, 727, 743, 811, 829, 877, 929, 953, 1021, 1031, 1033, 1097, 1123, 1129, 1151, 1187, 1213, 1237, 1277, 1297, 1423, 1459, 1471, 1483, 1499, 1531, 1549, 1559, 1583, 1621, 1637, 1699, 1753, 1783, 1879, 1889, 1907, 1979

Table 2

tation 10.3]. We use [15, Computation 10.6] to compute the Zariski decomposition of $K_X + C$, which by Theorem 3.10 gives curves $C_1, \dots, C_s$ contracted by the morphism to the minimal model Y, and the classes of proper transforms of these curves in $\widetilde{\mathbb{P}}_\Delta$. Whenever Δ has lattice width m in horizontal and vertical directions, these curves include 1-parameter subgroups $C_1 = (v = 1)$ and $C_2 = (u = 1)$. We use [15, Computation 10.7] to compute the root lattice T, $\mathrm{Cl}_0(Y)$, and the push-forward map to $\mathrm{Cl}_0(Y)$. Then [15, Computation 10.4] gives the equation of the unique member Γ of the linear system $\mathcal{L}_\Delta(m)$ and its Newton polygon, and [15, Computation 10.5] shows that the proper transform C of this curve in X is an elliptic curve. We use [15, Computation 10.8] to compute the minimal equation of C, intersection points of C with the toric boundary divisors, res(C) and the images of roots in $\mathbb{E}_8$. Reading off the Mordell–Weil group of C from the LMFDB database [49], we can deduce that Δ is Lang–Trotter. In the same [15, Computation 10.8], we apply Corollary 3.18 to test polyhedrality of specific primes from Table 2. Finally, we apply Lemma 5.2 or Lemma 5.5 to prove positive density of non-polyhedral primes. □

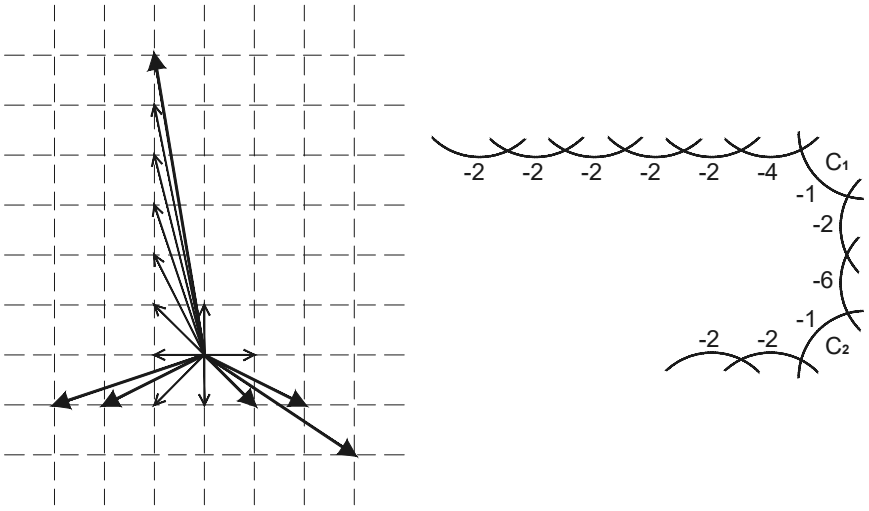


Figure 1. Polygon 19

Example 5.7 (Polygon 19). This polygon has vertices

$$\begin{bmatrix} 4 & 3 & 1 & 0 & 6 & 5 \\ 6 & 5 & 2 & 0 & 1 & 4 \end{bmatrix}. \tag{5.1}$$

The minimal resolution $\widetilde{\mathbb{P}}_\Delta$ has the fan from Figure 1, where bold arrows indicate the fan of $\mathbb{P}_\Delta$. Note that $\widetilde{\mathbb{P}}_\Delta$ has a toric map to $\mathbb{P}^1 \times \mathbb{P}^1$ and proper transforms of 1-parameter subgroups C_1, C_2 are preimages of rulings. Thus, they have self-intersection -1 after blowing up e. The minimal resolution of X contains the configuration of curves from the right of Figure 1 (toric boundary divisors and curves C_1, C_2). Only curves C_1 and C_2 contribute to the Zariski decomposition of $K + C$ and are contracted by the morphism $X \to Y$. Equivalently, the surface Y is obtained by contracting the chain of rational curves above. After blowing down (-1)-curves, this is equivalent to contracting a chain of seven (-2)-curves. Thus, Y has an A_7 singularity and Picard number 3. There are two conjugate classes of root sublattices of type A_7 in $\mathbb{E}_8$ (see [57, p. 85]). In our case, $\mathrm{Cl}_0(Y) \simeq \mathbb{Z}$ is torsion-free; thus the embedding is primitive. More precisely, we have $\mathrm{Cl}_0(Y) = \mathbb{E}_8/\mathbb{A}_7$, which corresponds to the $\mathbb{Z}$-grading of the Lie algebra $e_8 = \bigoplus_{\bar\beta \in \mathrm{Cl}_0(Y)} (e_8)_{\bar\beta}$ of the form

$$\begin{array}{ccccccc} \mathbb{C}^8 & \Lambda^2\mathbb{C}^8 & \Lambda^3\mathbb{C}^8 & \mathfrak{gl}_8 & \Lambda^3\mathbb{C}^8 & \Lambda^2\mathbb{C}^8 & \mathbb{C}^8 \\ 8 & 28 & 56 & 64 & 56 & 28 & 8. \end{array}$$

Let α be a generator of $\mathrm{Cl}_0(Y)$. The images of the roots of $\mathbb{E}_8$ are $\pm k\alpha$ for $k \le 3$. Thus, the non-polyhedrality condition is that $k\,\mathrm{res}(\alpha) \notin \langle \mathrm{res}(C) \rangle$ in char p for $k = 1, 2, 3$.

Next we compute $\mathrm{res}(\alpha)$ and $\mathrm{res}(C)$. The curve Γ has equation

$$\begin{aligned} f = {} & u^4v^6 + 6u^5v^4 - 2u^4v^5 - 14u^5v^3 - 17u^4v^4 - 4u^3v^5 + u^6v + 11u^5v^2 \\ & + 38u^4v^3 + 26u^3v^4 - 9u^5v - 27u^4v^2 - 34u^3v^3 + 22u^4v + 16u^3v^2 \\ & - 10u^2v^3 - 24u^3v + 10u^2v^2 + 15u^2v + 5uv^2 - 11uv + 1 = 0 \end{aligned}$$

and passes through e with multiplicity $m = 6$. When $p \neq 2, 3, 5$, C has Newton polygon (5.1) and is isomorphic to an elliptic curve with the minimal equation

$$y^2 + y = x^3 - x^2 - 24x + 54.$$

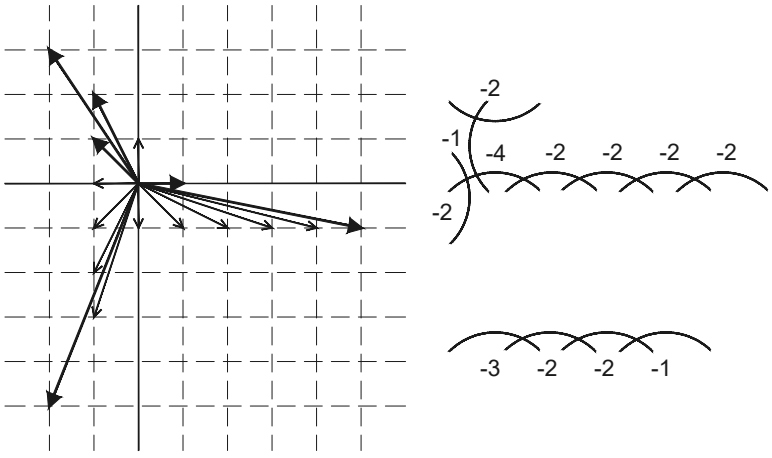


Figure 2. Polygon 24

The curve C is labeled 997.a1 in the LMFDB database [49], and its Mordell–Weil group $C(\mathbb{Q}) \simeq \mathbb{Z}^2$ is generated by $Q = (1, 5)$ and $P = (6, -10)$. We have

$$\operatorname{res}(C) = -Q, \quad \operatorname{res}(\alpha) = P - Q;$$

in particular, $\operatorname{res}(C)$ is not torsion in characteristic 0, and thus Δ is Lang–Trotter. Thus, $\overline{\operatorname{Eff}}(X)$ and $\overline{\operatorname{Eff}}(Y)$ are not polyhedral in characteristic 0.

In characteristic p, $k\bar{P}$ is not contained in the cyclic subgroup of $C(\mathbb{F}_p)$ generated by $\bar{Q}$ for $k = 1, 2, 3$ for all primes in Table 2. According to the LMFDB database [49], C has no complex multiplication. To prove positive density of non-polyhedral primes, we apply Lemma 5.2 to $x_0 = Q$ and $x_k = kP$ for $k = 1, 2, 3$.

Remark 5.8. Empirically, about 18 % of primes are not polyhedral for this polygon. It would be interesting to obtain heuristics for density of non-polyhedral primes.

Remark 5.9. Since C contains an irrational 2-torsion point, the Lang–Trotter conjecture [46] predicts that $\bar{Q}$ generates $C(\mathbb{F}_p)$ for a set of primes p of positive density. If true, the Lang–Trotter conjecture implies that $\overline{\operatorname{Eff}}(Y)$ is polyhedral in characteristic p for a set of primes of positive density. However, the Lang–Trotter conjecture is only known for curves with complex multiplication [39].

Example 5.10 (Polygon 24). This polygon has vertices

$$\begin{bmatrix} 0 & 2 & 5 & 6 & 1 & 0 \\ 0 & 1 & 3 & 4 & 6 & 1 \end{bmatrix}.$$

The minimal resolution $\widetilde{\mathbb{P}}_\Delta$ of $\mathbb{P}_\Delta$ has the fan from the left side of Figure 2, where bold arrows indicate the fan of $\mathbb{P}_\Delta$. As for the Polygon 19, the proper transforms of 1-parameter subgroups C_1, C_2 in X have self-intersection -1 and are the only curves contracted by the map to Y, which therefore can be obtained by contracting the configuration of rational curves from the right of Figure 2. It follows that Y has Picard number 3 and singularities A_1 and A_6. The

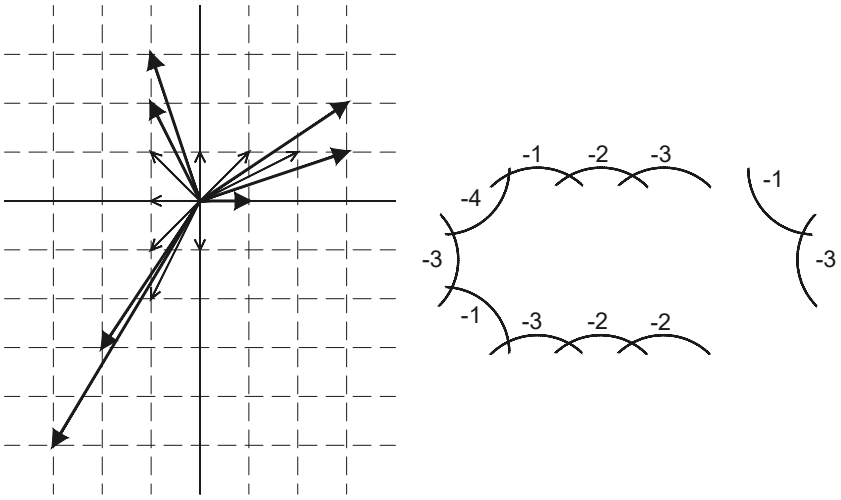


Figure 3. Polygon 111

curve Γ has a point of multiplicity 6 at e and equation

$$\begin{aligned} f = &-1 + 2v + 7uv - 3u^2v - 23uv^2 + 6u^2v^2 + 2u^3v^2 + 18uv^3 + 20u^2v^3 \\ &- 26u^3v^3 + 10u^4v^3 - 2u^5v^3 - 12uv^4 - 11u^2v^4 + 6u^3v^4 \\ &+ 5u^4v^4 - 4u^5v^4 + u^6v^4 + 5uv^5 + 3u^2v^5 - 2u^3v^5 - uv^6, \end{aligned}$$

which has a required Newton polygon when $p \neq 2, 3$. From the Dynkin classification, it follows that $\mathrm{Cl}_0(Y) \simeq \mathbb{Z}$. Let α be a generator. The images of roots of $\mathbb{E}_8$ are equal to $\pm k\alpha$ for $0 \leq k \leq 4$. Thus, the polyhedrality condition is $k\,\mathrm{res}(\alpha) \notin \langle \mathrm{res}(C) \rangle$ in char p for $k = 1, 2, 3, 4$. The minimal equation of the elliptic curve C is $y^2 + y = x^3 + x^2$. It is the curve 43.a1 from the LMFDB database [49] of elliptic curves. Its Mordell–Weil group is $\mathbb{Z}$ generated by $(0, 0)$. We have $\mathrm{res}(C) = Q = 6(0, 0)$ and $\mathrm{res}(\alpha) = P = -(0, 0)$. It follows that $\mathrm{res}(C)$ is not torsion, and thus Δ is Lang-Trotter and $\overline{\mathrm{Eff}}(X)$, $\overline{\mathrm{Eff}}(Y)$ are not polyhedral in characteristic 0. In characteristic p, $k\bar{P}$ is not contained in the cyclic subgroup of $C(\mathbb{F}_p)$ generated by $\bar{Q}$ for $k = 1, 2, 3, 4$ for all prime numbers in the table. Thus, these primes are not polyhedral. The positive density follows from Lemma 5.5 with $p = 223$, when the index of $\bar{P}$ is 1 and the index of $\bar{Q}$ is 6.

Example 5.11 (Polygon 111, discussed in Example 4.5, followed through in [15, Computations 10.3–10.8]). The corresponding curve has the required Newton polygon in all characteristics $p \neq 2, 3, 5$. The minimal resolution $\widetilde{\mathbb{P}}_\Delta$ has the fan from Figure 3, where bold arrows indicate the fan of $\mathbb{P}_\Delta$. Note that $\widetilde{\mathbb{P}}_\Delta$ has a toric map to $\mathbb{P}^1 \times \mathbb{P}^1$ and proper transforms of 1-parameter subgroups C_1, C_2 are preimages of rulings[8]; hence they have self-intersection -1 after blowing up e. The Zariski decomposition of $K + C$ is $2C_1 + C_2 + C_3$, where C_3 is a curve whose image in $\mathbb{P}_\Delta$ has multiplicity 3 at e. The Newton polygon of C_3 has vertices

$$\begin{bmatrix} 3 & 0 & 0 & 1 \\ 1 & 3 & 2 & 0 \end{bmatrix}$$

[8] The 1-parameter subgroups are in this case $\{u = 1\}$ and $\{u = v\}$.

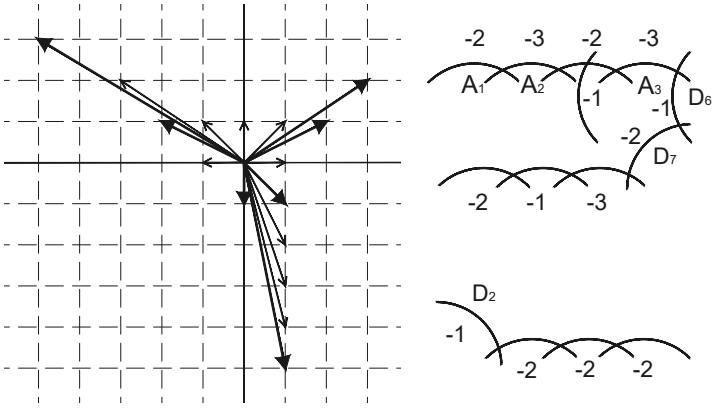


Figure 4. Polygon 128

and equation

$$u^3v - 3u^2v - uv^2 + 5uv - u + u^3 - 2u^2 = 0.$$

On X, the curve C_3 is disjoint from C_1 and C_2. The minimal resolution of X contains the configuration of curves from the right of Figure 3 (toric boundary divisors and curves C_1, C_2, C_3). The curves C_1, C_2, C_3 are contracted by the morphism $X \to Y$. Equivalently, the surface Y is obtained by contracting the chain of rational curves above. It follows that the root lattice is $\mathbb{A}_6 \oplus \mathbb{A}_1$ and the Picard number of Y is 3. From the Dynkin classification, we have

$$\mathrm{Cl}_0(Y) = \mathbb{E}_8/\mathbb{A}_6 \oplus \mathbb{A}_1 \simeq \mathbb{Z}.$$

Let α be a generator. The images of the roots of $\mathbb{E}_8$ are equal to $\pm k\alpha$ for $0 \le k \le 4$. Thus, in characteristic p, the non-polyhedrality condition is that $k\,\mathrm{res}(\alpha) \notin \langle \mathrm{res}(C) \rangle$ for $k = 1, 2, 3, 4$. To prove that this holds for a set of primes of positive density, we apply Lemma 5.2 to

$$x_i = \mathrm{res}(i\alpha), \quad x_0 = \mathrm{res}(C), \quad \text{for } i = 1, 2, 3, 4.$$

Let us check that the conditions in the lemma are satisfied. Using the minimal equation of the curve C (see Example 4.5) and [15, Computation 10.8], we find that $\mathrm{res}(\alpha) = P = (0, 2)$ and $\mathrm{res}(C) = Q = (-1, -2)$. The curve C (labeled 446.a1 in the LMFDB database [49]) has no complex multiplication and has Mordell–Weil group $\mathbb{Z} \times \mathbb{Z}$ generated by P and $-Q = (-1, 3)$. Hence, the points P and Q have infinite order, and no multiple of Q is contained in the subgroup generated by P.

Example 5.12 (Polygon 128). This is a polygon with vertices

$$\begin{bmatrix} 0 & 1 & 6 & 7 & 6 & 3 & 1 \\ 5 & 6 & 7 & 7 & 5 & 0 & 3 \end{bmatrix}.$$

The minimal resolution $\widetilde{\mathbb{P}}$ of $\mathbb{P}$ has the fan from the left side of Figure 4, where bold arrows indicate the fan of $\mathbb{P}$. The proper transforms of 1-parameter subgroups C_1, C_2 are the only curves contracted by the map $X \to Y$. Here Y can be obtained from $\mathrm{Bl}_e \widetilde{\mathbb{P}}$ by contracting a configuration of rational curves from the right of Figure 4, where we also indicate three boundary divisors, D_2, D_6 and D_7 (the only ones in Figure 4 that do not get contracted by

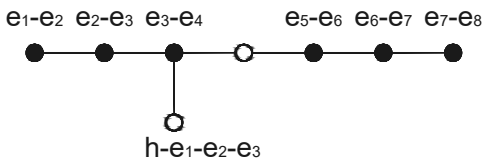


Figure 5. $\mathbb{A}_3 \oplus \mathbb{A}_3 \subset \mathbb{E}_8$

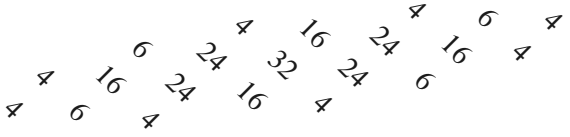
the map to Y). The root lattice is $\mathbb{A}_3 \oplus \mathbb{A}_3$; the Picard number of Y is 4. One of the $\mathbb{A}_3$'s is indicated with the chain A_1, A_2, A_3 of (-2)-curves (after contracting all (-1)-curves). By the Dynkin classification, $\mathbb{E}_8$ contains two lattices $\mathbb{A}_3 \oplus \mathbb{A}_3$, one primitive and one non-primitive. In our case, $\mathrm{Cl}_0(Y) \simeq \mathbb{Z}^2$ is torsion-free, and therefore we have the primitive one. Next we describe the images in $\mathrm{Cl}_0(Y)$ of roots in $\mathbb{E}_8$. In other words, we have a grading of the Lie algebra $\mathfrak{e}_8$ by the abelian group $\mathrm{Cl}_0(Y)$,

$$\mathfrak{e}_8 = \sum_{\bar\beta \in \mathrm{Cl}_0(Y)} (\mathfrak{e}_8)_{\bar\beta},$$

and we need to describe the subset of non-empty weight spaces $\mathcal{B} \subset \mathrm{Cl}_0(Y)$. A convenient interpretation of the lattice $\mathbb{E}_8$ is the lattice $K^\perp \subset \mathrm{Pic}(\mathrm{Bl}_8 \mathbb{P}^2)$ with standard basis $h, e_1, \dots, e_8$. The positive roots are

$$\begin{aligned}
&e_i - e_j \quad \text{for } i < j,\\
&h - e_i - e_j - e_k,\\
&2h - e_1 - \cdots - \widehat{e}_i - \cdots - \widehat{e}_j - \cdots - e_8,\\
&3h - e_1 - \cdots - 2e_i - \cdots - e_8.
\end{aligned}$$

The primitive sublattice $\mathbb{A}_3 \oplus \mathbb{A}_3$ is generated by simple roots marked black on Figure 5. It follows that the $\mathbb{Z}^2$ grading on $\mathbb{E}_8$ is obtained by pairing with fundamental weights h and $e_5 + e_6 + e_7 + e_8$ that correspond to white vertices of the Dynkin diagram. The $\mathbb{Z}^2$ grading of $\mathfrak{e}_8$ has the following non-empty weight spaces (in coordinates given by pairing with h and $e_5 + e_6 + e_7 + e_8$, respectively), where we also indicate dimensions:



It follows that the subset $\mathcal{B} \subset \mathrm{Cl}_0(Y)$ is given by the $\pm$ columns of the matrix

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 3 & 3 \\ 0 & 1 & 1 & 2 & 3 & 2 & 3 & 4 & 4 & 5 \end{pmatrix} \tag{5.2}$$

in the basis u, v, where u and v are the images of the simple roots $h - e_1 - e_2 - e_3$ and $e_4 - e_5$, respectively. Next we compute vectors u and v in $\mathrm{Cl}_0(Y)$. By inspecting Figure 4, one can prove that, in the minimal resolution Z of Y, $h - e_1 - e_2 - e_3$ corresponds to the (-2)-class $D_2 - D_7$ and $e_4 - e_5$ to $D_2 - D_6 - A_1 - A_2 - A_3$, which has push-forward $D_2 - D_6$ on X. Next we compute $\mathrm{res}(C)$, $\mathrm{res}(u)$ and $\mathrm{res}(v)$.

The curve Γ has a point of multiplicity 7 at e, and its Newton polygon is Δ for any prime $p \neq 2, 3, 7, 11$. The minimal equation of the elliptic curve C is

$$y^2 + y = x^3 + x^2 - 240x + 1190,$$

which is the curve 29157b1 from the LMFDB database of elliptic curves. It has Mordell–Weil group $\mathbb{Z}^3$ generated by $P = (12, 13)$, $R = (-6, 49)$ and $Q = (-15, 40)$. We have

$$\begin{aligned} \operatorname{res}(C) &= (15, -35) = P - Q - R, \\ \operatorname{res}(u) &= (120, 1309) = Q - R, \\ \operatorname{res}(v) &= (-6, 49) = R. \end{aligned}$$

We see that $\operatorname{res}(C)$ is not torsion in characteristic 0, and thus $\overline{\operatorname{Eff}}(Y)$ is not polyhedral. In characteristic p, the condition of polyhedrality is that there exist two linearly independent column vectors of the matrix (5.2) which, when dotted with the row vector $(\operatorname{res}(u), \operatorname{res}(v))$, are contained in the cyclic subgroup of $C(\mathbb{F}_p)$ generated by $\operatorname{res}(C)$. This gives the list of non-polyhedral primes in the table. To prove the positive density, we apply Lemma 5.2 (with $r = 10$).

Remark 5.13. In Example 5.12, by Lemma 5.2, we get positive density not only for the set of non-polyhedral primes but also for the set of primes p such that the Halphen pencil $|e_p C|$ on Y has only irreducible fibers. For example, $\operatorname{res}(C)$ has order 2 in characteristic 23 and none of the elements of $\mathcal{B}$, when restricted to C, are contained in the cyclic subgroup of $C(\mathbb{F}_{23})$ generated by $\operatorname{res}(C)$. It follows that $|2C|$ on Y is a Halphen pencil with only irreducible fibers. This property is stronger than non-polyhedrality: in characteristic 13, $\operatorname{res}(C)$ has torsion 5 and $\operatorname{res}(u + v)$ is contained in the cyclic subgroup generated by $\operatorname{res}(C)$ but no other linearly independent vector in $\mathcal{B}$ is. It follows that $\overline{\operatorname{Eff}}(Y)$ is not polyhedral, but the Halphen pencil $|5C|$ on Y contains a reducible fiber with two components and no other reducible fibers.

Remark 5.14. There is an infinite sequence of Lang–Trotter pentagons Δ_k with vertices

$$\begin{bmatrix} 0 & 2k & 2k+4 & 2k+2 & 2k+1 \\ 0 & 0 & 1 & 2k+4 & 2k+3 \end{bmatrix}$$

for $k \geq 1$. Indeed, consider an elliptic curve $C \subseteq \mathbb{P}^2$ with the Weierstrass equation

$$y^2 = x(x^2 + ax + b),$$

where $a = -(12k^2 + 24k + 11)$ and $b = 4(k+1)^2(3k+2)(3k+4)$. Let

$$x_0 = 2(k+1)(3k+2), \quad x_1 = 2(k+1)(3k+4),$$

and consider the points $d_1 = [0 : 1 : 0]$, $d_2 = [x_0 : -x_0 : 1]$ on C in homogeneous coordinates.

Let $\phi = (f, g) : C \dashrightarrow \mathbb{G}_m \times \mathbb{G}_m$ be the map given by the rational functions

$$f(x, y) = \frac{x^{k+1}(x - y)}{x - x_0}, \quad g(x, y) = \frac{(x - x_0)(x^{k+1} - x^k y - 2x_0^{k+1})}{x^k(x - y)}.$$

Then ϕ induces a morphism $C \to \mathbb{P}_{\Delta_k}$, birational onto its image Γ with equation

$$\begin{aligned} &(uv + 2x_0^{k+2})(u - 2x_0^{k+1})^{m-1} - 2u^{k+1}(v + x_0)^{k+2}(u - 2x_0^{k+1})^{k+2} \\ &\quad - u^{m-3}(v + x_0)^{m-1}\big(uv + u(x_0 - x_1) + 2x_1 x_0^{k+1}\big) = 0, \end{aligned}$$

where $m = 2k + 4$. Let $q \in \mathbb{P}_{\Delta_k}$ be a point with coordinates $u = 2x_0^{k+1}$, $v = -x_0$. An explicit calculation shows that the induced map $C \to \operatorname{Bl}_q \mathbb{P}_{\Delta_k}$ is an embedding and the linear system

$\mathcal{L}_{\Delta_k}(m)$ has C as an irreducible member. Furthermore, $(C, \mathrm{Bl}_q \mathbb{P}_{\Delta_k})$ is a toric elliptic pair, and we have

$$\mathcal{O}(C)|_C \cong \mathcal{O}_C(2d_1 - 2d_2).$$

We claim that this line bundle is not torsion. We choose d_1 as the identity element of the Mordell–Weil group $C(\mathbb{Q})$. By Mazur's theorem [51], it suffices to prove that $nd_2 \neq 0$ for $1 \leq n \leq 12$. We check this in [15, Computation 10.9]. Hence, Δ_k is a Lang–Trotter polygon. One can also view the curves C_k as fibers of an elliptic fibration $\mathcal{C} \to \mathbb{P}^1$ (where the field of rational functions on $\mathbb{P}^1$ is the field of rational functions in variable k). By [15, Computation 10.9], this is a rational elliptic fibration of Kodaira type $I_4 I_2^{\oplus 3} I_1^{\oplus 2}$. One can compute the Neron–Tate height of the section of this fibration corresponding to d_2 to conclude that it is not torsion in the Mordell–Weil group of the elliptic fibration. This shows that d_2 is not torsion in a fiber C_k for almost all k by Silverman's specialization theorem [60]. Mazur's theorem gives a more precise statement for every k as above.

Remark 5.15. For pentagons of Remark 5.14, one can show that all primes are polyhedral. But we also found an infinite sequence of Lang–Trotter heptagons Δ_k such that, for all but finitely many k, the set of non-polyhedral primes of Δ_k has positive density. The vertices are

$$\begin{bmatrix} 0 & 1 & 2k+4 & 2k+4 & 2k+3 & 2k+2 & k \\ 0 & 0 & 2 & 2k & 2k+4 & 2k+4 & k+1 \end{bmatrix}.$$

To see this, we use the same strategy as above. The elliptic curve C is given by the equation $y^2 + exy + by = x^3 + ax^2$, where

$$e = -(4k+2), \quad a = -\frac{k(2k+1)}{k+2}, \quad b = \frac{4k(k+1)^4(2k+1)}{(k+2)^2(k-1)^2}.$$

Let us consider the points $d_1 = [0:1:0]$, $d_2 = [0:0:1]$ and $d_3 = [x_0 : y_0 : 1]$, where

$$x_0 = \frac{2k(k+1)^2}{(k-1)(k+2)}, \quad y_0 = -\frac{2k(k+1)^2(5k+3)}{(k-1)^2(k+2)}.$$

There is a map $\phi = (f, g) : C \dashrightarrow \mathbb{G}_m \times \mathbb{G}_m$ given by rational functions

$$f(x,y) = \frac{x^{k+1}y}{\alpha(x - x_0 - 1) + \beta(x + a)}, \quad g(x,y) = \frac{x+a}{x^k(x-x_0)y},$$

where

$$\alpha = x_0 + a = \frac{k(5k+3)}{(k-1)(k+2)}, \quad \beta = x_0^{k+1} y_0.$$

The image $\Gamma = \phi(C)$ has equation

$$\begin{aligned} &\big((\alpha\beta)uv + (\alpha x_0)u - a\big)h_2(u,v)^{m-1} - h_1(u,v)^{m-2}h_3(u,v)^2v^2 \\ &\quad + \big(\beta(b + ex_0)uv + (ex_0\alpha)u - b\big)h_1(u,v)^k h_2(u,v)^{k+2}h_3(u,v)v = 0, \end{aligned}$$

where

$$\begin{aligned} h_1(u,v) &= (x_0\beta)uv + (x_0\alpha)u, \\ h_2(u,v) &= (\beta)uv - 1, \\ h_3(u,v) &= (x_0\alpha)u + x_0. \end{aligned}$$

A calculation shows that $(C, \mathrm{Bl}_e\, \mathbb{P}_{\Delta_k})$ is a toric elliptic pair, and [15, Computation 10.9] (based on Mazur's theorem) shows that $\mathcal{O}(C)|_C = \mathcal{O}(2d_3 - d_2 - d_1)$ is not torsion for $k \geq 2$. The point $p \in C$ such that $\mathcal{O}(2d_3 - d_2 - d_1) = \mathcal{O}(p - d_1)$ is given by

$$x = \frac{4k(k+1)^2(2k+1)}{(k-1)^2(k+2)}, \quad y = \frac{4k^2(k+1)^2(2k+1)(3k+1)}{(k-1)^2(k-2)}.$$

In particular, Δ_k is a Lang–Trotter polygon for $k \geq 3$. The root lattice is

$$T = \mathbb{A}_3 \oplus \mathbb{A}_2 \oplus \mathbb{A}_1^2$$

and has rank 7. In order to prove that $\overline{\mathrm{res}}(\gamma) \neq 0$ for any root $\gamma \in \mathbb{E}_8 \setminus \widehat{T}$ for a set of primes p of positive density, first of all, we compute the possible restrictions of these roots, showing that these are $i(d_1 - d_3)$ for $i \in \{\pm 1, \pm 2, \pm 3\}$. Then we apply Lemma 5.2 to

$$x_i = \mathrm{res}(\gamma) = \mathcal{O}_C(id_1 - id_3), \quad x_0 = \mathrm{res}\Big(\frac{1}{2}C\Big) = \mathcal{O}(d_1 + d_2 - 2d_3)$$

for $i = 1, 2, 3$. We check that the conditions in the lemma are satisfied. The curve C does not have complex multiplication because its j-invariant is not an integer (see [61, Theorem II.6.1]). We already proved that x_0 is not torsion in $\mathrm{Pic}^0(C)$. It remains to prove that $\mathcal{O}_C(d_1 - d_3)$ and $\mathcal{O}_C(d_2 - d_3)$ are linearly independent for almost all k. By [15, Computation 10.9], the elliptic fibration with fibers C_k is a K3 elliptic fibration of Kodaira type $I_4^{\oplus 3} IV^{\oplus 3}$. Using Silverman's specialization theorem [62, Appendix C, Theorem 20.3], it suffices to prove linear independence for a specific k, which we check by a computer calculation.

Remark 5.16. Consider a smooth lattice polygon Δ with $m = 30$ and with vertices

$$\begin{bmatrix} 3 & 6 & 8 & 23 & 27 & 30 & 30 & 29 & 21 & 18 & 16 & 13 & 12 & 11 & 9 & 7 & 1 & 0 & 0 \\ 0 & 1 & 2 & 12 & 15 & 18 & 19 & 20 & 26 & 28 & 29 & 30 & 30 & 29 & 25 & 20 & 4 & 1 & 0 \end{bmatrix}.$$

A computation shows that Δ is a good polygon. Observe that $X = \mathrm{Bl}\, \mathbb{P}_\Delta$ is smooth of Picard rank 18. The linear system $|K_X + C|$ contains eight disjoint (-1)-curves, three of which come from the one-parameter subgroups defined by the width directions of Δ, while the remaining ones come from curves of multiplicity 2, 3, 5, 5, 11 at $(1, 1)$. Contracting them gives a smooth minimal elliptic pair (C, Y).

The toric boundary divisors D_2, D_5 and D_{12} of X are (-1)-curves disjoint from the curves in $|K_X + C|$. As a consequence, each of the three divisors remains a (-1)-curve in Y. The linear system $|C + D_2 + D_5 + D_{12}|$ on X defines a rational map which factors through Y, and there, it is defined by $|-K_Y + D_2 + D_5 + D_{12}|$. The image of Y via this linear system is a smooth cubic surface of $\mathbb{P}^3$ whose equation can be calculated by determining the unique cubic relation between the elements of a basis of $H^0(X, C + D_2 + D_5 + D_{12})$. This allows us to find an equation of C as an explicit hyperplane section of the cubic surface and convert it to the Weierstrass equation which is

$$y^2 = x^3 + x^2 - 7860946299156x + 8357826814810214400.$$

The curve C has Mordell–Weil group of rank 9. Ordering counterclockwise the facets of Δ, starting from the facet $(0, 0)$–$(3, 0)$, the indices of facets of integer length one are

$$\{2, 3, 5, 7, 8, 10, 11, 12, 13, 14, 16, 18, 19\}.$$

For each such index, one can compute the point $d_i \in C(\mathbb{Q})$ cut out by the corresponding toric invariant divisor D_i. This information is then used to compute the images of the 240 roots and to determine the non-polyhedral primes of X. Using [15, Computation 10.10], we found 85 non-polyhedral primes in the interval $[1, 2000]$, or 28 %.

6. Halphen polygons

We consider a variant of the notion of arithmetic elliptic pairs as follows.

Definition 6.1. Let (C, X) be an elliptic pair with $e := e(C, X) < \infty$, defined over a finite extension K of $\mathbb{Q}$. Let $R \subset K$ be its ring of algebraic integers. There exist a dense open subset $U \subset \operatorname{Spec} R$ and a pair of schemes $(\mathcal{C}, \mathcal{X})$ flat over U, which we call an *arithmetic elliptic pair of finite order* $e < \infty$, such that the following holds.

- Each geometric fiber (C, X) of $(\mathcal{C}, \mathcal{X})$ is an elliptic pair of order e.
- The contraction morphism $X \to Y$ to the minimal elliptic pair extends to the contraction of schemes $\mathcal{X} \to \mathcal{Y}$ flat over U.

We call $(\mathcal{C}, \mathcal{Y})$ the *associated minimal arithmetic elliptic pair*. Let X, Y be geometric fibers over a place $b \in U$, $b \neq 0$. As before, we call b a *polyhedral prime* if $\overline{\operatorname{Eff}}(Y)$ is polyhedral. If b is not polyhedral, then $\overline{\operatorname{Eff}}(X)$ is also not polyhedral.

Since, over $\mathbb{C}$, the subgroup $\langle \operatorname{res}(C) \rangle \subset \operatorname{Pic}^0(C)$ is finite of order $e < \infty$, the order of the elliptic pair given by each geometric fiber of $(\mathcal{C}, \mathcal{X})$ stays constant on an open set in $\operatorname{Spec} R$, as it is defined by the condition that $i \operatorname{res}(C) \neq 0$ for $i = 1, \ldots, e-1$.

Proposition 6.2. *Let $(\mathcal{C}, \mathcal{X})$ be an arithmetic elliptic pair of finite order $e < \infty$ over some open set $U \subset \operatorname{Spec} R$. Let $(\mathcal{C}, \mathcal{Y})$ be the associated minimal arithmetic elliptic pair. Assume that*

- *the geometric fiber $Y_{\mathbb{C}}$ of $\mathcal{Y}$ has Du Val singularities,*
- *the cone $\overline{\operatorname{Eff}}(Y_{\mathbb{C}})$ is not polyhedral.*

Then all but finitely many primes $b \in U$ are non-polyhedral.

Proof. If the minimal elliptic pair $(C_{\mathbb{C}}, Y_{\mathbb{C}})$ has Du Val singularities, by replacing U with a smaller open set, we may assume that all geometric fibers (C, Y) of $(\mathcal{C}, \mathcal{Y})$ over U are minimal elliptic pairs of order e, with Du Val singularities and the same root lattice $T \subseteq \mathbb{E}_8$. Indeed, there exist a scheme $\mathcal{Z}$, smooth over (a possibly smaller) U, and a morphism $\pi \colon \mathcal{Z} \to \mathcal{Y}$, flat over U, such that, on geometric generic fibers Z and Y, of $\mathcal{Z}$ and $\mathcal{Y}$, this gives the minimal resolution $Z \to Y$. We may assume that the exceptional locus of π has geometric irreducible components $\mathcal{E}_1, \ldots, \mathcal{E}_r \subset \mathcal{Z}$, smooth over U, such that the geometric generic fibers $E_1, \ldots, E_r$ are the exceptional (-2)-curves of the resolution $Z \to Y$. As each $\mathcal{E}_i$ is flat over U, intersection numbers $E_i \cdot E_j$ of the geometric generic fibers do not depend on $b \in U$. In particular, the root lattice is the same for all $b \in U$, and all geometric fibers of $\mathcal{Y} \to U$ have Du Val singularities.

Consider now any geometric fiber (C, Y) of $(\mathcal{C}, \mathcal{Y})$, and let $Z \to Y$ be its minimal resolution. Recall that, by Lemma 3.14 and Corollary 3.18, the cone $\overline{\mathrm{Eff}}(Y)$ is polyhedral if and only if $\overline{\mathrm{Eff}}(Z)$ is polyhedral, or equivalently, the kernel of the map

$$\overline{\mathrm{res}}\colon \mathrm{Cl}_0(X) := C^\perp/\langle K\rangle \to \mathrm{Pic}^0(C)/\langle \mathrm{res}(K)\rangle$$

contains 8 linearly independent roots of $\mathbb{E}_8 = \mathrm{Cl}_0(Z)$. By assumption, the subgroup $\langle \mathrm{res}(C)\rangle$ of $\mathrm{Pic}^0(C)$ is finite of fixed order $e < \infty$ for all geometric fibers. By Theorem 3.8, $C \sim n(-K)$ for some integer n. It follows that the subgroup $\langle \mathrm{res}(K)\rangle$ of $\mathrm{Pic}^0(C)$ is finite of order at most e for every geometric fiber. Since there are finitely many roots in $\mathbb{E}_8$, it follows that, by eventually discarding a finite set of places $b \in U$, $b \neq 0$, the maximum number of linearly independent roots of $\mathbb{E}_8 = \mathrm{Cl}_0(Z)$ contained in $\mathrm{Ker}(\overline{\mathrm{res}})$ is constant. This finishes the proof. □

As in Notation 5.1, we may consider arithmetic *toric* elliptic pairs of finite order. Consider a lattice polygon $\Delta \subseteq \mathbb{Z}^2$, and let $\mathcal{P}$ be the projective toric scheme over $\mathrm{Spec}\,\mathbb{Z}$ given by the normal fan of Δ. Let $\mathcal{X}$ be the blow-up of $\mathcal{P}$ along the identity section of the torus group scheme. We will assume that Δ is a good but not Lang–Trotter polygon, a so-called Halphen polygon (Definition 4.3). Then $(C_{\mathbb{C}}, X_{\mathbb{C}})$ is an elliptic pair of finite order $e := e(C_{\mathbb{C}}, X_{\mathbb{C}}) < \infty$ and $(\mathcal{C}, \mathcal{X})$ an arithmetic elliptic pair of finite order, flat over an open subset $U \subset \mathrm{Spec}\,\mathbb{Z}$ (Definition 6.1). Let $\mathcal{X} \to \mathcal{Y}$ be the morphism inducing the map to the minimal model on each geometric fiber.

Definition 6.3. A polygon $\Delta \subseteq \mathbb{Z}^2$ such that the associated toric arithmetic elliptic pair $(\mathcal{C}, \mathcal{X})$ satisfies the conditions in Proposition 6.2 will be called a *Halphen*$^+$ polygon.

Theorem 6.4. *Let Δ be a Halphen$^+$ polygon. Then $\overline{\mathrm{Eff}}(X_\Delta)$ is not polyhedral in characteristic 0 and characteristic p, for all but finitely many primes p.*

Proof. This is an immediate consequence of Proposition 6.2. □

Theorem 6.5. *Consider the polygon Δ with vertices*

$$\begin{bmatrix} 0 & 1 & 6 & 8 & 7 & 5 & 1 \\ 0 & 0 & 1 & 2 & 5 & 8 & 2 \end{bmatrix}.$$

Then Δ is a Halphen$^+$ polygon and $\overline{\mathrm{Eff}}(X_\Delta)$ is not polyhedral in characteristic 0, and in characteristic p for all primes $p \neq 2, 3, 5, 7, 11, 19, 71$.

We will use this polygon later in the proof of Theorem 1.2.

Proof. We have

$$\mathrm{Vol}(\Delta) = 64 \quad \text{and} \quad |\partial\Delta \cap \mathbb{Z}| = 8$$

(see [15, Computation 10.3]). By [15, Computation 10.4], in characteristic 0, the linear system $\mathcal{L}_\Delta(8)$ has dimension 0 and the unique curve $\Gamma \in \mathcal{L}_\Delta(8)$ has equation

$$\begin{aligned} &4u^8v^2 + 24u^7v^5 - 61u^7v^4 + 58u^7v^3 - 53u^7v^2 + 10u^6v^6 - 126u^6v^5 + 244u^6v^4 \\ &\quad - 186u^6v^3 + 150u^6v^2 + 20u^6v - u^5v^8 + 8u^5v^7 - 48u^5v^6 + 230u^5v^5 \end{aligned}$$

$$
\begin{aligned}
&-286u^5v^4+120u^5v^3-159u^5v^2-88u^5v+10u^4v^6-66u^4v^5-56u^4v^4\\
&+144u^4v^3+94u^4v^2+154u^4v-6u^3v^5+89u^3v^4-26u^3v^3-135u^3v^2\\
&-146u^3v-54u^2v^3+52u^2v^2+114u^2v+19uv^2-46uv-5u+4=0.
\end{aligned}
$$

The exponents of the red monomials are the vertices of Δ so that the Newton polygon of Γ is Δ in characteristic 0 and characteristic $p \neq 2, 3, 5, 19$. By [15, Computations 10.5 and 10.8], the curve Γ is irreducible and its strict transform $C \subseteq X_\Delta$ is a smooth elliptic curve in characteristic 0, with minimal equation

$$y^2+xy+y=x^3+x^2-520x+4745. \tag{6.1}$$

This is the curve labeled 2130.j4 in the LMFDB database [49]. The Mordell–Weil group is $\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. By [15, Computation 10.4], in characteristic 0, the linear system $\mathscr{L}_{k\Delta}(8k)$ has dimension 0 if $k=2,3$ and dimension 1 if $k=4$. It follows that $\mathrm{res}(C)\in \mathrm{Pic}^0(C)(\mathbb{Q})$ is torsion, of order $e=4$. Hence, Δ is a Halphen polygon.

The theorem now follows from [15, Computation 10.11], and we give the details. By [15, Computation 10.11], the curve C is irreducible and smooth in characteristic 0 or characteristic $p \neq 2, 3, 5, 7, 11, 19, 71$. Unless otherwise specified, we will from now on assume we are in one of these situations.

The normal fan of Δ has rays $v_1=(0,1)$, $v_2=(-1,5)$, $v_3=(-1,2)$, $v_4=(-3,-1)$, $v_5=(-3,-2)$, $v_6=(3,-2)$, $v_7=(2,-1)$. We denote $D_1,\dots,D_7$ the corresponding torus invariant divisors in $\mathbb{P}_\Delta$ and, abusing notations, also their pull-backs to X_Δ. The divisors $D_1,\dots,D_5,E$ form a basis for $\mathrm{Cl}(X)$, and we have

$$
\begin{aligned}
D_6 &\sim 2D_1+9D_2+3D_3-5D_4-7D_5,\\
D_7 &\sim -3D_1-13D_2-4D_3+9D_4+12D_5,\\
K_X &\sim 3D_2-5D_4-6D_5+E,\\
C &\sim 2D_1+10D_2+7D_3+21D_4+24D_5-8E.
\end{aligned}
$$

Note that the class of C is independent of the characteristic if the Newton polygon stays the same. Since Δ has lattice width 8 in the horizontal and vertical direction, the proper transforms C_1 and C_2 on X_Δ of the 1-parameter subgroups $(u=1)$ and $(v=1)$ are among the curves that must be contracted by the morphism $X\to Y$ to the associated minimal elliptic pair. Using [15, Computation 10.6], we find that $K_X+C=2C_1+2C_2+C_3$, with curves C_i with classes

$$
\begin{aligned}
C_1 &\sim D_2+D_3+3D_4+3D_5-E,\\
C_2 &\sim D_1+5D_2+2D_3-E,\\
C_3 &\sim D_2+D_3+10D_4+12D_5-3E.
\end{aligned}
$$

Then [15, Computation 10.6] gives that the curve C_3 has equation

$$u^3v-u^2v^3+3u^2v^2-5u^2v+uv+2u-1=0,$$

and so its Newton polygon has vertices $(0,0)$, $(1,0)$, $(3,1)$, $(2,3)$ in all characteristics other than 2. This polygon has no non-trivial Minkowski decompositions, so the curve C_3 is irreducible in the situations we consider. The curves C_1, C_2 are irreducible in all characteristics, as they are proper transforms of 1-parameter subgroups.

From the intersection numbers $D_i \cdot D_j$ on $\mathbb{P}_\Delta$ (or using [15, Computation 10.7]), we find that $C_1^2 = -\frac{1}{4}$, $C_2^2 = -\frac{3}{14}$, $C_3^2 = -\frac{8}{3}$ and $C_i \cdot C_j = 0$ for all $i \neq j$. Since the intersection matrix $(C_i \cdot C_j)_{i,j}$ is negative definite, it follows that the Zariski decomposition of $K_X + C = N + P$ has the positive part $P \sim 0$. By Theorem 3.10, the minimal model Y has Du Val singularities. Denote $\overline{D}$ the class of a divisor D in $\mathrm{Cl}(Y)$. Setting the classes of C_1, C_2, C_3 to zero, we obtain that $\mathrm{Cl}(Y)$ is freely generated by $\overline{D}_2$, $\overline{D}_3$ and $\overline{D}_5$ and

$$\overline{D}_1 \sim 2\overline{D}_2 + 5\overline{D}_3 - 6\overline{D}_5, \qquad \overline{D}_4 \sim 2\overline{D}_2 + 2\overline{D}_3 - 3\overline{D}_5,$$
$$\overline{E} \sim 7\overline{D}_2 + 7\overline{D}_3 - 6\overline{D}_5, \quad C_Y = \overline{C} \sim 3\overline{D}_3 - 3\overline{D}_5.$$

We consider $\alpha := \overline{D}_2 - \overline{D}_5$, $\beta := \overline{D}_3 - \overline{D}_5$ in $\mathrm{Cl}(Y)$. Then $C_Y^\perp = \mathbb{Z}\{\alpha, \beta\}$ and

$$\mathrm{Cl}_0(Y) = \mathbb{Z}\{\alpha, \beta\}/\mathbb{Z}\{3\beta\} = \mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

By [15, Computation 10.7] or using a minimal resolution of $\mathbb{P}_\Delta$, it follows that the root lattice is $T = \mathbb{A}_2^3 \oplus \mathbb{A}_1$ and $\rho(Y) = 3$. By Corollary 3.18, the cone $\overline{\mathrm{Eff}}(Y)$ is non-polyhedral if and only if $\overline{\mathrm{res}}(\gamma) \neq 0$ for all roots $\gamma \in \mathbb{E}_8 \setminus \widehat{T}$. There is a unique way to embed $\mathbb{A}_2^3 \oplus \mathbb{A}_1$ in $\mathbb{E}_8$ (see [57, p. 86]). There are generators a, b of $\mathbb{E}_8/T$ with $\mathrm{ord}(a) = \infty$, $\mathrm{ord}(b) = 3$ such that the images of the roots of $\mathbb{E}_8$ in $\mathrm{Cl}_0(Y) = \mathbb{E}_8/T$ are

$$\begin{aligned} &\pm ka && (k = 0, 1, 2, 3, 12),\\ &\pm (ka - b) && (k = 2, 3, 4, 5, 6),\\ &\pm (ka - 2b) && (k = 6, 7, 8, 9, 10). \end{aligned}$$

The sets of generators $\{a, b\}$, $\{\alpha, \beta\}$ of $\mathrm{Cl}_0(Y)$ are related by $b \in \{\pm\beta\}$, $a \in \{\pm\alpha, \pm\alpha \pm \beta\}$. The images of the roots of $\mathbb{E}_8$ in $\mathrm{Cl}_0(Y)$, in terms of α, β, are

$$\pm k\alpha \ (k = 0, 1, 2, 3, 4, 5, 7, 8, 10, 12), \quad \pm k\alpha \pm \beta \ (k = 1, \dots, 10).$$

We denote d_i the effective divisor on C such that $\mathcal{O}(d_i) = \mathcal{O}(D_i)_{|C}$. For every $i \neq 6$, we have $d_i \in C(\mathbb{Q})$. It follows that, in $\mathrm{Pic}^0(C)$, we have

$$\mathrm{res}(\alpha) = \mathcal{O}_C(d_2 - d_5), \quad \mathrm{res}(\beta) = \mathcal{O}_C(d_3 - d_5).$$

Using [15, Computation 10.8] and (6.1), the points $d_2, d_3, d_5 \in \mathrm{Pic}^0(C)(\mathbb{Q})$ are $d_2 = (9, 25)$, $d_3 = (23, 63)$, $d_5 = (53, -387)$. Using Magma, we compute

$$\mathrm{res}(\alpha) = (-7, 93), \quad \mathrm{res}(\beta) = (13, 13), \quad \mathrm{res}(2\beta) = (-27, 13), \quad \mathrm{res}(3\beta) = (13, -27),$$

and the order of $\mathrm{res}(\beta)$ in $\mathrm{Pic}^0(C)(\mathbb{Q})$ is 4. As C has class 3β in $\mathrm{Cl}_0(Y)$, it follows that $\overline{\mathrm{Eff}}(Y)$ is non-polyhedral (in some characteristic) if and only if none of

$$\mathrm{res}(k\alpha) \ (k = 1, 2, 3, 4, 5, 7, 8, 10, 12), \quad \mathrm{res}(k\alpha \pm \beta) \ (k = 1, \dots, 10)$$

belong to $\{0, \mathrm{res}(\beta), \mathrm{res}(2\beta), \mathrm{res}(3\beta)\}$ of $\mathrm{Pic}^0(C)$, which is the subgroup generated by $\mathrm{res}(\beta)$ (from the above formulas, one can see that the order of $\mathrm{res}(\beta)$ is 4 in characteristic 0 or $p \neq 2, 5$). Clearly, this is equivalent to $\mathrm{res}(k\beta)$ for all $k = 7, 8, 9, 10, 12$, not belonging to this subgroup. This is done within [15, Computation 10.11], which gives that this is the case for all primes $p \neq 2, 3, 5, 7, 11, 19, 71$. □

7. On the effective cone of $\overline{M}_{0,n}$

For any toric variety X, we denote by $\mathrm{Bl}_e X$ the blow-up of X at the identity element of the torus. Let $\overline{\mathrm{LM}}_n$ be the Losev–Manin moduli space [50], which is also a toric variety. Its curious feature, noticed in [18], is that $\overline{\mathrm{LM}}_n$ is "universal" among all projective toric varieties. Moreover, $\mathrm{Bl}_e \overline{\mathrm{LM}}_n$ is universal among $\mathrm{Bl}_e X$. Here we make this philosophical statement very precise.

Theorem 7.1. *Let X be a projective toric variety. For any n large enough (see the proof for an effective estimate), there exist a sequence of projective toric varieties*

$$\overline{\mathrm{LM}}_n = X_1, \dots, X_s = X$$

and rational maps induced by toric rational maps

$$\mathrm{Bl}_e \overline{\mathrm{LM}}_n = \mathrm{Bl}_e X_1 \dashrightarrow \mathrm{Bl}_e X_2 \dashrightarrow \cdots \dashrightarrow \mathrm{Bl}_e X_s = \mathrm{Bl}_e X.$$

Every map

$$\mathrm{Bl}_e X_k \dashrightarrow \mathrm{Bl}_e X_{k+1}$$

decomposes as a small $\mathbb{Q}$-factorial modification (SQM) $\mathrm{Bl}_e X_k \dashrightarrow Z_k$ and a surjective morphism $Z_k \to \mathrm{Bl}_e X_{k+1}$. If the cone $\overline{\mathrm{Eff}}(\mathrm{Bl}_e \overline{\mathrm{LM}}_n)$ is (rational) polyhedral, then $\overline{\mathrm{Eff}}(\mathrm{Bl}_e X)$ is also (rational) polyhedral.

Remark 7.2. In [18], we used an analogous implication that if $\overline{\mathrm{Eff}}(\mathrm{Bl}_e \overline{\mathrm{LM}}_n)$ is a Mori Dream Space, then $\overline{\mathrm{Eff}}(\mathrm{Bl}_e X)$ is a Mori Dream Space.

The second statement in Theorem 7.1 follows from the first, using Lemma 2.2 and the fact that if $Z \dashrightarrow Z'$ is an SQM, then we can identify $\mathrm{Num}^1(Z)_{\mathbb{R}} = \mathrm{Num}^1(Z')_{\mathbb{R}}$ and $\overline{\mathrm{Eff}}(Z) = \overline{\mathrm{Eff}}(Z')$. The proof of the first statement in Theorem 7.1 is based on the main technical result of [18], which we give here in a slightly reformulated form.

Lemma 7.3 ([18, Proposition 3.1]). *Let $\pi\colon N \to N'$ be a surjective map of lattices with kernel of rank 1 spanned by a vector $v_0 \in N$. Let Γ be a finite set of rays in $N_{\mathbb{R}}$ spanned by elements of N, which includes both rays $\pm R_0$ spanned by $\pm v_0$. Let $\mathcal{F}' \subset N'_{\mathbb{R}}$ be a complete simplicial fan with rays given by $\pi(\Gamma)$ (ignore two zero vectors in the image). Suppose that the corresponding toric variety X' is projective (notice that it is also $\mathbb{Q}$-factorial because $\mathcal{F}'$ is simplicial). Then there exists a complete simplicial fan $\mathcal{F} \subset N_{\mathbb{R}}$ with rays given by Γ and such that the corresponding toric variety X is projective. Moreover, there exists a rational map $\mathrm{Bl}_e X \dashrightarrow \mathrm{Bl}_e X'$ which decomposes into an SQM $\mathrm{Bl}_e X \dashrightarrow Z$ and a surjective morphism $Z \to \mathrm{Bl}_e X'$ (of relative dimension 1).*

Corollary 7.4. *Let $\pi\colon N \to N'$ be a surjective map of lattices with kernel spanned by vectors $v_1, \dots, v_s \in N$. Let Γ be a finite set of rays in $N_{\mathbb{R}}$ spanned by elements of N, which includes the rays $\pm R_i$ spanned by $\pm v_i$ for $i = 1, \dots, s$. Let $\mathcal{F}' \subset N'_{\mathbb{R}}$ be a complete simplicial fan with rays given by $\pi(\Gamma)$ (ignore zero vectors in the image). Suppose that the corresponding toric variety X' is projective (notice that it is also $\mathbb{Q}$-factorial because $\mathcal{F}'$ is simplicial). Then there exists a complete simplicial fan $\mathcal{F} \subset N_{\mathbb{R}}$ with rays $\Gamma \cup \{\pm R_1\} \cup \cdots \cup \{\pm R_s\}$ and such that the corresponding toric variety X is projective. Moreover, there exists a sequence of toric*

varieties $X = X_1, \dots, X_s = X'$ *and rational maps induced by toric rational maps*

$$\mathrm{Bl}_e X = \mathrm{Bl}_e X_1 \dashrightarrow \mathrm{Bl}_e X_2 \dashrightarrow \cdots \dashrightarrow \mathrm{Bl}_e X_s = \mathrm{Bl}_e X'$$

such that every map $\mathrm{Bl}_e X_k \dashrightarrow \mathrm{Bl}_e X_{k+1}$ *decomposes as an SQM* $\mathrm{Bl}_e X_k \dashrightarrow Z_k$ *and a surjective morphism* $Z_k \to \mathrm{Bl}_e X_{k+1}$.

Proof. We argue by induction on s; the case $s = 1$ is Lemma 7.3. We can assume v_1 is a primitive vector. Let $N'' = N/\langle v_1 \rangle$. We have a factorization of π into $\pi_0 \colon N \to N''$ and $\pi' \colon N'' \to N'$. Let Γ'' be the image under π_0 of Γ (ignore zero vectors in the image). Then we are in the situation of Lemma 7.3. For the map π', we use the step of the induction. □

Proof of Theorem 7.1. We follow the same strategy as [18].

Applying $\mathbb{Q}$-factorialization, we can assume that X is a $\mathbb{Q}$-factorial toric projective variety of dimension r. The toric data of $\overline{\mathrm{LM}}_n$ is as follows. Fix general vectors

$$e_1, \dots, e_{n-2} \in \mathbb{R}^{n-3} \quad \text{such that} \quad e_1 + \cdots + e_{n-2} = 0.$$

The lattice N is generated by $e_1, \dots, e_{n-2}$. The rays of the fan of $\overline{\mathrm{LM}}_n$ are spanned by the primitive lattice vectors $\sum_{i \in I} e_i$ for each subset I of $S := \{1, \dots, n-2\}$ with $1 \le |I| \le n-3$. Notice that rays of this fan come in opposite pairs. We are not going to need cones of higher dimension of this fan. We partition $S = S_1 \sqcup \cdots \sqcup S_{r+1}$ into subsets of equal size $m \ge 3$ (so that $n = m(r+1) + 2$). We also fix some indices $n_i \in S_i$ for $i = 1, \dots, r+1$. Let $N'' \subset N$ be a sublattice spanned by the following vectors:

$$e_{n_i} + e_j \quad \text{for } j \in S_i \setminus \{n_i\},\ i = 1, \dots, r+1.$$

Let $N' = N/N''$ be the quotient group and let π be the projection map. Then we have the following:

(1) N' is a lattice;

(2) N' is spanned by the vectors $\pi(e_{n_i})$ for $i = 1, \dots, r+1$;

(3) $\pi(e_{n_1}) + \cdots + \pi(e_{n_{r+1}}) = 0$ is the only linear relation between these vectors.

Then the toric surface with lattice N' and rays spanned by $\pi(e_{n_i})$ for $i = 1, \dots, r+1$ is a projective space $\mathbb{P}^r$. Choose a basis $f_1, \dots, f_r$ for the lattice N' so that

$$\pi(e_{n_1}) = -f_1, \dots, \pi(e_{n_r}) = -f_r.$$

Fix one of the indices $1, \dots, r+1$ (we start with $r+1$), and choose $e = \sum_{i \in I} e_i$ such that $n_1, \dots, n_r \notin I$, $|I \cap S_1| = k_1, \dots, |I \cap S_r| = k_r$ and $|I| = k_1 + \cdots + k_r$. Then

$$\pi(e) = k_1 f_1 + \cdots + k_r f_r \quad \text{and} \quad \pi(e + e_{n_{r+1}}) = (k_1 + 1) f_1 + \cdots + (k_r + 1) f_r.$$

It follows that images of the rays of $\overline{\mathrm{LM}}_n$ contain all points with non-zero coordinates bounded by m. Repeating this for all $r+1$ octants shows that the images of the rays of $\overline{\mathrm{LM}}_n$ span all lattice points within the region illustrated in Figure 6 for $r = 2$, which contains all rays of X if m is large enough. To be precise, for each $i \in \{1, \dots, r\}$, in the octant spanned by

$$f_1, \dots, f_{i-1}, f_{i+1}, \dots, f_{r+1} \quad (f_{r+1} := \pi(-e_{n_{r+1}}) = -f_1 - \cdots - f_r),$$

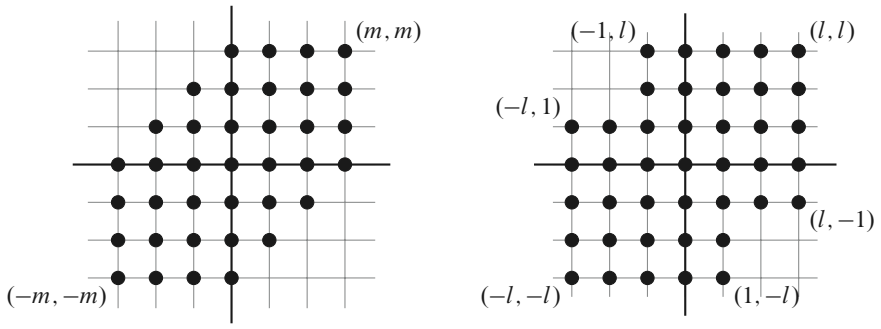


Figure 6

the region containing all the images of rays of $\overline{\mathrm{LM}}_n$ is determined by

$$mf_1, \ldots, mf_{i-1}, mf_{i+1}, \ldots, mf_{r+1} = -mf_1 - \cdots - mf_r.$$

It remains to notice (see [56], [18, Proposition 3.1]) that there exists a $\mathbb{Q}$-factorial projective toric variety W with rays given by the images of the rays of $\overline{\mathrm{LM}}_n$ and that the toric birational rational map $W \dashrightarrow X$ is a composition of birational toric morphisms and toric SQMs. Thus, we are done by Corollary 7.4. □

Corollary 7.5. *Let Y be a projective toric surface with lattice $\mathbb{Z}^2$ and with fan spanned by rays contained in the polygon with vertices*

$$(\pm m, \pm m),\ (0, \pm m),\ (\pm m, 0)$$

for some $m \geq 3$ (see Figure 6 on the left for $m = 3$). If $\overline{\mathrm{Eff}}(\mathrm{Bl}_e\, Y)$ is not (rational) polyhedral, then $\overline{\mathrm{Eff}}(\overline{M}_{0,3m+2})$ is not (rational) polyhedral.

Proof. We argue by contradiction. If $\overline{\mathrm{Eff}}(\overline{M}_{0,n})$ is (rational) polyhedral, then the pseudo-effective cone $\overline{\mathrm{Eff}}(\mathrm{Bl}_e\, \overline{\mathrm{LM}}_n)$ is also (rational) polyhedral by Lemma 2.2 and [18, Theorem 1.1]. In this case, $\overline{\mathrm{Eff}}(\mathrm{Bl}_e\, Y)$ is (rational) polyhedral by Theorem 7.1 (and effective estimates in its proof). □

Variations in the choice of projections used in the proof of Theorem 7.1 can lead to further variations and improvements, such as the following.

Corollary 7.6. *Let Y be a projective toric surface with lattice $\mathbb{Z}^2$ and with fan spanned by rays contained in the polygon with vertices*

$$(\pm l, \pm l),\ (\pm 1, \mp l),\ (\pm 1, \mp 1),\ (\pm l, \mp 1) \tag{7.1}$$

for some $l \geq 2$ (see Figure 6 on the right for $l = 3$). If $\overline{\mathrm{Eff}}(\mathrm{Bl}_e\, Y)$ is not (rational) polyhedral, then $\overline{\mathrm{Eff}}(\overline{M}_{0,2l+5})$ is not (rational) polyhedral.

Proof. Similarly, we argue by contradiction. If $\overline{\mathrm{Eff}}(\overline{M}_{0,n})$ is (rational) polyhedral, the pseudo-effective cone $\overline{\mathrm{Eff}}(\mathrm{Bl}_e\, \overline{\mathrm{LM}}_n)$ is also (rational) polyhedral by Lemma 2.2 and [18, Theorem 1.1]. In this case, $\overline{\mathrm{Eff}}(\mathrm{Bl}_e\, Y)$ is (rational) polyhedral using the same idea as in the proof of

Theorem 7.1. It suffices to prove that one can project in such a way that the images of the rays of the fan of $\overline{\mathrm{LM}}_n$ are contained in the polygon given by (7.1).

The rays of the fan of $\overline{\mathrm{LM}}_n$ are spanned by the primitive lattice vectors $\sum_{i\in I} e_i$ for each subset I of $S := \{1, \dots, n-2\}$ with $1 \le |I| \le n-3$. We partition

$$S = S_1 \sqcup S_2 \sqcup S_3, \quad |S_1| = |S_2| = l+1, \quad |S_3| = 1.$$

We fix some indices $n_i \in S_i$ for $i = 1, 2$ and let $S_3 = \{n_3\}$. Let $N'' \subset N$ be a sublattice spanned by the following vectors:

$$e_{n_i} + e_j \quad \text{for } j \in S_i \setminus \{n_i\},\ i = 1, 2.$$

Let $N' = N/N''$ be the quotient group and let π be the projection map. Then we have the following:

(1) N' is a lattice;

(2) N' is spanned by the vectors $\pi(e_{n_i})$ for $i = 1, 2, 3$;

(3) the only linear relation between these vectors is

$$-(l-1)\pi(e_{n_1}) + -(l-1)\pi(e_{n_2}) + \pi(e_{n_3}) = 0.$$

Choose a basis f_1, f_2 for the lattice N' given by $\pi(e_{n_1}) = f_1, \pi(e_{n_2}) = f_2$. Then

$$\pi(e_{n_3}) = (l-1)f_1 + (l-1)f_2.$$

We calculate the images $\pi(\sum_{i\in I} e_i)$ of the rays of the fan of $\overline{\mathrm{LM}}_n$. Consider the case when $n_1, n_2, n_3 \notin I$. If $|I \cap S_1| = i$, $|I \cap S_2| = j$, then clearly the images of such rays are given by $-if_1 - jf_2$ and all values $0 \le i, j \le l$ are possible. This gives a square P which, in the given basis, has coordinates

$$(-l, -l),\ (-l, 0),\ (0, -l),\ (0, 0).$$

If $n_1 \in I$, $n_2, n_3 \notin I$, the images $\pi(\sum_{i\in I} e_i)$ will be contained in the translation of P by $f_1 = (1, 0)$. Similarly, if $n_3 \notin I$, then $\pi(\sum_{i\in I} e_i)$ is contained in the union of P with its translates by $f_1 = (1, 0)$, $f_2 = (0, 1)$ and $f_1 + f_2 = (1, 1)$, i.e., the square Q with sides $(-l, -l)$, $(-l, 1)$, $(1, -l)$, $(1, 1)$. Finally, if $n_3 \in I$, then $\pi(\sum_{i\in I} e_i)$ will be contained in the translate Q' of Q by $f_3 = (l-1, l-1)$. Hence, all images of rays are contained in the sum of Q and Q', i.e., the polygon given in (7.1). □

Corollary 7.7. *Let Y be a projective toric surface with lattice $\mathbb{Z}^2$ and with fan spanned by rays contained in the polygon with vertices (Figure 7)*

$$(\pm 3, \pm 1),\ (\pm 3, \pm 5),\ (\pm 2, \pm 6),\ (\pm 1, \pm 6),\ (\pm 1, \mp 3).$$

If $\overline{\mathrm{Eff}}(\mathrm{Bl}_e\, Y)$ is not (rational) polyhedral, then $\overline{\mathrm{Eff}}(\overline{M}_{0,10})$ is not (rational) polyhedral.

Proof. It suffices to prove that $\overline{\mathrm{Eff}}(\mathrm{Bl}_e\, \overline{\mathrm{LM}}_{10})$ is not (rational) polyhedral. We do a variation of the method in the proof of Theorem 7.1, projecting the lattice $\mathbb{Z}^7$ of the Losev–Manin space $\overline{\mathrm{LM}}_{10}$ (spanned by $\{e_1, \dots, e_8\}$ and subject to the relation $\sum_{i=1}^{8} e_i = 0$) from the fol-

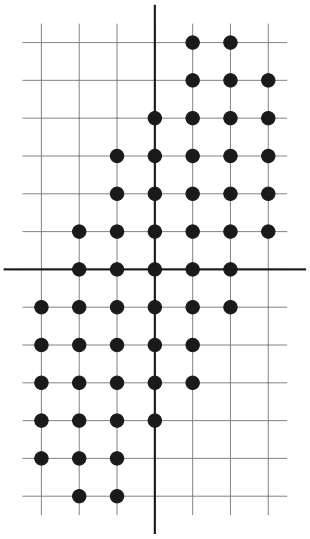


Figure 7

lowing rays of the fan of $\overline{\mathrm{LM}}_{10}$: $e_1+e_2+e_4+e_6$, $e_1+e_2+e_5+e_7$, $e_1+e_4+e_6+e_7$, e_5+e_6 and $e_1+e_5+e_8$. These vectors generate the kernel of the map $\pi\colon \mathbb{Z}^7 \to \mathbb{Z}^2$ given by

$$\begin{pmatrix} 1 & 0 & 1 & -2 & -1 & 1 & 0 \\ 0 & 1 & -1 & -3 & -2 & 2 & 1 \end{pmatrix}.$$

We conclude observing that the images of the rays of $\overline{\mathrm{LM}}_{10}$ via f are the points of Figure 7. □

Proof of Theorem 1.2. If the characteristic is 0 or any prime $p \neq 2,3,5,7,11,19,71$, one can use the Halphen$^+$ polygon Δ from Theorem 6.5. Indeed, after the shear transformation $(x,y) \mapsto (x, x-y)$, the rays of the normal fan of Δ are

$$(0,-1),\ (-1,-6),\ (-1,-3),\ (-3,-2),\ (-3,-1),\ (3,5),\ (2,3),$$

which are among the points of Figure 7 so that we can apply Corollary 7.7.

In order to conclude, we are going to produce, for any $p \in \{2,3,5,7,11,19,71\}$, a suitable good lattice polygon Δ, whose normal fan has rays among the points of Figure 7. In particular, since the characteristic is positive, Δ is Halphen, with $e := e(C, X_\Delta) < \infty$. The pencil $|eC|$ defines a fibration $\pi\colon X \to \mathbb{P}^1$. Let us denote by $S_i := \pi^{-1}(q_i)$ for $i = 1,\dots,\lambda$ the reducible fibers and by μ_i the number of irreducible components of S_i. It is not hard to see that any such irreducible component is defined over the field $\mathbb{F}_p$, so we only have to check a finite family. We then conclude showing that

$$\sum_{i=1}^{\lambda}(\mu_i - 1) < \mathrm{Rank}(\mathrm{Pic}(X)) - 2 = \#\,\mathrm{Vertices}(\Delta) - 3,$$

which, by Remark 2.4, implies that the effective cone is not polyhedral.

In [15, Computation 10.12], we analyze in detail the case $p = 2$, while in Table 3, we list, for any $p \in \{2,3,5,7,11,19,71\}$, the polygon Δ, the corresponding $e(C, X_\Delta)$ and the cardinality of the reducible fibers. □

p	Vertices	$e(C, X_\Delta)$	$[\mu_1, \dots, \mu_\lambda]$
2	$\begin{bmatrix} 0 & 6 & 9 & 10 & 9 & 3 & 1 \\ 0 & 2 & 4 & 5 & 6 & 10 & 4 \end{bmatrix}$	1	[2, 3]
3	$\begin{bmatrix} 0 & 5 & 7 & 12 & 13 & 14 & 12 & 6 & 2 \\ 0 & 2 & 3 & 6 & 8 & 11 & 12 & 14 & 6 \end{bmatrix}$	2	[2, 5]
5	$\begin{bmatrix} 0 & 2 & 12 & 13 & 13 & 12 & 11 & 9 & 4 \\ 0 & 1 & 7 & 8 & 9 & 11 & 12 & 13 & 12 \end{bmatrix}$	2	[3, 4]
7	$\begin{bmatrix} 0 & 1 & 4 & 8 & 10 & 4 & 3 & 1 \\ 0 & 0 & 1 & 4 & 7 & 10 & 8 & 3 \end{bmatrix}$	2	[2, 4]
11	$\begin{bmatrix} 0 & 12 & 13 & 13 & 12 & 11 & 9 & 7 & 1 \\ 0 & 4 & 8 & 9 & 11 & 12 & 13 & 12 & 2 \end{bmatrix}$	2	[3, 3]
19	$\begin{bmatrix} 0 & 2 & 8 & 9 & 3 & 2 \\ 0 & 1 & 5 & 6 & 10 & 8 \end{bmatrix}$	2	[2, 2]
71	$\begin{bmatrix} 0 & 3 & 8 & 12 & 13 & 12 & 11 & 5 & 4 \\ 0 & 1 & 4 & 7 & 8 & 10 & 11 & 13 & 12 \end{bmatrix}$	3	[2, 2, 4]

Table 3

Remark 7.8. By [15, Computation 10.3], the rays of the normal fan of Polygon 111 are among the points in Figure 7. By Example 4.5, Δ is a Lang–Trotter polygon so that, by Theorem 4.4, we have another proof that $\overline{\mathrm{Eff}}(\overline{M}_{0,10})$ is not polyhedral in characteristic 0. Moreover, in Database 8.2, we collect many more Lang–Trotter polygons such that their normal fans (sometimes after a shear transformation) fit into Figure 7. So one can also use Lang–Trotter polygons to show that $\overline{\mathrm{Eff}}(\overline{M}_{0,10})$ is not polyhedral in characteristic $p < 2000$.

8. Databases

Database 8.1. We give in Table 4 the list of all Lang–Trotter polygons with $m \leq 7$. It is obtained as follows. We consider all lattice polygons of volume up to 49 (modulo equivalence) appearing in the database [5]. We impose the conditions of Definition 4.3 using our Magma package. In particular, [15, Computation 10.3] gives (i) and (ii), while [15, Computations 10.4 and 10.5] give (iii), (iv) and the equation of Γ. This leaves 184 lattice polygons, and in all the cases, the curve C turns out to be smooth by [15, Computation 10.5]. Furthermore, for all but one polygon in this list, we also have that the point e is an ordinary multiple point of Γ. The exceptional case is Polygon 23, in which case the tangent cone to the curve Γ at e contains a double line. The curve C turns out to be tangent to the exceptional divisor at the corresponding point so that, also in this case, C is smooth. Therefore, for any polygon in the list, C is a smooth genus 1 curve, and moreover, since Δ has at least 4 vertices and $|\partial\Delta \cap \mathbb{Z}^2| = m \leq 7$, we also have that at least one edge F of Δ has lattice length 1. By Proposition 4.2, we conclude that the curve C has a rational point p_F that we can chose as the origin so that, in what follows, we can treat C as an elliptic curve. This fact allows to check the last condition of the definition of a Lang–Trotter polygon, i.e., that $\mathcal{O}_X(C)|_C = \mathrm{res}(C)$ is non-torsion. Indeed, we can compute the minimal equation of the elliptic curve C using [15, Computation 10.8]. We are then able to compute the order d of the torsion subgroup of the Mordell–Weil group of the elliptic curve, and we have that $\mathrm{res}(C)$ is not torsion if and only if $\mathrm{res}(dC)$ is non-trivial. By Definition-Lemma 3.2, this is equivalent to $h^0(X, dC) = 1$, and the latter condition can be checked by [15, Computation 10.4].

5	$\begin{bmatrix}0&4&2&1&5\\0&4&5&5&3\end{bmatrix}$	$\begin{bmatrix}4&0&2&5&3\\2&4&1&5&0\end{bmatrix}$	$\begin{bmatrix}4&0&5&1&2\\2&1&0&4&5\end{bmatrix}$	$\begin{bmatrix}4&0&0&5&1\\2&4&5&3&0\end{bmatrix}$	$\begin{bmatrix}3&1&0&5&0\\1&5&1&2&0\end{bmatrix}$	$\begin{bmatrix}4&0&0&5&1\\1&4&5&2&0\end{bmatrix}$		
6	$\begin{bmatrix}1&0&6&5&6\\3&4&2&6&0\end{bmatrix}$	$\begin{bmatrix}2&1&0&5&6\\0&0&6&1&2\end{bmatrix}$	$\begin{bmatrix}6&0&2&1&0\\4&2&1&6&0\end{bmatrix}$	$\begin{bmatrix}5&1&6&6&0\\6&5&1&0&4\end{bmatrix}$	$\begin{bmatrix}2&5&0&7&5\\5&1&4&0&6\end{bmatrix}$	$\begin{bmatrix}0&6&3&6&4\\6&4&1&5&0\end{bmatrix}$	$\begin{bmatrix}6&3&1&0&2\\1&5&0&0&6\end{bmatrix}$	
	$\begin{bmatrix}4&2&6&6&5&0\\5&1&5&6&0&2\end{bmatrix}$	$\begin{bmatrix}3&5&1&4&0&6\\5&2&2&0&3&6\end{bmatrix}$	$\begin{bmatrix}2&3&1&6&0&0\\5&0&1&2&5&6\end{bmatrix}$	$\begin{bmatrix}3&4&1&0&6&0\\6&1&0&1&2&0\end{bmatrix}$	$\begin{bmatrix}3&2&5&0&0&6\\5&0&2&5&6&3\end{bmatrix}$	$\begin{bmatrix}1&6&5&0&3&4\\2&1&4&0&5&6\end{bmatrix}$	$\begin{bmatrix}4&1&0&2&6&3\\1&6&6&1&4&0\end{bmatrix}$	$\begin{bmatrix}1&2&5&6&2&0\\5&6&0&1&1&2\end{bmatrix}$
	$\begin{bmatrix}5&0&5&3&6&6\\3&4&6&0&5&6\end{bmatrix}$	$\begin{bmatrix}5&0&2&5&6&3\\3&2&5&0&1&6\end{bmatrix}$	$\begin{bmatrix}1&2&5&0&6&0\\6&1&3&1&4&0\end{bmatrix}$	$\begin{bmatrix}3&1&2&5&0&6\\0&1&5&3&6&2\end{bmatrix}$	$\begin{bmatrix}2&3&5&2&6&0\\1&0&6&5&5&4\end{bmatrix}$	$\begin{bmatrix}4&0&0&5&1&6\\1&5&6&3&0&2\end{bmatrix}$	$\begin{bmatrix}1&6&5&6&0&4\\2&5&6&6&3&0\end{bmatrix}$	
7	$\begin{bmatrix}4&6&2&7&0\\7&4&8&5&0\end{bmatrix}$	$\begin{bmatrix}1&1&7&0&3\\3&0&1&0&7\end{bmatrix}$	$\begin{bmatrix}4&1&7&0&5\\2&6&0&5&8\end{bmatrix}$	$\begin{bmatrix}7&0&1&2&0\\4&3&6&7&0\end{bmatrix}$	$\begin{bmatrix}6&5&1&0&7\\6&7&3&4&0\end{bmatrix}$	$\begin{bmatrix}5&6&7&2&0\\1&7&0&3&5\end{bmatrix}$	$\begin{bmatrix}1&0&3&7&5\\0&0&5&1&7\end{bmatrix}$	$\begin{bmatrix}6&7&0&2&0\\7&7&4&0&6\end{bmatrix}$
	$\begin{bmatrix}1&4&2&7&0\\2&7&0&7&6\end{bmatrix}$	$\begin{bmatrix}0&0&5&1&7\\2&0&2&7&3\end{bmatrix}$	$\begin{bmatrix}7&2&6&0&4&5\\0&6&5&4&7&7\end{bmatrix}$	$\begin{bmatrix}0&7&6&4&7&5\\3&5&2&0&7&0\end{bmatrix}$	$\begin{bmatrix}4&7&2&6&7&0\\5&6&0&1&7&2\end{bmatrix}$	$\begin{bmatrix}2&1&0&5&6&7\\7&7&0&6&4&5\end{bmatrix}$	$\begin{bmatrix}6&7&5&2&0&0\\3&1&4&0&6&7\end{bmatrix}$	$\begin{bmatrix}0&1&7&5&2&3\\5&2&7&3&0&0\end{bmatrix}$
	$\begin{bmatrix}5&7&7&6&1&0\\6&6&7&0&3&2\end{bmatrix}$	$\begin{bmatrix}7&7&2&2&0&0\\5&4&1&7&1&0\end{bmatrix}$	$\begin{bmatrix}4&1&7&1&0&0\\0&4&5&7&6&7\end{bmatrix}$	$\begin{bmatrix}4&5&6&7&1&0\\7&7&0&0&5&4\end{bmatrix}$	$\begin{bmatrix}0&1&7&5&3&4\\7&4&5&1&1&0\end{bmatrix}$	$\begin{bmatrix}2&4&6&0&6&7\\7&0&3&7&6&5\end{bmatrix}$	$\begin{bmatrix}6&1&7&2&0&3\\2&5&0&1&2&7\end{bmatrix}$	$\begin{bmatrix}7&7&6&2&0&2\\6&7&3&5&4&0\end{bmatrix}$
	$\begin{bmatrix}5&1&7&4&0&2\\3&4&6&7&0&7\end{bmatrix}$	$\begin{bmatrix}5&7&6&5&1&0\\6&7&1&0&2&3\end{bmatrix}$	$\begin{bmatrix}7&1&0&2&2&0\\7&0&3&6&0&5\end{bmatrix}$	$\begin{bmatrix}6&7&1&5&1&0\\0&0&5&7&3&4\end{bmatrix}$	$\begin{bmatrix}5&1&0&3&5&7\\2&7&7&0&6&5\end{bmatrix}$	$\begin{bmatrix}1&5&4&7&0&2\\4&2&6&4&0&7\end{bmatrix}$	$\begin{bmatrix}3&1&6&0&5&7\\0&6&5&5&7&7\end{bmatrix}$	$\begin{bmatrix}2&1&6&0&7&0\\0&0&3&6&2&7\end{bmatrix}$
	$\begin{bmatrix}7&0&0&7&4&5\\5&1&2&7&0&0\end{bmatrix}$	$\begin{bmatrix}1&5&2&7&3&0\\3&5&0&3&6&7\end{bmatrix}$	$\begin{bmatrix}0&0&7&6&7&5\\1&0&4&6&2&7\end{bmatrix}$	$\begin{bmatrix}7&6&1&0&4&5\\1&5&0&0&6&7\end{bmatrix}$	$\begin{bmatrix}6&2&5&0&6&7\\1&7&0&7&6&5\end{bmatrix}$	$\begin{bmatrix}0&0&1&7&5&4\\1&0&3&2&6&7\end{bmatrix}$	$\begin{bmatrix}4&3&3&0&5&7\\6&7&1&3&0&2\end{bmatrix}$	$\begin{bmatrix}3&4&7&1&1&0\\6&7&2&3&0&0\end{bmatrix}$
	$\begin{bmatrix}6&7&0&1&3&2\\2&0&3&1&6&7\end{bmatrix}$	$\begin{bmatrix}6&5&0&7&6&7\\5&7&4&1&0&0\end{bmatrix}$	$\begin{bmatrix}6&7&2&4&1&0\\6&5&3&0&7&7\end{bmatrix}$	$\begin{bmatrix}6&7&2&1&0&4\\4&2&0&0&1&7\end{bmatrix}$	$\begin{bmatrix}6&7&4&0&1&2\\4&3&1&6&7&0\end{bmatrix}$	$\begin{bmatrix}7&0&6&0&4&5\\7&2&3&3&0&0\end{bmatrix}$	$\begin{bmatrix}4&2&7&6&7&0\\2&6&2&7&0&5\end{bmatrix}$	$\begin{bmatrix}1&0&7&7&5&4\\2&0&3&2&7&7\end{bmatrix}$
	$\begin{bmatrix}3&0&5&2&3&7\\6&5&3&0&0&7\end{bmatrix}$	$\begin{bmatrix}5&2&0&7&3&4\\2&5&1&7&0&0\end{bmatrix}$	$\begin{bmatrix}2&3&6&7&7&0\\5&7&2&4&3&0\end{bmatrix}$	$\begin{bmatrix}7&1&7&0&4&6\\5&1&7&2&0&1\end{bmatrix}$	$\begin{bmatrix}2&0&7&6&7&5\\6&5&2&0&3&7\end{bmatrix}$	$\begin{bmatrix}1&0&6&7&5&3\\3&5&4&7&2&0\end{bmatrix}$	$\begin{bmatrix}0&2&7&5&3&4\\4&1&7&1&0&0\end{bmatrix}$	$\begin{bmatrix}0&6&5&0&3&7\\4&5&7&5&0&7\end{bmatrix}$
	$\begin{bmatrix}3&2&4&5&0&7\\6&7&0&0&2&1\end{bmatrix}$	$\begin{bmatrix}0&1&6&3&7&2\\5&7&3&0&2&0\end{bmatrix}$	$\begin{bmatrix}4&7&6&1&0&5\\1&0&4&5&4&7\end{bmatrix}$	$\begin{bmatrix}7&7&1&0&3&6\\2&0&6&5&7&6\end{bmatrix}$	$\begin{bmatrix}5&7&1&4&3&0\\6&5&4&1&0&7\end{bmatrix}$	$\begin{bmatrix}4&3&0&7&7&5\\6&1&3&6&7&0\end{bmatrix}$	$\begin{bmatrix}3&2&5&0&7&7\\0&0&4&7&1&2\end{bmatrix}$	$\begin{bmatrix}6&4&5&1&0&7\\2&0&0&3&1&7\end{bmatrix}$
	$\begin{bmatrix}1&2&3&7&0&0\\5&7&1&3&1&0\end{bmatrix}$	$\begin{bmatrix}3&2&1&0&7&0\\5&0&0&5&2&7\end{bmatrix}$	$\begin{bmatrix}2&3&5&7&3&0\\5&7&2&6&1&0\end{bmatrix}$	$\begin{bmatrix}1&0&5&4&6&7\\0&0&6&7&1&2\end{bmatrix}$	$\begin{bmatrix}5&2&0&7&0&1\\3&7&2&5&1&0\end{bmatrix}$	$\begin{bmatrix}4&3&0&6&7&7\\6&7&2&0&1&0\end{bmatrix}$	$\begin{bmatrix}0&5&0&7&2&1\\2&6&0&5&7&7\end{bmatrix}$	$\begin{bmatrix}7&3&1&0&6&5\\2&5&2&0&7&7\end{bmatrix}$
	$\begin{bmatrix}3&4&3&1&0&0&7\\5&0&0&1&6&7&2\end{bmatrix}$	$\begin{bmatrix}6&4&2&5&0&5&7\\5&6&0&7&1&1&2\end{bmatrix}$	$\begin{bmatrix}6&1&7&0&0&3&4\\4&3&2&1&0&6&7\end{bmatrix}$	$\begin{bmatrix}1&7&2&3&2&0&0\\5&4&1&7&7&1&0\end{bmatrix}$	$\begin{bmatrix}1&4&6&0&7&4&7\\5&1&4&4&1&7&0\end{bmatrix}$	$\begin{bmatrix}5&1&4&4&1&7&0\\1&4&6&0&7&4&6\end{bmatrix}$	$\begin{bmatrix}1&6&0&5&7&7&4\\1&3&3&6&6&7&0\end{bmatrix}$	$\begin{bmatrix}6&5&1&0&4&6&7\\4&7&3&4&1&0&0\end{bmatrix}$
	$\begin{bmatrix}2&7&1&6&0&6&5\\1&6&3&7&2&2&0\end{bmatrix}$	$\begin{bmatrix}3&0&2&0&5&1&7\\2&1&7&0&6&7&5\end{bmatrix}$	$\begin{bmatrix}6&5&1&8&0&0&3\\1&4&3&2&6&7&0\end{bmatrix}$	$\begin{bmatrix}1&4&5&4&7&0&0\\6&1&5&7&0&5&4\end{bmatrix}$	$\begin{bmatrix}0&0&6&4&7&3&1\\1&0&6&7&5&7&6\end{bmatrix}$	$\begin{bmatrix}1&3&6&2&7&3&0\\2&6&5&0&7&0&5\end{bmatrix}$	$\begin{bmatrix}2&6&7&6&1&0&5\\1&7&7&2&3&2&0\end{bmatrix}$	$\begin{bmatrix}5&4&4&1&0&7&6\\1&0&6&4&3&6&7\end{bmatrix}$
	$\begin{bmatrix}5&1&4&4&2&7&0\\2&1&6&0&5&7&2\end{bmatrix}$	$\begin{bmatrix}1&7&2&3&3&0&0\\1&7&0&6&0&3&4\end{bmatrix}$	$\begin{bmatrix}5&6&1&7&0&2&0\\2&4&5&3&1&7&0\end{bmatrix}$	$\begin{bmatrix}3&0&4&6&3&7&7\\1&3&6&3&7&1&0\end{bmatrix}$	$\begin{bmatrix}4&5&5&7&1&0&0\\6&7&1&2&0&1&0\end{bmatrix}$	$\begin{bmatrix}1&1&0&6&7&6&4\\2&0&0&6&4&2&7\end{bmatrix}$	$\begin{bmatrix}2&6&7&4&1&3&0\\5&3&5&7&0&7&0\end{bmatrix}$	$\begin{bmatrix}6&0&0&1&6&3&7\\2&5&4&2&0&7&0\end{bmatrix}$
	$\begin{bmatrix}3&3&6&0&6&7&7\\1&7&3&3&0&1&0\end{bmatrix}$	$\begin{bmatrix}0&0&6&7&7&4&2\\4&3&3&1&0&6&7\end{bmatrix}$	$\begin{bmatrix}4&6&1&5&0&4&7\\6&1&5&0&7&0&4\end{bmatrix}$	$\begin{bmatrix}1&6&6&7&1&0&3\\3&5&7&7&6&5&0\end{bmatrix}$	$\begin{bmatrix}6&5&1&5&0&7&7\\0&0&7&6&7&4&5\end{bmatrix}$	$\begin{bmatrix}2&7&6&7&0&6&5\\3&3&1&2&0&6&7\end{bmatrix}$	$\begin{bmatrix}5&6&1&4&7&5&0\\6&2&2&0&7&0&3\end{bmatrix}$	$\begin{bmatrix}1&0&6&7&6&4&5\\6&5&0&0&4&7&7\end{bmatrix}$
	$\begin{bmatrix}6&2&5&1&0&5&7\\3&4&0&3&1&6&7\end{bmatrix}$	$\begin{bmatrix}6&4&4&5&0&0&7\\2&5&0&0&1&2&7\end{bmatrix}$	$\begin{bmatrix}5&6&4&1&0&4&7\\6&4&7&3&4&1&0\end{bmatrix}$					

Table 4. List of Lang–Trotter polygons for $m \leq 7$

Vertices	Non-polyhedral primes
$\begin{bmatrix} 0 & 6 & 9 & 10 & 9 & 3 & 1 \\ 0 & 2 & 4 & 5 & 6 & 10 & 4 \end{bmatrix}$	2, 19, 29, 31, 53, 71, 83, 97, 103, 131, 167, 211, 233, 257, 263, 269, 277, 313, 347, 373, 419, 439, 461, 487, 491, 577, 593, 619, 643, 653, 661, 709, 761, 827, 907, 919, 941, 953, 991, 1013, 1061, 1097, 1123, 1213, 1223, 1231, 1249, 1289, 1367, 1451, 1481, 1483, 1499, 1543, 1549, 1583, 1721, 1723, 1741, 1787, 1871, 1873
$\begin{bmatrix} 10 & 10 & 9 & 6 & 3 & 0 & 2 & 7 \\ 4 & 3 & 1 & 0 & 1 & 10 & 9 & 6 \end{bmatrix}$	7, 11, 13, 53, 59, 71, 107, 109, 127, 149, 157, 167, 173, 179, 181, 263, 271, 277, 283, 293, 337, 419, 421, 443, 449, 463, 487, 593, 601, 619, 643, 653, 677, 727, 751, 757, 761, 773, 797, 857, 859, 877, 887, 911, 929, 937, 997, 1019, 1031, 1049, 1061, 1069, 1087, 1091, 1103, 1163, 1231, 1249, 1291, 1301, 1319, 1373, 1427, 1439, 1447, 1451, 1459, 1489, 1493, 1523, 1553, 1559, 1571, 1609, 1613, 1669, 1721, 1741, 1747, 1777, 1787, 1811, 1871, 1889, 1901, 1933, 1973, 1987, 1993, 1997
$\begin{bmatrix} 5 & 6 & 9 & 11 & 12 & 2 & 0 & 2 & 3 \\ 0 & 0 & 1 & 2 & 4 & 10 & 11 & 5 & 3 \end{bmatrix}$	23, 29, 41, 59, 67, 71, 131, 139, 179, 181, 191, 199, 223, 229, 241, 251, 307, 311, 331, 337, 349, 379, 401, 409, 419, 421, 443, 461, 491, 547, 571, 577, 587, 601, 631, 647, 661, 673, 701, 733, 739, 751, 787, 827, 839, 857, 859, 911, 919, 937, 971, 977, 983, 991, 1013, 1019, 1021, 1039, 1061, 1063, 1087, 1109, 1123, 1129, 1171, 1187, 1213, 1223, 1229, 1237, 1249, 1259, 1277, 1279, 1307, 1327, 1381, 1409, 1429, 1447, 1459, 1493, 1511, 1549, 1571, 1579, 1583, 1597, 1619, 1621, 1699, 1723, 1741, 1759, 1811, 1823, 1831, 1847, 1873, 1913, 1931, 1933, 1979, 1987
$\begin{bmatrix} 0 & 5 & 9 & 10 & 12 & 11 & 5 & 4 \\ 12 & 10 & 7 & 6 & 3 & 2 & 0 & 0 \end{bmatrix}$	23, 31, 37, 41, 47, 53, 73, 101, 131, 139, 197, 199, 223, 233, 307, 317, 331, 383, 389, 401, 421, 439, 449, 461, 479, 487, 499, 509, 569, 571, 593, 599, 607, 631, 641, 673, 701, 709, 743, 787, 811, 829, 857, 863, 877, 881, 907, 911, 941, 1019, 1021, 1123, 1151, 1153, 1171, 1217, 1231, 1237, 1259, 1291, 1297, 1423, 1429, 1481, 1583, 1609, 1657, 1723, 1753, 1783, 1823, 1871, 1879, 1889, 1901, 1907, 1973, 1979, 1987, 1997
$\begin{bmatrix} 0 & 2 & 12 & 13 & 13 & 11 & 9 & 4 \\ 0 & 1 & 7 & 9 & 10 & 12 & 13 & 12 \end{bmatrix}$	31, 37, 47, 79, 131, 139, 151, 181, 211, 223, 239, 257, 271, 281, 307, 331, 373, 389, 409, 433, 457, 461, 479, 523, 569, 577, 587, 641, 659, 683, 709, 719, 733, 743, 761, 769, 809, 821, 823, 853, 859, 863, 887, 953, 997, 1013, 1063, 1093, 1103, 1117, 1129, 1153, 1163, 1181, 1201, 1237, 1249, 1283, 1361, 1367, 1439, 1471, 1531, 1553, 1601, 1609, 1699, 1721, 1741, 1789, 1867, 1871, 1873, 1889, 1907, 1931, 1973, 1979, 1997
$\begin{bmatrix} 0 & 2 & 12 & 13 & 12 & 11 & 8 & 7 & 4 \\ 0 & 1 & 7 & 9 & 11 & 12 & 13 & 13 & 12 \end{bmatrix}$	31, 61, 71, 89, 97, 109, 127, 139, 149, 163, 173, 191, 193, 227, 233, 257, 271, 281, 311, 313, 347, 349, 353, 389, 421, 433, 457, 463, 467, 479, 491, 499, 541, 563, 571, 587, 607, 613, 631, 643, 683, 733, 743, 751, 757, 769, 797, 809, 821, 853, 857, 863, 907, 941, 967, 971, 991, 997, 1013, 1019, 1031, 1049, 1051, 1063, 1087, 1091, 1093, 1097, 1109, 1153, 1163, 1193, 1217, 1279, 1283, 1303, 1321, 1433, 1439, 1451, 1481, 1483, 1493, 1499, 1511, 1543, 1559, 1571, 1597, 1621, 1667, 1693, 1723, 1759, 1823, 1867, 1913, 1931, 1973, 1979, 1987

Table 5. Lang Trotter polygons for non-polyhedral primes < 2000

Vertices	Non-polyhedral primes
$\begin{bmatrix} 13 & 9 & 5 & 4 & 2 & 1 & 0 & 1 & 11 \\ 8 & 0 & 3 & 4 & 7 & 9 & 12 & 13 & 9 \end{bmatrix}$	11, 19, 59, 83, 101, 107, 113, 163, 167, 181, 197, 269, 293, 307, 313, 317, 337, 347, 349, 359, 373, 401, 461, 491, 499, 509, 521, 569, 617, 643, 647, 661, 677, 683, 739, 787, 797, 809, 821, 827, 829, 839, 859, 883, 887, 941, 983, 1087, 1109, 1117, 1163, 1213, 1237, 1277, 1283, 1291, 1303, 1307, 1429, 1451, 1483, 1493, 1553, 1597, 1621, 1637, 1667, 1733, 1801, 1901, 1933, 1993, 1997
$\begin{bmatrix} 0 & 1 & 10 & 12 & 13 & 12 & 10 & 7 & 1 \\ 0 & 0 & 3 & 4 & 6 & 9 & 13 & 12 & 2 \end{bmatrix}$	11, 23, 29, 31, 43, 59, 67, 73, 137, 149, 157, 223, 229, 271, 277, 281, 283, 293, 353, 367, 439, 457, 461, 491, 503, 577, 599, 601, 641, 643, 647, 653, 661, 691, 733, 757, 941, 977, 997, 1019, 1049, 1051, 1061, 1069, 1193, 1249, 1301, 1303, 1327, 1373, 1451, 1471, 1487, 1543, 1553, 1559, 1579, 1597, 1607, 1627, 1669, 1699, 1723, 1753, 1777, 1789, 1831, 1847, 1877, 1913, 1933, 1949, 1997, 1999
$\begin{bmatrix} 0 & 12 & 13 & 13 & 11 & 9 & 7 & 1 \\ 0 & 4 & 9 & 10 & 12 & 13 & 12 & 2 \end{bmatrix}$	7, 11, 67, 101, 139, 199, 251, 313, 331, 337, 353, 373, 383, 419, 421, 431, 503, 541, 557, 571, 587, 601, 607, 617, 619, 659, 709, 719, 733, 751, 857, 877, 883, 911, 947, 967, 1033, 1093, 1123, 1163, 1193, 1277, 1279, 1283, 1289, 1303, 1319, 1327, 1381, 1409, 1423, 1429, 1439, 1453, 1459, 1499, 1531, 1549, 1621, 1657, 1663, 1667, 1787, 1879, 1913, 1951
$\begin{bmatrix} 0 & 2 & 12 & 13 & 13 & 12 & 11 & 9 & 4 \\ 0 & 1 & 7 & 8 & 9 & 11 & 12 & 13 & 12 \end{bmatrix}$	5, 17, 23, 29, 41, 43, 67, 73, 79, 101, 103, 107, 113, 157, 173, 179, 191, 193, 227, 229, 239, 251, 263, 277, 281, 283, 313, 331, 337, 349, 353, 367, 379, 389, 397, 443, 449, 457, 463, 467, 479, 487, 503, 509, 521, 557, 563, 587, 617, 641, 643, 647, 653, 659, 701, 773, 787, 809, 823, 859, 887, 907, 911, 937, 941, 947, 983, 991, 1009, 1013, 1019, 1039, 1049, 1087, 1091, 1097, 1103, 1187, 1217, 1279, 1289, 1303, 1307, 1321, 1327, 1373, 1399, 1409, 1427, 1429, 1453, 1471, 1483, 1487, 1493, 1511, 1523, 1553, 1579, 1619, 1621, 1663, 1667, 1693, 1697, 1709, 1721, 1723, 1733, 1759, 1777, 1831, 1867, 1871, 1873, 1877, 1889, 1907, 1931, 1951, 1973, 1993, 1997
$\begin{bmatrix} 0 & 5 & 10 & 12 & 14 & 14 & 5 & 4 \\ 0 & 2 & 5 & 7 & 10 & 11 & 14 & 12 \end{bmatrix}$	31, 37, 47, 79, 103, 127, 137, 149, 151, 163, 199, 211, 223, 229, 257, 269, 271, 311, 347, 353, 359, 389, 397, 401, 419, 439, 443, 457, 461, 463, 487, 499, 503, 523, 569, 571, 631, 677, 701, 727, 751, 773, 823, 853, 883, 911, 919, 947, 953, 967, 991, 1019, 1039, 1063, 1097, 1123, 1151, 1153, 1171, 1193, 1201, 1217, 1223, 1231, 1279, 1283, 1289, 1303, 1307, 1327, 1373, 1423, 1447, 1453, 1471, 1499, 1511, 1523, 1543, 1567, 1571, 1607, 1693, 1699, 1723, 1733, 1753, 1759, 1777, 1783, 1801, 1831, 1861, 1877, 1879, 1889, 1913, 1951, 1987, 1999
$\begin{bmatrix} 0 & 5 & 7 & 12 & 13 & 14 & 12 & 6 & 2 \\ 0 & 2 & 3 & 6 & 8 & 11 & 12 & 14 & 6 \end{bmatrix}$	3, 17, 19, 61, 67, 127, 197, 223, 241, 251, 263, 271, 277, 307, 359, 367, 431, 463, 487, 563, 641, 659, 701, 719, 733, 751, 761, 797, 823, 829, 839, 877, 887, 911, 967, 977, 1031, 1049, 1093, 1123, 1153, 1163, 1223, 1249, 1277, 1321, 1327, 1433, 1447, 1453, 1481, 1571, 1613, 1627, 1663, 1709, 1733, 1759, 1787, 1801, 1847, 1901, 1997

Table 5 (continued)

Another approach is to find a multiple of d using the Nagell–Lutz Theorem [63]: if p is a prime of good reduction for C, then the specialization map induces an injective homomorphism of abelian groups $C(\mathbb{Q})_{\text{tors}} \to C(\mathbb{F}_p)$. Therefore, the torsion order d of $C(\mathbb{Q})$ divides the order of $C(\mathbb{F}_p)$ for any prime p of good reduction, which is easy to compute from the defining equation of Γ. We then find a multiple of d by taking the greatest common divisor of the orders of $C(\mathbb{F}_p)$ as p varies.

Database 8.2. A database of Lang–Trotter polygons that can be used to show that every prime $p < 2000$ is not polyhedral for some Lang–Trotter polygon (see also Remark 7.8). For each polygon, its non-polyhedral primes are displayed in Table 5.

Acknowledgement. We thank Igor Dolgachev, Gavril Farkas and Brian Lehmann for useful discussions and for answering our questions. We are especially grateful to Tom Weston for sharing and explaining his paper [68]. In the REU directed by Jenia Tevelev in 2017, Stephen Obinna [55] has started to collect evidence for existence of blown-up toric surfaces with non-polyhedral effective cone. The software Magma [11] was used extensively. Some of the graphics are by the Plain Form Studio.

References

[1] *V. Alexeev* and *D. Swinarski*, Nef divisors on $\overline{M}_{0,n}$ from GIT, in: Geometry and arithmetic, EMS Ser. Congr. Rep., European Mathematical Society, Zürich (2012), 1–21.

[2] *N. Arkani-Hamed*, *J. L. Bourjaily*, *F. Cachazo*, *A. Postnikov* and *J. Trnka*, On-shell structures of MHV amplitudes beyond the planar limit, J. High Energy Phys. **2015** (2015), no. 6, Paper No. 179

[3] *M. Artin*, Some numerical criteria for contractability of curves on algebraic surfaces, Amer. J. Math. **84** (1962), 485–496.

[4] *I. Arzhantsev*, *U. Derenthal*, *J. Hausen* and *A. Laface*, Cox rings, Cambridge Stud. Adv. Math. **144**, Cambridge University, Cambridge 2015.

[5] *G. Balletti*, Enumeration of lattice polytopes by their volume, Discrete Comput. Geom. **65** (2021), no. 4, 1087–1122.

[6] *M. I. Bašmakov*, Cohomology of Abelian varieties over a number field, Russian Math. Surveys **27** (1972), no. 6, 25–70.

[7] *T. Bauer*, A simple proof for the existence of Zariski decompositions on surfaces, J. Algebraic Geom. **18** (2009), no. 4, 789–793.

[8] *P. Belkale* and *A. Gibney*, Basepoint free cycles on $\overline{\mathrm{M}}_{0,n}$ from Gromov–Witten theory, Int. Math. Res. Not. IMRN **2021** (2021), no. 2, 855–884.

[9] *E. Bombieri* and *D. Mumford*, Enriques' classification of surfaces in char. p. III, Invent. Math. **35** (1976), 197–232.

[10] *E. Bombieri* and *D. Mumford*, Enriques' classification of surfaces in char. p. II, in: Complex analysis and algebraic geometry, Iwanami Shoten, Tokyo (1977), 23–42.

[11] *W. Bosma*, *J. Cannon* and *C. Playoust*, The Magma algebra system. I. The user language, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265.

[12] *S. Boucksom*, *J.-P. Demailly*, *M. Păun* and *T. Peternell*, The pseudo-effective cone of a compact Kähler manifold and varieties of negative Kodaira dimension, J. Algebraic Geom. **22** (2013), no. 2, 201–248.

[13] *S. Cantat* and *I. Dolgachev*, Rational surfaces with a large group of automorphisms, J. Amer. Math. Soc. **25** (2012), no. 3, 863–905.

[14] *A.-M. Castravet*, The Cox ring of $\overline{M}_{0,6}$, Trans. Amer. Math. Soc. **361** (2009), no. 7, 3851–3878.

[15] *A.-M. Castravet*, *A. Laface*, *J. Tevelev* and *L. Ugaglia*, Blown-up toric surfaces with non-polyhedral effective cone, preprint 2021, `https://arxiv.org/abs/2009.14298v3`.

[16] *A.-M. Castravet* and *J. Tevelev*, Rigid curves on $\overline{M}_{0,n}$ and arithmetic breaks, in: Compact moduli spaces and vector bundles, Contemp. Math. **564**, American Mathematical Society, Providence (2012), 19–67.

[17] *A.-M. Castravet* and *J. Tevelev*, Hypertrees, projections, and moduli of stable rational curves, J. reine angew. Math. **675** (2013), 121–180.

[18] *A.-M. Castravet* and *J. Tevelev*, $\overline{M}_{0,n}$ is not a Mori dream space, Duke Math. J. **164** (2015), no. 8, 1641–1667.

[19] *A.-M. Castravet* and *J. Tevelev*, Derived category of moduli of pointed curves. I, Algebr. Geom. **7** (2020), no. 6, 722–757.

[20] *D. A. Cox*, The homogeneous coordinate ring of a toric variety, J. Algebraic Geom. **4** (1995), no. 1, 17–50.

[21] *D. A. Cox*, *J. B. Little* and *H. K. Schenck*, Toric varieties, Grad. Stud. Math. **124**, American Mathematical Society, Providence 2011.

[22] *O. Debarre*, Higher-dimensional algebraic geometry, Universitext, Springer, New York 2001.

[23] *B. Doran*, *N. Giansiracusa* and *D. Jensen*, A simplicial approach to effective divisors in $\overline{M}_{0,n}$, Int. Math. Res. Not. IMRN **2017** (2017), no. 2, 529–565.

[24] *E. B. Dynkin*, Semisimple subalgebras of semisimple lie algebras, Trans. Amer. Math. Soc. **6** (1957), 111–244.

[25] *M. Fedorchuk*, Symmetric f-conjecture for $g \leq 35$, preprint 2020, `https://arxiv.org/abs/2007.13457`.

[26] *M. Fedorchuk* and *D. I. Smyth*, Ample divisors on moduli spaces of pointed rational curves, J. Algebraic Geom. **20** (2011), no. 4, 599–629.

[27] *O. Fujino*, On minimal model theory for algebraic log surfaces, Taiwanese J. Math. **25** (2021), no. 3, 477–489.

[28] *O. Fujino* and *H. Tanaka*, On log surfaces, Proc. Japan Acad. Ser. A Math. Sci. **88** (2012), no. 8, 109–114.

[29] *M. Fulger*, Seshadri constants for curve classes, Int. Math. Res. Not. IMRN **2021** (2021), no. 21, 16448–16493.

[30] *M. Fulger* and *B. Lehmann*, Zariski decompositions of numerical cycle classes, J. Algebraic Geom. **26** (2017), no. 1, 43–106.

[31] *N. Giansiracusa* and *A. Gibney*, The cone of type A, level 1, conformal blocks divisors, Adv. Math. **231** (2012), no. 2, 798–814.

[32] *N. Giansiracusa*, *D. Jensen* and *H.-B. Moon*, GIT compactifications of $M_{0,n}$ and flips, Adv. Math. **248** (2013), 242–278.

[33] *A. Gibney*, Numerical criteria for divisors on $\overline{M}_g$ to be ample, Compos. Math. **145** (2009), no. 5, 1227–1248.

[34] *A. Gibney*, *S. Keel* and *I. Morrison*, Towards the ample cone of $\overline{M}_{g,n}$, J. Amer. Math. Soc. **15** (2002), no. 2, 273–294.

[35] *A. Gibney* and *D. Maclagan*, Lower and upper bounds for nef cones, Int. Math. Res. Not. IMRN **2012** (2012), no. 14, 3224–3255.

[36] *J. L. González* and *K. Karu*, Some non-finitely generated Cox rings, Compos. Math. **152** (2016), no. 5, 984–996.

[37] *S. Goto*, *K. Nishida* and *K. Watanabe*, Non-Cohen–Macaulay symbolic blow-ups for space monomial curves and counterexamples to Cowsik's question, Proc. Amer. Math. Soc. **120** (1994), no. 2, 383–392.

[38] *J. Grivaux*, Parabolic automorphisms of projective surfaces (after M. H. Gizatullin), Mosc. Math. J. **16** (2016), no. 2, 275–298.

[39] *R. Gupta* and *M. R. Murty*, Primitive points on elliptic curves, Compos. Math. **58** (1986), no. 1, 13–44.

[40] *J. Harris* and *D. Mumford*, On the Kodaira dimension of the moduli space of curves, Invent. Math. **67** (1982), no. 1, 23–88.

[41] *B. Hassett* and *Y. Tschinkel*, On the effective cone of the moduli space of pointed rational curves, in: Topology and geometry: Commemorating SISTAG, Contemp. Math. **314**, American Mathematical Society, Providence (2002), 83–96.

[42] *J. Hausen*, *S. Keicher* and *A. Laface*, On blowing up the weighted projective plane, Math. Z. **290** (2018), no. 3–4, 1339–1358.

[43] *Y. Hu* and *S. Keel*, Mori dream spaces and GIT, Michigan Math. J. **48** (2000), 331–348.

[44] *S. Keel* and *J. McKernan*, Contractible extremal rays on $\overline{M}_{0,n}$, preprint 1996, `https://arxiv.org/abs/alg-geom/9607009`.

[45] *J. Kollár* and *S. Mori*, Birational geometry of algebraic varieties, Cambridge Tracts in Math. **134**, Cambridge University, Cambridge 1998.

[46] *S. Lang* and *H. Trotter*, Primitive points on elliptic curves, Bull. Amer. Math. Soc. **83** (1977), no. 2, 289–292.

[47] *R. Lazarsfeld*, Positivity in algebraic geometry. I, Ergeb. Math. Grenzgeb. (3) **49**, Springer, Berlin 2004.

[48] *R. Lazarsfeld*, Positivity in algebraic geometry. II, Ergeb. Math. Grenzgeb. (3) **49**, Springer, Berlin 2004.

[49] *LMFDB*, The l-functions and modular forms database, Technical report, 2020, `http://www.lmfdb.org`.

[50] *A. Losev* and *Y. Manin*, New moduli spaces of pointed curves and pencils of flat connections, Michigan Math. J. **48** (2000), 443–472.

[51] *B. Mazur*, Modular curves and the Eisenstein ideal, Publ. Math. Inst. Hautes Études Sci. **47** (1977), 33–186.

[52] *D. Mumford*, The topology of normal singularities of an algebraic surface and a criterion for simplicity, Publ. Math. Inst. Hautes Études Sci. **9** (1961), 5–22.

[53] *D. Mumford*, Lectures on curves on an algebraic surface, Ann. of Math. Stud. **59**, Princeton University, Princeton 1966.
[54] *V. V. Nikulin*, A remark on algebraic surfaces with polyhedral Mori cone, Nagoya Math. J. **157** (2000), 73–92.
[55] *S. Obinna*, Database of blow-ups of toric surfaces of picard number 2, Technical report, 2017, `https://people.math.umass.edu/~tevelev/obinna/`.
[56] *T. Oda* and *H. S. Park*, Linear Gale transforms and Gel'fand–Kapranov–Zelevinskij decompositions, Tohoku Math. J. (2) **43** (1991), no. 3, 375–399.
[57] *K. Oguiso* and *T. Shioda*, The Mordell–Weil lattice of a rational elliptic surface, Comment. Math. Univ. St. Paul. **40** (1991), no. 1, 83–99.
[58] *M. Opie*, Extremal divisors on moduli spaces of rational curves with marked points, Michigan Math. J. **65** (2016), no. 2, 251–285.
[59] *J.-P. Serre*, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), no. 4, 259–331.
[60] *J. H. Silverman*, Heights and the specialization map for families of abelian varieties, J. reine angew. Math. **342** (1983), 197–211.
[61] *J. H. Silverman*, Advanced topics in the arithmetic of elliptic curves, Grad. Texts in Math. **151**, Springer, New York 1994.
[62] *J. H. Silverman*, The arithmetic of elliptic curves, 2nd ed., Grad. Texts in Math. **106**, Springer, Dordrecht 2009.
[63] *J. H. Silverman* and *J. T. Tate*, Rational points on elliptic curves, 2nd ed., Undergrad. Texts Math., Springer, Cham 2015.
[64] *H. Tanaka*, Minimal models and abundance for positive characteristic log surfaces, Nagoya Math. J. **216** (2014), 1–70.
[65] *J. Tevelev*, Scattering amplitudes of stable curves, preprint 2020, `https://arxiv.org/abs/2007.03831`.
[66] *N. Tschebotareff*, Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören, Math. Ann. **95** (1926), no. 1, 191–228.
[67] *P. Vermeire*, A counterexample to Fulton's conjecture on $\overline{M}_{0,n}$, J. Algebra **248** (2002), no. 2, 780–784.
[68] *T. Weston*, Kummer theory of abelian varieties and reductions of Mordell–Weil groups, Acta Arith. **110** (2003), no. 1, 77–88.

Ana-Maria Castravet, UVSQ, CNRS, Laboratoire de Mathématiques de Versailles,
Université Paris-Saclay, 78000 Versailles, France
e-mail: ana-maria.castravet@uvsq.fr

Antonio Laface, Departamento de Matemática, Universidad de Concepción,
Casilla 160-C, Concepción, Chile
e-mail: alaface@udec.cl

Jenia Tevelev, Department of Mathematics and Statistics, University of Massachusetts Amherst,
710 North Pleasant Street, Amherst, MA 01003, USA
e-mail: tevelev@math.umass.edu

Luca Ugaglia, Dipartimento di Matematica e Informatica, Università degli studi di Palermo,
Via Archirafi 34, 90123 Palermo, Italy
e-mail: luca.ugaglia@unipa.it

Eingegangen 24. Januar 2022, in revidierter Fassung 17. Januar 2023