MINIMIZATION OF HYPERSURFACES

ANDREAS-STEPHAN ELSENHANS AND MICHAEL STOLL

Abstract. Let $F \in \mathbb{Z}[x_0, \dots, x_n]$ be homogeneous of degree d and assume that F is not a 'nullform', i.e., there is an invariant I of forms of degree d in $n + 1$ variables such that $I(F) \neq 0$. Equivalently, F is semistable in the sense of Geometric Invariant Theory. Minimizing F at a prime p means to produce $T \in \mathrm{Mat}(n+1, \mathbb{Z}) \cap \mathrm{GL}(n+1, \mathbb{Q})$ and $e \in \mathbb{Z}_{\geq 0}$ such that $F_1 = p^{-e}F([x_0, \dots, x_n] \cdot T)$ has integral coefficients and $v_p(I(F_1))$ is minimal among all such F_1. Following Kollár [Kol97], the minimization process can be described in terms of applying weight vectors $w \in \mathbb{Z}_{\geq 0}^{n+1}$ to F. We show that for any dimension n and degree d, there is a complete set of weight vectors consisting of $[0, w_1, w_2, \dots, w_n]$ with $0 \leq w_1 \leq w_2 \leq \dots \leq w_n \leq 2nd^{n-1}$. When $n = 2$, we improve the bound to d. This answers a question raised by Kollár.

Based on this result and a further study of the minimization process in the planar case $n = 2$, we devise an efficient minimization algorithm for ternary forms (equivalently, plane curves) of arbitrary degree d. We also describe a similar algorithm that allows to minimize (and reduce) cubic surfaces. The algorithms are available in Magma.

1 Introduction

When one wants to do explicit computations with algebraic varieties over $\mathbb{Q}$ (or, more generally, over a number field), it is advantageous to use an explicit model that is given by equations with small integral coefficients. So it is an interesting question how one can try to simplify or optimize a given model in this sense. This involves two aspects. One aspect is that one strives to minimize the absolute value (in general, the norm) of a suitable invariant, for example, the discriminant in the common situation when the variety is smooth. This can be seen as optimizing the reduction properties of the model at all primes; this is usually known as *minimization* of the given model. The other aspect concerns making the coefficients small while staying in the same isomorphism class over $\mathbb{Z}$. This has a different flavor and is known as *reduction*. Minimization and reduction have been studied for 2-, 3-, 4- and 5-coverings of elliptic curves in [CFS10] and [Fis13]. The reduction theory of binary forms is studied in [SC03] and [HS19] and that of point clusters in projective space in [Sto11]. The latter can be used to obtain a reduction method also for more general projective varieties; for example, we can reduce equations of plane curves by reducing their multiset of inflection points.

In this paper, we will discuss minimization in the case of hypersurfaces. This problem has been considered by Kollár in [Kol97] in some detail. Kollár writes (at the end of the introduction of [Kol97]) that "so far I could not prove a bound on the weights occurring in (4.3), except in some special cases." One goal of this paper is to provide such a bound, which is completely explicit and close to optimal in the case of plane curves; see Theorems 1.6 and 1.5 below. The availability of an explicit bound on the weights

Date: Ocotber 9, 2021.

2020 *Mathematics Subject Classification.* Primary 11D25, 11D41; Secondary 11G30, 14G25, 14Q05, 14Q10, 14Q25, 11Y99.

Key words and phrases. minimization, reduction, hypersurfaces, plane curves, cubic surfaces.

(see below for definitions) leads, at least in principle, to a minimization algorithm for hypersurfaces of given degree and dimension; see Section 6. In the context of plane curves of degree d, the case $d = 1$ is not interesting and the case $d = 2$ is classical. Plane cubics ($d = 3$) are 3-coverings of elliptic curves and are therefore considered in [CFS10]. We work out the case of plane curves in general: we show that minimization can be achieved by successive steps using only the two most basic weight vectors. Combined with the bound on the weights, this leads to a reasonably efficient algorithm that produces a p-minimal (planar) model for any semistable plane curve. See Section 7.

We include a short discussion on the minimization of binary forms (Section 2), which can serve as a warm-up section before dealing with the general theory and the case of plane curves.

When working over $\mathbb{Q}$ or, more generally, over an algebraic number field of class number 1, minimization can be considered for each prime p independently, in the sense that we can produce another integral model whose discriminant (say) has minimal possible p-adic valuation and unchanged valuation at all other primes. So we just have to perform this *minimization at* p successively for each potentially non-minimal prime p to arrive at a minimal model.

We describe how one can find a small set of primes that contains the primes at which a given plane curve is not minimal in a reasonably efficient way and how to reduce a plane curve, i.e., to find a unimodular transformation that makes the coefficients small; see Section 8. We add some discussion of the problem of finding representatives of all $\mathrm{GL}(n+1, \mathbb{Z})$-equivalence classes of (globally) minimal models in Section 9.

As a further application, we give an explicit minimization algorithm for cubic surfaces in Section 11; we add a discussion of reduction for cubic surfaces in Section 12 so as to have a complete treatment of this case as well. Unfortunately, one important ingredient that allows us to obtain a general algorithm for plane curves whose complexity mainly depends on the degree d and only to a small extent on p does not carry over to the case of surfaces in $\mathbb{P}^3$. This prevents us from generalizing the minimization algorithm for plane curves to higher dimensions; see Section 10.

Our results and algorithms are formulated in terms of $\mathbb{Z}$, $\mathbb{Q}$ and a prime number p, but we really only need the fact that the p-adic valuation is a valuation. In particular, everything we do remains valid if we replace $\mathbb{Z}$ and p by a discrete valuation ring R and a uniformizer π of R. For the algorithms, we have of course to assume that we can do computations in R and in the residue class field $k = R/\langle \pi \rangle$. For the general statement of Proposition 6.4, we also need to assume that k is finite, but we would like to stress that this assumption is not needed for the minimization algorithms for plane curves or cubic surfaces.

For the following, Kollár's paper [Kol97] is the main reference. We fix $n \geq 1$ and $d \geq 1$ and consider homogeneous polynomials F of degree d in the $n+1$ Variables $x_0, \ldots, x_n$, with integral coefficients. We also fix a prime number p and write $v_p(F)$ for the minimum of the p-adic valuations of the coefficients of F. Vectors will be row vectors; vectors and matrices are denoted using square brackets. If $T \in \mathrm{GL}(n+1, \mathbb{Q})$, then ${}^{T}F$ denotes $F([x_0, \ldots, x_n] \cdot T)$. If $T \in \mathrm{GL}(n+1, \mathbb{Z})$, then it follows that $v_p({}^{T}F) = v_p(F)$. As a matter of notation, ${}^{T}F([x_0, \ldots, x_n]M)$ means $({}^{T}F)([x_0, \ldots, x_n] \cdot M) = {}^{MT}F$ and not ${}^{T}(F([x_0, \ldots, x_n] \cdot M)) = {}^{TM}F$, where $M \in \mathrm{Mat}(n+1, \mathbb{Q})$ is another matrix. This applies in particular to

$$ {}^{T}F(p^{w_0}x_0, \dots, p^{w_n}x_n) = ({}^{T}F)(p^{w_0}x_0, \dots, p^{w_n}x_n)\,. $$

Definition 1.1. A *weight system* is a pair (T, w), where $T \in \mathrm{GL}(n+1, \mathbb{Z})$ and $w \in \mathbb{Z}_{\geq 0}^{n+1}$; w is called the *weight vector* of the weight system.

Definition 1.2. A homogeneous polynomial $F \in \mathbb{Z}[x_0, \dots, x_n]$ is *unstable* at p for a weight system (T, w) with $w = [w_0, \dots, w_n]$ if

$$ v_p\big({}^{T}F(p^{w_0}x_0, p^{w_1}x_1, \dots, p^{w_n}x_n)\big) > \frac{d}{n+1}(w_0 + w_1 + \cdots + w_n)\,. $$

For example, a polynomial F is unstable at p for $(T, [0, \dots, 0])$ if and only if $v_p(F) > 0$, i.e., if p divides the gcd of the coefficients of F.

Definition 1.3. Let $S \subset \mathbb{Z}_{\geq 0}^{n+1}$ be a set of weight vectors. The set S is a *complete set of weight vectors* (for dimension n and degree d) if the following holds. If $F \in \mathbb{Z}[x_0, \dots, x_n]$, homogeneous of degree d, is unstable at p for some weight system (T, w), then F is also unstable at p for a weight system (T', w') with $w' \in S$.

Kollár raises the question (in [Kol97, 1.9]) whether there is a bound on the weights that one needs to consider, or equivalently, whether there is always a finite complete set of weight vectors. This question was answered positively by the first author of this note in [Els09], but without giving explicit bounds. If we have an explicit bound, then we have an explicit finite complete set of weight vectors, which allows us to construct an algorithm for minimizing a given hypersurface at a given prime, see Section 6. Experimental evidence suggests the following.

Conjecture 1.4. *For given dimension n and degree d, there is a complete set of weight vectors whose entries are bounded by d^{n-1}.*

This is trivially true when $n = 1$; in this case, $\{[0, 0], [0, 1]\}$ is a complete set of weight vectors for every degree d.

We can prove Conjecture 1.4 in the case of plane curves, $n = 2$. This results in the following theorem.

Theorem 1.5. *For every $d \geq 1$, there is a complete set of weight vectors for ternary forms of degree d whose entries are bounded by d.*

See Section 4 for the proof.

We can also prove the following general result, which is slightly weaker (by a factor of $2n$ at worst) than Conjecture 1.4.

Theorem 1.6. *For every dimension $n \geq 2$ and degree $d \geq 1$, the subset of*

$$ W_n = \{[w_0, w_1, \dots, w_n] \in \mathbb{Z}^{n+1} : 0 = w_0 \leq w_1 \leq \cdots \leq w_n\} $$

consisting of (primitive) vectors with

$$ w_n \leq 2n \frac{d}{\gcd(d, n+1)} d^{n-2} $$

is a complete set of weight vectors for homogeneous polynomials of degree d in $n+1$ variables.

Note that it is easy to see that w dominates all its positive integral multiples in the sense of Definition 3.1 below; therefore we can restrict to primitive (i.e., with gcd 1) weight vectors.

We give the proof of Theorem 1.6 in Section 5.

2 Binary forms

Before we begin with the general theory, we consider the case $n = 1$ of binary forms. As mentioned in the introduction, the two weight vectors $[0, 0]$ and $[0, 1]$ form a (minimal) complete set of weight vectors in this case, regardless of the degree d. Consider a binary form

$$F = a_0 x_1^d + a_1 x_0 x_1^{d-1} + \ldots + a_{d-1} x_0^{d-1} x_1 + a_d x_0^d$$

of degree d, with coefficients in $\mathbb{Z}$. This form is unstable at p for $(T, [0, 0])$ (with any $T \in \mathrm{GL}(2, \mathbb{Z})$) if and only if p divides the gcd of the coefficients. So the first step in the minimization procedure for binary forms is to divide F by the gcd of its coefficients. Then we only need to consider the other weight vector, $[0, 1]$. The condition that F be unstable at p for $(E_2, [0, 1])$ is that

$$v_p(a_j) > j - \frac{d}{2} \qquad \text{for all } j \geq \frac{d}{2}.$$

In particular, the reduction $\bar{F}$ of F mod p must be divisible by $x_1^{\lceil (d+1)/2 \rceil}$. This implies that if F is unstable at p for $(T, [0, 1])$ with some $T \in \mathrm{GL}(2, \mathbb{Z})$, then $\bar{F}$ has a linear factor of multiplicity $> d/2$; such a linear factor is then uniquely determined. This leads to the following algorithm for minimizing a binary form at a prime p.

Algorithm 2.1. The input of MinimizeBinaryFormOneStep and MinimizeBinaryForm consists in a semistable binary form $F \in \mathbb{Z}[x_0, x_1]$ of degree $d \geq 2$ and a prime number p. The result of MinimizeBinaryFormOneStep consists of a boolean flag indicating whether a minimization step could be performed successfully and in this case, a form G of degree d, a matrix T and a number $e \in \mathbb{Z}_{\geq 0}$ such that $G = p^{-e} \cdot {}^T F$ is the result of the minimization step; otherwise F, E_2 and 0 are returned as the last three values. The result of MinimizeBinaryForm consists of a form G of degree d that is a minimized representative of the orbit of F, together with a matrix T and a number $e \in \mathbb{Z}_{\geq 0}$ as above.

```
MinimizeBinaryFormOneStep(F, p)
  $d := \deg(F)$;
  $\bar{F} = F \bmod p \in \mathbb{F}_p[x_0, x_1]$;
  if $\bar{F}$ has a factor $L^m$ with $\deg(L) = 1$ and $m > d/2$ then
    $T :=$ a matrix in $\mathrm{GL}(2, \mathbb{Z})$ such that ${}^{\bar{T}}L = \lambda x_1$;
    $G := {}^T F$; // now $\bar{G}$ is divisible by $x_1^{\lceil (d+1)/2 \rceil}$
    $G_1 := G(x_0, p x_1)$; $e := v_p(G_1)$; // apply $w = [0, 1]$
    if $e > d/2$ then // unstable?
      return true, $p^{-e} G_1$, $T$, $e$;
    end if;
  end if;
  return false, $F$, $E_2$, $0$;

MinimizeBinaryForm(F, p)
  $T := E_2$; $e := v_p(F)$; $G := p^{-e} F$; // initialize; do $w = [0, 0]$
```

```
success, G, $T_1$, $e_1$ := MinimizeBinaryFormOneStep(G, p);
while success do
    $T := T_1 T$; $e := e + e_1$; // update transformation data
    success, G, $T_1$, $e_1$ := MinimizeBinaryFormOneStep(G, p);
end while;
return G, T, e;
```

This algorithm is available in Magma [BCP97] under the name `MinimizeAtP`.

Note that we use a geometric condition on the reduction $\bar{F}$ of F mod p (existence of a high-multiplicity factor) to restrict to essentially just one possibility for the minimization step. We will use a similar idea later when dealing with plane curves (the case $n = 2$).

To obtain a complete minimization procedure, we also have to determine a finite set of primes p at which the given form F might be unstable. We use the same geometric condition: either all of $a_0, a_1, \ldots, a_{\lfloor d/2 \rfloor}$ are divisible by p (this is the condition for $x_0^{\lceil (d+1)/2 \rceil}$ to divide $\bar{F}$), or, setting $f(x) = F(1, x)$, the divided derivatives

$$f,\ f',\ \frac{1}{2}f'',\ \frac{1}{3!}f''',\ \ldots,\ \frac{1}{\lfloor d/2 \rfloor !} f^{(\lfloor d/2 \rfloor)}$$

have a common root ξ mod p (then $(x_1 - \xi x_0)^{\lceil (d+1)/2 \rceil}$ divides $\bar{F}$). To find the primes satisfying the first condition, we determine the prime factors of the gcd of the relevant coefficients. To deal with the second condition, we use a Groebner basis computation to determine the positive generator of the intersection with $\mathbb{Z}$ of the ideal generated by the divided derivatives; its prime divisors are the relevant primes. For each of the finitely many primes p found in this way, we then apply MinimizeBinaryForm to F and p and replace F by the result (and keep track of the transformations made). This results in a minimal integral representative F_0 of the orbit of F (together with the transformation matrix and scaling factor used to obtain it).

This minimal form can still have quite large coefficients. So we want to find a matrix $T \in \mathrm{GL}(2, \mathbb{Z})$ such that ${}^T F_0$ has small coefficients. (Since T is unimodular, acting on F_0 by T does not affect the minimality property.) This is known as *reduction*; algorithms that perform it are described in [SC03, HS19].

A combination of minimization and reduction for binary forms with integral coefficients is available in Magma as `MinRedBinaryForm`.

3 Dominating weights

In this section n and d are fixed.

The following notion is key for the proofs of Theorems 1.5 and 1.6.

Definition 3.1. Let w and w' be two weight vectors. We say that w *dominates* w' if whenever $F \in \mathbb{Z}[x_0, \ldots, x_n]$ is a homogeneous polynomial of degree d that is unstable at p for a weight system (T, w'), then F is also unstable at p for the weight system (T, w).

This definition is independent of T; by considering ${}^T F$, we can take T to be the identity matrix $E = E_{n+1}$.

Since we can always adjust T by a permutation matrix, it suffices to consider weight vectors with weakly increasing entries. Also, since F is unstable at p for (T, w) if and only if F is unstable at p for $(T, w + \mathbf{1})$, where $\mathbf{1} = \mathbf{1}_{n+1}$ is the vector $[1, \ldots, 1]$ of length $n + 1$, it is sufficient to consider weight vectors $w = [w_0, \ldots, w_n]$ such that $0 = w_0 \leq w_1 \leq \cdots \leq w_n$. We denote by $W = W_n$ the set of these vectors.

The dominance relation is clearly transitive. A set $S \subset W$ of weight vectors is complete, if for every $w' \in W$ there is some $w \in S$ such that w dominates w'. We will see below that there is always a finite *minimal complete set of weight vectors* for our parameters n and d; 'minimal' here refers to minimality with respect to inclusion. Starting from any finite complete set S of weight vectors (for example, as provided by Theorems 1.5 or 1.6), we arrive at such a minimal set by successively selecting an element w of S and removing all elements from S other than w that are dominated by w, until no element of the remaining set dominates any other element.

We give a combinatorial description of the dominance relation. Let

$$J = J_{n,d} = \{i = [i_0, \ldots, i_n] \in \mathbb{Z}_{\geq 0}^{n+1} : i_0 + \cdots + i_n = d\}$$

be the index set for the monomials occurring in homogeneous polynomials of degree d in $n + 1$ variables. We write $F = \sum_{i \in J} a_i x^i$ (with the usual abbreviation $x^i = x_0^{i_0} \ldots x_n^{i_n}$). Then F is unstable at p for (E, w) if and only if

$$(n+1)v_p(a_i) > \langle d\mathbf{1} - (n+1)i, w \rangle = \langle v_i, w \rangle \tag{3.1}$$

for all $i \in J$, where $v_i = d\mathbf{1} - (n + 1)i$. Here $\langle \cdot, \cdot \rangle$ denotes the standard inner product. Since $v_p(a_i) \geq 0$, such a condition is vacuous if $\langle v_i, w \rangle < 0$. Otherwise, the condition is equivalent to

$$v_p(a_i) \geq \left\lfloor \frac{1}{n+1} \langle v_i, w \rangle \right\rfloor + 1 \,.$$

For $w \in W$, define the function

$$f_w \colon J \longrightarrow \mathbb{Z}_{\geq 0} \,, \quad i \longmapsto \max\left\{0, \left\lfloor \frac{\langle v_i, w \rangle}{n+1} \right\rfloor + 1\right\}.$$

Then F is unstable for (E, w) if and only if $v_p(a_i) \geq f_w(i)$ for all $i \in J$. This implies that w dominates w' if and only if $f_{w'} \geq f_w$ (pointwise). This description leads to an easy proof that a finite set of weight vectors is always sufficient.

Proposition 3.2. *Fix $n \geq 1$ and $d \geq 1$. Then there is a finite complete set of weight vectors for forms of degree d in $n + 1$ variables, and every minimal complete set of weight vectors for these parameters is finite.*

Proof. We can consider f_w as a point in $\mathbb{Z}_{\geq 0}^J$. Then w dominates w' if and only if $f_w \leq f_{w'}$ in the product order on $\mathbb{Z}_{\geq 0}^J$. By Dickson's Lemma (which follows from the fact that a polynomial ring in finitely many variables over a field is noetherian, applied to monomial ideals), the non-empty set $\{f_w : w \in W\} \subset \mathbb{Z}_{\geq 0}^J$ has finitely many minimal elements, and each element of the set is bounded below by a minimal one. The corresponding vectors w then form a finite complete set of weight vectors. The minimal complete sets of weight vectors are obtained by taking one $w \in W$ such that $f_w = s$ for each minimal element s of $\{f_w : w \in W\}$, so in particular, such a minimal set is finite (and all minimal complete sets of weight vectors for given parameters n and d have the same cardinality). □

Our combinatorial description also allows us to show that in many cases, there is a *unique* minimal complete set of weight vectors.

Lemma 3.3. *If $d \geq n+1$, then the map $W \to \mathbb{Z}_{\geq 0}^J$, $w \mapsto f_w$, is injective. In particular, the set*

$$S = \{w \in W : w \text{ is not dominated by any } w' \in W \setminus \{w\}\}$$

is the unique minimal complete set of weight vectors.

Proof. We have that

$$\left\lfloor \frac{1}{n+1} \langle v_i, w \rangle \right\rfloor = \left\lfloor \frac{d}{n+1} \sum_{j=0}^{n} w_j \right\rfloor - \langle i, w \rangle .$$

We write $\mathbf{e}_j$ for the jth standard basis vector in $\mathbb{Z}^{n+1}$ (with $j \in \{0, 1, \dots, n\}$) and set $\Sigma w := \sum_{j=0}^{n} w_j$. We find that

$$w_j = f_w(d\mathbf{e}_0) - f_w((d-1)\mathbf{e}_0 + \mathbf{e}_j) \qquad \text{if } w_j \leq \frac{d}{n+1} \Sigma w.$$

If $d \geq n+1$, the condition is satisfied for all j, and so we can recover w from f_w.

The last statement then follows from the description of the minimal sets in the proof of Proposition 3.2. □

We note that the map $W \to \mathbb{Z}_{\geq 0}^J$ is in general *not* injective when $d \leq n$. However, in concrete cases it can be checked explicitly whether a minimal complete set of weight vectors involves a weight vector that dominates and is dominated by another weight vector. If this is not the case, then there is still a unique minimal complete set of weight vectors.

We obtain the following simple sufficient condition for dominance.

Lemma 3.4. *Let $w', w \in W$. If $\langle v_i, w' \rangle \geq \langle v_i, w \rangle$ for all $i \in J$ such that $\langle v_i, w \rangle \geq 0$, then w dominates w'.*

Proof. Let $F = \sum_i a_i x^i$ be a polynomial that is unstable at p for (E, w'). Then we have that $(n+1)v_p(a_i) > \langle v_i, w' \rangle \geq \langle v_i, w \rangle$ for all $i \in J$ such that $\langle v_i, w \rangle \geq 0$, so F is also unstable for (E, w). □

Here is a geometric interpretation. For every $i \in J$, the condition '$\langle v_i, w \rangle \geq 0$' defines a closed half-space $H_i \subset \mathbb{R}^{n+1}$. For a given $w \in W$, let $C_w = \bigcap_{i \in J : w \in H_i} H_i$ denote the cone that is the intersection of the half-spaces containing w. Then all weights that lie in the shifted cone $w + C_w$ are dominated by w.

If we write the weight vectors as $[0, z_1, z_1 + z_2, \dots, z_1 + \dots + z_n]$ with $z_j \geq 0$, then we get a similar picture in $\mathbb{R}^n$ for the coordinates z_j. For $n = 2$ and some values of d, this is shown in Figure 1. We set $x = z_1$ and $y = z_2$. The light blue area is the region $x + y \leq d$; the cones in shades between green and red are shifted cones $w + C_w$ for the points w in the blue triangle. We see in each case that all lattice points in the positive quadrant are covered by these shifted cones (which sometimes degenerate into rays); this illustrates Theorem 1.5.

Remark 3.5. The criterion given in Lemma 3.4 is not an equivalence, since the left hand side in (3.1) is a multiple of $n+1$, which allows a slightly larger value of $\langle v_i, w\rangle$ than $\langle v_i, w'\rangle$ in some cases. For example, it turns out that for $n=2$, $d=4$, $[0,1,2]$ is actually dominated by $[0,1,1]$, even though the criterion of Lemma 3.4 is not satisfied. Here is a table of the values of $\langle v_i, w\rangle$ for $w=[0,1,1]$ and $w=[0,1,2]$.

i	004	013	022	031	040	103	112	121	130	202	211	220	301	310	400
$[0,1,1]$	<0	<0	<0	<0	<0	<0	<0	<0	<0	$\mathbf{2}$	2	2	5	5	8
$[0,1,2]$	<0	<0	<0	<0	0	<0	<0	0	3	$\mathbf{0}$	3	6	6	9	12

We see that the criterion of Lemma 3.4 is satisfied for all i except $i=[2,0,2]$. However, both $[0,1,1]$ and $[0,1,2]$ give the same condition $v_p(a_i)\geq 1$, and hence $[0,1,1]$ indeed dominates $[0,1,2]$. So the minimal complete set of weight vectors for this case is $\{[0,0,1],[0,1,1],[0,1,3]\}$ instead of $\{[0,0,1],[0,1,1],[0,1,2],[0,1,3]\}$.

When d is a multiple of $n+1$, however, then both sides are divisible by $n+1$, and thus the criterion is indeed an equivalence.

From now on, we will work with the coordinates $z_1,\dots,z_n$ in $\mathbb{R}^n$. In particular, we identify W_n with $\mathbb{Z}^n_{\geq 0}\subset\mathbb{R}^n$.

4 Proof of Theorem 1.5

Fix the degree d. The statement of Theorem 1.5 is equivalent to the claim that every weight vector $w=[0,z_1,z_1+z_2]$ with $z_1+z_2>d$ is dominated by another weight vector whose last coordinate is $\leq d$. We write $\|w\|=z_1+z_2$.

Since a weight vector w dominates all multiples mw with $m\geq 1$, we can assume that w is primitive, so $\gcd(z_1,z_2)=1$. We then have a one-to-one correspondence between primitive weight vectors and fractions z_2/z_1 between $0=0/1$ and $+\infty=1/0$. We will write ζ for the fraction associated to w in this way.

Let $I=\mathbf{[}\zeta,\zeta'\mathbf{]}$ be an interval with rational endpoints satisfying $0\leq\zeta<\zeta'\leq\infty$. (To avoid confusion with our notation for vectors, we use boldface square brackets to denote closed intervals.) We say that I is *basic* if $\zeta=a/b$, $\zeta'=a'/b'$ in lowest terms with $a'b-ab'=1$. It is well-known that every nonnegative rational number occurs as an endpoint of a basic interval and that if $c/d\in I$, then $[c,d]=k[a,b]+k'[a',b']$ with $k,k'\in\mathbb{Z}_{\geq 0}$.

To show that a given weight vector w is dominated by a weight vector w' with $\|w'\|\leq d$, we will use the criterion of Lemma 3.4. Consider some $i=[i_0,i_1,i_2]\in J=J_{2,d}$; then

$$\langle v_i, w\rangle=(2d-3i_1-3i_2)z_1+(d-3i_2)z_2=g(a_iz_1+b_iz_2),$$

where $g=\gcd(d-3i_1,d-3i_2)$ and $a_i=(2d-3i_1-3i_2)/g$, $b_i=(d-3i_2)/g$. Then $\langle v_i,w\rangle\geq 0$ for all w when $a_i,b_i\geq 0$ and $\langle v_i,w\rangle<0$ for all w when $a_i,b_i<0$. When $a_i\geq 0>b_i$, the condition on w to have $\langle v_i,w\rangle\geq 0$ is $\zeta\leq|a_i/b_i|$, whereas when $b_i\geq 0>a_i$, the condition is $\zeta\geq|a_i/b_i|$. We note that $g(|a_i|+|b_i|)\leq d$ in the first case and $\max\{g|a_i|,g|b_i|\}\leq d$ in the second case. We set

$$S_{\leq}=\left\{-\frac{a_i}{b_i}: i\in J, a_i\geq 0>b_i\right\}\quad\text{and}\quad S_{\geq}=\left\{-\frac{a_i}{b_i}: i\in J, b_i\geq 0>a_i\right\}.$$

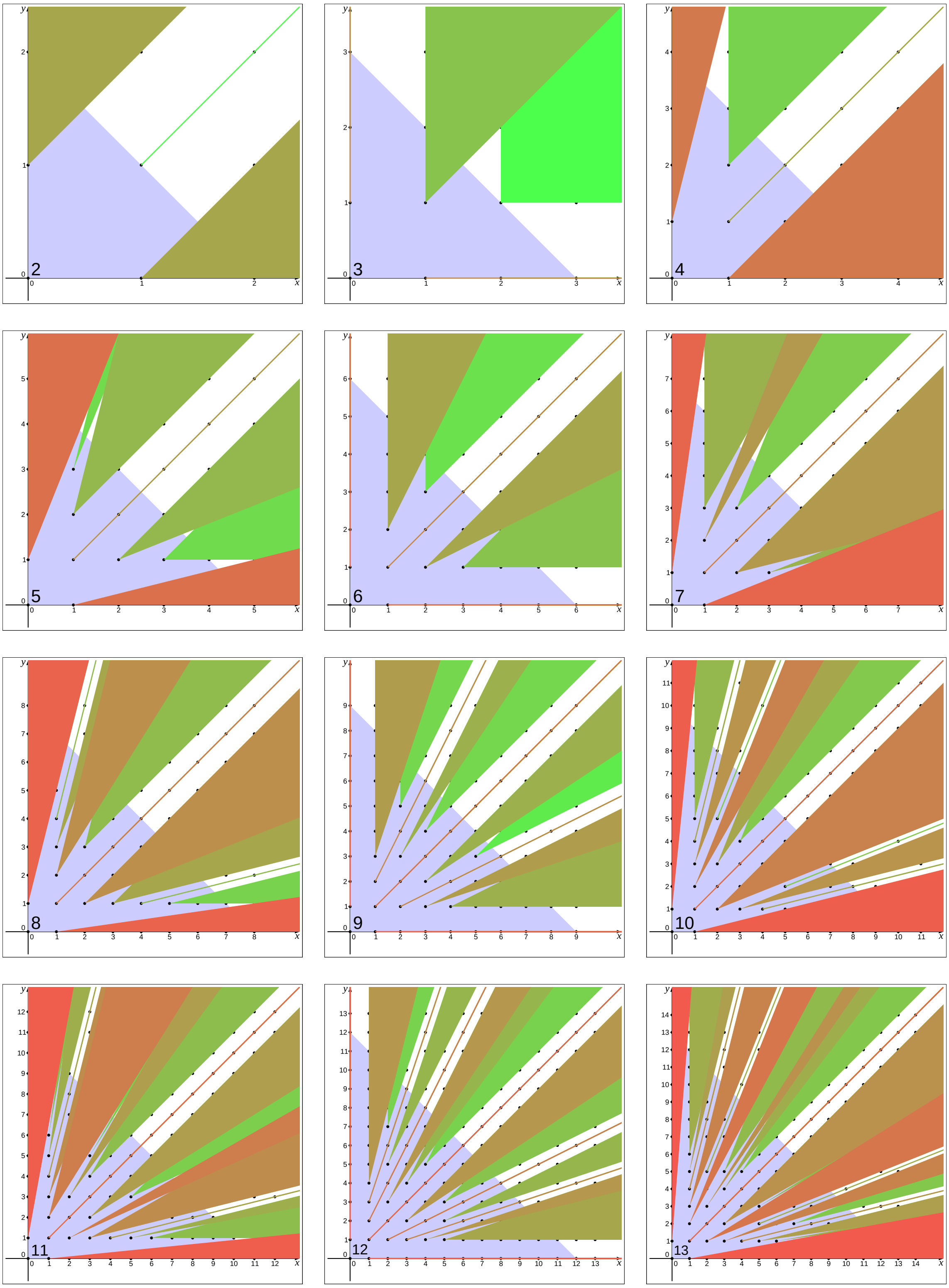

FIGURE 1. Complete set of weight vectors for $n = 2$ and $d = 2, 3, \ldots, 13$. The lattice points are $[z_1, z_2]$, corresponding to $w = [0, z_1, z_1 + z_2]$; the colored wedges contain the vectors dominated by their vertex.

Lemma 4.1. *Let $I = [\zeta_-, \zeta_+]$ be a basic interval and let w be a primitive weight vector such that $\zeta \in I$ for the associated fraction ζ. Write w_- and w_+ for the primitive weight vectors associated to ζ_- and ζ_+, respectively.*

If $I \cap S_\le \subset \{\zeta_+\}$ or $I \cap S_\ge \subset \{\zeta_-\}$, then w is dominated by w_- or by w_+.

Proof. If $\zeta = \zeta_-$ or $\zeta = \zeta_+$, then the claim is trivially true. So we now assume that $\zeta_- < \zeta < \zeta_+$; then $w = k_- w_- + k_+ w_+$ with $k_-, k_+ \in \mathbb{Z}_{\ge 1}$. We also assume that $I \cap S_\le \subset \{\zeta_+\}$; we claim that w_- dominates w in this case. We use the criterion of Lemma 3.4. So consider $i \in J$ such that $\langle v_i, w_- \rangle \ge 0$. Then not both of a_i and b_i can be negative. We claim that $\langle v_i, w_+ \rangle \ge 0$ as well. This is clear if $a_i, b_i \ge 0$ and also if $b_i \ge 0 > a_i$ (since $\zeta_+ > \zeta_-$). If $a_i \ge 0 > b_i$, let $\zeta_i = -a_i/b_i$; then $\zeta_i \in S_\le$ and the condition on w_- is $\zeta_- \le \zeta_i$. Our assumption on I then implies that $\zeta_i \ge \zeta_+$, so $\langle v_i, w_+ \rangle \ge 0$ as well. Now

$$\langle v_i, w \rangle = \langle v_i, w_- \rangle + \bigl((k_- - 1)\langle v_i, w_- \rangle + k_+ \langle v_i, w_+ \rangle\bigr) \ge \langle v_i, w_- \rangle ,$$

so the criterion is satisfied. In the case that $I \cap S_\ge \subset \{\zeta_-\}$, we show in the same way (mutatis mutandis) that w_+ dominates w. □

The idea for the proof of Theorem 1.5 is now to cover $[0, \infty]$ with basic intervals whose endpoints dominate everything in the interval. We use minimal basic intervals whose endpoints are fractions in lowest terms such that the sum of their numerator and denominator is bounded by d. This means that $I = [a_-/b_-, a_+/b_+]$ with

$$a_- + b_- \le d\,, \quad a_+ + b_+ \le d\,, \quad a_+ b_- - a_- b_+ = 1 \quad \text{and} \quad a_- + a_+ + b_- + b_+ > d\,.$$

It is clear that these intervals cover $[0, \infty]$. We show that Lemma 4.1 applies to each such interval. Since $\|w_-\|, \|w_+\| \le d$, the theorem then follows.

We first consider the case that d is a multiple of 3, so $d = 3\delta$ with $\delta \in \mathbb{Z}_{\ge 1}$. In this case g as defined above is always divisible by 3. It follows that

$$S_\le = \Bigl\{\frac{a}{b} : a, b \ge 0,\ a \perp b,\ a + b \le \delta\Bigr\} \quad \text{and} \quad S_\ge = \Bigl\{\frac{a}{b} : a, b \ge 0,\ a \perp b,\ a, b \le \delta\Bigr\}.$$

Here we write $a \perp b$ to denote that a and b are coprime. Since $a + b \le 2\delta < d$ in both cases, this implies that I can meet $S_\le \cup S_\ge$ at most in its endpoints. We have to rule out the possibility that $\zeta_- \in S_\le$ and $\zeta_+ \in S_\ge$. But then we would have that

$$d < a_- + a_+ + b_- + b_+ \le \delta + 2\delta = d\,,$$

a contradiction. So Lemma 4.1 is always applicable.

Now we consider the case that d is not divisible by 3. Then

$$g a_i = 2d - 3(i_1 + i_2) \equiv -d \bmod 3 \quad \text{and} \quad g b_i = d - 3 i_2 \equiv d \bmod 3\,.$$

We deduce that

$$S_\le = S_\le^{\text{small}} \cup S_\le^{\text{large}} \qquad \text{and} \qquad S_\ge = S_\ge^{\text{small}} \cup S_\ge^{\text{large}}$$

with

$$\begin{aligned}
S_{\leq}^{\text{large}} &= \left\{ \frac{a}{b} : a, b \geq 0,\ a \perp b,\ a \equiv b \equiv -d \bmod 3,\ a + b \leq d \right\}, \\
S_{\leq}^{\text{small}} &= \left\{ \frac{a}{b} : a, b \geq 0,\ a \perp b,\ a \equiv b \equiv d \bmod 3,\ a + b \leq \frac{d}{2} \right\}, \\
S_{\geq}^{\text{large}} &= \left\{ \frac{a}{b} : a, b \geq 0,\ a \perp b,\ a \equiv b \equiv d \bmod 3,\ a, b \leq d \right\}, \\
S_{\geq}^{\text{small}} &= \left\{ \frac{a}{b} : a, b \geq 0,\ a \perp b,\ a \equiv b \equiv -d \bmod 3,\ a, b \leq \frac{d}{2} \right\}.
\end{aligned}$$

We see that $I \cap S_{\leq}$ consists of endpoints of I. If $\zeta_- \notin S_{\leq}$, then we can apply Lemma 4.1. So we assume now that $\zeta_- \in S_{\leq}$, and we want to show that $I \cap S_{\geq} \subset \{\zeta_-\}$. If this is not the case, then there is $\zeta \in S_{\geq}$ with $\zeta_- < \zeta \leq \zeta_+$. Writing $\zeta = a/b$ in lowest terms, we then have that $[a, b] = k_-[a_-, b_-] + k_+[a_+, b_+]$ with $k_- \in \mathbb{Z}_{\geq 0}$ and $k_+ \in \mathbb{Z}_{\geq 1}$ coprime. The congruence conditions mod 3 imply that the determinant

$$\begin{vmatrix} a & a_- \\ b & b_- \end{vmatrix} = k_- \begin{vmatrix} a_- & a_- \\ b_- & b_- \end{vmatrix} + k_+ \begin{vmatrix} a_+ & a_- \\ b_+ & b_- \end{vmatrix} = k_+$$

is divisible by 3. This implies that $k_- \geq 1$ and $k_+ \geq 3$, so $a + b \geq a_- + a_+ + b_- + b_+ > d$; in particular, $\zeta \in S_{\geq}^{\text{large}}$. If $k_- = 1$, then $[a, b] \equiv [a_-, b_-] \bmod 3$, so $\zeta_- \in S_{\leq}^{\text{small}}$. Then $a_+ + b_+ > d - (a_- + b_-) \geq d/2$, and it follows that

$$a + b \geq (a_- + a_+ + b_- + b_+) + 2(a_+ + b_+) > 2d\,,$$

a contradiction. If $k_- \geq 2$, then

$$a + b \geq 2(a_- + a_+ + b_- + b_+) > 2d\,,$$

a contradiction again. So in both cases, we find that $I \cap S_{\geq} \subset \{\zeta_-\}$, and so we can again apply Lemma 4.1. This finishes the proof.

It is not hard to turn the proof given here into an algorithm that computes a complete set of weight vectors for plane curves of any given degree d. We can then extract the minimal complete set of weight vectors from it by removing weight vectors that are dominated by some other vector in the set. We have computed minimal complete sets of weight vectors for all $d \leq 150$. In Figure 2 we show the difference between the largest entry in one of the weight vectors and d. This difference is ≤ 0 by Theorem 1.5. Write $m(d)$ for the largest entry. For $d \leq 150$, we see that $m(d) = d - 2$ when $d \equiv 3 \bmod 6$ and $d \geq 15$ and that $m(d) = d - 5$ when $d \equiv 0 \bmod 6$ and $d \geq 18$. This can be shown to be true in general by considering the possibilities for $\zeta_- \in S_{\leq}$ and $\zeta_+ \in S_{\geq}$ when $a_- + a_+ + b_- + b_+$ is close to $d = 3\delta$ in the proof above. It is helpful that when d is divisible by 3, the descriptions of $S_{\leq}$ and $S_{\geq}$ are rather simple, and that Lemma 3.4 actually characterizes dominance.

When d is not divisible by 3, the values $m(d) - d$ do not seem to follow a simple pattern. In any case, they appear to get more and more negative as d increases.

5 Proof of Theorem 1.6

We fix n and d. Our goal will be to show that every $w' \in W$ is dominated by some vector in W whose largest entry is at most $2nd^{n-1}/\gcd(d, n + 1)$; this then implies the statement of Theorem 1.6.

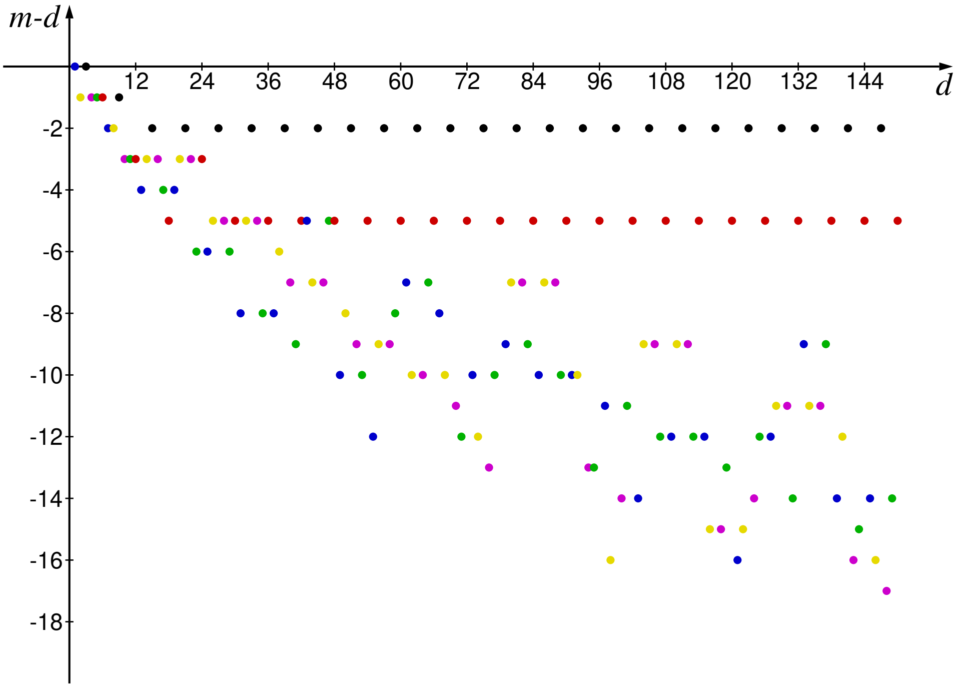

FIGURE 2. Values of $m-d$ where m is the largest entry occurring in some vector in the minimal complete set of weight vectors for plane curves of degree d, for $1 \leq d \leq 150$. The data points are color-coded according to $d \bmod 6$.

We formalize the situation a bit more.

Definition 5.1. A *cone collection* in $\mathbb{R}^n$ is a set $\mathcal{C}$ of closed cones in $\mathbb{R}^n$ (with vertex at the origin) such that

(1) the intersection of any two cones in $\mathcal{C}$ is again in $\mathcal{C}$ and
(2) $\bigcup \mathcal{C} \supset \mathbb{R}^n_{\geq 0}$.

If $\mathcal{C}$ is a cone collection and $w \in \mathbb{R}^n_{\geq 0}$, then there is a smallest cone in $\mathcal{C}$ containing w (by the first property above). We call it the *minimal cone of w* (w.r.t. $\mathcal{C}$) and write it $\mathcal{C}(w)$.

For example, any set $\mathcal{H}$ of closed half-spaces in $\mathbb{R}^n$ whose union contains $\mathbb{R}^n_{\geq 0}$ defines a cone collection. It consists of all intersections of subsets of $\mathcal{H}$.

Definition 5.2. The cone collection defined by the set of closed half-spaces $\langle v_i, w \rangle \geq 0$ for $i \in J_{n,d}$ is the *collection of weight cones* (for n and d), $\mathcal{W}_{n,d}$.

Definition 5.3. Let $\mathcal{C}$ be a cone collection in $\mathbb{R}^n$. A subset $S \subset \mathbb{Z}^n_{\geq 0}$ is *complete for $\mathcal{C}$* if

$$\mathbb{Z}^n_{\geq 0} \subset \bigcup_{s \in S} \bigl(s + \mathcal{C}(s)\bigr) .$$

Lemma 3.4 then says the following.

Corollary 5.4. *If a subset $S \subset \mathbb{Z}^n_{\geq 0}$ is complete for $\mathcal{W}_{n,d}$, then S is a complete set of weights for dimension n and degree d.*

We now prove a lemma that gives us a bound on the sizes of the vectors in a minimal dominating set for the relative interior C^0 of a cone C in terms of the sizes of the vectors spanning the cone. We measure the 'size' of a vector v in terms of the absolute value of the sum Σv of the entries.

Lemma 5.5. *Let $C \subset \mathbb{R}^n$ be a polyhedral cone spanned by integral vectors $u_1, \dots, u_m$ such that $0 \le \Sigma u_j \le a$ for $j = 1, \dots, m$. Assume that C has dimension $k \le n$. Then for every $z \in \mathbb{Z}^n \cap C^0$, there is $z' \in \mathbb{Z}^n \cap C^0$ such that $\Sigma z' \le ka$ and $z \in z' + C$.*

Proof. It suffices to show that if $z \in \mathbb{Z}^n \cap C^0$ with $\Sigma z > ka$, then there is some j such that $z' = z - u_j \in C^0$ and $\Sigma u_j > 0$. (Then $z \in z' + C$ and $\Sigma z' < \Sigma z$; by induction we reach $\Sigma z' \le ka$.) Since $z \in C^0$, we can write $z = \sum_{j=1}^m \lambda_j u_j$ with all $\lambda_j > 0$. Pick $\varepsilon > 0$ such that $\lambda_j > \varepsilon$ for all j and such that $\Sigma z > ka + \varepsilon \sum_{j=1}^m \Sigma u_j$. The point $z^* = z - \varepsilon \sum_{j=1}^m u_j$ is still in C, hence it is in the closed cone spanned by some subset of k vectors u_j; we can assume that they are $u_1, \dots, u_k$. We therefore have $z^* = \sum_{j=1}^k \mu_j u_j$ with $\mu_j \ge 0$. Now we observe that

$$ka < \Sigma z^* = \sum_{j=1}^k \mu_j \Sigma u_j \le \sum_{j=1}^k \mu_j a$$

and conclude that one of the μ_j such that $\Sigma u_j > 0$, say μ_{j_0}, must be greater than 1. But then $z^* - u_{j_0}$ is still a nonnegative linear combination of the u_j, and $z - u_{j_0}$ is a linear combination of $u_1, \dots, u_m$ with all coefficients positive, hence $z' = z - u_{j_0} \in C^0$. □

Note that the bound in the lemma is sharp, as can be seen by taking $C = \mathbb{R}^n_{\ge 0}$, which is spanned by the standard basis vectors of size 1, but for which we need to take $z' = \mathbf{1}_n$ of size $n = \dim C$.

The cone collection $\mathcal{W}_{n,d}$ can contain minimal cones of vectors such that one cone is properly contained in the other, but they have the same dimension. This makes $\mathcal{W}_{n,d}$ somewhat unwieldy to work with. We remedy this by 'regularizing' our cone collection in some sense. We first introduce the following notion.

Definition 5.6. Let $\mathcal{C}$ and $\mathcal{C}'$ be two cone collections. We say that $\mathcal{C}$ *refines* $\mathcal{C}'$ if every cone of $\mathcal{C}$ is contained in a cone of $\mathcal{C}'$.

Lemma 5.7. *Let $\mathcal{C}$ and $\mathcal{C}'$ be two cone collections such that $\mathcal{C}$ refines $\mathcal{C}'$, and let S be a complete set for $\mathcal{C}$. Then S is also a complete set for $\mathcal{C}'$.*

Proof. For every $s \in \mathbb{Z}_{\ge 0}$, we have that $\mathcal{C}(s) \subset \mathcal{C}'(s)$. Hence

$$\mathbb{Z}^n_{\ge 0} \subset \bigcup_{s \in S} \big(s + \mathcal{C}(s)\big) \subset \bigcup_{s \in S} \big(s + \mathcal{C}'(s)\big) . \qquad \square$$

If $\mathcal{C}$ is defined by a set of closed half-spaces, then any larger set of closed half-spaces defines a refinement of $\mathcal{C}$. We refine $\mathcal{W}_{n,d}$ by including the 'opposite' half-spaces.

Definition 5.8. We let $\widetilde{\mathcal{W}}_{n,d}$ be the refinement of $\mathcal{W}_{n,d}$ that is generated by the set of closed half-spaces given by

$$\langle v_i, w \rangle \ge 0 \quad \text{or} \quad \langle v_i, w \rangle \le 0$$

for all $i \in J_{n,d}$, together with $\sum_{j=1}^n z_j \ge 0$.

We now prove the following proposition, which by Lemma 5.7 and Corollary 5.4 implies the statement of Theorem 1.6 for general n and d.

Proposition 5.9. *The set*

$$S_{n,d} = \left\{(z_1, \dots, z_n) \in \mathbb{Z}^n_{\geq 0} : z_1 + \cdots + z_n \leq \frac{2nd^{n-1}}{\gcd(d, n+1)}\right\}$$

is complete for $\widetilde{W}_{n,d}$.

Proof. In terms of the coordinates $z_1, \dots, z_n$, we have for $i \in J_{n,d}$ (using $\sum_j i_j = d$)

$$\begin{aligned}\left\langle d\mathbf{1}_{n+1} - (n+1)i, w\right\rangle &= \sum_{j=0}^{n} (d - (n+1)i_j) \sum_{k=1}^{j} z_k \\ &= \sum_{k=1}^{n} \sum_{j=k}^{n} (d - (n+1)i_j) z_k \\ &= \sum_{k=1}^{n} \Big((n+1) \sum_{j=0}^{k-1} i_j - kd\Big) z_k \,.\end{aligned}$$

Each $i \in J = J_{n,d}$ defines a hyperplane and a half-space in $\mathbb{R}^n$. The rays that occur as intersections of $n-1$ independent such hyperplanes are spanned by integer vectors whose entries are obtained as $(n-1) \times (n-1)$ minors of the $(n-1) \times n$ matrix whose rows are the coefficient vectors defining the hyperplanes. Let

$$I = (i^{(1)}, \dots, i^{(n-1)}) \in J_{n,d}^{n-1}$$

be a linearly independent family and define A_I to be the corresponding matrix. Then

$$A_I = (n+1)B_I - d\mathbf{1}_{n-1}^\top \cdot \mathbf{k}$$

with $\mathbf{k} = [1, 2, \dots, n]$ and $B_I = \left(\sum_{j=0}^{k-1} i_j^{(l)}\right)_{1 \leq l \leq n, 1 \leq j \leq n-1}$. If for a matrix M, $M^{[j]}$ denotes M with the jth column removed, then a vector spanning the intersection of the relevant hyperplanes is

$$\tilde{v}_I = \left[(-1)^j \det A_I^{[j]}\right]_{1 \leq j \leq n} = \left[(-1)^j \det\big((n+1)B_I^{[j]} - d\mathbf{1}_{n-1}^\top \cdot \mathbf{k}^{[j]}\big)\right]_{1 \leq j \leq n}.$$

Now

$$\det\big((n+1)B_I^{[j]} - d\mathbf{1}_{n-1}^\top \cdot \mathbf{k}^{[j]}\big) = (n+1)^{n-1} \det B_I^{[j]} - (n+1)^{n-2} d \sum_{k \neq j} k \det \tilde{B}_I^{[j,k]},$$

where $\tilde{B}_I^{[j,k]}$ is the matrix B_I with the kth column replaced by all ones and the jth column removed. We see that all entries of $\tilde{v}_I$ are divisible by $(n+1)^{n-2} \gcd(d, n+1)$. We set

$$v_I = \frac{1}{(n+1)^{n-2} \gcd(d, n+1)} \tilde{v}_I \in \mathbb{Z}^n.$$

We are interested in the maximal absolute value of the sum of the entries of v_I. Recall the notation Σv for the sum of the entries of a vector v. The sum Σv_I is affine linear as a function of each entry in I separately (it is the determinant of the matrix A_I with the row $\mathbf{1}_n$ added, up to the factor of $(n+1)^{n-2} \gcd(d, n+1)$ that we have removed; the

lth row of A_I is an affine linear function of $i^{(l)}$), therefore it takes its extremal values when the $i^{(l)}$ are extremal (and linearly independent) points in the simplex

$$\{i \in \mathbb{R}^{n+1} : i_0, \dots, i_n \geq 0, i_0 + \cdots + i_n = d\}.$$

This means that for such an extremal value, B_I arises from the $(n+1) \times n$ matrix

$$B = d \begin{bmatrix} 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & \cdots & 1 & 1 \\ \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 1 & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix}$$

by removing two rows, so A_I arises from $A = (n+1)B - d\mathbf{1}_{n+1}^{\top} \cdot \mathbf{k}$ in the same way. To get $\Sigma\tilde{v}_I$, we add the row $\mathbf{1}_n$ at the top of A_I and take the determinant. This determinant is unchanged when we multiply the matrix from the right by the $n \times n$ matrix

$$C = \begin{bmatrix} 1 & -1 & 0 & \cdots & 0 \\ 0 & 1 & -1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & -1 \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}.$$

(This is essentially going back from the z coordinates to the w coordinates.) We obtain the determinant of the following matrix with two rows (but not the first one) removed.

$$\begin{bmatrix} \mathbf{1}_n \\ A \end{bmatrix} C = \begin{bmatrix} \mathbf{1}_n C \\ (n+1)BC - d\mathbf{1}_{n+1}^{\top} \cdot \mathbf{k}C \end{bmatrix} = \begin{bmatrix} 1 & \mathbf{0}_{n-1} \\ dn & -d\mathbf{1}_{n-1} \\ -d\mathbf{1}_{n-1}^{\top} & d(n+1)E_{n-1} - d\mathbf{1}_{n-1}^{\top} \cdot \mathbf{1}_{n-1} \\ -d & -d\mathbf{1}_{n-1} \end{bmatrix}$$

Here E_m denotes the $m \times m$ identity matrix. We can remove the first column and first row without changing the value of the determinant. The remaining matrix has two equal rows, so to get a nonzero determinant, at least one of them has to be removed. So what we are looking at is d^{n-1} times the $(n-1) \times (n-1)$ minors of the $n \times (n-1)$ matrix

$$D = \begin{bmatrix} (n+1)E_{n-1} - \mathbf{1}_{n-1}^{\top} \cdot \mathbf{1}_{n-1} \\ -\mathbf{1}_{n-1} \end{bmatrix}.$$

Such a minor is $\pm(n+1)^{n-2}$ when the last row is included, whereas the remaining minor has the value $2(n+1)^{n-2}$. We conclude that

$$|\Sigma v_I| = \frac{|\Sigma\tilde{v}_I|}{(n+1)^{n-2}\gcd(d, n+1)} \leq \frac{2d^{n-1}}{\gcd(d, n+1)}.$$

The cones of the cone collection $\widetilde{\mathcal{W}}_{n,d}$ are closed polyhedral cones C that are spanned by vectors $\pm v_I$ for suitable tuples I, plus perhaps by some vectors in the hyperplane $\sum z_j = 0$.

Since the hyperplanes themselves and their intersections are elements of $\widetilde{\mathcal{W}}_{n,d}$, it follows that the cone $\widetilde{\mathcal{W}}_{n,d}(w)$ is the unique cone C in the collection that contains w in its relative interior C^0.

We apply Lemma 5.5 to each of the cones in $\widetilde{\mathcal{W}}_{n,d}$, which as we have seen are spanned by vectors v with $\Sigma v \leq 2d^{n-1}/\gcd(d, n+1)$. The lemma shows that everything in the relative interior of each of these cones C is dominated by some vector of size at most $2(\dim C)d^{n-1}/\gcd(d, n+1) \leq 2nd^{n-1}/\gcd(d, n+1)$. Recall that $S_{n,d}$ denotes the subset of $\mathbb{Z}_{\geq 0}$ of vectors w with $\Sigma w \leq 2nd^{n-1}/\gcd(d, n+1)$. We conclude that

$$\mathbb{Z}^n_{\geq 0} = \bigcup_{C\in\widetilde{\mathcal{W}}_{n,d}} (\mathbb{Z}^n_{\geq 0} \cap C^0) \subset \bigcup_{C\in\widetilde{\mathcal{W}}_{n,d}} \bigcup_{s\in C^0\cap S_{n,d}} (s + C) = \bigcup_{s\in S_{n,d}} (s + \widetilde{\mathcal{W}}_{n,d}(s)).$$

This proves Proposition 5.9. □

Remark 5.10. In our proof, we throw away some information: the cones $\mathcal{W}_{n,d}(w)$ are in general larger than $\widetilde{\mathcal{W}}_{n,d}(w)$. The difference is shown in Figure 3 in the case $n = 2$, $d = 5$. On the left, the relevant half-planes are shown, with the resulting shifted cones covering the weight vectors dominated by the vertex. On the right, the fan resulting from the subdivision by all the rays is shown, together with the resulting shifted cones. We see that the maximal weight needed for a complete covering increases from 4 to 7. (In particular, it is larger than $d^{n-1} = 5$.)

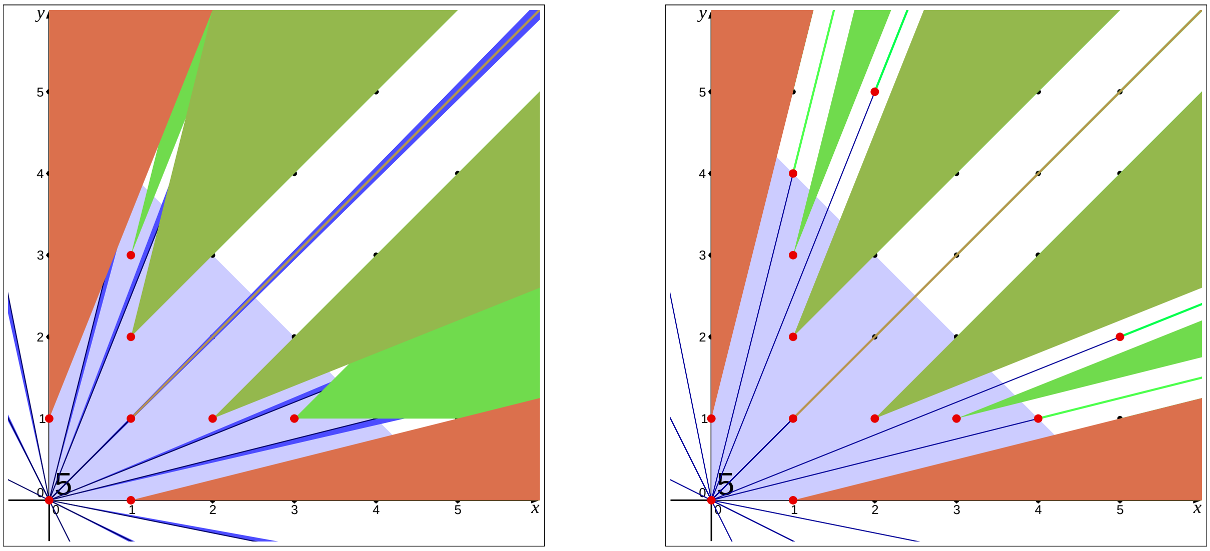

FIGURE 3. Illustration for Remark 5.10

This is likely related to the factor 2 that arises in the largest minor of the matrix D. To get rid of that seems to necessitate working with the original cone collection $\mathcal{W}_{n,d}$ instead of the refinement.

There is also the factor of n that comes from Lemma 5.5.

Remark 5.11. In any case, our result leads to an algorithm that determines the minimal complete set of weights for given dimension n and degree d. We initialize S to be the set of primitive weight vectors in $S_{n,d}$. Then we successively take some $w \in S$ (in some order such that the last coordinate $w_n = z_1 + \cdots + z_n$ weakly increases) and eliminate all vectors from S that are dominated by w.

6 Effective minimization

As discussed in Remark 5.11 above, we can determine the minimal complete set of weight vectors relevant for a reduction algorithm for hypersurfaces of degree d in $\mathbb{P}^n$.

Table 1 gives some examples. (In all these cases, the minimal complete set of weight vectors is unique, even when $d \leq n$.) The list for plane cubics recovers [CFS10, Lemma 4.4]. We note that the minimal complete set of weights for cubic surfaces is already mentioned (without proof) in [Kol97, Prop. 6.4.2].

case	minimal complete set of weight vectors
conic	$[0,0,1], [0,1,1]$
plane cubic	$[0,0,1], [0,1,1], [0,1,2], [0,2,3]$
plane quartic	$[0,0,1], [0,1,1], [0,1,3]$
plane quintic	$[0,0,1], [0,1,1], [0,1,2], [0,1,3], [0,2,3], [0,3,4]$
quadric surface	$[0,0,0,1], [0,0,1,2], [0,1,1,1]$
cubic surface	$[0,0,0,1], [0,0,1,1], [0,1,1,1], [0,1,2,2], [0,2,2,3]$
quadric in $\mathbb{P}^4$	$[0,0,0,1,1], [0,0,1,1,2], [0,1,1,1,1]$

TABLE 1. Minimal complete sets of weight vectors for certain classes of hypersurfaces.

For any given weight vector w, it is a finite problem to determine whether a given form F is unstable for (T, w) for a suitable unimodular matrix T. This is a consequence of the following result. Note that this is where in the more general setting of a DVR we have to assume that the residue class field is finite.

Lemma 6.1. *Let $w \in \mathbb{Z}_{\geq 0}^{n+1}$ be a weight vector; we write $M_w = \operatorname{diag}(p^{w_0}, \ldots, p^{w_n})$ for the diagonal matrix with entries the powers of p given by w. We set $G = \mathrm{GL}(n+1, \mathbb{Z})$ and define $G_w = G \cap M_w^{-1} G M_w$. Then G_w is a finite-index subgroup of G. Let $F \in \mathbb{Z}[x_0, \ldots, x_n]$ and $T \in G_w$; write $F' = {}^T F$. Then we have that*

$$v_p(F'(p^{w_0}x_0, \ldots, p^{w_n}x_n)) = v_p(F(p^{w_0}x_0, \ldots, p^{w_n}x_n)) .$$

Proof. Let $m = \max\{w_0, \ldots, w_n\}$. Then any $T \in G$ such that $T \equiv E_{n+1} \bmod p^m$ is in G_w. Since the principal congruence subgroup mod p^m has finite index in G, the same is true of G_w.

Now consider F and T as in the statement above. Let $T' = M_w T M_w^{-1} \in G$. Note that $F(p^{w_0}x_0, \ldots, p^{w_n}x_n) = {}^{M_w}F$. We then have that

$$\begin{aligned} v_p(F'(p^{w_0}x_0, \ldots, p^{w_n}x_n)) &= v_p({}^{M_w}F') = v_p({}^{M_w T}F) = v_p({}^{T' M_w}F) = v_p({}^{T'}({}^{M_w}F)) \\ &= v_p({}^{M_w}F) = v_p(F(p^{w_0}x_0, \ldots, p^{w_n}x_n)) . \end{aligned}$$ □

It follows that when F is unstable for the weight system (T, w), then F is also unstable for every weight system (T', w) with $T' \in G_w T$. To check whether F is unstable for w, it is therefore sufficient to test one representative of each coset of G_w in G. Since G_w has finite index in G, this is a finite problem. Assuming as usual that $w_0 \leq w_1 \leq \ldots \leq w_n$, the condition for T to be in G_w is that the reduction of T mod p is a block lower triangular matrix, and each (i, j) entry above the diagonal must be divisible by $p^{w_j - w_i}$. In particular, the coset is determined by the reduction of T modulo p^{w_n}.

In our algorithms, we will make use of the following procedure. The input consists of a form $F \in \mathbb{Z}[x_0, \ldots, x_n]$ of degree d, a unimodular matrix T of size $n+1$, a weight vector $w \in W_n$ and the prime p.

ApplyWeight(F, T, w, p)

```
  $F_1 := {}^{T}F$;
  $F_2 := F_1(p^{w_0}x_0, p^{w_1}x_1, \ldots, p^{w_n}x_n)$;
  $e := v_p(F_2)$;
  return $p^{-e}F_2$, $e$.
```

We say that w *applies to* F, if there is a T such that $e > d\Sigma w/(n+1)$ in the above. This is shorthand for saying that F is unstable with respect to (T, w) for some unimodular matrix T.

Definition 6.2. An *invariant* of forms of degree d in $n+1$ variables is a homogeneous polynomial I with integral coefficients in the coefficients of the form F such that $I({}^{T}F) = I(F)$ for all $T \in SL(n+1)$.

Definition 6.3. A form $F \in k[x_0, \ldots, x_n]$ of degree d over a field k is *semistable* if it is not a 'nullform' in the sense of Hilbert [Hil93a], i.e., there is an invariant I of forms of degree d in $n+1$ variables such that $I(F) \neq 0$. (This agrees with the notion of semistability in Geometric Invariant Theory [Mum77, Table 1].) Otherwise, F is *unstable*.

Proposition 6.4. *There is an algorithm that, given a semistable form* $F \in \mathbb{Z}[x_0, \ldots, x_n]$ *of degree* d *and a prime* p*, computes a matrix* $T \in GL(n+1, \mathbb{Q}) \cap Mat(n+1, \mathbb{Z})$ *and* $e \in \mathbb{Z}_{\geq 0}$ *such that* $p^{-e} \cdot {}^{T}F$ *has coefficients in* $\mathbb{Z}$ *and is minimal at* p.

Proof. By Theorems 1.5 (for $n = 2$) or 1.6 (in general), we can effectively find a complete set S of weight vectors for forms of degree d in $n+1$ variables. For a given $w \in S$, we can determine a finite set T_w of coset representatives for G_w by Lemma 6.1. Let $P_{n,d} = \bigcup_{w \in S} T_w \times \{w\}$. The algorithm then is as follows.

```
MinimizeForm(F, p)
  $d := \deg(F)$; $n :=$(number of variables in F) $-1$;
  $T := E_{n+1}$; $e := 0$; // initialize transformation data
  success := true; // flag indicating if a minimization step was successful
  while success do
    success := false; // no success yet in this round
    for $(T_1, w) \in P_{n,d}$ do
      $F_1, e_1 :=$ ApplyWeight$(F, T_1, w, p)$;
      if $(n+1)e_1 > d\Sigma w$ then
        // minimization step successful
        $F := F_1$; $T := T_1 T$; $e := e + e_1$; // update data
        success := true;
      end if;
    end for;
  end while;
  return $F, T, e$;
```

When F is not unstable at p for any $(T, w) \in P_{n,d}$, then F is minimal at p. So when the algorithm terminates, the return values satisfy the specification. Since F is semistable, there is some invariant $I(F)$ of F that is nonzero. Since $I(F) \in \mathbb{Z}$ and $v_p(I(F_1)) < v_p(I(F))$ when F_1 is obtained from F by a successful minimization step, the procedure must terminate after finitely many passes through the loop. □

In practice, running through all the cosets would be much too inefficient: their number grows like a power of p. Therefore we look for necessary 'geometric' conditions the form F has to satisfy for a minimization step to be possible. We will see in the next section that this can be done in the case $n = 2$ of plane curves.

7 Minimization of plane curves at a prime p

In this section we explain how one can construct an algorithm that minimizes a (semistable) plane curve of any degree d at a prime p. There are two main ingredients.

The first ingredient is that we can split a minimization step with respect to some weight vector w into a succession of steps with respect to the simplest weight vectors $[0, 0, 1]$ and $[0, 1, 1]$. During these intermediate steps, the current form will not be 'more minimal' than the original one, but the last step will make it so (if the form can indeed be strictly minimized). We are thus led to explore a tree of steps of this kind, until we either find a more minimal form (then we restart the procedure with the new form), or else can determine that progress is impossible; this is based on the bound from Theorem 1.5.

The second ingredient consists in establishing a geometric criterion in terms of the singular locus of the reduction of the curve mod p that reduces the set of 'directions' (corresponding to the cosets of G_w in Lemma 6.1) that we have to consider for each of the two simple weight vectors to an easily computable set of size bounded in terms of the degree d only; in particular, this bound does not depend on p.

We note that the minimization algorithm for plane cubics given in [CFS10, Theorem 4.3] proceeds along similar lines.

The key result underlying this approach is as follows.

Proposition 7.1. *Let $F \in \mathbb{Z}[x_0, x_1, x_2]$ be a form of degree d that is unstable at p for the weight system $(E, [0, w_1, w_2])$ with $0 \le w_1 \le w_2$ and $w_2 > 0$, so that $t := w_1/w_2 \in [0, 1]$. We set*

$$v_{011}(F) = v_p\bigl(F(x_0, px_1, px_2)\bigr) \quad \textit{and} \quad v_{001}(F) = v_p\bigl(F(x_0, x_1, px_2)\bigr) .$$

Then

$$v_{011}(F) > (1 + t)\frac{d}{3} \qquad \textit{and} \qquad v_{001}(F) > \max(0, 1 - 2t)\frac{d}{3} .$$

Proof. Write $F = \sum_{i+j+k=d} a_{i,j,k} x_0^i x_1^j x_2^k$. By assumption, we have

$$v_p\bigl(F(x_0, p^{w_1}x_1, p^{w_2}x_2)\bigr) \ge e = \left\lfloor \frac{w_1 + w_2}{3} d \right\rfloor + 1 > \frac{w_1 + w_2}{3} d ,$$

so $v_p(a_{i,j,k}) \ge \max(0, e - w_1 j - w_2 k)$. From this we get

$$\begin{aligned}
v_{011}(F) &= \min\{i + v_p(a_{d-i,j,i-j}) : 0 \le j \le i \le d\} \\
&\ge \min\{i + \max(0, e - w_1 j - w_2(i - j)) : 0 \le j \le i \le d\} \\
&= \min\{i + \max(0, e - w_2 i) : 0 \le i \le d\} \qquad (\text{as } w_1 \le w_2) \\
&\ge \frac{e}{w_2} \qquad (\text{this is the minimum for } i \in \mathbb{R} \text{ such that } 0 \le i \le d) \\
&> \frac{w_1 + w_2}{w_2}\frac{d}{3} = (1 + t)\frac{d}{3} .
\end{aligned}$$

This proves the first claim. The second claim is clear when $t > \frac{1}{2}$. Otherwise, we get in a similar way

$$\begin{aligned} \nu_{001}(F) &= \min\{i + \nu_p(a_{d-j,j-i,i}) : 0 \le i \le j \le d\} \\ &\ge \min\{i + \max(0, e - w_1(j-i) - w_2 i) : 0 \le i \le j \le d\} \\ &= \min\{i + \max(0, e - w_1 d - (w_2 - w_1)i) : 0 \le i \le d\} \\ &\ge \frac{e - w_1 d}{w_2 - w_1} > \frac{w_2 - 2w_1}{w_2 - w_1}\frac{d}{3} = \frac{1-2t}{1-t}\frac{d}{3} \ge (1-2t)\frac{d}{3}\,. \end{aligned}$$
□

Remark 7.2. It is easily seen that $\nu_{011}(F)$ is a lower bound for the multiplicity of the point $[1:0:0]$ on the reduction of the curve $F = 0$ and that $\nu_{001}(F)$ is a lower bound for the multiplicity of the line $x_2 = 0$ as a component of the reduction of $F = 0$. So Proposition 7.1 implies a similar statement, where $\nu_{011}(F)$ is replaced by the multiplicity of $[1:0:0]$ and $\nu_{001}(F)$ is replaced by the multiplicity of $x_2 = 0$ with respect to the reduction of the curve.

We can view changing the model of a plane curve as moving from one $\mathbb{Z}_p$-lattice in $\mathbb{Q}_p^3$ to another one, where the original lattice is generated by the standard basis and we express the form F on a basis of the new lattice and then scale by a power of p to normalize the resulting form. Any two lattices are commensurable, and so we can define the distance $d(\Lambda, \Lambda')$ of two lattices by

$$p^{d(\Lambda,\Lambda')} = (\Lambda : \Lambda \cap \Lambda') \cdot (\Lambda' : \Lambda \cap \Lambda')\,.$$

If F is unstable at p for $(T, [0, w_1, w_2])$, then changing F to ${}^T F$ does not change the initial lattice (we just move to a different basis), but the subsequent scaling of the variables according to the weight vector enlarges the original lattice to one that contains it with index $p^{w_1+w_2}$, so the distance between the two is $w_1 + w_2$. (Note that $F \mapsto {}^M F$ corresponds to $\Lambda \mapsto \Lambda \cdot M^{-1}$.) Moving instead to an intermediate lattice will possibly not yet minimize F, but will bring us closer to a minimized model. We can use Proposition 7.1 to tell us which way to go.

Before we formulate this more precisely, we make the following observations.

Lemma 7.3. *Let $\Lambda_0 = \mathbb{Z}_p^3$ and $\Lambda = \Lambda_0 \cdot M_{[0,w_1,w_2]}^{-1} = \langle [1,0,0], [0,p^{-w_1},0], [0,0,p^{-w_2}] \rangle$, where $0 \le w_1 \le w_2$ and $w_2 > 0$.*

(1) *If $T \in \mathrm{GL}(3,\mathbb{Z}_p)$ is a matrix such that $\bar{T}$ fixes the line $x_2 = 0$ in $\mathbb{P}^2(\mathbb{F}_p)$ and $\Lambda' = \Lambda_0 \cdot (M_{[0,0,1]}T)^{-1}$, then $\Lambda_0 \subset \Lambda' \subset \Lambda$; in particular, $d(\Lambda', \Lambda) = w_1 + w_2 - 1$.*
(2) *Assume that $w_1 \ge 1$. If $T \in \mathrm{GL}(3,\mathbb{Z}_p)$ is a matrix such that $\bar{T}$ fixes the point $[1:0:0] \in \mathbb{P}^2(\mathbb{F}_p)$ and $\Lambda' = \Lambda_0 \cdot (M_{[0,1,1]}T)^{-1}$, then $\Lambda_0 \subset \Lambda' \subset \Lambda$; in particular, $d(\Lambda', \Lambda) = w_1 + w_2 - 2$.*
(3) *If $T \in p\,\mathrm{Mat}(3,\mathbb{Z}_p) \cap \mathrm{GL}(3,\mathbb{Q}_p)$ and $\Lambda' = \Lambda_0 \cdot T^{-1}$, then $\Lambda' \not\subset \Lambda$; in particular, $d(\Lambda_0, \Lambda') + d(\Lambda', \Lambda) > w_1 + w_2$.*

Proof. The ‘in particular’ statements follow from the fact that for three lattices Λ_1, Λ_2, Λ_3 with $\Lambda_1 \subset \Lambda_3$, we have

$$d(\Lambda_1, \Lambda_2) + d(\Lambda_2, \Lambda_3) = d(\Lambda_1, \Lambda_3) \iff \Lambda_1 \subset \Lambda_2 \subset \Lambda_3\,.$$

(1) The condition is ${}^{\bar{T}}x_2 = \gamma x_2$ with $\gamma \in \mathbb{F}_p^\times$, so the third column of $\bar{T}^{-1}$ is $[0, 0, \gamma^{-1}]^\top$, which implies that

$$(M_{[0,0,1]}T)^{-1} = T^{-1}\operatorname{diag}(1, 1, p^{-1}) = \begin{pmatrix} t_{11} & t_{12} & t_{13} \\ t_{21} & t_{22} & t_{23} \\ t_{31} & t_{32} & p^{-1}t_{33} \end{pmatrix}$$

with $t_{ij} \in \mathbb{Z}_p$. The lattice Λ' is generated by the rows of this matrix and is visibly contained in Λ.

(2) Here the condition is that the first row of $\bar{T}^{-1}$ has the form $[\gamma, 0, 0]$ with $\gamma \in \mathbb{F}_p^\times$. So

$$(M_{[0,1,1]}T)^{-1} = T^{-1}\operatorname{diag}(1, p^{-1}, p^{-1}) = \begin{pmatrix} t_{11} & t_{12} & t_{13} \\ t_{21} & p^{-1}t_{22} & p^{-1}t_{23} \\ t_{31} & p^{-1}t_{32} & p^{-1}t_{33} \end{pmatrix}$$

with $t_{ij} \in \mathbb{Z}_p$, and we conclude as in the previous case.

(3) In this case, $\Lambda_0 \cdot T^{-1}$ contains $p^{-1}\Lambda_0$, but $[p^{-1}, 0, 0] \notin \Lambda$. □

Corollary 7.4. *Assume that the form $F \in \mathbb{Z}[x_0, x_1, x_2]$ of degree d is unstable at p for a weight system $(T, [0, w_1, w_2])$ with $0 \le w_1 \le w_2$ and $w_2 > 0$. We denote by $\Lambda = \mathbb{Z}_p^3 \cdot (M_{[0,w_1,w_2]}T)^{-1}$ the lattice associated with this weight system. As usual, we write $\bar{F}$ for the reduction of F mod p and $\bar{T}$ for the reduction of T mod p. Then one of the following is true.*

(1) *$\bar{F} = L^m \cdot G$ with a linear form L and $m > \frac{d}{3}$, with the property that if $T' \in \mathrm{GL}(3, \mathbb{Z})$ is such that ${}^{\bar{T}'}L = \lambda x_2$, then the lattice associated to $(T', [0, 0, 1])$ has distance $w_1 + w_2 - 1$ from Λ.*

(2) *$\bar{F} = L^m \cdot G$ with a linear form L and $0 < m \le \frac{d}{3}$ such that $L \nmid G$ and the line $L = 0$ intersects $G = 0$ in a point P of multiplicity $> \frac{d-3m}{2}$ on $G = 0$, with the property that if $T' \in \mathrm{GL}(3, \mathbb{Z})$ is such that ${}^{\bar{T}'}L = \lambda x_2$, then the lattice associated to $(T', [0, 0, 1])$ has distance $w_1 + w_2 - 1$ from Λ.*

(3) *The curve $\bar{F} = 0$ has a point P of multiplicity $> \frac{d}{2}$ that does not lie on a line contained in the curve, with the property that if $T' \in \mathrm{GL}(3, \mathbb{Z})$ is such that $[1 : 0 : 0] \cdot \bar{T}' = P$, then the lattice associated to $(T', [0, 1, 1])$ has distance $w_1 + w_2 - 2$ from Λ. Such a point P is unique.*

This allows us to find candidates for $\bar{T}$ by determining the possible points P or lines L from $\bar{F}$. Note that the number of these objects is bounded in terms of d only. The worst case is when F is a product of distinct linear factors with the corresponding lines passing through a common point; then we have to consider these d linear factors.

Proof. We write X for the curve defined by $\bar{F} = 0$ and X' for the curve defined by ${}^{\bar{T}}\bar{F} = 0$ (then $X = X' \cdot \bar{T}$). The assumption on F implies that ${}^{T}F$ satisfies the assumption of Proposition 7.1. Let m_P denote the multiplicity of the point $[1 : 0 : 0]$ on X' and let m_L denote the multiplicity of x_2 as a factor of ${}^{\bar{T}}\bar{F}$. Then by Remark 7.2, $m_P \ge \nu_{011}({}^{T}F)$ and $m_L \ge \nu_{001}({}^{T}F)$.

Let $t = w_1/w_2$ as before. According to Proposition 7.1, if $t \ge \frac{1}{2}$, then $m_P \ge \nu_{011}({}^{T}F) > \frac{d}{2}$, which implies that there is a point $P = [1 : 0 : 0] \cdot \bar{T}$ of multiplicity $> \frac{d}{2}$ on X. If P is not on a line contained in this curve, then we have case (3). Since the line joining two distinct points of multiplicity $> \frac{d}{2}$ on X must be contained in X, there can be at most one such point. The claim regarding the lattice then follows from Lemma 7.3 (2). If P

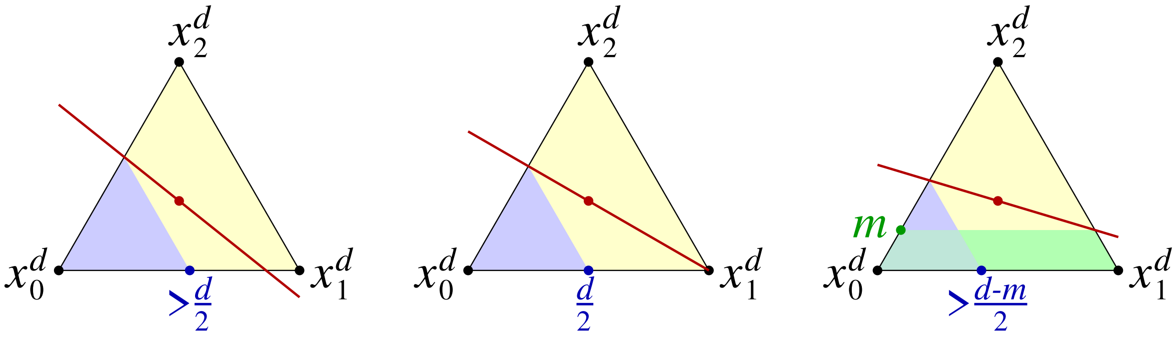

FIGURE 4. Illustration of Corollary 7.4. The slope of the red line depends on w_1/w_2; up to symmetry, it can have one of the indicated positions. The coefficients of $\bar{F}$ corresponding to the area on and below the line vanish. The blue triangle of vanishing coefficients corresponds to a point of high multiplicity, and the green trapezoid in the right-hand figure corresponds to a multiple line.

is on a line contained in X, then we are in cases (2) or (1), where the line is $L = 0$, and the claim on the lattice follows from Lemma 7.3 (1).

If $t < \frac{1}{2}$, then $m_L \geq \nu_{001}({}^{T}F) > 0$, so ${}^{T}\bar{F}$ splits off a factor x_2^m for some $m \geq 1$. If $m \leq \frac{d}{3}$, then $m > (1-2t)\frac{d}{3}$ implies $t > \frac{1}{2} - \frac{3m}{2d}$, hence $m_P > (1+t)\frac{d}{3} > \frac{d-m}{2}$. So $[1:0:0]$ must have multiplicity $> \frac{d-m}{2} - m = \frac{d-3m}{2}$ on the remaining part of X'. Applying T, we see that X contains a line of multiplicity m that intersects the remaining part of X in a point P that has multiplicity $> \frac{d-3m}{2}$ on this remaining part, so we are in case (2). If, finally, $m > \frac{d}{3}$, then we are in case (1). In both cases, the claim on the lattice follows from Lemma 7.3 (1). □

In each case, if we apply $(T', [0,0,1])$ or $(T', [0,1,1])$ to F and then normalize the resulting form, we either obtain a form F' with smaller valuation of the invariants (in which case we have successfully performed a minimization step), or else F' can be minimized using some $(T'', [0, w_1', w_2'])$ such that $w_1' + w_2' = w_1 + w_2 - 1$ (in cases (3) or (2)) or $w_1' + w_2' = w_1 + w_2 - 2$ (in case (1)). We can use Lemma 7.3 (3) to detect when we deviate from the path (at least in some cases). Since we know that $w_1 + w_2 \leq 2d - 1$ (when $d \geq 2$) by Theorem 1.5 and the fact that we can take w_1 and w_2 coprime, we have a bound on the number of steps that are maximally necessary to achieve minimization when minimization is possible.

This results in the following algorithm.

Algorithm 7.5. The input of MinimizePlaneCurveOneStep and MinimizePlaneCurve consists in a semistable ternary form $F \in \mathbb{Z}[x_0, x_1, x_2]$ of degree $d \geq 2$ and a prime number p. The result of MinimizePlaneCurveOneStep consists of a boolean flag indicating whether a minimization step could be performed successfully and in this case, a form G of degree d, a matrix T and a number $e \in \mathbb{Z}_{\geq 0}$ such that $G = p^{-e} \cdot {}^{T}F$ is the result of the minimization step; otherwise F, E_3 and 0 are returned as the last three values. The result of MinimizePlaneCurve consists of a form G of degree d that is a minimized representative of the orbit of F, together with a matrix T and a number $e \in \mathbb{Z}_{\geq 0}$ as above.

We define $\delta(d)$ to be the maximum of $w_1 + w_2$ over the minimal complete set of weight vectors $[0, w_1, w_2]$ for plane curves of degree d (or an upper bound for this quantity). This can be precomputed for the relevant values of d using the procedure hinted at near the end of Section 4; alternatively, we can set $\delta(d) := 2d - 1$; compare Theorem 1.5.

```
MinimizePlaneCurveOneStep($F$, $p$)
  $d := \deg(F)$;
  function Recurse($F$, $r$, $\gamma$, $T_0$)
    // $r \in \mathbb{Z}$: bound for the distance to the goal lattice,
    // $\gamma \in \mathbb{Z}$: change of valuation so far,
    // $T_0 \in \mathrm{Mat}(3, \mathbb{Z})$: transformation matrix so far
    if $\gamma < 0$ then return true, $F$, $T_0$, $0$; end if; // success!
    if $T_0 \bmod p = 0$ or $r \le 0$ then
      return false, $F$, $T_0$, $0$; // veering off the path or maximal distance reached
    end if;
    $\bar{F} = F \bmod p \in \mathbb{F}_p[x_0, x_1, x_2]$;
    write $\bar{F} = L_1^{m_1} \cdots L_s^{m_s} G$
      with pairwise non-proportional linear forms $L_j$, $m_j \ge 1$,
      and $G$ not divisible by a linear form;
    for $j := 1$ to $s$ do
      $T :=$ a matrix in $\mathrm{GL}(3, \mathbb{Z})$ such that ${}^{\bar{T}}L_j = \lambda x_2$;
      if $m_j \le d/3$ then // see Corollary 7.4 (2)
        $H(X, Y) := ({}^{\bar{T}}\bar{F}/x_2^{m_j})(x_0, x_1, 0) \in \mathbb{F}_p[x_0, x_1]$;
        if $H$ has no linear factors of multiplicity $> \frac{d-3m}{2}$ then go to the next $j$; end if;
      end if; // else we use Corollary 7.4 (1)
      $F_1, e :=$ ApplyWeight($F$, $T$, $[0, 0, 1]$, $p$);
      success, $F_2$, $T_1$, $e_1 :=$ Recurse($F_1$, $r - 1$, $\gamma + d - 3e$, $M_{[0,0,1]}TT_0$);
      if success then return true, $F_2$, $T_1$, $e + e_1$; end if;
    end for;
    if there is a point $P$ of multiplicity $> d/2$ on $G = 0$ with $\forall j\colon L_j(P) \neq 0$ then
      // Corollary 7.4 (3)
      $T :=$ a matrix in $\mathrm{GL}(3, \mathbb{Z})$ such that $[1 : 0 : 0] \cdot \bar{T} = P$;
      $F_1, e :=$ ApplyWeight($F$, $T$, $[0, 1, 1]$, $p$);
      success, $F_2$, $T_1$, $e_1 :=$ Recurse($F_1$, $r - 2$, $\gamma + 2d - 3e$, $M_{[0,1,1]}TT_0$);
      if success then return true, $F_2$, $T_1$, $e + e_1$; end if;
    end if;
    return false, $F$, $T_0$, $0$;
  end function;
  return Recurse($F$, $\delta(d)$, $0$, $E_3$);
```

The quantity γ is used to keep track of the increase and decrease in the p-adic valuation of the invariants caused by scaling the variables and the form by powers of p. If γ is negative, then the condition for instability with respect to the weight vector accumulated so far is satisfied.

```
MinimizePlaneCurve($F$, $p$)
  $T := E_3$; $e := v_p(F)$; $G := p^{-e}F$; // initialize; do $w = [0, 0, 0]$
  success, $G$, $T_1$, $e_1 :=$ MinimizePlaneCurveOneStep($G$, $p$);
```

```
while success do
    $T := T_1T$; $e := e + e_1$; // update transformation data
    success, $G$, $T_1$, $e_1$ := MinimizePlaneCurveOneStep($G$, $p$);
end while;
return $G$, $T$, $e$;
```

As written, the algorithm performs a depth-first search in the tree of lattices that are constructed depending on the lines and points found on the reduction. Alternatively, one can implement a breadth-first version or also a best-first version that expands the node with the smallest value of γ. Experiments seem to indicate that the tree rarely branches heavily, so that we expect there to be no penalty in practice for using the simpler depth-first code.

An implementation of this algorithm is available in Magma [BCP97] under the name `MinimizeTernaryFormAtp`.

We note that the algorithm can be adapted to an arbitrary discrete valuation ring R with uniformizer π in place of $\mathbb{Z}$ and p, as long as we can do computations in R and its residue class field $k = R/\langle\pi\rangle$, and the map $R \to k$ is computable and allows the determination of a preimage for a given element of k. Modulo computations in k and in R, its complexity depends only on d.

8 Global minimization and reduction of plane curves

When presented with a plane curve X over $\mathbb{Q}$ defined by a ternary form F, for which we would like to find a nice model, we first have to determine a finite set of primes p such that the given model might be non-minimal at p, so that we can then apply the procedure derived in Section 7 for these finitely many primes p.

If the curve is smooth (and the degree d satisfies $d \geq 2$), then a necessary condition is that the reduction of X mod p is singular. So we could compute the discriminant of the given model and find its prime divisors, or alternatively, set up a system of equations that a singular point has to satisfy and do a Gröbner basis computation over $\mathbb{Z}$ to obtain a nonzero integer N such that all relevant primes must divide N. The disadvantage of this approach is that usually there are quite a few large primes p such that X is singular, but still semistable, mod p (in the sense that there is an invariant I such that $p \nmid I(F)$), and so we have to factor a large number, even though we are interested only in certain of its prime factors. So instead, we should try to cut the set of primes down as closely as possible to the set of primes such that the reduction of X mod p is unstable (i.e., $\bar{F}$ is a nullform). For this, we can use the necessary conditions coming from the 'geometric' version of Proposition 7.1 as mentioned in Remark 7.2. Write $\bar{X}$ for the reduction of X mod p. Then for $\bar{X}$ to be unstable, $\bar{X}$ either has to contain a line L of multiplicity m such that $m > d/3$ or else there is a point of multiplicity (on $\bar{X}$) $> (d-m)/2$ on L, or $\bar{X}$ has a point of multiplicity $> d/2$ (which is the case $m = 0$ of the previous condition). For each $m = 0, 1, \ldots, \lfloor d/3 \rfloor + 1$, we can write down equations (depending on the location of the line and/or the point relative to the standard affine patches) that must be satisfied; a Gröbner basis computation over $\mathbb{Z}$ then results in a basis of the corresponding ideal that contains a unique nonzero integer N (here we assume that the curve X over $\mathbb{Q}$ does not generically satisfy one of these conditions; otherwise X would be very close to being unstable), whose prime divisors give us candidates for the primes at which we might be able to minimize X. Unless d is very small, the conditions we impose cut out subvarieties of codimension at least 2 of the moduli space of plane curves of degree d, and so we can expect 'spurious' large primes to occur only in rare cases.

The Gröbner basis computations can still take some time, though. They will be more efficient if we can add the information that the relevant primes have to divide some given nonzero integer N. (This has the effect of computing over $\mathbb{Z}/N\mathbb{Z}$ and thus avoids intermediate coefficient growth.) A necessary condition for the curve to be non-minimal at p is that the form defining it becomes unstable when reduced mod p. This means that all its invariants are divisible by p. So we can get a suitable integer by computing some invariants and taking their gcd. Recall that an *invariant* of ternary forms of degree d is a homogeneous polynomial $I(F)$ with integral coefficients in the coefficients of the form F such that $I({}^TF) = I(F)$ for all $T \in SL(3)$. A *covariant* is a map associating to a form F of degree d another form $C(F)$ of some degree whose coefficients are homogeneous polynomials with integral coefficients in the coefficients of F and such that $C({}^TF) = {}^TC(F)$ for all $T \in SL(3)$. Covariants of covariants are again covariants, and invariants of covariants are invariants. One possibility of generating covariants is to use the kth *Überschiebung*. We define the differential operator

$$\Delta = \det \begin{pmatrix} \frac{\partial}{\partial x_0} & \frac{\partial}{\partial x_1} & \frac{\partial}{\partial x_2} \\ \frac{\partial}{\partial y_0} & \frac{\partial}{\partial y_1} & \frac{\partial}{\partial y_2} \\ \frac{\partial}{\partial z_0} & \frac{\partial}{\partial z_1} & \frac{\partial}{\partial z_2} \end{pmatrix} .$$

Then the kth Überschiebung (or transvectant) of three ternary forms F, G, H is

$$\ddot{U}^k(F, G, H) = \Delta^k F(x_0, x_1, x_2) G(y_0, y_1, y_2) H(z_0, z_1, z_2)\Big|_{y_j, z_j \leftarrow x_j} .$$

One can show that when F, G, H are covariants of a form, then $\ddot{U}^k(F, G, H)$ is again a covariant. (This comes down to the fact that the determinant of a matrix does not change when the matrix is multiplied by a matrix in $SL(3)$. The analogous statement for binary forms is classical.) For example, $\ddot{U}^2(F, F, F)$ is the Hessian of F, and $\ddot{U}^1(F, G, H)$ is the Wronskian determinant of F, G and H. In particular, we obtain an invariant when the Überschiebung is constant. It is easy to see that $\ddot{U}^k(F, G, H) = 0$ when k is odd and two of F, G, H are the same. When $d = \deg F$ is even, then $I_1(F) = \ddot{U}^d(F, F, F)$ is an invariant that is generically nonzero, and $G = \ddot{U}^{d-2}(F, F, F)$ is a sextic covariant of F such that $I_2(F) = \ddot{U}^6(G, G, G)$ is another invariant that is generically nonzero and independent of $I_1(F)$. We can then use $\gcd(I_1(F), I_2(F))$ in the approach described above. When d is odd, then $G = \ddot{U}^{d-1}(F, F, F)$ is a cubic covariant of F, and we can use the invariants of G instead.

After we have determined a finite set of candidate primes p, we can successively minimize our curve at these p using MinimizePlaneCurve. We then have a globally minimal plane model $F(x_0, x_1, x_2) = 0$ of our curve. This minimal model can still have quite large coefficients. To remedy this, we want to find a transformation $T \in SL(3, \mathbb{Z})$ so that ${}^TF$ has reasonably small coefficients. (Note that applying T does not change the invariants of F, hence preserves minimality.) This process is called *reduction*. As explained in [Sto11], one possible approach is to associate to the curve X a zero-dimensional subscheme (or point cluster) C of $\mathbb{P}^2$ and then reduce C using the algorithm described in loc. cit. A suitable choice is the scheme of inflection points, which is given as the intersection of $F = 0$ with $H = 0$, where H is the Hessian of F (i.e., the determinant of the matrix of second partial derivatives of F, up to a constant factor). This has the disadvantage that the degree of this scheme grows quadratically with $d = \deg F$. Instead we can use any scheme obtained from the intersection of the curves defined by two covariants of F, as long as it is stable in the sense of [Sto11]. When d is odd, we can also take the cubic covariant G from above and reduce it (if it is stable), which is equivalent to using the scheme of inflection points of the curve given by $G = 0$.

In practice, it seems to be most efficient to do an 'ad-hoc' reduction first (or only). For this, we apply a certain set of 'small' elements of $\mathrm{SL}(3, \mathbb{Z})$ to our form F and check if the size of F (measured, for example, as the euclidean length of the coefficient vector) gets smaller for one of them, say T. If so, we replace F by ${}^{T}F$ and continue; otherwise, we stop. Combining our general minimization algorithm with this reduction procedure finally results in an algorithm that produces a 'maximally nice' model of the curve, in the sense that it is globally minimal and its defining equation has small coefficients.

We have implemented this procedure in Magma [BCP97]. Global minimization is performed by `MinimizeTernaryForm`, reduction by `ReduceTernaryForm`, and both together by `MinRedTernaryForm`.

The following examples give some indication of the performance of the implementation.

Example 8.1. The following sextic form occurs in [DNS20].

$$\begin{aligned} F = 5x^6 - 50x^5y + 206x^4y^2 - 408x^3y^3 + 321x^2y^4 + 10xy^5 - 100y^6 + 9x^4z^2 \\ - 60x^3yz^2 + 80x^2y^2z^2 + 48xy^3z^2 + 15y^4z^2 + 3x^2z^4 - 10xyz^4 + 6y^2z^4 - z^6 \,. \end{aligned}$$

The plane curve defined by it has four simple double points (hence geometric genus 6); it is a model of a certain modular curve.

We compute the two invariants $I_1(F)$ and $I_2(F)$ and find that

$$N = \gcd(I_1(F), I_2(F)) = 867041280 \,.$$

(The prime divisors of N are 2, 3, 5 and 7, but we don't need to know this.) Then we do the Gröbner basis computations with N added to the generators of the ideals. This shows that F can be non-minimal at most at $p = 2$ and $p = 7$. This part of the procedure took about a quarter second.

The minimization algorithm with $p = 2$ traverses a tree with 13 nodes and finds a successful minimization step on the way. The minimization algorithm with $p = 7$ traverses a tree with three nodes before it concludes that no proper minimization is possible. This part of the procedure took less than a tenth of a second.

Finally, we apply ad-hoc reduction (in fact, this is done first and also in between the local minimization steps to keep the coefficients of reasonable size) and the cluster reduction, which does not actually improve the final result, to obtain the polynomial below. This part of the procedure took about a third of a second. The total time was about 0.7 seconds.

$$\begin{aligned} F_0 &= -x^6 - 2x^5y + 2x^5z + 23x^4yz - 5x^3y^3 - x^3y^2z + x^3yz^2 + 5x^3z^3 - x^2y^4 - 8x^2y^3z \\ &\qquad + 17x^2y^2z^2 - 8x^2yz^3 - x^2z^4 + 3xy^5 - 7xy^4z + 10xy^3z^2 - 10xy^2z^3 + 7xyz^4 \\ &\qquad - 3xz^5 + y^6 - 3y^5z + 3y^4z^2 - 6y^3z^3 + 3y^2z^4 - 3yz^5 + z^6 \\ &= \frac{1}{16}{}^{T}F(x_0, x_1, x_2) \end{aligned}$$

with

$$T = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} .$$

We note that F is even as a polynomial in z, showing that the curve has an involution. This feature is lost after minimization.

Example 8.2. We start with a form of degree 10 with small random coefficients,

$$\begin{aligned} F = 7x^{10} &+ 4x^9y - 9x^9z - x^8y^2 + 9x^8yz - 5x^8z^2 - 4x^7y^3 - 8x^7y^2z - 7x^7yz^2 - 9x^7z^3 \\ &- 3x^6y^4 - 5x^6y^3z + 2x^6y^2z^2 - 7x^6yz^3 + 4x^6z^4 + 8x^5y^5 + 10x^5y^4z + 5x^5y^3z^2 \\ &- 3x^5y^2z^3 + 2x^5yz^4 - x^4y^6 + 9x^4y^5z - 3x^4y^4z^2 + 5x^4y^3z^3 + x^4yz^5 - 2x^4z^6 \\ &+ 6x^3y^7 + 8x^3y^6z + 9x^3y^4z^3 + 9x^3y^3z^4 + 5x^3y^2z^5 - 5x^3yz^6 + 3x^3z^7 - 10x^2y^8 \\ &+ 8x^2y^6z^2 - 5x^2y^5z^3 + 8x^2y^4z^4 - 10x^2y^3z^5 - 5x^2y^2z^6 - x^2z^8 - 3xy^9 + 8xy^8z \\ &- 10xy^7z^2 + 7xy^6z^3 + 4xy^5z^4 - 9xy^4z^5 + xy^3z^6 - 4xy^2z^7 - 9xyz^8 - 2xz^9 - 9y^{10} \\ &- 7y^9z + 5y^8z^2 - 7y^7z^3 + 2y^6z^4 - 2y^5z^5 + 3y^4z^6 - 2y^3z^7 + 2y^2z^8 + 8yz^9 + 5z^{10} . \end{aligned}$$

We set up a random integral 3×3 matrix with ten-digit entries,

$$T = \begin{pmatrix} -6822460139 & -8617905122 & 4801170083 \\ 5588128275 & 3128463726 & 3491404315 \\ -3274111511 & 371050596 & 2931443838 \end{pmatrix} ;$$

then $F_1 = {}^T F$ is an integral form of degree 10 with coefficients of about a hundred digits. Running our implementation on F_1 recovers the original form F up to interchanging x and z. The time for this is less than four minutes, most of which is spent in determining the (potentially, but in this instance really) unstable primes 2, 5573747 and 2748254186176163904623.

9 Determination of all minimal models

Minimal models of plane curves (and more generally, of projective hypersurfaces) need not be unique modulo the action of $\mathrm{GL}(n+1, \mathbb{Z})$. This comes from the corresponding statement on minimality at a prime p. The following example shows that a semistable form can have infinitely many pairwise $\mathbb{Z}_p$-inequivalent models.

Example 9.1. Let p be a prime and consider

$$F = xyz + y^3 + z^3 \in \mathbb{Z}_p[x, y, z] .$$

Then F is minimal (its invariants c_4 and c_6 are 1 and -1; see [Fis06, Sect. 1] for a definition) and is $\mathbb{Q}_p$-equivalent with

$$F_{i,j} = p^{-i-j} F(x, p^i y, p^j z) = xyz + p^{2i-j} y^3 + p^{2j-i} z^3 \in \mathbb{Z}_p[x, y, z]$$

for all $i, j \in \mathbb{Z}_{\geq 0}$ with $i \leq 2j$ and $j \leq 2i$, and $F_{i,j}$ has the same invariants as F.

Among the $F_{i,i}$ for $i \geq 0$, there are infinitely many pairwise $\mathbb{Z}_p$-inequivalent ones. Otherwise, there would be $\lambda_i \in \mathbb{Z}_p^\times$ and $M_i \in \mathrm{GL}(3, \mathbb{Z}_p)$ such that $\lambda_i{}^{M_i}F = F_i$ for infinitely many i. Since $\mathbb{Z}_p^\times \times \mathrm{GL}(2, \mathbb{Z}_p)$ is compact, there would be a convergent sub-sequence $(\lambda_{i_k}, M_{i_k})_{k \geq 0}$ with $i_k \to \infty$ as $k \to \infty$; let (λ, M) be its limit. Then

$$\lambda\, {}^M F = \lim_{k \to \infty} \lambda_{i_k}{}^{M_{i_k}} F = \lim_{k \to \infty} F_{i_k, i_k} = xyz ,$$

so F would be equivalent to xyz, which is clearly absurd.

When F is stable, there are finitely many pairwise $\mathbb{Z}_p$-inequivalent models of F, but their number is not uniformly bounded.

Example 9.2. Fix $k \in \mathbb{Z}_{>0}$ and a prime p and consider

$$F = xyz + p^k x^3 + y^3 + z^3 \in \mathbb{Z}_p[x, y, z] .$$

This form defines a smooth cubic over $\mathbb{Q}_p$ (its discriminant is $-p^k(27p^k + 1)^3 \neq 0$). It is minimal, since it is congruent mod p to the form F in Example 9.1.

For all pairs $(i, j) \in \mathbb{Z}^2_{\geq 0}$ with $i \leq 2j$, $j \leq 2i$ and $i + j \leq k$, F is $\mathbb{Q}_p$-equivalent to the form

$$F_{i,j} = p^{-i-j} F(x, p^i y, p^j z) = xyz + p^{k-i-j} x^3 + p^{2i-j} y^3 + p^{2j-i} z^3 \in \mathbb{Z}_p[x, y, z]$$

with the same invariants. The forms $F_{i,j}$ and $F_{i',j'}$ are $\mathbb{Z}_p$-equivalent if and only if the multisets $\{2i - j, 2j - i, k - i - j\}$ and $\{2i' - j', 2j' - i', k - i' - j'\}$ agree, so the number of pairwise $\mathbb{Z}_p$-inequivalent p-minimal models becomes arbitrarily large as $k \to \infty$.

This raises the question how one can determine a system of representatives of the $\mathbb{Z}_p$-isomorphism classes of p-minimal models of a given form F. We can certainly assume that F is p-minimal itself (otherwise we apply the minimization algorithm to it first). Replacing the strict inequality in Definition 1.2 and in (3.1) by a non-strict one, we obtain a similar theory of dominance of weight vectors (we have to exclude the vectors $[k, k, \ldots, k]$, though, which would otherwise dominate everything; they correspond to applying a unimodular transformation, which gives an equivalent form), so that we can determine a set of weight vectors w such that if there is another p-minimal model of F that is not equivalent to F over $\mathbb{Z}_p$, then one such model can be obtained via an application of w. Note that the minimal complete sets of weight vectors we obtain can be different from those we use for minimization. For example, the set for conics is now $\{[0, 0, 1], [0, 1, 2]\}$ instead of $\{[0, 0, 1], [0, 1, 1]\}$, and for plane cubics, we can use $\{[0, 0, 1], [0, 1, 1]\}$.

This leads to an algorithm that decides if another p-minimal model (or a "more minimal" one) exists, and if so, produces one. One then has to repeat the procedure with each new model that was found (taking care of keeping only one representative of each equivalence class over $\mathbb{Z}_p$) until no new models are found. Note that the 'distance' between two p-minimal models in the sense of Section 7 can be arbitrarily large as shown by Example 9.2, so we cannot hope to find all of them in one go by applying a finite set of weight vectors.

To construct a list of representatives of all $\mathbb{Z}$-equivalence classes of (globally) minimal models of F, one combines the various p-minimal models for all p. The problem is then to produce a finite list of primes p such that F can have several inequivalent p-minimal models. Note that the reduction of F mod p does not need to be unstable; the reduction can be semistable but not stable (this is illustrated by Example 9.2 above), so one has to use slightly weaker geometric conditions. It is not clear (to us, at least) how to determine invariants that vanish on all semistable forms that are not stable; if we had two or more independent such invariants, we could use a method like that described in Section 8. The discriminant is one such invariant (at least when the degree d is not very small), so one can use it, at least when dealing with smooth hypersurfaces, to avoid intermediate expression growth in the Groebner basis computations, but this will be significantly less efficient than using the gcd of two suitable invariants.

We leave the task of devising a reasonably efficient algorithm that finds representatives of all equivalence classes of locally or globally minimal models to future work.

10 Minimization in higher dimensions

Our approach to minimization of plane curves is based on the following four observations.

(1) If the ternary form F is unstable at p for some weight system (T, w), then the curve given by $\bar{F} = 0$ contains a flag of linear subspaces with certain multiplicities. (Concretely, we have a line containing a point, with multiplicities m for the line and $\max\{m, \lfloor \frac{d-m}{2} \rfloor + 1\}$ for the point, with $0 \le m \le d$; see Corollary 7.4.)

(2) The number of such flags that can be contained in the reduced curve is bounded in terms of the degree d only.

(3) In each case, we can use one of the linear subspaces contained in the flag with positive multiplicity to move closer to the form obtained by applying (T, w) to F (in the sense of lattice distance; see again Corollary 7.4).

(4) The number of simple steps from one lattice to another is bounded in terms of d by Theorem 1.5.

Part of this carries over to the case $n \ge 3$. Part (4) is taken care of by Theorem 1.6. Part (1) generalizes as follows.

Proposition 10.1. *Let $F \in \mathbb{Z}[x_0, \ldots, x_n]$ be a form of degree d that is unstable at p for the weight system (E, w) with $w = [w_0, w_1, \ldots, w_n] \in W$ (so $0 = w_0 \le w_1 \le \ldots \le w_n$). We assume that $v_p(F) = 0$; then $w_n > 0$. Write L_k for the k-dimensional linear subspace of $\mathbb{P}^n_{\mathbb{F}_p}$ given by $x_{k+1} = \ldots = x_n = 0$. Then the hypersurface defined by $\bar{F} = 0$ contains L_k with multiplicity at least*

$$m_k = \begin{cases} 0 & \text{if } (n+1)w_k > \Sigma w, \\ \left\lfloor \dfrac{d}{n+1} \dfrac{\Sigma w - (n+1)w_k}{w_n - w_k} \right\rfloor + 1 & \text{otherwise.} \end{cases}$$

Proof. Write $F = \sum_{i \in I} a_i x^i$ as usual. We have to show that $v_p(a_i) > 0$ if the degree of x^i in $x_{k+1}, \ldots, x_n$ is less than m_k. By our assumption on F, we know that

$$v_p(a_i) \ge \max\left\{0, 1 + \left\lfloor \frac{d}{n+1} \Sigma w \right\rfloor - \langle i, w \rangle \right\}.$$

Thus, $v_p(a_i) > 0$ whenever $\frac{d}{n+1} \Sigma w \ge \langle i, w \rangle$. Let m denote the degree of x^i in $x_{k+1}, \ldots, x_n$. Then the weak monotonicity of the entries of w implies that

$$\langle i, w \rangle \le (d-m)w_k + m w_n = d w_k + m(w_n - w_k).$$

We can assume that $(n+1)w_k \le \Sigma w$; otherwise, there is nothing to show. Then

$$\begin{aligned} \frac{d}{n+1}\Sigma w - \langle i, w \rangle &\ge \frac{d}{n+1}\Sigma w - d w_k - m(w_n - w_k) \\ &\ge \frac{d}{n+1}\Sigma w - d w_k - (m_k - 1)(w_n - w_k) \ge 0 \end{aligned}$$

as desired. □

From the proof, it is clear that the bound in Proposition 10.1 is sharp.

Remark 10.2. In a similar way as in the proof of Proposition 7.1, one can show the stronger statement that

$$\nu_p\bigl(F(x_0,\dots,x_k,px_{k+1},\dots,px_n)\bigr) \ge m_k\,.$$

Lemma 7.3 extends in an obvious way to a general version of Part (3) above.

The obstacle in establishing an efficient general minimization procedure for surfaces in $\mathbb{P}^3$ (say) is in Part (2) above: it is in general no longer true that the number of flags with multiplicities that we have to consider can be bounded in terms of d alone (for fixed dimension n). For example, $w = [0,1,2,2]$ is an element of the minimal complete set of weight vectors for cubic surfaces (see Table 1). The multiplicities given by Proposition 10.1 for w are

$$(m_2,m_1,m_0) = (0,1,2)\,,$$

so we can conclude that there is a line on $\bar{F} = 0$ that passes through a singular point, but no flag with higher multiplicities needs to occur. Now consider the case that $\bar{F} = 0$ is a cone over a nodal cubic curve. This surface contains a one-parameter family of lines passing through the vertex of the cone and in addition a double line, which gives a one-parameter family of lines with a singular point on them (by fixing the line and varying the point). So we would have to run through on the order of p lines or points and try the corresponding directions for minimization. What saves us in the cubic case is that when $[0,1,2,2]$ applies to F and the reduction of F defines a cone, then $[0,1,1,1]$ also applies to F, and here the direction is determined by the point of multiplicity 3.

Similarly, for $w = [0,2,2,3]$, we find

$$(m_2,m_1,m_0) = (0,0,2)\,,$$

so the only geometric condition we obtain is that there is a singular point. Again, if the reduction is a cone over a cubic curve, then $[0,1,1,1]$ applies as well. In addition, we can use for both $[0,1,2,2]$ and $[0,2,2,3]$ that the singular point is 'very singular' in the sense that the value of F at any lift of it is divisible by p^2; the number of such points is uniformly bounded when neither $[0,0,0,1]$ nor $[0,0,1,1]$ apply. See Section 11 below for details.

For quartic surfaces, we have a similar situation. For the weight vectors $[0,2,3,6]$ and $[0,3,5,9]$ (which both are in the minimal complete set), the multiplicity bounds are $(m_2,m_1,m_0) = (0,1,2)$ as above, and there are configurations for the reduced surface that contain one-parameter families of lines and singular points. For example, this is the case when the reduced surface is a union of two quadrics of rank 3 or 4 (and at least one of the two is of rank 3 or split). It is well possible that in cases like these, another weight vector applies or more stringent conditions can be obtained that depend on $F \bmod p^2$ (like in the cubic case), so that one can work around these potential difficulties. However, we will not attempt to follow this line in the present paper. Instead, we will focus on the case of cubic surfaces; we present a suitable algorithm in the next section.

11 Minimization of cubic surfaces

Unstable cubic surfaces were already studied by Hilbert. Their classification is as follows:

Remark 11.1. A cubic surface is unstable if and only if it satisfies one of the following.

(1) It has a singular point such that the tangent cone degenerates to a plane of multiplicity 2.
(2) It has a singular point such that the tangent cone degenerates to two planes and the intersection of the two planes is a line contained in the surface.
(3) It has a triple point. I.e., the surface degenerates to a cone.

This list is given in [MF82, Chap. 4.2, page 80]. The first two options are already listed in [Hil93b, page 367]. Note that reducible cubic surfaces and cubic surfaces with a singular line are covered by the above.

In more modern language, a normal cubic surface that is not a cone is unstable if and only if it has a singular point of type A_3, A_4, A_5, D_4, D_5 or E_6. This follows from a comparison of the list [Dol12, Table 9.1] with the above result.

We now describe the ingredients for an algorithm that minimizes semistable (e.g., smooth) cubic surfaces. Note that $w = [0, \dots, 0]$ applies to F if and only if $\nu_p(F) \geq 1$, so all coefficients are divisible by p. We will always scale our equations to have coprime coefficients, so we do not have to consider this case, or rather, we normalize the equation right at the beginning and keep it so during the procedure. So we do not have to consider the zero weight vector further. The simplest remaining weight vector is $[0, 0, 0, 1]$.

Lemma 11.2. *Let* $F \in \mathbb{Z}[x_0, x_1, x_2, x_3]$ *be primitive and homogeneous of degree* 3*. Then* $[0, 0, 0, 1]$ *applies to* F *if and only if* $\bar{F}$ *splits off a linear factor.*

Proof. First assume that $[0, 0, 0, 1]$ applies to F, so there is a unimodular matrix T such that

$$\nu_p\left({}^T F(x_0, x_1, x_2, px_3)\right) \geq 1 + \left\lfloor \frac{3}{4} \cdot 1 \right\rfloor = 1\,. \tag{11.1}$$

Reducing mod p, we see that ${}^{\bar{T}}\bar{F}(x_0, x_1, x_2, 0) = 0$, which means that x_3 divides ${}^{\bar{T}}\bar{F}$. This implies that $\bar{F}$ splits off a linear factor as well.

Conversely, assume that $\bar{F}$ splits off a linear factor. After applying a suitable unimodular matrix T, we can assume that x_3 divides $\bar{F}$. Then ${}^{\bar{T}}\bar{F}(x_0, x_1, x_2, 0) = 0$, which implies (11.1). □

This has the following consequence.

Corollary 11.3. *Each semistable (for example, smooth) cubic surface over* $\mathbb{Q}$ *has an integral model such that the reduction modulo all primes is irreducible.*

Proof. Since the given surface is semistable, there is some invariant I that does not vanish on equations for the surface. Let $F(x_0, x_1, x_2, x_3) \in \mathbb{Z}[x_0, x_1, x_2, x_3]$ be a defining polynomial of the surface such that the absolute value of $I(F)$ is minimal among all integral defining equations. If the reduction of F mod p were reducible for some prime p, then Lemma 11.2 would imply that we can apply the weight vector $[0, 0, 0, 1]$, leading to a new model with smaller absolute value of the invariant, contradicting our choice of F. □

Remark 11.4. A similar argument shows the analogous statement for any quadric in $\mathbb{P}^n$ with $n \geq 2$ and any cubic in $\mathbb{P}^n$ with $n \geq 3$.

Before we look at the other weight vectors, we state some facts on singular points on cubic surfaces. We will use the terms ‘k-plane’, ‘k-line’ and ‘k-point’ to refer to a plane, line or point defined over the field k.

Lemma 11.5. *Let $F \in k[x_0, x_1, x_2, x_3]$ be nonzero and homogeneous of degree 3. We denote by $X \subset \mathbb{P}^3_k$ the cubic surface defined by F and by X_{sing} its singular subscheme.*

If X does not contain a k-plane, then either $X_{\text{sing}}(k)$ consists of the k-points on a single k-line, or else of finitely many affinely independent points (in particular, $\#X_{\text{sing}}(k) \leq 4$ in this case).

Proof. As X does not contain a k-plane, F is either absolutely irreducible or a norm form. In the later case $X_{\text{sing}}(k)$ consists of the intersection of three planes and is therefore either a single point or a line.

Now, let F be absolutely irreducible. If X_{sing} has a one-dimensional part, it is a line; see [Dol12, Sec. 9.2.1]. As cubic surfaces contain the line joining each pair of singular points, we can conclude that a cubic surface containing a singular line and a singular point not on the line will contain the plane spanned by them and is therefore reducible.

Next we inspect the case that 3 singular points are one a line. Then the intersection of the cubic surface with any plane containing this line is a cubic curve with at least these 3 singular points. Thus, all these cubic curves contain a double line and therefore the entire line is singular.

Finally, the bound 4 for the number of singular points is proven in [Dol12, Cor. 9.2.3]. □

Definition 11.6. For the discussion below, we say that a point $\bar{P}$ on the surface $\bar{X}$ defined by $\bar{F} = 0$ (where $F \in \mathbb{Z}[x_0, x_1, x_2, x_3]$ is a cubic form) is *very singular* if $\bar{P}$ is a singular point of $\bar{X}$ and $v_p(F(P)) \geq 2$ for some lift P of $\bar{P}$. This latter condition is independent of the choice of the lift.

Lemma 11.7. *Keeping the notation of Definition 11.6, we assume that $\bar{X}$ does not contain an $\mathbb{F}_p$-plane. If there are more than four very singular $\mathbb{F}_p$-points on $\bar{X}$, then the very singular $\mathbb{F}_p$-points are the $\mathbb{F}_p$-points of a line that consists of very singular points.*

Proof. This follows from Lemma 11.5 and the fact that a singular line that contains points that are not very singular can contain at most three very singular points: let the line be given by $x_2 = x_3 = 0$. Since the line is singular, F can be written in the form

$$F = f_3(x_2, x_3) + f_{2,0}(x_2, x_3)x_0 + f_{2,1}(x_2, x_3)x_1 + px_2g_{2,2}(x_0, x_1) + px_3g_{2,3}(x_0, x_1) + pg_3(x_0, x_1),$$

where f_3 and g_3 are binary cubic forms and $f_{2,0}$, $f_{2,1}$, $g_{2,2}$, $g_{2,3}$ are binary quadratic forms. A point $(\xi_0 : \xi_1 : 0 : 0)$ on the line is very singular if and only if $\bar{g}_3(\xi_0, \xi_1) = 0$. Either $\bar{g}_3$ is identically zero, then the line consists of very singular points, or else $\bar{g}_3$ has at most three zeros on $\mathbb{P}^1_{\mathbb{F}_p}$. □

We now consider the weight vector $[0, 0, 1, 1]$. We keep the notation $\bar{X}$ for the surface given by $\bar{F} = 0$.

Lemma 11.8. *Let $F \in \mathbb{Z}[x_0, x_1, x_2, x_3]$ be primitive and homogeneous of degree 3. We assume that $[0, 0, 0, 1]$ does not apply to F.*

(1) *If $[0, 0, 1, 1]$ applies to F, then $\bar{X}$ contains a (unique) singular line defined over $\mathbb{F}_p$ that consists of very singular points.*

(2) *If $\bar{X}$ is singular along the line $x_2 = x_3 = 0$, then $w = [0,0,1,1]$ applies to F if and only if F is unstable at p for (E, w), i.e., if and only if $v_p(F(x_0, x_1, px_2, px_3)) \geq 2$. Equivalently, the line consists of very singular points.*

Proof. By Lemma 11.2, the assumption that $[0,0,0,1]$ does not apply to F means that $\bar{F}$ is irreducible.

(1) We have that $v_p({}^T F(x_0, x_1, px_2, px_3)) \geq 2$ with a suitable unimodular matrix T. This implies that ${}^{\bar{T}}\bar{F} \in \langle x_2, x_3\rangle^2$, and so $\bar{X}$ is singular along the line $x_2 = x_3 = 0$. We also see that g_3 for ${}^T F$ as in the proof of Lemma 11.7 is divisible by p, which implies that the line consists of very singular points.

(2) The 'if' direction is clear. For the 'only if', first note that by part (1) and its proof, there must be a unimodular matrix T such that $\bar{T}$ fixes the line $x_2 = x_3 = 0$ and F is unstable w.r.t. (T, w). Now one easily checks that the latter condition is independent of the choice of T with these properties, so it holds for some T if and only if it holds for $T = E$. □

So to check whether $[0,0,1,1]$ applies to F, we find the singular $\mathbb{F}_p$-lines on $\bar{X}$, of which there is at most one. If such a line exists, we check the criterion given in part (2).

When neither $[0,0,0,1]$ nor $[0,0,1,1]$ apply, Lemmas 11.5 and 11.7 tell us that there are at most four very singular $\mathbb{F}_p$-points on $\bar{X}$. This will be useful for dealing with the remaining minimal weight vectors. We begin with $[0,1,1,1]$

Lemma 11.9. *Let $F \in \mathbb{Z}[x_0, x_1, x_2, x_3]$ be primitive and homogeneous of degree 3. We assume that $[0,0,0,1]$ does not apply to F.*

(1) *If $[0,1,1,1]$ applies to F, then $\bar{X}$ is a cone over a cubic curve. The vertex of the cone is an $\mathbb{F}_p$-point $\bar{P}$ of multiplicity 3 that is very singular.*

(2) *If the point $[1:0:0:0]$ has multiplicity 3 and is very singular on $\bar{X}$, then F is unstable at p for some (T, w) such that $\bar{T}$ fixes $[1:0:0:0]$ if and only if this is true for $T = E$, i.e., if and only if $v_p(F(x_0, px_1, px_2, px_3)) \geq 3$.*

Proof. As before, $\bar{F}$ is irreducible.

(1) We have that $v_p({}^T F(x_0, px_1, px_2, px_3)) \geq 3$ with a suitable unimodular matrix T. This implies that ${}^{\bar{T}}\bar{F} \in \langle x_1, x_2, x_3\rangle^3$, and so $\bar{X}$ is a cone; its vertex $\bar{P}$ is defined over $\mathbb{F}_p$ and has multiplicity 3. There is one lift P such that $v_p(F(P)) \geq 3$; this implies that $\bar{P}$ is very singular.

(2) This is shown in a similar way as part (2) of Lemma 11.8. □

Finally, we deal with the weight vectors $[0,1,2,2]$ and $[0,2,2,3]$.

Lemma 11.10. *Let $F \in \mathbb{Z}[x_0, x_1, x_2, x_3]$ be primitive and homogeneous of degree 3. We assume that $[0,0,0,1]$, $[0,0,1,1]$ and $[0,1,1,1]$ do not apply to F.*

(1) *If $[0,1,2,2]$ or $[0,2,2,3]$ applies to F, then $\bar{X}$ contains a very singular $\mathbb{F}_p$-point $\bar{P}$ with the following property. Lift $\bar{P}$ to a point P and write*

$$F(P + x) = f_0 + f_1(x) + f_2(x) + f_3(x)$$

with f_j homogeneous of degree j. Then $p^2 \mid f_0$, $p \mid f_1$, and the quadric $\bar{f}_2$ has rank 1 or 2.

(2) *Assume that the point* $[1:0:0:0]$ *is very singular on* $\bar{X}$*; then*

$$F_1 := p^{-2}F(x_0, px_1, px_2, px_3) \in \mathbb{Z}[x_0, x_1, x_2, x_3]$$

is primitive. Write

$$\bar{F}(x_0, x_1, x_2, x_3) = x_0 f_2(x_1, x_2, x_3) + f_3(x_1, x_2, x_3) \in \mathbb{F}_p[x_0, x_1, x_2, x_3]$$

with f_j *homogeneous of degree* j *and assume that* f_2 *has rank* 1 *or* 2*. Then* F *is unstable for* $(T, [0,1,2,2])$ *or* $(T, [0,2,2,3])$ *for some* T *such that* $\bar{T}$ *fixes* $[1:0:0:0]$ *if and only if*

(a) *either* f_2 *has rank* 2 *and* $[0,0,1,1]$ *applies to* F_1 *(which is the case if and only if the singular line of* $f_2 = 0$ *is very singular on* $\bar{F}_1 = 0$*); then* $[0,1,2,2]$ *applies to* F*,*

(b) *or else* f_2 *has rank* 1 *and after applying* $[0,0,0,1]$ *to* F_1 *with respect to a plane not containing* $[1:0:0:0]$*, either* $[0,0,0,1]$ *or* $[0,1,1,1]$ *applies to the resulting form. In the first case,* $[0,1,2,2]$ *applies to* F*, in the second case,* $[0,2,2,3]$ *applies.*

Proof. By assumption, $\bar{F}$ is irreducible and $\bar{X}$ does not contain a very singular line.

(1) After applying a suitable unimodular transformation T, we can assume that F is unstable for $(E, [0,1,2,2])$ or $(E, [0,2,2,3])$, i.e., that

$$v_p\big(F(x_0, px_1, p^2x_2, p^2x_3)\big) \geq 4 \quad \text{or} \quad v_p\big(F(x_0, p^2x_1, p^2x_2, p^3x_3)\big) \geq 6\,.$$

This implies in both cases that $[1:0:0:0]$ is very singular on $\bar{X}$ and that

$$\bar{F} = x_0 f_2(x_2, x_3) + f_3(x_1, x_2, x_3)$$

with a binary quadratic form f_2 and a ternary cubic form f_3. If $f_2 = 0$, then one easily checks that F is unstable with respect to $(E, [0,1,1,1])$, but this is excluded by assumption. Therefore f_2 must have rank 1 or 2.

(2) The first claim is easily checked. Note that F_1 cannot be divisible by p, since otherwise $[0,1,1,1]$ would apply to F. It is also easily checked that in both cases (2a) and (2b) the resulting form is 'more minimal' than F. Moving the line in case (2a) to $x_2 = x_3 = 0$, we also see that the sequence of steps amounts to an application of $[0,1,2,2]$. Similarly, moving the double plane in case (2b) to $x_3^2 = 0$, the application of $[0,0,0,1]$ to F_1 is with respect to $x_3 = 0$, and we see that together with the last step, we obtain an application of $[0,1,2,2]$ or $[0,2,2,3]$ to F. It remains to show that when one of $[0,1,2,2]$ and $[0,2,2,3]$ applies to F, then we are in one of the two cases. This can again be seen by moving the line or plane as mentioned above and checking the valuations of the various coefficients. □

So after checking whether $[0,0,0,1]$ or $[0,0,1,1]$ apply and finding that they do not, we determine the at most four very singular $\mathbb{F}_p$-points on $\bar{X}$, and for each of them, check the criteria of Lemma 11.9 (2) and Lemma 11.10 (2) to see if one of $[0,1,1,1]$, $[0,1,2,2]$ or $[0,2,2,3]$ applies. Putting all these steps together gives us a procedure MinimizeCubicSurfaceOneStep similar to MinimizePlaneCurveOneStep, which can then be called successively by a procedure MinimizeCubicSurface while successful minimization steps are performed. In this way, the results of this section can be turned into an algorithm. This has been implemented by the first author in Magma [BCP97]; the procedure is available under the name `MinimizeCubicSurface`.

12 Reduction of cubic surfaces

In a similar way as for plane curves, we have to perform a reduction of a minimized cubic surface to obtain an equation with small coefficients. Instead of a cluster-based approach we will use a representation as a sum of cubes of linear forms. This is based on the following classical result.

Theorem 12.1 (Sylvester [Dol12, Theorem 9.4.1]). *Let $F = 0$ be a general cubic surface over $\mathbb{C}$. Then there exist five linear forms $l_1, \dots, l_5$ such that*

$$F = l_1^3 + l_2^3 + l_3^3 + l_4^3 + l_5^3 .$$

These linear forms are unique up to order and multiplication by third roots of unity. This is called the ***pentahedral form of*** *F.*

Remark 12.2. This statement does not hold for so-called *cyclic* cubic surfaces. They are, up to linear equivalence, of the shape $w^3 + g(x, y, z) = 0$ with a ternary cubic form g; see [Dol12, Sec. 9.4.1].

One of the most extreme examples is the diagonal cubic surface $x_0^3 + x_1^3 + x_2^3 + x_3^3 = 0$. It has infinitely many such representations. To overcome the difficulties, the algorithm will deform cyclic cubic surfaces to nearby non-cyclic ones.

Definition 12.3. Let $F = 0$ be a cubic surface. Its *kernel surface* (sometimes also called the *Hessian*) is the quartic surface given by the equation

$$\det \left(\frac{\partial^2 F}{\partial x_i \partial x_j} \right)_{i,j} = 0 .$$

Theorem 12.4 (Clebsch [Cle61, Theorem 7], [Dol12, Sec. 9.4.2]). *Let*

$$F = l_1^3 + l_2^3 + l_3^3 + l_4^3 + l_5^3$$

be a general cubic surface in pentahedral form. Choose coefficients $a_1, \dots, a_5$ and linear forms $k_1, \dots, k_5$ such that $k_1 + k_2 + k_3 + k_4 + k_5 = 0$ and $a_i k_i = l_i$. Then the singular points of the kernel surface of F are the points given by

$$k_{i_1} = 1, \quad k_{i_2} = -1, \quad k_{i_3} = 0, \quad k_{i_4} = 0, \quad k_{i_5} = 0$$

for $\{i_1, i_2, i_3, i_4, i_5\} = \{1, 2, 3, 4, 5\}$.

The theorem above allows us to derive the pentahedral form of a cubic surface from the singular points of its Hessian. Each plane $l_i = 0$ (equivalently, $k_i = 0$) contains six singular points of the kernel surface. Thus, as soon as the combinatorial structure of the singular points is known, one can compute the planes $k_i = 0$ by solving linear systems. This is used in the algorithm below.

Algorithm 12.5. Let $F = 0$ be a general cubic surface over $\mathbb{Q}$. This algorithm computes a reduced form in the $GL(4, \mathbb{Z})$-orbit of F and the transformation matrix.

```
ReduceCubicSurface(F)
    Q := $\det \left( \frac{\partial^2 F}{\partial x_i \partial x_j} \right)_{i,j}$;
    Compute the singular points of $Q = 0$;
    // If we do not find 10 isolated singularities, we add a small perturbation to $F$.
    Solve the linear system of Theorem 12.4 to obtain $k_1, \dots, k_5 \in \mathbb{C}[x]$;
    Solve the linear system for the $b_i = a_i^3$ given by $F = b_1 k_1^3 + \dots + b_5 k_5^3$;
    $H(x) := |\sqrt[3]{b_1} k_1(x)|^2 + |\sqrt[3]{b_2} k_2(x)|^2 + |\sqrt[3]{b_3} k_3(x)|^2 + |\sqrt[3]{b_4} k_4(x)|^2 + |\sqrt[3]{b_5} k_5(x)|^2$;
```

```
// $H$ is a positive definite Hermitian form with real coefficients,
//     so it is actually a positive definite real quadratic form
Compute a matrix $T$ whose rows are an LLL-reduced basis of $\mathbb{Z}^4$ with respect to $H$;
return $F(xT^{-1}), T^{-1}$;
```

If one does not want to detect the combinatorial structure of the singular points by a floating point computation, one can use the approach described in [EJ15, Algo. A.4]. I.e., one computes the field of definition of one of the planes $l_i = 0$ and splits the singular subscheme of the kernel surface over that field. One of the components will contain all the singular points contained in $l_i = 0$ and a second component will contain all the other ones.

This algorithm has been implemented by the first author in Magma [BCP97]. It is available via `ReduceCubicSurface` and `MinimizeReduce`.

One could also try to apply the cluster reduction of [Sto11] to the singular points of the kernel surface and apply to transformation matrix obtained in this way to the initial cubic surface. In most cases, the results obtained by Algorithm 12.5 are slightly better.

$$\begin{aligned}
&- 866812507957452012700721792086587937x^3\\
&+ 372881298214760677373808189830554731\,0x^2y\\
&+ 6428376377098595278643602332790828416\,0x^2z\\
&+ 4977183550864666375906321517504492463\,96x^2w\\
&- 2224457988918835408417289662282253310\,0xy^2\\
&- 4319233199646988689825516823513172736\,00xyz\\
&- 2446192338737080630831681553231971375\,920xyw\\
&- 1618017788538827453488905618589376819\,200xz^2\\
&+ 1574715552732197466028065002725550148\,6080xzw\\
&- 6602520308883212330092956615284568947\,9856xw^2\\
&- 654561387289364799086880983235520230\,00y^3\\
&- 357488525368202220577902927288300403\,2000y^2z\\
&+ 207629445102785872778120666532285589\,75600y^2w\\
&+ 200137279444380575756681286064718755\,84000yz^2\\
&+ 647215004648674393371118931877126910\,97600yzw\\
&- 351425459041632833836477745377146122\,692640yw^2\\
&+ 575920685563555808513465696645708185\,6000z^3\\
&- 406645509553946606042771346800156046\,540800z^2w\\
&- 328485329712224304612237337404060764\,8010240zw^2\\
&- 268106050681753140543157949595922173\,9841728w^3
\end{aligned}$$

FIGURE 5. Cubic form defining S_0 (see Example 12.6).

Example 12.6. Let S_0 be the cubic surface given by the form in the variables x, y, z, w shown in Figure 5. S_0 has bad reduction at

$$p = 2,\ 3,\ 5,\ 7,\ 13,\ 113,\ 463,\ 733,\ 2141,\ 9643,\ 14143,\ 17278361,\ 22436341\,.$$

Choosing better models and running the LLL-based reduction algorithm, one gets the new surface S given by

$$\begin{aligned}&2x^3 + 16x^2z - 12x^2w - 17xy^2 + 61xyz - 26xyw\\ &- 20xz^2 + 95xzw + 18xw^2 + 5y^3 + 33y^2z + 10y^2w\\ &- 25yzw - 22yw^2 - 11z^3 - 21z^2w + 50zw^2 - 52w^3 = 0\,.\end{aligned}$$

S has bad reduction at

$$p = 2,\ 3,\ 5,\ 7,\ 13,\ 733,\ 22436341\,.$$

The reduction of S modulo 3, 5, 7, 13 and 22436341 has a unique singularity of type A_1. The reduction modulo 2 has one singular point of type A_1 and one of type A_3. Finally, the reduction modulo 733 is a cone over a smooth curve.

Remark 12.7. The initial equation for S_0 was constructed by [EJ10] such that the 27 lines form orbits of lengths 6, 9 and 12 under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. In particular, the field K of definition of the 27 lines is a degree 144 number field. The surface is of arithmetic Picard rank 1, and the lines in the orbit of length 12 form a double-six. The construction was started with the polynomial

$$t^6 + 330t^4 + 1452t^3 + 13705t^2 + 123508t + 835540\,.$$

The field K is generated by $\sqrt{5}$ together with all the roots of this polynomial.

References

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478 ↑2, 7, 8, 11, 12

[Cle61] A. Clebsch, *Ueber die Knotenpunkte der Hesseschen Fläche, insbesondere bei Oberflächen dritter Ordnung*, J. Reine Angew. Math. **59** (1861), 193–228, DOI 10.1515/crll.1861.59.193 (German). MR1579178 ↑12.4

[CFS10] John E. Cremona, Tom A. Fisher, and Michael Stoll, *Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves*, Algebra Number Theory **4** (2010), no. 6, 763–820, DOI 10.2140/ant.2010.4.763. MR2728489 ↑1, 6, 7

[DNS20] Maarten Derickx, Filip Najman, and Samir Siksek, *Elliptic curves over totally real cubic fields are modular*, Algebra Number Theory **14** (2020), no. 7, 1791–1800, DOI 10.2140/ant.2020.14.1791. MR4150250 ↑8.1

[Dol12] Igor V. Dolgachev, *Classical algebraic geometry*, Cambridge University Press, Cambridge, 2012. A modern view. MR2964027 ↑11.1, 11, 12.1, 12.2, 12.4

[Els09] Andreas-Stephan Elsenhans, *Good models for cubic surfaces*, 2009. Preprint, available at https://math.uni-paderborn.de/fileadmin/mathematik/AG-Computeralgebra/Preprints-elsenhans/red_5.pdf. ↑1

[EJ10] Andreas-Stephan Elsenhans and Jörg Jahnel, *Cubic surfaces with a Galois invariant double-six*, Cent. Eur. J. Math. **8** (2010), no. 4, 646–661, DOI 10.2478/s11533-010-0036-1. MR2671217 ↑12.7

[EJ15] ———, *Moduli spaces and the inverse Galois problem for cubic surfaces*, Trans. Amer. Math. Soc. **367** (2015), no. 11, 7837–7861, DOI 10.1090/S0002-9947-2015-06277-1. MR3391901 ↑12.5

[Fis06] Tom Fisher, *Testing equivalence of ternary cubics*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 333–345, DOI 10.1007/11792086_24. MR2282934 ↑9.1

[Fis13] ———, *Minimisation and reduction of 5-coverings of elliptic curves*, Algebra Number Theory **7** (2013), no. 5, 1179–1205, DOI 10.2140/ant.2013.7.1179. MR3101076 ↑1

[Hil93a] David Hilbert, *Theory of algebraic invariants*, Cambridge University Press, Cambridge, 1993. Translated from the German and with a preface by Reinhard C. Laubenbacher; Edited and with an introduction by Bernd Sturmfels. MR1266168 ↑6.3

[Hil93b] ———, *Ueber die vollen Invariantensysteme*, Math. Ann. **42** (1893), no. 3, 313–373, DOI 10.1007/BF01444162 (German). MR1510781 ↑11.1

[HS19] Benjamin Hutz and Michael Stoll, *Smallest representatives of* $\mathrm{SL}(2,\mathbb{Z})$*-orbits of binary forms and endomorphisms of* $\mathbb{P}^1$, Acta Arith. **189** (2019), no. 3, 283–308, DOI 10.4064/aa180618-9-12. MR3956143 ↑1, 2

[Kol97] János Kollár, *Polynomials with integral coefficients, equivalent to a given polynomial*, Electron. Res. Announc. Amer. Math. Soc. **3** (1997), 17–27, DOI 10.1090/S1079-6762-97-00019-X. MR1445631 ↑(document), 1, 1, 6

[Mum77] David Mumford, *Stability of projective varieties*, Monographies de L'Enseignement Mathématique [Monographs of L'Enseignement Mathématique], No. 24, L'Enseignement Mathématique, Geneva, 1977. Lectures given at the "Institut des Hautes Études Scientifiques", Bures-sur-Yvette, March-April 1976. MR0450273 ↑6.3

[MF82] David Mumford and John Fogarty, *Geometric invariant theory*, 2nd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete [Results in Mathematics and Related Areas], vol. 34, Springer-Verlag, Berlin, 1982. MR719371 ↑11.1

[Sto11] Michael Stoll, *Reduction theory of point clusters in projective space*, Groups Geom. Dyn. **5** (2011), no. 2, 553–565, DOI 10.4171/GGD/139. MR2782185 ↑1, 8, 12

[SC03] Michael Stoll and John E. Cremona, *On the reduction theory of binary forms*, J. Reine Angew. Math. **565** (2003), 79–99, DOI 10.1515/crll.2003.106. MR2024647 ↑1, 2

Institut für Mathematik, Universität Würzburg, Emil-Fischer-Strasse 30, 97074 Würzburg, Germany.

Email address: stephan.elsenhans@mathematik.uni-wuerzburg.de

URL: https://www.mathematik.uni-wuerzburg.de/computeralgebra/team/elsenhans-stephan-prof-dr/

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany.

Email address: Michael.Stoll@uni-bayreuth.de

URL: http://www.mathe2.uni-bayreuth.de/stoll/