K.A.E. Keijzer

Good models for quartic plane curves

Bachelor thesis

July 31, 2019

Thesis supervisor: dr. M. Streng

Leiden University
Mathematical Institute

Contents

1 Introduction

Motivation Let an equation $f = 0$ be given by some homogeneous polynomial f of degree $d > 0$ in $n+1 > 0$ variables and integer coefficients. (For example, $f = 0$ could be a model for a plane quartic with complex multiplication [6].) Doing calculations with (the zero set of) f can be computationally difficult if the coefficients of f are large. It would be convenient to have a method that finds a linear transformation such that our equation becomes simpler after this transformation. We clarify what we mean by this with an example.

Example 1.1. The equations

$$\begin{aligned}
&127140936503136239179440295995394767961088465632530 83u^4 + 28093295766866394308740265541643493393159804727598913u^3v + \\
&232782991286552970161615943512832474601882951449363 12u^2v^2 + 85726931644706728153129187924543531213774906162383 59uv^3 + \\
&118389880558910132719205821116851801044908071657186 3v^4 + 61607745430876337857813473712129634827358782266294u^3w + \\
&102097207724086991818093281289934229621706693702445u^2vw + 56398968193324967401002530976464782170810974976759uv^2w + \\
&103850166724368698629801516459856675353030590246797v^3w + 11194803975415617012897089746009408793144135 1306u^2w^2 + \\
&123681226433975794180339836915954751526318881822uvw^2 + 34161039813214943704376262035984335856149586475v^2w^2 + \\
&904097259355113305606483147344786348399120 08uw^3 + 49942749376496026536668781774851347277793120vw^3 + \\
&273807336031228033527194243066710597844 76w^4 = 0
\end{aligned}$$

and

$$X^4 + 307Y^4 + X^3Z + 309763X^2YZ + X^2Z^2 + 309763XYZ^2 + 95953116169Y^2Z^2 = 0,$$

with rational coefficients are isomorphic in the sense that we can get the latter out of the former via the substitution

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} -134 & 507527 & 25952626511649655 10 \\ 125291 & -474537745 & -2426590201174992561362 \\ -57022414 & 215971516999 & 1104389230626074904530729 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix},$$

and dividing out the factor 13699152495470303943258981418 07.

Reduction We will focus on homogeneous polynomials of degree 4 in 3 variables with rational coefficients. (The zero set of such polynomials are plane quartic curves.) Denote with $R[X, Y, Z]_4$ the set of homogeneous polynomials of degree 4 for any commutative ring R.

First, we make precise what is meant with a transformation. For matrices $A \in \mathrm{GL}_3(\mathbf{Q})$ and forms $f \in \mathbf{Z}[X, Y, Z]_4$ we define $f \circ A := f(A \cdot (X, Y, Z)^\intercal)$ where we mean the matrix-vector product of the matrix A with the vector $(X, Y, Z)^\intercal$. With this notation we state our goal: we want to find a rational $u \in \mathbf{Q}$ and a matrix $A \in \mathrm{GL}_3(\mathbf{Q})$ such that $uf \circ A$ is integral and has 'small' coefficients. A method of doing this is to first find a transformation that minimalizes the discriminant Δf of f. How the discriminant is defined for forms in more than 1 variable is discussed in [5].

After such a transformation is applied to f, methods of Stoll [11] can find a transformation M such that $f \circ M$ has in practice small coefficients and the same discriminant as f.

We make use of the fact that the discriminant is an *invariant*. An invariant is a polynomial map $I : \mathbf{C}[X, Y, Z]_4 \to \mathbf{C}$ with integer coefficients with the following property: there exists an integer $l \in \mathbf{Z}_{>0}$ such that for all matrices $A \in \mathrm{GL}_3(\mathbf{C})$ and homogeneous polynomials $h \in \mathbf{C}[X, Y, Z]_4$ it holds that

$$I(h \circ A) = \det(A)^l I(h).$$

Minimizing the discriminant Let $f \in \mathbf{Q}[X, Y, Z]_4$ be given. By multiplying f with the smallest common multiple of the denominators of the coefficients of f we may assume without loss of generality that $f \in \mathbf{Z}[X, Y, Z]_4$. In this case the discriminant Δf of f is an integer. Let p be a prime divisor of the discriminant of f. We give a method that finds (if they exist) a matrix M with integer coefficients and determinant equal to a power of p, and an exponent $e \in \mathbf{Z}_{>0}$ such that for $g_1 := \frac{1}{p^e} f \circ M \in \mathbf{Z}[X, Y, Z]_4$ it holds that,

$$\mathrm{ord}_p(\Delta g_1) < \mathrm{ord}_p(\Delta f),$$

and for all other primes $q \neq p$ dividing Δf that $\mathrm{ord}_q(\Delta g_1) = \mathrm{ord}_q(\Delta f)$. We call such a matrix M an *improvement*[1] for g at p (here p^e is implicitly taken to be the greatest common divisor of the coefficients of $f \circ M$).

[1] In further sections we use a different but equivalent definition: Definition 2.4.

By repeatedly applying this procedure we get a sequence of integral forms $g_1, g_2, g_3 \ldots$ with decreasing p-adic valuation of the discriminant:

$$\mathrm{ord}_p(\Delta(g_1)) > \mathrm{ord}_p(\Delta(g_2)) > \mathrm{ord}_p(\Delta(g_3)) > \ldots .$$

As the p-adic valuation of the discriminant of an integral form is non-negative, this sequence ends with some integral form g_n that has minimal p-adic valuation for its discriminant.

We will see that if we do this for all prime divisors of the discriminant of f we eventually get a form $\tilde{f}$ that has minimal discriminant.

Results Elsenhans [3] gave an algorithm that, given a model of a cubic surface $f = 0$ over $\mathbf{Q}$ with non-zero discriminant and p a prime dividing the discriminant, returns a model for the same surface that has minimal p-adic valuation for its discriminant. His method generalizes to quartic plane curves as is implemented in the method *MinimizePlaneQuartic* of the software package MAGMA [1]. We do the same for quartic plane curves, see Algorithm 6.1.

In Section 2.2 we prove the following theorem (restated: Theorem 2.12).

Theorem. *Let $g \in \mathbf{Z}[X, Y, Z]_4$ be a form with coprime coefficients and let p be a prime. Suppose that there exists an improvement M for g at p. Then there exists a matrix $P \in \mathrm{GL}_3(\mathbf{Z})$ and a 3-tuple of integers*

$$(0, w_1, w_2) \in \{(0, 0, 1), (0, 1, 1), (0, 1, 3)\},$$

such that the matrix

$$P \begin{pmatrix} 1 & 0 & 0 \\ 0 & p^{w_1} & 0 \\ 0 & 0 & p^{w_2} \end{pmatrix},$$

is an improvement for g at p.

With a *weight system* we (for now) mean one of the 3-tuples in the theorem.

Let $g \in \mathbf{Z}[X, Y, Z]_4$ be a form and p a prime divisor of the discriminant of g. We want to know if there exists a matrix M such that M is an improvement for g at p. Using this theorem we can do this as follows. For each weight system $w = (0, w_1, w_2)$ we do the following: We give an explicit construction of a matrix $\tilde{P}_w \in \mathrm{GL}_3(\mathbf{Z})$ such that: If there exists a matrix $P_w \in \mathrm{GL}_3(\mathbf{Z})$ such that $P_w \,\mathrm{diag}(1, p^{w_1}, p^{w_2})$ is an improvement for g at p, then $M_w := \tilde{P}_w \,\mathrm{diag}(1, p^{w_1}, p^{w_2})$ is an improvement for g at p

We test for each weight system w if M_w is indeed an improvement for g at p. We do this in order, so first we test $(0, 0, 1)$, then $(0, 1, 1)$ and finally $(0, 1, 3)$. If we find an improvement, then we apply it to g and start over. If none of these weight systems give an improvement, then we are certain that no improvement exists at p.

We will see in Section 3.1 that finding $\tilde{P}_{(0,0,1)}$ comes down to finding a linear factor of multiplicity 2 of $(g \bmod p)$. In Section 4 we illustrate how such an linear factor can be found.

In the Sections 3.2 and 3.3 we will see that for finding $\tilde{P}_{(0,1,1)}$ and $\tilde{P}_{(0,1,3)}$ for g at p, we need to find special singularities of $(g \bmod p)$. We can not always pinpoint these special singularities, but we can give a 'small' set $\mathcal{L}$ in such a way that these special singularities are contained in $\mathcal{L}$. Now we can iterate over the points in $\mathcal{L}$, and treat each point as if it is this special singularity and test if our algorithms give an improvement. As we iterate over $\mathcal{L}$ it is important that $\mathcal{L}$ has few elements. In Section 5 we give for both the weight systems $(0, 1, 1)$ and $(0, 1, 3)$ methods for finding a set $\mathcal{L}$ that contains this special singularity of $(g \bmod p)$ such that the size of $\mathcal{L}$ is not too big. In Section 6 we combine all the theory and state the full algorithm.

2 Invariants, improvements and weight systems

This section is based on a pre-print of Elsenhans [3].

Given an integer homogeneous polynomial g in the variables X, Y, and Z of degree 4, our goal is to find a rational $u \in \mathbf{Q}$ and a matrix M such that

$$|\Delta\left(ug(M \cdot (X, Y, Z))\right)| < |\Delta(g)|,$$

where Δ denotes the discriminant. In this section, we categorise such 'improvements' M as above. What we exactly mean by improvement is the subject of Definition 2.4. We show in Proposition 2.9 that, if a matrix M as above exists, then there exists a prime p, an integer e and matrices $P \in \mathrm{GL}_3(\mathbf{Z})$ and $D \in \mathrm{GL}_3(\mathbf{Q})$ where D is a diagonal matrix such that the form

$$\frac{1}{p^e} g(PD \cdot (X, Y, Z)),$$

is an integer polynomial and has in absolute value smaller discriminant than g. In Theorem 2.12 we show that D can be chosen to be one of the following matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & p \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & p \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & p^3 \end{pmatrix}.$$

2.1 Invariants and improvements

We will mostly consider homogeneous polynomials in 3 variables of degree 4 (the zero sets of which are called quartic plane curves), however our first definitions are more general so we postpone this restriction.

Let d and n be positive integers. Define for every commutative ring R:

$$R[X_0, \ldots, X_n]_d := \{f \in R[X_0, \ldots, X_n] : f \text{ is homogenous of degree } d\}.$$

We call the elements of $R[X_0, \ldots, X_n]_d$ *forms*, or *form of degree d*. We take the zero polynomial to be homogeneous of every degree.

Definition 2.1. Define for every commutative ring R the map $\Phi : R[X_0, \ldots, X_n] \times \mathrm{GL}_{n+1}(R) \to R[X_0, \ldots, X_n]$ by

$$(f, A) \mapsto f(A \cdot X), \quad \text{where } \text{`}\cdot\text{'} \text{ denotes the matrix-vector product and } X = (X_0, \ldots, X_n)^\intercal.$$

Instead of $\Phi(f, A)$ we write $f \circ A$. Note that if $f \in R[X_0, \ldots, X_n]_d$, then for all $A \in \mathrm{GL}_{n+1}(R)$ it holds that $f \circ A \in R[X_0, \ldots, X_n]_d$.

Let R be a commutative ring. Definition 2.1 defines a right $\mathrm{GL}_{n+1}(R)$ action on $R[X_0, \ldots, X_n]$. Let $A \in \mathrm{GL}_{n+1}(R)$ be a matrix. It can be verified that the map $(\_ \circ A) : R[X_0, \ldots, X_n] \to R[X_0, \ldots, X_n]$ given by $(\_ \circ A)(f) = f \circ A$ satisfies

$$\begin{aligned} (rf) \circ A &= r(f \circ A), \\ (f + g) \circ A &= f \circ A + g \circ A, \\ (fg) \circ A &= (f \circ A)(g \circ A) \text{ and} \\ 1 \circ A &= 1, \end{aligned}$$

for $f, g \in R[X_0, \ldots, X_n]$ and $r \in R$.

Definition 2.2. Let $f, g \in \mathbf{Q}[X_0, \ldots, X_n]_d$ be two forms. We say that f and g are *equivalent* if there exists a matrix $M \in \mathrm{GL}_{n+1}(\mathbf{Q})$ and a rational $u \in \mathbf{Q}^*$ such that:

$$g = u(f \circ M).$$

As explained in the introduction, our goal is, given $g \in \mathbf{Z}[X, Y, Z]_4$, to find a form $\tilde{g} \in \mathbf{Z}[X, Y, Z]_4$ equivalent to g that has smaller discriminant. How to define the discriminant is explained in [5], to calculate the discriminant of elements of $\mathbf{Q}[X, Y, Z]_4$ the code of J. Sijsling [9, 7] can be used. There are two properties of the discriminant that we will need. The first is that the discriminant of a form is zero if and only if that form has a *singular point* (see Definition 3.9). The second property is that the discriminant is an invariant, as in the following definition.

Definition 2.3. An *invariant* $I : \mathbf{C}[X_0, \ldots, X_n]_d \to \mathbf{C}$ of *weight* $l \in \mathbf{Z}_{>0}$ is a polynomial map with integer coefficients such that for all $f \in \mathbf{C}[X_0, \ldots, X_n]_d$ and $A \in \mathrm{GL}_{n+1}(\mathbf{C})$ the following holds:

$$I(f \circ A) = I(f) \cdot \det(A)^l.$$

The *degree* of an invariant is the degree of the defining polynomial.

From the requirement that the coefficients of an invariant I are integers it follows that if $f \in \mathbf{Z}[X_0, \ldots, X_n]_d$, then $I(f) \in \mathbf{Z}$. An invariant $I : \mathbf{C}[X_0, \ldots, X_n]_d \to \mathbf{C}$ of weight l is homogeneous of degree $\frac{(n+1)l}{d}$. The discriminant $\Delta : \mathbf{C}[X, Y, Z]_4 \to \mathbf{C}$ is an invariant of degree 27 and hence of weight 36.

Definition 2.4. Let $n, d > 0$ be positive integers, $f \in \mathbf{Z}[X_0, \ldots, X_n]_d$ a form and p a prime. Let $M \in \mathrm{GL}_{n+1}(\mathbf{Q})$ be a matrix with integer coefficients. We say that M is an *improvement* for f at p if $\det(M)$ is a power of p and there exists a positive integer $e \in \mathbf{Z}_{>0}$ such that $\frac{1}{p^e}(f \circ M) \in \mathbf{Z}[X_0, \ldots, X_n]_d$ and

$$e > \frac{d \operatorname{ord}_p(\det(M))}{n+1}.$$

The following lemma explains why we call this an improvement. Note that the definition of an improvement does not mention any invariants.

Lemma 2.5. *Let $f \in \mathbf{Z}[X_0, \ldots, X_n]_d$ be a form, and suppose that $I : \mathbf{C}[X_0, \ldots, X_n]_d \to \mathbf{C}$ is an invariant such that $I(f) \neq 0$. Let p be a prime such that $p \mid I(f)$. Let $M \in \mathrm{GL}_{n+1}(\mathbf{Q})$ be a matrix with integer coefficients such that $\det(M)$ is a power of p. Then the following are equivalent:*

1. *The matrix M is an improvement of f at p.*
2. *There is a positive integer $u \in \mathbf{Z}_{>0}$ such that $\frac{1}{p^u} f \circ M \in \mathbf{Z}[X_0, \ldots, X_n]_d$ and*

$$\operatorname{ord}_p\left(I\left(\frac{1}{p^u} f \circ M\right)\right) < \operatorname{ord}_p\left(I(f)\right).$$

Proof. Let $l \in \mathbf{Z}_{>0}$ be the weight of I. Denote for any $t \in \mathbf{Z}_{>0}$ the polynomial $\frac{1}{p^t} f \circ M \in \mathbf{Q}[X_0, \ldots, X_n]_d$ by g_t. Let us first calculate $\operatorname{ord}_p\left(I\left(g_t\right)\right)$ for each $t \in \mathbf{Z}_{>0}$. Using the fact that multiplying f by any $x \in \mathbf{Z}_{>0}$ is the same as acting on f with a matrix $\mathrm{id}_{n+1} \cdot x^{\frac{1}{d}}$ (with $x^{\frac{1}{d}}$ some d-th root of x) we see that

$$I(g_t) = p^{-\frac{t(n+1)l}{d}} \det\left(M\right)^l I\left(f\right) \in \mathbf{Q}.$$

So we get that,

$$\operatorname{ord}_p\left(I\left(g_t\right)\right) = \operatorname{ord}_p\left(I(f) \det(M)^l p^{-l\frac{(n+1)t}{d}}\right).$$

Using that $\operatorname{ord}_p(xy) = \operatorname{ord}_p(x) + \operatorname{ord}_p(y)$ and $\operatorname{ord}_p(x^z) = z \operatorname{ord}_p(x)$ for any $x, y \in \mathbf{Q}^*$ and $z \in \mathbf{Z}$ we get the following formula,

$$\operatorname{ord}_p\left(I\left(g_t\right)\right) = \operatorname{ord}_p\left(I(f)\right) + l \operatorname{ord}_p\left(\det(M)\right) - l\frac{(n+1)t}{d}. \tag{1}$$

Now we prove that (*1* $\Rightarrow$ *2*). Suppose that M is an improvement for f at p. Then there exists an integer $e \in \mathbf{Z}_{>0}$ such that $\frac{1}{p^e} f \circ M \in \mathbf{Z}[X_0, \ldots, X_n]_d$ and

$$e > \frac{d \operatorname{ord}_p\left(\det(M)\right)}{n+1}.$$

We show that we can take $u = e$ in *2*. Using Equation (1) it follows that

$$\operatorname{ord}_p\left(I\left(g_e\right)\right) = \operatorname{ord}_p(I(f)) + l\left(\operatorname{ord}_p(\det(M)) - \frac{(n+1)e}{d}\right) < \operatorname{ord}_p(I(f)).$$

This proves the first implication. For the second implication, suppose that there exists an $u \in \mathbf{Z}_{>0}$ such that $g_u \in \mathbf{Z}[X_0, \ldots, X_n]_d$ and $\operatorname{ord}_p(I(g_u)) < \operatorname{ord}_p(I(f))$. Take e to be equal to u. Then from Equation (1) it is again immediate that the following holds:

$$\operatorname{ord}_p\left(I\left(g_e\right)\right) - \operatorname{ord}_p(I(f)) = l\left(\operatorname{ord}_p(\det(M)) - \frac{(n+1)e}{d}\right).$$

Since the left hand side of this equation is negative, this implies that $e > \frac{d \operatorname{ord}_p(\det(M))}{n+1}$. Per assumption $\det(M)$ is a p-th power, so it is an improvement for f at p. □

In Definition 2.4 we require that the determinant of an improvement is a prime power. This corresponds with the property that the valuation of all other primes of the invariant is the same as before an improvement is applied. We show in Proposition 2.9 that this is not a restriction.

Let $g \in \mathbf{Z}[X,Y,Z]_4$ be a form and I an invariant. Assume that $I(g) \neq 0$. Let $M \in \mathrm{GL}_3(\mathbf{Q})$ be some matrix and u a non-zero rational such that $ug \circ M \in \mathbf{Z}[X,Y,Z]_4$ and

$$|I(ug \circ M)| < |I(g)|\,.$$

Without loss of generality we may assume that M has coprime integer coefficients (we just have to change u). So there is some prime p such that

$$\mathrm{ord}_p(I(ug \circ M)) < \mathrm{ord}_p(I(g)).$$

It may very well be the case that there is some prime $q \neq p$ different from p such that the q-adic valuation of the invariants is not the same. It could even be that the q-adic valuation is becomes bigger:

$$\mathrm{ord}_q(I(ug \circ M)) > \mathrm{ord}_q(I(g)).$$

This motivates the following definition.

Definition 2.6. Let $f \in \mathbf{Z}[X,Y,Z]_4$ be a form and p a prime. A matrix $M \in \mathrm{GL}_3(\mathbf{Q})$ with integer coefficients is called a *local improvement for f at p* if there exists a positive integer e such that $\frac{1}{p^e} f \circ M \in \mathbf{Z}[X,Y,Z]_4$ and

$$e > \frac{4}{3}\,\mathrm{ord}_p(\det(M)).$$

In the next section, we will see in Proposition 2.9 that the existence of a local improvement implies the existence of an improvement.

2.2 Weight systems

In this section we prove Theorem 2.12 which implies that we only have to look for improvements that have a very specific form.

Theorem 2.7 (Smith normal form)**.** *Let $n \in \mathbf{Z}_{\geq 0}$ and let $M \in \mathrm{GL}_{n+1}(\mathbf{Q})$ be a matrix with integer coefficients. There exist matrices $P, Q \in \mathrm{GL}_{n+1}(\mathbf{Z})$ such that the matrix $D = P^{-1}MQ^{-1}$ in $\mathrm{GL}_{n+1}(\mathbf{Q})$ has integer coefficients, is diagonal and satisfies the following property: If we write $D = \mathrm{diag}(d_0, \ldots, d_n)$, then $d_i \mid d_{i+1}$ for $i \in \{0, \ldots, n-1\}$.*

Proof. See [8] Theorem II.9 (Smith normal form). □

For a prime p, we denote with $\mathbf{Z}_{(p)}$ the ring

$$\mathbf{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbf{Q} : p \nmid b \text{ and } a, b \in \mathbf{Z} \right\},$$

which has group of units

$$\mathbf{Z}_{(p)}^* = \left\{ \frac{a}{b} \in \mathbf{Z}_{(p)} : p \nmid a \text{ and } a, b \in \mathbf{Z} \text{ coprime} \right\}.$$

Corollary 2.8. *Let $f \in \mathbf{Z}[X,Y,Z]_4$ be a form, suppose that $M \in \mathrm{GL}_3(\mathbf{Q})$ is a local improvement for f at some prime p such that all the entries of M do not have a common divisor. Then there exist matrices P and Q with $P \in \mathrm{GL}_3(\mathbf{Z})$ and $Q \in \mathrm{GL}_3(\mathbf{Z}_{(p)})$ and a diagonal matrix $D \in \mathrm{GL}_3(\mathbf{Q})$ such that D is of the form*

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & p^{w_1} & 0 \\ 0 & 0 & p^{w_2} \end{pmatrix},$$

with w_1 and w_2 non-negative integers and $w_1 \leq w_2$, such that $M = PDQ$.

Proof. It follows from Theorem 2.7 that there exist matrices $P, Q' \in \mathrm{GL}_3(\mathbf{Z})$ and $D' = \mathrm{diag}(d_0, d_1, d_2)$ such that $M = PD'Q'$ and $d_0 \mid d_1 \mid d_3$.

As every entry of D' is divisible by d_0, it follows that d_0 divides all the coefficients of M. As the latter are coprime, we have that $d_0 = 1$.

Define $w_i = \mathrm{ord}_p(d_i)$ for each diagonal entry d_i of D'. As $1 = d_1 \mid d_2 \mid d_3$ we have that $0 = w_0 \leq w_1 \leq w_2$. Take $D = \mathrm{diag}(1, p^{w_1}, p^{w_2})$. Then it follows that the determinant of $D^{-1}D'$ is not divisible by p. So $D^{-1}D' \in \mathrm{GL}_n(\mathbf{Z}_{(p)})$. With $Q = D^{-1}D'Q' \in \mathrm{GL}_3(\mathbf{Z}_{(p)})$, we have that

$$M = PD'Q' = PDD^{-1}D'Q' = PDQ.$$

□

The next proposition comes with a proof of the already stated fact that the existence of a local improvement implies the existence of an improvement.

Proposition 2.9. *Let $f \in \mathbf{Z}[X,Y,Z]_4$ be a form and let $M \in \mathrm{GL}_3(\mathbf{Q})$ be a local improvement of f at some prime p. Let P, D and Q be matrices as in Corollary 2.8. Then PD is an improvement of f at p.*

Proof. Since M is a local improvement of f at p there is a positive integer $e \in \mathbf{Z}_{>0}$ such that

$$\frac{1}{p^e} f \circ M \in \mathbf{Z}[X,Y,Z]_4, \quad \text{and } e > \frac{4 \operatorname{ord}_p(M)}{3}.$$

We know that $\det(PD) = \pm p^{\operatorname{ord}_p(\det(M))}$. As $Q \in \mathrm{GL}_3(\mathbf{Z}_{(p)})$ it follows that

$$\frac{1}{p^e} f \circ PD = (\frac{1}{p^e} f \circ M) \circ Q^{-1} \in \mathbf{Z}_{(p)}[X,Y,Z]_4.$$

But as PD is an integral matrix $f \circ PD \in \mathbf{Z}[X,Y,Z]_4$ so it follows that $\frac{1}{p^e} f \circ PD \in \mathbf{Z}[X,Y,Z]_4$. Thus PD is an improvement of f at p. □

We see that finding an improvement reduces to finding a matrix $P \in \mathrm{GL}_3(\mathbf{Z})$ and a diagonal matrix $D \in \mathrm{GL}_3(\mathbf{Q})$ with integer coefficients and certain properties. We shall first focus on this diagonal matrix. The matrix D is completely determined by the exponents w_1, w_2, so we give them a name.

Definition 2.10. A *weight system* is a triple $(0, w_1, w_2)$ of integers such that $0 \leq w_1 \leq w_2$. We say that a form $f \in \mathbf{Z}[X,Y,Z]_4$ *can be improved* at some prime p with a weight system $(0, w_1, w_2)$ or that a weight system $(0, w_1, w_2)$ is an *improvement* for f at p, if $\operatorname{diag}(1, p^{w_1}, p^{w_2})$ is an improvement for f at p.

We also say that an improvement M is of *type* $(0, w_1, w_2)$ if $M = P \operatorname{diag}(1, p^{w_1}, p^{w_2})$ for some matrix $P \in \mathrm{GL}_3(\mathbf{Z})$.

Lemma 2.11. *Let $f \in \mathbf{Z}[X,Y,Z]_4$ be a form. Let p be a prime. Then a weight system $(0, w_1, w_2)$ is an improvement for f at p if and only if for $k = \lfloor \frac{4}{3}(w_1 + w_2) \rfloor + 1$:*

$$f(X, p^{w_1}Y, p^{w_2}Z) \equiv 0 \pmod{p^k}.$$

Proof. Suppose that for $k = \lfloor \frac{4}{3}(w_1 + w_2) \rfloor + 1$:

$$f(X, p^{w_1}Y, p^{w_2}Z) \equiv 0 \pmod{p^k}.$$

Then all the coefficients of $f \circ \operatorname{diag}(1, p^{w_1}, p^{w_2})$ are divisible by p^k so $\frac{1}{p^k} f(X, p^{w_1}Y, p^{w_2}Z) \in \mathbf{Z}[X,Y,Z]_4$. It holds that $k > \frac{4}{3}(w_1 + w_2)$. So the weight system $(0, w_1, w_2)$ is an improvement.

Suppose that $(0, w_1, w_2)$ is an improvement for f at p. Then there exists a positive integer $e > \frac{4}{3} \operatorname{ord}_p(p^{w_1+w_2})$ such that $\frac{1}{p^e} f \circ \operatorname{diag}(1, p^{w_1}, p^{w_2}) \in \mathbf{Z}[X,Y,Z]_4$. But this means that:

$$f(X, p^{w_1}Y, p^{w_2}Z) \equiv 0 \pmod{p^e}.$$

Note that as $e \geq k$, it is true that

$$f(X, p^{w_1}Y, p^{w_2}Z) \equiv 0 \pmod{p^k}.$$ □

Now we are able to state one of the main theorem of this section.

Theorem 2.12. *Let $f \in \mathbf{Z}[X,Y,Z]_4$ be a form with coprime coefficients. Let $(0, w_1, w_2)$ be a weight system and suppose that f can be improved at some prime p with this weight system. Then f can be improved at p with one of the following weight systems:*

$$(0,0,1), \quad (0,1,1) \quad \textit{or} \quad (0,1,3).$$

This theorem implies that we only have to consider improvements of the form $P \operatorname{diag}(1, p^{w_1}, p^{w_2})$ with $P \in \mathrm{GL}_3(\mathbf{Z})$ and where $(0, w_1, w_2)$ is a weight system as in the theorem.

To prove this theorem we give three lemmas that give conditions on when we can replace a weight system with one of the theorem's. Then we observe that always at least one of these conditions is satisfied, proving the theorem. This is explained more visually in Remark 2.16.

Lemma 2.13. *Let $f \in \mathbf{Z}[X,Y,Z]_4$ be a form and suppose that $(0,w_1,w_2)$ is an improvement for f at some prime p. Suppose that:*

$$w_1 = 0 \quad \text{and} \quad w_2 \geq 1.$$

Then the weight system $(0,0,1)$ is an improvement for f at p.

Proof. We may suppose that w_2 is at least 1, otherwise there is nothing to prove. Write $f = \sum_e a_e X^{e_0} Y^{e_1} Z^{e_2}$ where $e = (e_0, e_1, e_2)$ such that $e_0, e_1, e_2 \geq 0$ and $e_0 + e_1 + e_2 = 4$. Define $k = \lfloor \frac{4}{3} w_2 \rfloor + 1$. Note that as $w_2 \geq 1$ we have $k \geq 2$. Since $(0,0,w_2)$ is an improvement, all coefficients of $f(X,Y,p^{w_2}Z)$ are divisible by p^k, i.e.

$$\operatorname{ord}_p(a_e) + w_2 e_2 \geq k. \tag{2}$$

To show that $(0,0,1)$ is an improvement, we shall prove that $\operatorname{ord}_p(a_e) + e_2 \geq 2$. If $e_2 = 0$, then $\operatorname{ord}_p(a_e) \geq k \geq 2$. If $e_2 = 1$, then subtracting w_2 from both sides of inequality (2) we get

$$\operatorname{ord}_p(a_e) \geq \lfloor \frac{1}{3} w_2 \rfloor + 1,$$

so $\operatorname{ord}_p(a_e) + 1 \geq 2$. For $e_2 \geq 2$ it is clear since $\operatorname{ord}_p(a_e) \geq 0$. □

Lemma 2.14. *Let $f \in \mathbf{Z}[X,Y,Z]_4$ be a form and suppose that $(0,w_1,w_2)$ is an improvement for f at some prime p. Suppose that:*

$$w_1 \geq 1 \quad \text{and} \quad w_2 \leq 2w_1.$$

Then the weight system $(0,1,1)$ is an improvement for f at p.

Proof. We use the same strategy as in the proof of Lemma 2.13. Again write $f = \sum_e a_e X^{e_0} Y^{e_1} Z^{e_2}$ and define $k = \lfloor \frac{4}{3}(w_1 + w_2) \rfloor + 1$. Knowing that $\operatorname{ord}_p(a_e) + w_1 e_1 + w_2 e_2 \geq k$ we shall prove that $\operatorname{ord}_p(a_e) + e_1 + e_2 \geq 3$, showing that the weight system $(0,1,1)$ is an improvement for f at p.

The case $(e_1, e_2) = (0,0)$ is trivial since $k \geq 3$.

If $e_1 + e_2 \geq 3$, then it is clear that $\operatorname{ord}_p(a_e) + e_1 + e_2 \geq 3$. Hence, if e_1, e_2 are both at least 1, then we only have to consider the option where $(e_1, e_2) = (1,1)$.

So we are left with three cases: $(0,1)$, $(1,0)$ and $(1,1)$. Note that in the former two cases we need to show that

$$\operatorname{ord}_p(a_e) \geq k - w_i \geq 2, \quad \text{for } i = 1, 2.$$

As $w_1 \leq w_2$ it suffices to show that $k - w_2 \geq 2$. Hence we are left with two cases: $(0,1)$ and $(1,1)$.

First, the $(0,1)$ case: We know that

$$\operatorname{ord}_p(a_e) + w_2 \geq k = \left\lfloor \frac{4}{3}(w_1 + w_2) \right\rfloor + 1,$$

and we show that $k - w_2 \geq 2$. Using the assumptions we see that

$$\left\lfloor \frac{4}{3}(w_1 + w_2) \right\rfloor - w_2 = \left\lfloor \frac{4w_1 + w_2}{3} \right\rfloor \geq w_2 \geq w_1 \geq 1.$$

Hence $\operatorname{ord}_p(a_e) \geq k - w_2 \geq 2$. This shows that $\operatorname{ord}_p(a_e) + 1 \geq 3$.

Finally, the $(1,1)$ case: Note that

$$\left\lfloor \frac{4}{3}(w_1 + w_2) \right\rfloor - w_1 - w_2 = \left\lfloor \frac{w_1 + w_2}{3} \right\rfloor \geq 0.$$

Hence, $k - w_1 - w_2 \geq 1$. So we see that

$$\operatorname{ord}_p(a_e) \geq k - w_1 - w_2 \geq 1, \quad \text{thus} \quad \operatorname{ord}_p(a_e) + 2 \geq 3.$$

Thus the weight system $(0,1,1)$ is indeed an improvement for f. □

Lemma 2.15. *Let $f \in \mathbf{Z}[X,Y,Z]_4$ be a form and suppose that the weight system $(0,w_1,w_2)$ is an improvement for f at prime p. Suppose that*

$$w_1 \geq 1 \quad \text{and } w_2 > 2w_1.$$

Then the weight system $(0,1,3)$ is an improvement for f at p.

Proof. We use the same strategy as in the proofs of Lemmas 2.13 and 2.14. Write $f = \sum_e a_e X^{e_0} Y^{e_1} Z^{e_2}$ and define $k = \lfloor \frac{4}{3}(w_1 + w_2) \rfloor + 1$. We need to show that $\mathrm{ord}_p(a_e) + e_1 + 3e_2 \geq 6$, knowing that $\mathrm{ord}_p(a_e) + w_1 e_1 + w_2 e_2 \geq k$.

First the case $(e_1, e_2) = (0, 0)$. We show that $k \geq 6$. Using our assumptions we have that,

$$\left\lfloor \frac{4w_1 + 4w_2}{3} \right\rfloor > \left\lfloor \frac{12w_1}{3} \right\rfloor = 4w_1. \tag{3}$$

As $w_1 \geq 1$ it follows that $k > 5$, and as k is an integer that $k \geq 6$.

If e_2 is at least 2 or if $(e_1, e_2) = (3, 1)$, then it is clear that $\mathrm{ord}_p(a_e) + e_1 + 3e_2 \geq 6$. We are left with the cases: $e_2 = 0$, and (e_1, e_2) is one of the following $(0, 1)$, $(1, 1)$ and $(2, 1)$.

Now, the cases where $e_2 = 0$. We show that $\mathrm{ord}_p(a_e) + e_1 \geq 6$ knowing that $\mathrm{ord}_p(a_e) + e_1 w_1 \geq k$. As we already discussed the $(0, 0)$ case we may assume that e_1 is at least 1. It follows from inequality (3) that

$$k > 4w_1 + 1$$

From this we get, using that $w_1 \geq 1$ and $e_1 < 4$, that

$$\mathrm{ord}_p(a_e) + e_1 > 4w_1 + 1 + (1 - w_1)e_1 = w_1(4 - e_1) + 1 + e_1 \geq 5.$$

Hence $\mathrm{ord}_p(a_e) + e_1 \geq 6$,

Finally, the cases where $e_2 = 1$ and $e_1 < 3$. Using $w_2 > 2w_1$, we have that

$$\mathrm{ord}_p(a_e) + e_1 w_1 \geq k - w_2 \geq 1 + \left\lfloor \frac{4w_1 + w_2}{3} \right\rfloor \geq 2w_1 + 1.$$

From this it follows, using that $w_1 \geq 1$ and $e_1 < 3$, that

$$\mathrm{ord}_p(a_e) + e_1 \geq 2w_1 + 1 + e_1(1 - w_1) = w_1(2 - e_1) + 1 + e_1 \geq 3$$

So we conclude that $\mathrm{ord}_p(a_e) + e_1 + 3 \geq 6$. Hence the weight system $(0, 1, 3)$ is an improvement for f at p. □

Proof of Theorem 2.12. Let $f \in \mathbf{Z}[X, Y, Z]_4$ be a form with coprime coefficients. Suppose that the weight system $(0, w_1, w_2)$ is an improvement.

First, suppose that $w_1 = 0$. Since the coefficients of f are coprime the weight system $(0, 0, 0)$ can not be an improvement. Hence $w_2 \geq 1$, using Lemma 2.13, we see that $(0, 0, 1)$ is an improvement.

Now, suppose that $w_1 \geq 1$. Then there are two options:

$$2w_1 \geq w_2 \quad \text{or} \quad 2w_1 < w_2.$$

In the first case it follows from Lemma 2.14 that the weight system $(0, 1, 1)$ is an improvement. In the second case it follows from Lemma 2.15 that the weight system $(0, 1, 3)$ is an improvement. □

Remark 2.16. We may interpret this proof a bit more geometrically. If we let a weight system $(0, w_1, w_2)$ correspond with a point $w \in \mathbf{Z}^2 \subseteq \mathbf{R}^2$ given by $w = (w_1, w_2)$, then the lemmas above give regions in $\mathbf{R}^2$ and per region a special point. This happens in such away that if a weight system w that improves some form were to lie in one of those regions, then the weight system corresponding to the special point of this region is an improvement.

Then the proof of the theorem is observing that all possible weight systems lie in a region. This is illustrated in Figure 1.

Example 2.17. We list three examples of forms that can only be improved by one of the weight systems in Theorem 2.12. This shows that indeed all these weight systems are needed.

1. Let $f = 7^2X^4 + 7^2Y^4 + Z^4$. Then $(0, 0, 1)$ is an improvement for f at 7. Let $(0, w_1, w_2)$ be a weight system with $k = \lfloor \frac{4}{3}(w_1 + w_2) \rfloor + 1$. Suppose that $k > 2$. Then the weight system $(0, w_1, w_2)$ is not an improvement for f at 7 since $f(X, 7^{w_1}Y, 7^{w_2}Z) \pmod{7^k}$ always contains 7^2X^4 as a monomial. So $(0, 1, 1)$ and $(0, 1, 3)$ are not improvements for f.
2. Let $f = 7^3X^4 + 7X^2Y^2 + Z^4$. Then $(0, 0, 1)$ is not an improvement at 7, since $f(X, Y, 7Z) \equiv 7X^2Y^2 \pmod{7^2}$ is not zero. However $(0, 1, 1)$ is an improvement, since $f(X, 7Y, 7Z) \equiv 0 \pmod{7^3}$. But $(0, 1, 3)$ is not an improvement since $f(X, 7Y, 7^3Z) \equiv 7^3X^4 + 7^3X^2Y^2 + 7^4Z^4 \pmod{7^6}$

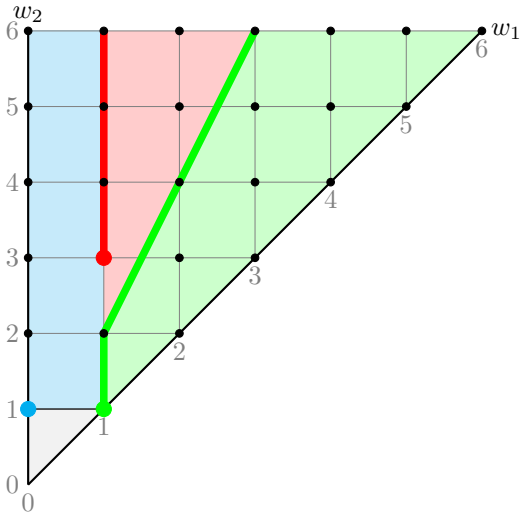

Figure 1: Every weight system $(0, w_1, w_2)$ corresponds with a lattice point $w = (w_1, w_2) \in \mathbf{R}^2$. We see that w always lies in one of the coloured regions. If w lies in a coloured region we may use the weight system corresponding with the marked point of the same colour. The thick coloured lines on the edges of a region indicate that the points on that line belong to the region with that colour.

3. Let $f = 7^6X^4 + Y^3Z + X^2Z^2$. Then $f(X, Y, 7Z) \equiv Y^3Z \pmod{7^2}$ so $(0, 0, 1)$ is not an improvement. Also $f(X, 7Y, 7Z) \equiv 7^2X^2Z^2 \pmod{7^3}$ thus $(0, 1, 1)$ is not an improvement. But $f(X, 7X, 7^3Z) \equiv 0 \pmod{7^6}$, so $(0, 1, 3)$ is an improvement.

Let $g \in \mathbf{Z}[X, Y, Z]_4$ be a form and I an invariant such that $I(g) \neq 0$. Suppose that

$$|I(g)| > \min\{|I(h)| : h \in \mathbf{Z}[X, Y, Z] \text{ and } h \text{ is equivalent with } g\}.$$

Denote with h a form equivalent to g with $|I(h)| < |I(g)|$. Then there is a rational $u \in \mathbf{Q}$ and a matrix $M \in \mathrm{GL}_3(\mathbf{Q})$ such that

$$h = ug \circ M.$$

By taking a different rational for u, we may assume without loss of generality that M is an integer matrix with coprime coefficients. Then there is some prime p such that the left-hand-side of the inequality above has lower p-adic valuation than the right-hand-side. So M is an local improvement for g at p. Hence, it follows from Proposition 2.9 that there exists an improvement for g at p. Theorem 2.12 implies that to find an improvement for g at p we only need to consider matrices of the form $P\,\mathrm{diag}(1, p^{w_1}, p^{w_2})$, with $P \in \mathrm{GL}_3(\mathbf{Z})$ and $(0, w_1, w_2)$ a weight system as in Theorem 2.12.

In the next section, we give for each of these weight systems w a method to find a matrix M_w with the following property. If there exists a matrix $P \in \mathrm{GL}_3(\mathbf{Z})$ such that $g \circ P$ can be improved with the weight system w, then $g \circ M_w$ can be improved by the weight system w.

By repeatedly finding these improvements we eventually find a form $\hat{g}$ that is equivalent to g such that

$$|I(\hat{g})| = \min\{|I(h)| : h \in \mathbf{Z}[X, Y, Z] \text{ and } h \text{ is equivalent with } g\}.$$

3 Finding an improvement

Let $g \in \mathbf{Z}[X, Y, Z]_4$ be a form and p a prime. We demonstrated that finding an improvement M for g comes down to finding a determinant 1 integral matrix P and a diagonal matrix D satisfying certain properties. Theorem 2.12 implies that there are three different possible options for D that we need to consider. In this section, we give for every weight system $(0, w_1, w_2)$ of Theorem 2.12 a method that gives an improvement of the form $P\,\mathrm{diag}(1, p^{w_1}, p^{w_2})$ with $P \in \mathrm{GL}_3(\mathbf{Z})$ if such a matrix exists.

3.1 Weight system $(0,0,1)$

Let $g \in \mathbf{Z}[X,Y,Z]_4$ be a form and p a prime. We construct a matrix $M \in \mathrm{GL}_3(\mathbf{Z})$ such that if there exists an (unknown) improvement of type $(0,0,1)$, then $M\,\mathrm{diag}(1,1,p)$ is an improvement for g at p. We do this by considering the linear factors of $(g \bmod p)$. In Section 4 we give a method for finding the relevant linear factor of $(g \bmod p)$ (if it exists).

Lemma 3.1. *Extend for any integers $m > 0$ the projection map $\tilde{q} : \mathbf{Z} \to \mathbf{Z}/p^m\mathbf{Z}$ to $q : \mathbf{Z}[X_0,\ldots,X_n] \to (\mathbf{Z}/p^m\mathbf{Z})[X_0,\ldots X_n]$, where $n \in \mathbf{Z}_{>0}$, by applying $\tilde{q}$ coefficient wise. Let $A \in \mathrm{GL}_{n+1}(\mathbf{Q})$ be a matrix with integer coefficients. Then $q(f) \circ (A \bmod p^m) = q(f \circ A)$ for all $f \in \mathbf{Z}[X_0,\ldots,X_n]$.*

Proof. Let $f \in \mathbf{Z}[X,Y,Z]$ be a form. As q is a ring homomorphism and since $f \circ A$ is defined using ring operations it follows that $q(f \circ M) = q(f) \circ (A \bmod p^m)$. □

For a prime p, positive integers m, n and polynomial $f \in \mathbf{Z}[X_1,\ldots,X_n]$ we write $(f \bmod p^m)$ instead of $q(f)$.

Proposition 3.2. *Let $g \in \mathbf{Z}[X,Y,Z]_4$ be a form and p a prime. Then the following are equivalent:*

1. *There is a matrix $P \in \mathrm{GL}_3(\mathbf{Z})$ such that $P\,\mathrm{diag}(1,1,p)$ is an improvement for g at p.*
2. *There is a linear form $l \in \mathbf{Z}[X,Y,Z]_1$ such that $(l^2 \bmod p)$ divides $(g \bmod p)$ and $(l \bmod p^2)$ divides $(g \bmod p^2)$.*

Proof. Let $P \in \mathrm{GL}_3(\mathbf{Z})$ as in *1.* The matrix $\mathrm{diag}(1,1,p)$ is an improvement for the form $f := g \circ P$. Writing $f = \sum a_{ijk}X^iY^jZ^k$, this implies that for every monomial a_{ijk} of f,

$$\mathrm{ord}_p(a_{ijk}) + k \geq 2.$$

Hence, for monomials a_{ijk} with $p \nmid a_{ijk}$ it holds that $k \geq 2$. Similarly for monomials a_{ijk} with $p^2 \nmid a_{ijk}$ it holds that $k \geq 1$. Thus Z divides $(f \bmod p^2)$ and Z^2 divides $(f \bmod p)$. So we can take $l = Z \circ P^{-1}$.

Now the other way around. Let $l \in \mathbf{Z}[X,Y,Z]_1$ be as in *2.* Let S be a permutation matrix such that $\deg_Z((l \circ S) \bmod p) > 0$. Write $((l \circ S) \bmod p) = aX + bY + cZ \in \mathbf{F}_p[X,Y,Z]$ (so $c \neq 0$). Per assumption we may write for some $\alpha, \beta, \gamma \in \mathbf{Z}[X,Y,Z]$,

$$g = \alpha p^2 + \beta pl + \gamma l^2.$$

Define the matrix

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ s & t & 1 \end{pmatrix},$$

with $s,t \in \{0,\ldots,p-1\} \subseteq \mathbf{Z}$ such that $s \equiv -ac^{-1} \pmod p$ and $t \equiv -bc^{-1} \pmod p$. We see that $((l \circ SM) \bmod p) \in Z\mathbf{F}_p$. Hence $l \circ SM \in \mathbf{Z}[pX,pY,Z]_1$, so

$$l \circ SM\,\mathrm{diag}(1,1,p) \in p\mathbf{Z}[X,Y,Z]_1.$$

As a consequence $l^2 \circ SM\,\mathrm{diag}(1,1,p) \in p^2\mathbf{Z}[X,Y,Z]_1$. So it follows that

$$g \circ SM\,\mathrm{diag}(1,1,p) \equiv 0 \pmod{p^2}.$$

So we may take $P = SM$. □

We now state what we need from this proposition more explicitly.

Proposition 3.3. *Let $g \in \mathbf{Z}[X,Y,Z]_4$ be a form and p a prime. Let $P \in \mathrm{GL}_3(\mathbf{Z})$ be a matrix such that the weight system $(0,0,1)$ is an improvement of $g \circ P$ at p. Then $(g \bmod p)$ contains a linear factor $(l \bmod p)$, where $l = Z \circ P^{-1}$, of multiplicity at least 2. Write $(l \bmod p) = aX + bY + cZ \in \mathbf{F}_p[X,Y,Z]$ and suppose $c \neq 0$. Let $s,t \in \{0,\ldots,p-1\} \subseteq \mathbf{Z}$ be lifts of $-c^{-1}a, -c^{-1}b \in \mathbf{F}_p$ respectively. Define*

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ s & t & 1 \end{pmatrix} \in \mathrm{SL}_3(\mathbf{Z}).$$

Then the weight system $(0,0,1)$ is an improvement for $g \circ M$ at p and $l \circ M \in \mathbf{Z}[pX,pY,Z]_1$.

Proof. This follows from the proof of Proposition 3.2. □

We have to make a choice for the permutation matrix in the proof of Proposition 3.2. The following algorithm gives, given a commutative ring R and 3-tuple v, a permutation matrix S such that the first entry of Sv is non-zero. In Proposition 3.3 the assumption is that the last entry is non-zero, this is repaired by swapping the X and Z afterwards. We make this choice since we will need it in the later sections, and it gives only a minor inconvenience right now.

Algorithm 3.4: Permutation algorithm.

input : A commutative ring R and a 3-tuple $v = (a, b, c) \in R^3$ not all zero.
output: A permutation matrix S such that the first entry of Sv is non-zero.

$S \leftarrow 3 \times 3$-identity matrix with coefficients in R;
if $a = 0$ **then**
  if $b \neq 0$ **then**
    $S \leftarrow \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in R^{3\times 3}$;
  else
    $S \leftarrow \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \in R^{3\times 3}$;
return S;

In Section 3.3 we will make use of Proposition 3.2. There it will be important which linear factor of $(g \bmod p)$ we use for the construction of our improvement. Since $(g \bmod p)$ is of degree 4 it can have at most two different linear factors of multiplicity 2, in this case we want to differentiate the two different improvements that can be constructed.

Definition 3.5. Let $g \in \mathbf{Z}[X, Y, Z]_4$ and p a prime. Let $M = P\,\mathrm{diag}(1, 1, p)$ and $N = Q\,\mathrm{diag}(1, 1, p)$ be two improvements for g with $P, Q \in \mathrm{GL}_3(\mathbf{Z})$. We call M and N $(0, 0, 1)$-equivalent if there is an element $u \in \mathbf{F}_p$ such that

$$Z \circ P^{-1} \equiv uZ \circ Q^{-1} \pmod{p}.$$

Now we state our algorithm. It returns a list of improvements (with no more than 2 elements), if we are only interested in one improvement of type $(0, 0, 1)$ then we can take any matrix from this list (if it is non-empty). In Section 3.3 it is important which improvement we take.

Algorithm 3.6: Try $(0, 0, 1)$.

input : A form $g \in \mathbf{Z}[X, Y, Z]_4$ with coprime coefficients and a prime p.
output: The list of improvements of g at p of the form $P\,\mathrm{diag}(1, 1, p)$ with $P \in \mathrm{GL}_3(\mathbf{Z})$ up to $(0, 0, 1)$-equivalence.

$L \leftarrow \varnothing$;
Find all linear factors of multiplicity at least 2 of $(g \bmod p)$, see Section 4;
for *each linear factor* l *of multiplicity at least* 2 *of* $(g \bmod p)$ **do**
  Write $l = a'X + b'Y + c'Z$ with $a', b', c' \in \mathbf{F}_p$;
  $S \leftarrow$ run Algorithm 3.4 with $\mathbf{F}_p$ and (c', b', a');
  $S \leftarrow S \cdot \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$;
  $l \leftarrow l \circ S$;
  Write $l = aX + bY + cZ$ with $a, b, c \in \mathbf{F}_p$;
  $s \leftarrow$ lift of $-c^{-1}a$ in $\{0, \ldots, p-1\} \subseteq \mathbf{Z}$;
  $t \leftarrow$ lift of $-c^{-1}b$ in $\{0, \ldots, p-1\} \subseteq \mathbf{Z}$;
  $M \leftarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ s & t & 0 \end{pmatrix}$;
  if $g \circ (SM\,\mathrm{diag}(1, 1, p)) \equiv 0 \mod p^2$ **then**
    Append $SM\,\mathrm{diag}(1, 1, p)$ to L ;
return L;

Proof of Algorithm 3.6. Note that this algorithm ends in finite time, all loops and procedures are finite. Before the append statement in line 13 there is an explicit check if the matrix that gets appended is indeed an improvement. Thus all matrices in the output are indeed improvements for g at p.

Let $P \in \mathrm{GL}_3(\mathbf{Z})$ be such that $P\,\mathrm{diag}(1,1,p)$ is an improvement of g at p. We need to prove that there is an improvement in the output L that is $(0,0,1)$-equivalent with $P\,\mathrm{diag}(1,1,p)$.

As $Z \circ P^{-1}$ is a linear factor of multiplicity at least 2 of $(g \bmod p)$, we execute the steps in the loop with $l = Z \circ P^{-1}$ (up to an element of $\mathbf{F}_p$). From Proposition 3.3 we know that the matrix $M\,\mathrm{diag}(1,1,p)$ is an improvement for $g \circ S$, so $SM\,\mathrm{diag}(1,1,p)$ gets appended to L. As $l \circ (SM) \equiv cZ \pmod p$ we see that

$$Z \circ (SM)^{-1} \equiv c^{-1}(cZ) \circ (SM)^{-1} \equiv c^{-1} l \equiv c^{-1} Z \circ P^{-1} \pmod p.$$

So $SM\,\mathrm{diag}(1,1,p)$ and $P\,\mathrm{diag}(1,1,p)$ are indeed $(0,0,1)$-equivalent. □

Example 3.7. It is in general not the case, for a form $f \in \mathbf{Z}[X,Y,Z]_4$ and prime p, that if $(f \bmod p)$ is divisible by a linear factor of multiplicity 2 that the matrix M described in Proposition 3.3 makes $(0,0,1)$ an improvement for $f \circ M$. Take for example f to be equal to $f = 7^2X^4 + 7Y^4 + Z^2XY$. Then $f \equiv Z^2XY \pmod 7$, so $M = P\,\mathrm{diag}(1,1,p)$, with P the identity matrix. But $f(X,Y,7Z) \equiv 7Y^4 \pmod{7^2}$, so $(0,0,1)$ is not an improvement for f.

3.2 Weight system $(0,1,1)$

Let $g \in \mathbf{Z}[X,Y,Z]_4$ be a form, and suppose that there exists a matrix $P \in \mathrm{GL}_3(\mathbf{Z})$ such that the form $f := g \circ P$ can be improved by the weight system $(0,1,1)$ at some prime p. We give a method that, given g and p but not P, finds a matrix $M \in \mathrm{GL}_3(\mathbf{Z})$ such that $g \circ M$ can be improved with the weight system $(0,1,1)$ at p.

We will show that this can be done by considering the singularities of f. More specifically, if we know what $P(1,0,0)$ is, then we can construct an improvement for g. In section 5.2 we give methods for finding this point.

First we introduce the terms: gradient, singular point and triple point. We also prove the chain and product rule for the gradient.

Definition 3.8. For every commutative ring R and polynomial $f \in R[X,Y,Z]$ define

$$\nabla f = \left(\tfrac{\partial}{\partial X} f, \tfrac{\partial}{\partial Y} f, \tfrac{\partial}{\partial Z} f\right)$$

For $f \in \mathbf{Z}[X,Y,Z]_4$ we sometimes write ∇f as column vector instead of row vector, but this will be clear from the context.

Definition 3.9. Let k be a field and let $d > 0$ be an integer. Let $f \in k[X,Y,Z]_d$ be a form. We call a point $\alpha \in \mathbf{P}^2(k)$ *singular*, or *singular with respect to* f if $f(\alpha) = 0$ and $\nabla f(\alpha) = 0$. We call a point $\alpha \in \mathbf{P}^2(k)$ a *triple point*, or a *triple point with respect to* f if it is a singular point and if for all $i \in \{1,2,3\}$,

$$\nabla f_i(\alpha) = 0,$$

where we write $\nabla f = (f_1, f_2, f_3)$.

Lemma 3.10. *Let R be a commutative ring and $f, g \in R[X,Y,Z]$ be polynomials. Then*

$$\nabla(fg) = f\nabla g + g\nabla f.$$

Proof. This is immediate by applying the product rule component wise. □

Proposition 3.11 (Chain rule for ∇)**.** *Let R be a commutative ring and $f \in R[X,Y,Z]$. For every matrix $A \in \mathrm{GL}_3(R)$ we have*

$$\nabla\,(f \circ A) = ((\nabla f) \circ A) \cdot A,$$

where '$\cdot$' means matrix-matrix multiplication (or left vector-matrix multiplication) and $(\nabla f) \circ A$ is defined component wise.

Proof. We write X_1, X_2, X_3 instead of X, Y, Z. From the R-linearity of the maps involved we see that it suffices to check the statement on monomials. Let $f = \prod_{i=1}^{3} X_i^{n_i}$ be a monomial where for each index $i : n_i \in \mathbf{Z}_{\geq 0}$.

We prove this with induction on the degree of f. We first prove the base case. Note that,

$$\nabla(1 \circ A) = 0 = ((\nabla 1) \circ A) \cdot A.$$

Write $(a_{ij})_{ij} = A$ and let e_1, e_2, e_3 be the standard basis for R^3 (as R module). For each monomial X_i it holds that,

$$\nabla(X_i \circ A) = \nabla\left(\sum_{j=1}^{3} a_{ij} X_i\right) = (a_{ij})_{j=1}^{3},$$

and also

$$((\nabla X_i) \circ A) \cdot A = (e_i \circ A) \cdot A = e_i \cdot A = (a_{ij})_{j=1}^{3}.$$

This proves the base cases. Let $N \in \mathbf{Z}_{>1}$ be given. For the induction step assume the statement for all monomials of degree less than N. Assume that the degree of f is N, write $f = gh$ with $\deg g = 1$. Then from Lemma 3.10,

$$\nabla(f \circ A) = (g \circ A)\nabla(h \circ A) + (h \circ A)\nabla(g \circ A).$$

From the induction hypothesis it follows that,

$$\nabla(h \circ A) = ((\nabla h) \circ A) \cdot A \quad \text{and} \quad \nabla(g \circ A) = ((\nabla g) \circ A) \cdot A,$$

hence

$$\nabla(f \circ A) = (g \circ A)((\nabla h) \circ A) \cdot A + (h \circ A)((\nabla g) \circ A) \cdot A.$$

Then it follows by linearity that

$$\nabla(f \circ A) = ((g \nabla h + h \nabla g) \circ A) \cdot A.$$

Again applying Lemma 3.10 we see that $\nabla(f \circ A) = ((\nabla f) \circ A) \cdot A$.

By induction the statement is proven. □

The following corollary states that it does not depend on coordinates if a point is a singular/triple point.

Corollary 3.12. *Let $g \in \mathbf{Z}[X, Y, Z]_4$ and $P \in \mathrm{GL}_3(\mathbf{Z})$ a matrix. Let $m > 0$ be a positive integer. Suppose that for some point $\alpha \in \mathbf{Z}^3$ we have that $\nabla g(\alpha) \equiv 0 \pmod{m}$. Then $\nabla(g \circ P)(\beta) \equiv 0 \pmod{m}$ where $\beta = P^{-1}\alpha$.*

Proof. This is immediate from the following calculation:

$$\nabla(g \circ P)(\beta) = (((\nabla g) \circ P) \cdot P)(\beta) = (((\nabla g) \circ P)(\beta)) \cdot P = \nabla g(\alpha) \cdot P \equiv 0 \pmod{m}.$$ □

We now apply the introduced terms to our problem of finding a improvement.

Proposition 3.13. *Let $g \in \mathbf{Z}[X, Y, Z]_4$ be a form, and suppose that there is a matrix $P \in \mathrm{GL}_3(\mathbf{Z})$ such that $(0, 1, 1)$ is an improvement for $g \circ P$ at some prime p. Define $\alpha \in \mathbf{P}^2(\mathbf{F}_p)$ to be the projection of the point $P(1, 0, 0)$. Then α is a triple point for $(g \bmod p) \in \mathbf{F}_p[X, Y, Z]_4$.*

Proof. Write $f := g \circ P$. Since the weight system $(0, 1, 1)$ is an improvement we have $f(X, pY, pZ) \equiv 0 \pmod{p^3}$, so we may expand f as follows:

$$f = p^3 X^4 c + p^2 X^3 l(Y, Z) + p X^2 q(Y, Z) + X r(Y, Z) + h(Y, Z), \tag{4}$$

where l is linear, q is quadratic, r is cubic and h is quartic in $\mathbf{Z}[Y, Z]$ and c is an integer such that $cp^3 = f(1, 0, 0)$. Now consider f modulo p:

$$f \equiv X r(Y, Z) + h(Y, Z) \pmod{p}.$$

This gives us,

$$\nabla f \equiv \left(r(Y, Z), X \tfrac{\partial}{\partial Y} r(Y, Z) + \tfrac{\partial}{\partial Y} h(Y, Z), X \tfrac{\partial}{\partial Z} r(Y, Z) + \tfrac{\partial}{\partial Z} h(Y, Z)\right) \pmod{p},$$

which vanishes on the point $(1, 0, 0)$. Together with Corollary 3.12 this proves that $\nabla g(\alpha)$ is a singular point.

Denote with h_i the i-th component of ∇f for $i = 1, 2, 3$. Note that r and h are homogeneous elements of $\mathbf{Z}[Y, Z]$ of degree at least 3, hence their first and second partial derivative vanish on $(1, 0, 0)$. As, for each index i, the

form h_i is a combination of r, h and their first partial derivatives, it follows that every partial derivative of h_i is a combination of r, h and their first and second partial derivatives none of which are constant. Hence

$$\nabla h_i(1,0,0) \equiv 0 \pmod{p}.$$

So $(1,0,0)$ is a triple point for $(f \bmod p)$. Then it follows from Corollary 3.12 that $\alpha = P(1,0,0)$ is a triple point for $(g \bmod p)$. □

Let $g \in \mathbf{Z}[X,Y,Z]_4$ and suppose that there exists a matrix $P \in \mathrm{GL}_3(\mathbf{Z})$ such that $f := g \circ P$ can be improved with $(0,1,1)$ at some prime p. In the next proposition we prove that finding the point $\alpha = P(1,0,0)$ as in Proposition 3.13 is sufficient for finding an improvement for g at p.

Proposition 3.14. *Let $g \in \mathbf{Z}[X,Y,Z]_4$ be a form and $P \in \mathrm{GL}_3(\mathbf{Z})$ a matrix such that the weight system $(0,1,1)$ is an improvement for $g \circ P$ at some prime p. Let $\alpha \in \mathbf{P}^2(\mathbf{F}_p)$ be the projection of $P(1,0,0)$, write $\alpha = (\alpha_1, \alpha_2, \alpha_3)$ and suppose that $\alpha_1 \neq 0$. Let $s,t \in \{0,\dots,p-1\} \subseteq \mathbf{Z}$ be lifts of $\alpha_2\alpha_1^{-1}, \alpha_3\alpha_1^{-1} \in \mathbf{F}_p$ respectively. Define*

$$A = \begin{pmatrix} 1 & 0 & 0 \\ s & 1 & 0 \\ t & 0 & 1 \end{pmatrix} \in \mathrm{SL}_3(\mathbf{Z}).$$

Then the weight system $(0,1,1)$ is an improvement of $g \circ A$ at p.

Proof. We show that $g \circ A\,\mathrm{diag}(1,p,p) \in p^3\mathbf{Z}[X,Y,Z]_4$. First we introduce notation. For $b \in \mathbf{Z}[X,Y,Z]$ we write $\tilde{b} = b \circ P^{-1}A \in \mathbf{Z}[X,Y,Z]$. Define $f = g \circ P$. With the introduced notation it holds that $\tilde{f} = g \circ A$. We want to show that $\mathrm{diag}(1,p,p)$ is an improvement for $\tilde{f}$.

Note that for all $b \in \mathbf{Z}[X,Y,Z]$ it holds that $\tilde{b} = b(\tilde{X},\tilde{Y},\tilde{Z})$. To show that $\mathrm{diag}(1,p,p)$ is an improvement for $\tilde{f}$ we show that $p\tilde{f} \in \mathbf{Z}[pX,Y,Z]$. From this it will follow that $\tilde{f}(X,pY,pZ) \equiv 0 \pmod{p^3}$.

To do this, we prove that $\tilde{Y}$ and $\tilde{Z}$ are elements of $\mathbf{Z}[pX,Y,Z]_1$. For this write β^1, β^2 and β^3 for the rows of P^{-1} and $(\gamma_{ij})_{ij} := P^{-1}A$. Then for the bottom two rows ($i \in \{2,3\}$) of $P^{-1}A$ it holds that

$$\gamma_{i1} \equiv \beta^i \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} \alpha_1^{-1} \equiv 0 \pmod{p}.$$

From this it follows that,

$$\begin{aligned} \tilde{Y} &= \gamma_{21}X + \gamma_{22}Y + \gamma_{23}Z \equiv \gamma_{22}Y + \gamma_{23}Z \pmod{p} \text{ and} \\ \tilde{Z} &= \gamma_{31}X + \gamma_{32}Y + \gamma_{33}Z \equiv \gamma_{32}Y + \gamma_{33}Z \pmod{p}. \end{aligned}$$

The matrix $\mathrm{diag}(1,p,p)$ is an improvement for f, so by expanding f as in equation (4) we see that $pf \in \mathbf{Z}[pX,Y,Z]_4$. As $\tilde{Y}$ and $\tilde{Z}$ are elements of $\mathbf{Z}[pX,Y,Z]$, it follows that

$$p\tilde{f} \in \mathbf{Z}[p\tilde{X},\tilde{Y},\tilde{Z}]_4 \subseteq \mathbf{Z}[pX,Y,Z]_4.$$

From this we see that

$$p\tilde{f} \circ \begin{pmatrix} 1 & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & p \end{pmatrix} \in \mathbf{Z}[pX,pY,pZ]_4 = p^4\mathbf{Z}[X,Y,Z],$$

so $g \circ A\,\mathrm{diag}(1,p,p) = \tilde{f} \circ \mathrm{diag}(1,p,p) \in p^3\mathbf{Z}[X,Y,Z]_4$. □

Let $g \in \mathbf{Z}[X,Y,Z]_4$ and suppose that there exists a matrix $P \in \mathrm{GL}_3(\mathbf{Z})$ such that $f := g \circ P$ can be improved with $(0,1,1)$ at some prime p. To use Proposition 3.14 we need to find this special point $\alpha = P(1,0,0)$.

The idea to find α is to find a list $\mathcal{L}$ of points in $\mathbf{P}^2(\mathbf{F}_p)$ that contains α. As we do not know which point of $\mathcal{L}$ is α, we test each point in $\mathcal{L}$ and see if it gives an improvement. For large p, it takes to long to loop through all points of $\mathbf{P}^2(\mathbf{F}_p)$. So it is important that we choose a suitable set $\mathcal{L}$ with few elements.

For now we will just assume that we have such a small list $\mathcal{L}$, in Section 5.2 we give methods of finding a suitable $\mathcal{L}$. We see in Example 3.17 that we can not simply take $\mathcal{L}$ to be all the triple points of $(g \bmod p)$ if p is large.

In Section 3.3 we will need something more general than just an improvement. Namely a list of matrices as in the following definition.

Definition 3.15. Let $g \in \mathbf{Z}[X,Y,Z]_4$ be a form. Let $\alpha \in \mathbf{P}^2(\mathbf{F}_p)$ and write $\alpha = (\alpha_1, \alpha_2, \alpha_3)$. Define the *permutation matrix* S *of* α as the first matrix in the list

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \text{ and } \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

such that the first entry of the vector $(\beta_1, \beta_2, \beta_3) := S\alpha$ is non-zero. Define

$$M_\alpha := S \begin{pmatrix} 1 & 0 & 0 \\ s & 1 & 0 \\ t & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & p \end{pmatrix},$$

where $s, t \in \{0, 1, \ldots p-1\} \subseteq \mathbf{Z}$ are such that $s \equiv \beta_1^{-1}\beta_2 \pmod{p}$ and $t \equiv \beta_1^{-1}\beta_3 \pmod{p}$. Let $\mathcal{L} \subseteq \mathbf{P}^2(\mathbf{F}_p)$ be a set of points. For $k \in \mathbf{Z}_{>0}$ define

$$\mathcal{L}_{p^k} = \left\{\alpha \in \mathcal{L} : g \circ M_\alpha \in p^k \mathbf{Z}[X,Y,Z]_4\right\},$$

and also define

$$\xi_k(g, p, \mathcal{L}) = \left\{ (\frac{1}{p^k} g \circ M_\alpha, M_\alpha) : \alpha \in \mathcal{L}_{p^k} \right\}.$$

Note that, for a small set $\mathcal{L}$, the definitions of $\mathcal{L}_{p^k}$ and $\xi_k(g, p, \mathcal{L})$ are 'algorithmic' in the sense that their definition is actually an algorithm.

All this leads to Algorithm 3.16, which we will need to use again when we consider the weight system $(0, 1, 3)$.

Algorithm 3.16: Try $(0, 1, 1)$.

input :
- A form $g \in \mathbf{Z}[X,Y,Z]_4$ with coprime coefficients.
- A prime p.
- A list $\mathcal{L} \subseteq \mathbf{P}^2(\mathbf{F}_p)$ of points.

output: An improvement for g at p or the set $\xi_2(g, p, \mathcal{L})$ (the latter we will need in section 3.3). The output is guaranteed to be an improvement if there exists a matrix $P \in \mathrm{GL}_3(\mathbf{Z})$ such that $P\,\mathrm{diag}(1, p, p)$ is an improvement for g at p and $P(1, 0, 0) \in \mathcal{L}$.

```
if ξ_3(g, p, L) ≠ ∅ then
    return the matrix of an element of ξ_3(g, p, L);
return ξ_2(g, p, L);
```

Proof. As $\mathcal{L}$ is a subset of the finite set $\mathbf{P}^2(\mathbf{F}_p)$, every procedure terminates. Also note that if an matrix is returned, it is per construction an improvement. If no matrix is returned, it is clear that the output is $\xi_2(g, p, \mathcal{L})$.

Suppose that there exists a matrix $P \in \mathrm{GL}_3(\mathbf{Z})$ such that $P\,\mathrm{diag}(1, p, p)$ is an improvement for g at p and suppose that $(P(1, 0, 0) \bmod p) \in \mathcal{L}$. We have to show that $\xi_3(g, p, \mathcal{L})$ is non-empty. But this is immediate from Proposition 3.14. □

The following example gives a form that can not be improved by an improvement of type $(0, 0, 1)$ but can be improved by an improvement of type $(0, 1, 1)$. This form has many triple points, so a method is needed to find a smaller list of points that contain the right point.

Example 3.17. Fix some prime p and define $f = Z^4 + p(p^2X^4 + Y^4) \in \mathbf{Z}[X,Y,Z]_4$. Then $(f \bmod p) = Z^4$ has a linear factor of multiplicity at least 2 namely Z. If an improvement of $P\,\mathrm{diag}(1, 1, p)$ with $P \in \mathrm{GL}_3(\mathbf{Z})$ where possible for f it would follow from Proposition 3.3 that $\mathrm{diag}(1, 1, p)$ is an improvement for f at p. This is obviously not the case.

Note that $f(X, pY, pZ) \equiv 0 \pmod{p^3}$, so $\mathrm{diag}(1, p, p)$ is an improvement for f. But if we calculate the set of triple points of f we get

$$\left\{(a, b, 0) : a, b \in \mathbf{F}_p^2 \setminus \{(0, 0)\}\right\}.$$

For large values of p this set is too large to enumerate through.

3.3 Weight system $(0,1,3)$

Let $g \in \mathbf{Z}[X,Y,Z]_4$ be a known form and $P \in \mathrm{GL}_3(\mathbf{Z})$ a unknown matrix such that $\mathrm{diag}(1,p,p^3)$ is an improvement for $f := g \circ P$ at some known prime p.

To find an improvement for g, using only g and p, we roughly do the following. First we try weight system $(0,1,1)$ (Algorithm 3.16), if this does not give an improvement it makes g at first 'worse'. However, if we now try the weight system $(0,0,1)$ (Algorithm 3.16) twice, we do get an improvement. To be more precise we apply the following algorithm.

Algorithm 3.18: Try $(0,1,3)$.

input :
- A form $g \in \mathbf{Z}[X,Y,Z]_4$ with coprime coefficients such that for all $A \in \mathrm{GL}_3(\mathbf{Z})$ neither the weight system $(0,0,1)$ nor the weight system $(0,1,1)$ is an improvement for $g \circ A$ at p.
- A prime p.
- A list $\mathcal{L} \subseteq \mathbf{P}^2(\mathbf{F}_p)$ of points.

output: An improvement g at p or $\varnothing$. If there is a matrix $P \in \mathrm{GL}_3(\mathbf{Z})$ such that $P\,\mathrm{diag}(1,p,p^3)$ is an improvement for g at p and $P(1,0,0) \in \mathcal{L}$ then the output is an improvement.

```
L_1 ← run Algorithm 3.16 with g, p and L;
for (h_1, M_α) ∈ L_1 do
    L_2 ← run Algorithm 3.6 with h_1 and p;
    for M_2 ∈ L_2 do
        L_3 ← run Algorithm 3.6 with (1/p^2) h_1 ∘ M_2 and p;
        if L_3 ≠ ∅ then
            Let M be an element of L_3;
            return M_α M_2 M;
return ∅;
```

First we prove that there is indeed a point that is singular on $(g \bmod p)$, because we will need that for Algorithm 3.16. It can be seen in Example 3.20 below that unlike what happens in Proposition 3.13 there is not always a triple point of $(g \bmod p)$.

If we write $f = \sum a_{ijk} X^i Y^j Z^k$, then for all monomials of f it holds that $\mathrm{ord}_p(a_{ijk}) + j + 3k \geq 6$. Using this, we will prove that there is a point that is singular on $(g \bmod p)$. This is done in the following proposition.

Proposition 3.19. *Let $g \in \mathbf{Z}[X,Y,Z]_4$ be a form and p a prime. Let $P \in \mathrm{GL}_3(\mathbf{Z})$ be such that $g \circ P$ can be improved with $(0,1,3)$. Define the point $\alpha := P(1,0,0)$. Then*

$$g(\alpha) \equiv 0 \quad \textit{and} \quad \nabla g(\alpha) \equiv 0 \pmod{p}.$$

Proof. Write $f := g \circ P$. As $(0,1,3)$ is an improvement for f we may write

$$\begin{aligned} f =& X^4 c_6 p^6 + X^3 Y c_5 p^5 + X^2 Y^2 c_4 p^4 + (XY^3 c_{3,1} + X^3 Z c_{3,2}) p^3 \\ &+ (Y^4 c_{2,1} + X^2 Y Z c_{2,1}) p^2 + XY^2 Z c_1 p + Y^3 Z c_0 + Z^2 h, \end{aligned} \tag{5}$$

where for all indices i in the above formula, $c_i \in \mathbf{Z}$ and $h \in \mathbf{Z}[X,Y,Z]_2$. Note that $g(\alpha) = (g \circ P)(1,0,0) = c_6 p^6$. So $g(\alpha) \equiv 0 \pmod{p}$. From this we see that $f \equiv Y^3 Z c_0 + Z^2 h \pmod{p}$, so

$$\nabla f \equiv \left(Z^2 \tfrac{\partial h}{\partial X},\ 3Y^2 Z c_0 + Z^2 \tfrac{\partial h}{\partial Y},\ Y^3 c_0 + 2Zh + Z^2 \tfrac{\partial h}{\partial Z} \right) \pmod{p}.$$

We see that $\nabla f(1,0,0) \equiv 0 \pmod{p}$, hence from Corollary 3.12 it follows that $\nabla g(\alpha) \equiv 0 \pmod{p}$. □

Example 3.20. Let $g = X^4 p^6 + p^2 Y^4 + Z^4 + Z^2 X^2$ with an odd prime p. Then we see that $g(X, pY, p^3 Z) \in p^6 \mathbf{Z}[X,Y,Z]_4$, so we can take matrix P in Proposition 3.19 to be the identity matrix and $\alpha = (1,0,0)$. Now we calculate

$$\nabla(g \bmod p) = \left(2Z^2 X,\ 0,\ 2ZX^2\right) \quad \text{and} \quad \nabla(2ZX^2) = \left(4ZX,\ 0,\ X^2\right).$$

We see that α is indeed singular but, as X^2 does not vanish on α, it is not a triple point.

Suppose that we have some method of finding a list $\mathcal{L} \subseteq \mathbf{P}^2(\mathbf{F}_p)$ of points such that $P(1,0,0) \in \mathcal{L}$. Using this $\mathcal{L}$ we find an improvement for g using Algorithm 3.18. A method of finding $\mathcal{L}$ is described in subsection 5.3.

Proof of Algorithm 3.18. Every **for** loop, loops over a finite list. All other algorithms that are called are also finite. Hence the algorithm terminates.

If a matrix M is returned, then it is an improvement. Since per construction its determinant is $\pm p^4$, and $g \circ M \in p^6\mathbf{Z}[X,Y,Z]_4$.

Let $P \in \mathrm{GL}_3$ such that $g \circ P$ can be improved with the weight system $(0,1,3)$ and $P(1,0,0) \in \mathcal{L}$. We prove that an improvement for g at p is returned.

Write $f := g \circ P$, and $f = f_1 + f_2 Z + f_3 Z^2$ with $f_1, f_2 \in \mathbf{Z}[X,Y]$ and $f_3 \in \mathbf{Z}[X,Y,Z]_2$. From the expansion of f in equation (5) it follows that $f_1 \in p^2\mathbf{Z}[pX,Y]_4$ and $f_2 \in \mathbf{Z}[pX,Y]_3$. With this notation we introduce $l := Z \circ P^{-1}$ and for $i \in \{1,2,3\}$,

$$g_i := f_i \circ P^{-1}.$$

Note that as $g = f \circ P^{-1}$ we have that $g = g_1 + g_2 l + g_3 l^2$.

As $\alpha := P(1,0,0)$ is an element of $\mathcal{L}$ and since (per assumption) there is no improvement of the form $H \operatorname{diag}(1,p,p)$ with $H \in \mathrm{GL}_3(\mathbf{Z})$ it follows that $L_1 = \xi(g,p,\mathcal{L})$.

Let M_α be the matrix of Definition 3.15. Write $\hat{g} = \frac{1}{p^2} g \circ M_\alpha$.

Claim: It holds that $(\hat{g}, M_\alpha) \in L_1$. Proof of the claim: It suffices to prove that $g \circ M_\alpha \in p^2\mathbf{Z}[X,Y,Z]_4$. Let $A \in \mathrm{GL}_3(\mathbf{Z})$ be such that $A \operatorname{diag}(1,p,p) = M_\alpha$. As in the proof of Proposition 3.14 we have that $Y \circ P^{-1}A$ and $Z \circ P^{-1}A$ are both elements of $\mathbf{Z}[pX,Y,Z]_1$. It follows that

$$\begin{aligned} g_1 \circ A &= f_1 \circ P^{-1}A \in p^2\mathbf{Z}[pX,Y,Z]_4 \text{ and} \\ g_2 \circ A &= f_2 \circ P^{-1}A \in \mathbf{Z}[pX,Y,Z]_3. \end{aligned}$$

From this it follows that

$$\begin{aligned} g_1 \circ M_\alpha &\in p^6\mathbf{Z}[X,Y,Z]_4, \\ g_2 \circ M_\alpha &\in p^3\mathbf{Z}[X,Y,Z]_3 \text{ and} \\ g_3 \circ M_\alpha &\in \mathbf{Z}[X,Y,Z]_2. \end{aligned}$$

Note that per construction of M_α we have $l \circ M_\alpha \in p\mathbf{Z}[X,Y,Z]_1$. So we know that $g \circ M_\alpha$ is an element of $p^2\mathbf{Z}[X,Y,Z]_4$. So $(\hat{g}, M_\alpha) \in L_1$. This proves the claim.

It follows that we do the steps in the **for** loop with $(\hat{g}, M_\alpha)$. Let L_2 be the output of Algorithm 3.6 run with $\hat{g}$ and p as input.

In line with our hat notation for $\hat{g}$ we define $\hat{l} = \frac{1}{p} l \circ M_\alpha$ and for $i \in \{1,2,3\}$,

$$\hat{g}_i := \frac{1}{p^{3-i}} g_i \circ M_\alpha.$$

With this notation we have $\hat{g} = \hat{g}_1 + \hat{g}_2 \hat{l} + \hat{g}_3 \hat{l}^2$. Note that $\hat{l} \in \mathbf{Z}[X,Y,Z]_1$ and

$$\begin{aligned} \hat{g}_1 &\in p^4\mathbf{Z}[X,Y,Z]_4, \\ \hat{g}_2 &\in p^2\mathbf{Z}[X,Y,Z]_3 \text{ and} \\ \hat{g}_3 &\in \mathbf{Z}[X,Y,Z]_2. \end{aligned}$$

Claim: There is a matrix $M_2 \in L_2$ such that $\hat{l} \circ M_2 \in p\mathbf{Z}[X,Y,Z]_1$. Proof of the claim: As $g \equiv \hat{l}^2 \hat{g}_3 \pmod{p}$ and $g \equiv \hat{l}^2 \hat{g}_3 \pmod{p^2}$ it follows from Proposition 3.2 that there exists an improvement of the form $N \operatorname{diag}(1,1,p)$ with $N \in \mathrm{GL}_3(\mathbf{Z})$ and $\hat{l} \circ N \in \mathbf{Z}[pX,pY,Z]_1$. Hence there is a matrix M_2 in L_2 with M_2 and $N \operatorname{diag}(1,1,p)$ $(0,0,1)$-equivalent. This implies that $\hat{l} \circ M_2 \in p\mathbf{Z}[X,Y,Z]_1$. This proves the claim. Write $\tilde{g} := \frac{1}{p^2} g \circ M_2$.

We will enter the second **for** loop with $(\tilde{g}, M_2)$.

We will now introduce the last bit of notation for this proof. Write $\tilde{l} := \frac{1}{p} \hat{l} \circ M_2$ and for $i \in \{1,2,3\}$,

$$\tilde{g}_i = \frac{1}{p^{3-i}} \hat{g}_i \circ M_2.$$

Now we have that $\tilde{l} \in \mathbf{Z}[X,Y,Z]_1$ and

$$\begin{aligned}\tilde{g}_1 &\in p^2\mathbf{Z}[X,Y,Z]_4,\\ \tilde{g}_2 &\in p\mathbf{Z}[X,Y,Z]_3 \text{ and}\\ \tilde{g}_3 &\in \mathbf{Z}[X,Y,Z]_2.\end{aligned}$$

So we can write $\tilde{g} = \tilde{g}_1 + \tilde{g}_2\tilde{l} + \tilde{g}_3\tilde{l}^2$.

Let L_3 be the output of Algorithm 3.6 run with $\tilde{g}$ and p.

We show that L_3 is non-empty. As $\tilde{g} \equiv \tilde{l}^2\tilde{g}_3 \pmod{p}$ and $\tilde{g} \equiv \tilde{l}\tilde{g}_2 + \tilde{l}^2\tilde{g}_3 \pmod{p^2}$ it follows from Proposition 3.2 that there is an improvement of the form $N\,\mathrm{diag}(1,1,p)$ with $N \in \mathrm{GL}_3(\mathbf{Z})$. Hence L_3 is non-empty and we return an improvement. □

4 Finding the linear form for weight system $(0,0,1)$

We show how we can find l as in step 2 of Algorithm 3.6. Note that we only need to find l up to an element of $\mathbf{F}_p$. Let $g \in \mathbf{Z}[X,Y,Z]_4$ be a form, p a prime and $P \in \mathrm{GL}_3(\mathbf{Z})$ such that $\mathrm{diag}(1,1,p)$ is an improvement for $f := g \circ P$ at p. Write $l \equiv Z \circ P^{-1} \bmod p$. We saw that $l^2 \mid (g \bmod p)$. As we only need to identify l up to a scalar, we may assume without loss of generality that $(g \bmod p)$ is monic in X.

For $p = 2, 3$ we can just factor $(g \bmod p)$ into irreducible factors, and from the factorisation identify l; the sets $\mathbf{F}_2[X,Y,Z]_1$ and $\mathbf{F}_3[X,Y,Z]_1$ both have few elements. So assume that $p > 3$. We know that $(\mathbf{F}_p[Y,Z])[X]$ is an unique factorisation domain, so (as is shown in [10]) we have a notion of greatest common divisor. As $\mathbf{F}_p(Y,Z)[X]$ is an Euclidean domain, we can use the Euclidean algorithm to find the greatest common divisor $d \in (\mathbf{F}_p(Y,Z))[X]$ of the partial derivatives of $(g \bmod p)$. Note that, as g is monic in $(\mathbf{F}_p(Y,Z))[X]$ it follows from Gauss [10, Lemma 13.5] that $d \in \mathbf{F}_p[X,Y,Z]$.

If $d \in \mathbf{F}_p$, then l does not divide all of the derivatives of $(g \bmod p)$, which contradicts Lemma 5.5.

If the degree of d is 1, then $l = d$. So we suppose that the degree of d is at least 2. There are now two possibilities: Either $d = ul^m$ for some $u \in \mathbf{F}_p$ and positive integer $m \in \{2,3\}$ or d is the product of two different linear factors. As we do not know in which case we are, we give for both cases a method to find l. After a candidate l is found, we test if l^2 indeed divides $(g \bmod p)$.

First, the case where $d = ul^m$ for some $u \in \mathbf{F}_p$ and integer $m \in \{2,3\}$. Write $l = aX + bY + cZ$ with $a,b,c \in \mathbf{F}_p$ not all zero. Assume that $a \neq 0$ (the case where a is zero and b or c is non-zero is similar). Find $B, C \in \mathbf{F}_p$ such that

$$d = \text{some constant} \cdot \left(X^m + BX^{m-1}Y + CX^{m-1}Z + \text{other terms}\right).$$

If we multiply out $(X + \frac{b}{a}Y + \frac{c}{a}Z)^m$ we see that

$$B = m\frac{b}{a} \quad \text{and} \quad C = m\frac{c}{a}.$$

So we can use the linear form $X + \frac{B}{m}Y + \frac{C}{m}Z$.

Now, suppose that $d = l_1 l_2$ for some $l_1, l_2 \in \mathbf{F}_p[X,Y,Z]_1$. Assume that the coefficients of the X monomial of l_1 and l_2 are both non-zero. Then we can write for some $u \in \mathbf{F}_p$

$$d = l_1 l_2 = u\hat{l}_1\hat{l}_2,$$

where

$$\hat{l}_i = X + b_iY + c_iZ \quad \text{for} \quad i \in \{1,2\}.$$

Then we get that

$$d = u\left(X^2 + (b_1+b_2)XY + (b_1b_2)Y^2 + (c_1+c_2)XZ + (b_1c_2 + c_1b_2)YZ + (c_1c_2)Z^2\right).$$

As $b_1 + b_2$ and b_1b_2 are known, we can find b_1 and b_2 as roots of the polynomial

$$t^2 - (b_1+b_2)t + b_1b_2 \in \mathbf{F}_p[t].$$

Roots of a second degree polynomial can be found using the quadratic formula. We then do need to find a square root of $(b_1+b_2)^2 - 4b_1b_2$ in $\mathbf{F}_p$. One could use the algorithm of Tonelli and Shanks to find square roots

modulo p (see [2, Algorithm 1.5.1]). So we have found b_1 and b_2. If $b_1 \neq b_2$, then we find c_1 and c_2 as the unique solution of the system

$$\begin{cases} b_1c_2 + b_2c_1 & = \text{coefficient of } YZ \text{ of } d \\ c_2 + c_1 & = \text{coefficient of } XZ \text{ of } d. \end{cases}$$

Otherwise we find c_1 and c_2 as the roots of polynomial

$$t^2 - (c_1 + c_2)t + c_1c_2 \in \mathbf{F}_p[t],$$

where again $c_1 + c_2$ and c_1c_2 are known.

5 Finding a small list of critical points

This section is based on the source code of the function *MinimizePlaneQuartic* of the software package MAGMA [1].

Let $g \in \mathbf{Z}[X, Y, Z]_4$ be a form and let p be a prime. Let $P \in \mathrm{GL}_3(\mathbf{Z})$ be a matrix such that $P\,\mathrm{diag}(1, p^{w_1}, p^{w_2})$ is an improvement for g at p where

$$(0, w_1, w_2) \in \{(0, 1, 1), (0, 1, 3)\}.$$

In this section we give for both these weight systems a method of finding a small list $\mathcal{L}$ that contains $(P(1, 0, 0) \bmod p)$. It is important that $\mathcal{L}$ is small, because both Algorithm 3.16 (weight system $(0, 1, 1)$) as Algorithm 3.18 (weight system $(0, 1, 3)$) loop over $\mathcal{L}$. We will assume that $p > 4$, since the cases where $p = 2$ or $p = 3$ we can take $\mathcal{L}$ to just be equal to the set of all singular points of $(g \bmod p)$.

We first state Bézout's theorem, then we define parametrisations and give some results about them that we will need.

5.1 Bézout and parametrisations

We make use of the following well known theorem.

Theorem 5.1 (Bézout)**.** *Let $f, g \in \mathbf{F}_p[X, Y, Z]$ be forms. Suppose that f and g do not share a common factor. Then the number of points that lie on the zero set of both f and g in $\mathbf{P}^2(\mathbf{F}_p)$ (counted with multiplicity) is less than or equal to* $\deg(f) \cdot \deg(g)$.

Proof. This follows from "Bézout's theorem" as stated in [4]. □

We will also make use of the following definition and lemmas.

Definition 5.2. Let $l \in \mathbf{Z}[X, Y, Z]_1$ be a linear form. A *parametrisation of l* is a map $\varphi : \mathbf{P}^1(\mathbf{Q}) \to \mathbf{P}^2(\mathbf{Q})$ given by $\varphi = (\varphi_1, \varphi_2, \varphi_3)$ with $\varphi_1, \varphi_2, \varphi_3 \in \mathbf{Z}[s, t]_1$ with the following properties. If we write

$$\varphi_i = v_is + w_it \quad \text{for} \quad i \in \{1, 2, 3\},$$

with $v = (v_1, v_2, v_3)$ and $w = (w_1, w_2, w_3)$ vectors in $\mathbf{Z}^3$, then (v, w) must be a $\mathbf{Z}$-basis for $\{x \in \mathbf{Z}^3 : l(x) = 0\}$.

Note that for every $l \in \mathbf{Z}[X, Y, Z]_1$ the set $\{x \in \mathbf{Z}^3 : l(x) = 0\}$ is a subgroup of $\mathbf{Z}^3$, thus there is an $\mathbf{Z}$-basis for $\{x \in \mathbf{Z}^3 : l(x) = 0\}$. Hence for every $l \in \mathbf{Z}[X, Y, Z]_1$ there exists a parametrisation.

Let $g \in \mathbf{Z}[X, Y, Z]$ be a form and φ a parametrisation of some $l \in \mathbf{Z}[X, Y, Z]_1$. Then $g(\varphi) \in \mathbf{Z}[s, t]$ is a polynomial in s and t defined up to sign. Also,

$$l(\varphi) = 0 \in \mathbf{Z}[s, t].$$

Lemma 5.3. *Let $l \in \mathbf{Z}[X, Y, Z]_1$ be a linear form, φ a parametrisation of l and $P \in \mathrm{GL}_3(\mathbf{Z})$ a matrix. Then $\psi := P^{-1}\varphi$ is a parametrisation for $l \circ P$.*

Proof. Let v, w be the $\mathbf{Z}$-basis of $\{x \in \mathbf{Z}^3 : l(x) = 0\}$ corresponding to the parametrisation φ. Writing $\psi = (\psi_1, \psi_2, \psi_3)$ we see that for each $i \in 1, 2, 3$

$$\psi_i = P^{-1}\varphi_i = sP^{-1}v_i + tP^{-1}w_i.$$

It then follows that $\left(P^{-1}v, P^{-1}w\right)$ is a $\mathbf{Z}$-basis for $\{x \in \mathbf{Z}^3 : (l \circ P)(x) = 0\}$. So ψ is a parametrisation of $l \circ P$. □

We call a form $aX + bY + cZ \in \mathbf{Z}[X, Y, Z]_1$ *primitive* if a, b and c are coprime.

Lemma 5.4. *Let $g \in \mathbf{Z}[X, Y, Z]_4$ and $l \in \mathbf{Z}[X, Y, Z]_1$ be given. Suppose that l is primitive. Let $p > 4$ be a prime, $n \in \mathbf{Z}_{>0}$ an integer and φ a parametrisation of l. Then*

$$(l \bmod p^n) \mid (g \bmod p^n) \iff g(\varphi) \equiv 0 \pmod{p^n}.$$

Proof. Suppose that $l \mid g \pmod{p^n}$. Then there exists a $h \in \mathbf{Z}[X, Y, Z]_3$ such that $g \equiv lh \pmod{p^n}$. As φ is a parametrisation of l we find that $l(\varphi) = 0$. Hence $g(\varphi) \equiv l(\varphi)h(\varphi) = 0 \pmod{p^n}$.

Suppose that $g(\varphi) \equiv 0 \pmod{p^n}$. The proof of this implication has two steps: First we show that we may assume that $l = X$ and $\varphi = (0, s, t)$. Then we prove the lemma for the case $l = X$ and $\varphi = (0, s, t)$.

Write $l = aX + bY + cZ$ with $a, b, c \in \mathbf{Z}$ coprime. We have the injection $\mathbf{Z} \hookrightarrow \mathbf{Z}^3$ by $1 \mapsto (a, b, c)$. Denote the quotient of this map by $G = \mathbf{Z}^3/(a, b, c)\mathbf{Z}$. Then from the structure theorem of finitely generated Abelian groups it follows that

$$G \cong \mathbf{Z}^2 \oplus T,$$

with T torsion. As (a, b, c) is primitive, $T = 0$. Let x and y be representatives in $\mathbf{Z}^3$ for a $\mathbf{Z}$-basis of G.

Claim: $((a, b, c), x, y)$ is a $\mathbf{Z}$-basis for $\mathbf{Z}^3$. Proof of claim: Let $r \in \mathbf{Z}^3$ be given. We show that we can write r as a linear combination of (a, b, c), x and y. We use the notation $[t]$ for the projection of an element $t \in \mathbf{Z}^3$ to G. We may write $[r] = \lambda_1[x] + \lambda_2[y]$ for some $\lambda_1, \lambda_2 \in \mathbf{Z}$. For $s = r - \lambda_1 x - \lambda_2 y$ we have that $[s] = 0 \in G$, so it follows that $s \in (a, b, c)\mathbf{Z}$. Let $\mu \in \mathbf{Z}$ such that $s = \mu(a, b, c)$ and write

$$r = s + \lambda_1 x + \lambda_2 y = \mu(a, b, c) + \lambda_1 x + \lambda_2 y.$$

This means that we have three vectors in $\mathbf{Z}^3$ that span $\mathbf{Z}^3$, so they must be linearly independent. This proves the claim.

So the matrix A with first row (a, b, c), second row x and third row y is an element of $\mathrm{GL}_3(\mathbf{Z})$. Note that $X \circ A = l$, so $l \circ A^{-1} = X$.

So we may assume without loss of generality that $l = X$ and that φ is some parametrisation of X. We now show that there exists a matrix $A \in \mathrm{GL}_3(\mathbf{Z})$ such that $X \circ A = X$ and $A^{-1}\varphi = (0, s, t)$. Let v and w be the $\mathbf{Z}$-basis of $\{(0, y, z) \in \mathbf{Z}^3\}$ corresponding to φ. Writing $v = (v_1, v_2, v_3)$ and $w = (w_1, w_2, w_3)$ we see that $v_1 = w_1 = 0$. Then the matrix

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & v_2 & w_2 \\ 0 & v_3 & w_3 \end{pmatrix}$$

has determinant ± 1. Note that $\varphi = A(0, s, t)$. Then $X \circ A = X$ and

$$A^{-1}\varphi = A^{-1}A \begin{pmatrix} 0 \\ s \\ t \end{pmatrix} = \begin{pmatrix} 0 \\ s \\ t \end{pmatrix}.$$

We may assume without loss of generality that $l = X$ and $\varphi = (0, s, t)$. As $0 = g(\varphi) = g(0, s, t) \in \mathbf{Z}[s, t]$ it follows that all terms that do not contain a X have a coefficient of 0. Thus $X \mid g$. □

Lemma 5.5. *Let k be a field of characteristic greater than 4. Let $g \in k[X, Y, Z]_4$ and $l \in k[X, Y, Z]_1$ be given. Then $l^2 \mid g$ if and only if $l \mid g$ and for all $v \in \{X, Y, Z\}$ it holds that $l \mid \frac{\partial}{\partial v} g$.*

Proof. Suppose that $l^2 \mid g$. Then it holds that $l \mid g$. Let $h \in k[X, Y, Z]_2$ be such that $g = l^2 h$. For $v \in \{X, Y, Z\}$ we calculate the derivative of g with respect to v:

$$\frac{\partial g}{\partial v} = 2l\frac{\partial l}{\partial v}h + l^2\frac{\partial h}{\partial v} = l(2\frac{\partial l}{\partial v}h + l\frac{\partial h}{\partial v}).$$

So we see that for all $v \in \{X, Y, Z\}$ it holds that $l \mid \frac{\partial g}{\partial v}$.

Now for the other way around, suppose that for all $v \in \{X, Y, Z\}$ we have $l \mid \frac{\partial g}{\partial v}$ and suppose that $l \mid g$. We may suppose that l is non-zero. Let $h \in k[X, Y, Z]_3$ be such that $g = lh$. As l is non-zero there is a $v \in \{X, Y, Z\}$ such that $\frac{\partial l}{\partial v} \in k$ is non-zero. For such v we write $\frac{\partial g}{\partial v} = l g_v$ for some $g_v \in k[X, Y, Z]_3$. Then we calculate the derivative of g with respect to v,

$$\frac{\partial g}{\partial v} = \frac{\partial l}{\partial v}h + l\frac{\partial h}{\partial v}.$$

So it follows that,

$$\frac{\partial l}{\partial v}h = l(g_i - \frac{\partial h}{\partial v}),$$

as per assumption on v we can divide out by $\frac{\partial l}{\partial v} \in k^*$ and see that $l \mid h$. Hence $l^2 \mid lh = g$. □

5.2 Weight system $(0,1,1)$

Let $g \in \mathbf{Z}[X,Y,Z]_4$ be a form and $p > 4$ be a prime. Let $P \in \mathrm{GL}_3(\mathbf{Z})$ be such that $P\,\mathrm{diag}(1,p,p)$ is an improvement for g at p. In this subsection we give a list $\mathcal{L} \subseteq \mathbf{P}^2(\mathbf{F}_p)$ with at most 20 elements, and such that $(P(1,0,0) \bmod p) \in \mathcal{L}$. Then $\mathcal{L}$ can be used for Algorithm 3.16 to find an improvement.

Write $f = g \circ P$ and $\alpha = (P(1,0,0) \bmod p)$. In our final algorithm we try the weight system $(0,0,1)$ before we try $(0,1,1)$, so we may suppose that for all $A \in \mathrm{GL}_3(\mathbf{Z})$ the matrix $A\,\mathrm{diag}(1,1,p)$ is not an improvement for g at p. Write $(g \bmod p) = \prod_{i=1}^n h_i^{e_i}$ with $h_i \in \mathbf{F}_p[X,Y,Z]$ irreducible and $e_i \in \mathbf{Z}_{>0}$ such that $h_1, \ldots, h_n$ are pair wise coprime. We saw in Proposition 3.13 that α is a triple point for $(g \bmod p)$.

We define $\mathcal{L}$ as the union of other sets. Define $\mathrm{rad}(g \bmod p) = \prod_{i=1}^n h_i$, and

$$\mathcal{L}_1 := \left\{x \in \mathbf{P}^2(\mathbf{F}_p) : x \text{ is a singular point for } \mathrm{rad}(g \bmod p)\right\}.$$

For all $i \in \{1,\ldots,n\}$ with $e_i > 1$ and $\deg(h_i) = 1$ choose a parametrisation φ^i of a primitive lift of h_i. Note that for each index i, $\frac{g\circ\varphi^i}{p}$ is an integer polynomial in two variables. Hence for each index i evaluating $(\frac{g\circ\varphi^i}{p} \bmod p)$ on a point $(x,y) \in \mathbf{Z}^2$ does not depend on a choice of representatives for $(x \bmod p)$ and $(y \bmod p)$. Define for $i = 1,\ldots,n$:

$$\mathcal{L}^0_{2,i} := \begin{cases} \left\{(x \bmod p, y \bmod p) \in \mathbf{P}^1(\mathbf{F}_p) : \frac{g\circ\varphi^i}{p}(x,y) \equiv 0 \pmod p\right\} & \text{if } e_i > 1 \text{ and } \deg(h_i) = 1, \\ \varnothing & \text{otherwise.} \end{cases}$$

Write for each index i, $\mathcal{L}_{2,i} = \varphi^i(\mathcal{L}^0_{2,i})$; and write $\mathcal{L}_2 = \bigcup_i \mathcal{L}_{2,i}$. Then we pick $\mathcal{L} = \mathcal{L}_1 \cup \mathcal{L}_2$.

Lemma 5.6. *Let $g \in \mathbf{Z}[X,Y,Z]_4$ be a form, $p > 3$ a prime and $P \in \mathrm{GL}_3(\mathbf{Z})$ a matrix such that $\mathrm{diag}(1,p,p)$ is an improvement for $f := g \circ P$ at p. Define $\alpha := (P(1,0,0) \bmod p)$ and let $\mathcal{L}$ be as above. Then it holds that $\alpha \in \mathcal{L}$.*

Proof. Suppose first that there are $i,j \in \{1,\ldots,n\}$ such that $i \neq j$ and $h_i(\alpha) = h_j(\alpha) = 0 \in \mathbf{F}_p$. We show that α is a singular point for $\mathrm{rad}(g \bmod p)$. Note that

$$\nabla(\mathrm{rad}(g \bmod p))(\alpha) = \nabla h_i(\alpha) \prod_{s\neq i} h_s(\alpha) + \nabla(\prod_{s\neq i} h_s(\alpha)) h_i(\alpha) = 0,$$

since $\prod_{s\neq i} h_s(\alpha) = h_j(\alpha) \prod_{j\neq s\neq i} h_s(\alpha) = 0$. Then α is a singular point of $\mathrm{rad}(g \bmod p)$ so $\alpha \in \mathcal{L}_1 \subseteq \mathcal{L}$.

Assume that there is exactly one index $\hat{i} \in \{1,\ldots,n\}$ such that $h_{\hat{i}}(\alpha) = 0$. We consider three different cases:

Case 1: $e_{\hat{i}} = 1$.

Case 2: $e_{\hat{i}} > 1$ and $\deg(h_{\hat{i}}) = 1$.

Case 3: $e_{\hat{i}} > 1$ and $\deg(h_{\hat{i}}) = 2$.

Note that, as $(g \bmod p)$ is of degree 4; If $e_{\hat{i}} > 1$, then $\deg(h_{\hat{i}}) \leq 2$.

Case 1. Suppose that $e_{\hat{i}} = 1$. We show that $\alpha \in \mathcal{L}_1$. We have to prove that α is a singular point of $\mathrm{rad}(g \bmod p)$. Recall that α is a singular point of $(g \bmod p)$. Note that $(g \bmod p) = \mathrm{rad}(g \bmod p) \prod_{i=1}^n h_i^{e_i-1}$. So it follows that

$$\nabla(g \bmod p) = \nabla(\mathrm{rad}(g \bmod p)) \prod_{i=1}^n h_i^{e_i-1} + \mathrm{rad}(g \bmod p) \nabla(\prod_{i=1}^n h_i^{e_i-1})$$

As α vanishes on $\mathrm{rad}(g \bmod p)$ and it does not on $\prod_{i=1}^n h_i^{e_i-1}$ we conclude that α is a singular point of $\mathrm{rad}(g \bmod p)$. So $\alpha \in \mathcal{L}_1 \subseteq \mathcal{L}$.

Case 2. Suppose that $e_{\hat{i}} > 1$ and that $\deg(h_{\hat{i}}) = 1$. We show that $\alpha \in \mathcal{L}_{2,\hat{i}} \subseteq \mathcal{L}_2 \subseteq \mathcal{L}$. Let $l \in \mathbf{Z}[X,Y,Z]_1$ be a primitive linear form such that $l \equiv h_{\hat{i}} \pmod p$, and let φ be a parametrisation of l. Write $b := l \circ P$ and $\psi := P^{-1}\varphi$.

From equation (4) on page 14 it follows that we may write

$$f \equiv pX^2q(Y,Z) + Xr(Y,Z) + h(Y,Z) \pmod{p^2},$$

with $q \in \mathbf{Z}[Y,Z]_2$, $r \in \mathbf{Z}[Y,Z]_3$ and $h \in \mathbf{Z}[Y,Z]_4$.

Per assumption $h_{\hat{i}}^2$ divides $(g \bmod p)$, so $(b^2 \bmod p)$ divides $((Xr+h) \bmod p)$. Then we have that,

$$(b^2 \bmod p) \mid (r \bmod p) \quad \text{and} \quad (b^2 \bmod p) \mid (h \bmod p).$$

From this, it follows that we may write

$$r = b^2 r_1 + p\tilde{r}, \quad \text{and} \quad h = b^2 h_1 + p\tilde{h},$$

with $r_1, \tilde{r} \in \mathbf{Z}[Y,Z]_3$ and $h_1, \tilde{h} \in \mathbf{Z}[Y,Z]_4$.

This gives us that

$$f \equiv p\left(X^2q + X\tilde{r} + \tilde{h}\right) + b^2\left(Xr_1 + h_1\right) \pmod{p^2}.$$

As $(b \circ \psi) \equiv 0 \pmod{p}$, it follows that

$$\left(b^2(Xr_1 + h_1)\right) \circ \psi \equiv 0 \pmod{p^2}.$$

Hence

$$f \circ \psi \equiv p(\psi_1^2 q \circ \psi + \psi_1 \tilde{r} \circ \psi + \tilde{h} \circ \psi) \pmod{p^2},$$

where $\psi = (\psi_1, \psi_2, \psi_3)$. So

$$\frac{f \circ \psi}{p} \in \mathbf{Z}[s,t].$$

As $b \in \mathbf{Z}[Y,Z]_1$, it follows that there are some $s', t' \in \mathbf{Z}$ such that $\psi(s',t') \equiv (1,0,0) \pmod{p}$. Then we have that

$$\frac{f \circ \psi}{p}(s',t') = 0 \pmod{p},$$

because q, $\tilde{r}$ and $\tilde{h}$ are all homogeneous elements of $\mathbf{Z}[Y,Z]$ of degree at least 2. Now substituting $\psi = P^{-1}\varphi$ we get

$$0 \equiv \frac{f \circ \psi}{p}(s',t') = \frac{g \circ \varphi}{p}(s',t') \pmod{p}.$$

The last thing to note is that $\psi(s',t') = P^{-1}\varphi(s',t')$ and that $\psi(s',t') \equiv (1,0,0) \pmod{p}$, so $\varphi(s',t') \equiv \alpha \pmod{p}$. This shows that $\alpha \in \mathcal{L}_{2,\hat{i}}$.

Case 3. Suppose that $e_{\hat{i}} > 1$ and $\deg(h_{\hat{i}} = 2)$. We prove that $\alpha \in \mathcal{L}_1$. Write $Q := h_{\hat{i}}$. Note that $(g \bmod p) = Q^2$ and $\operatorname{rad}(g \bmod p) = Q$. We show that α is a singular point for Q. Note that α is a triple point of $(g \bmod p)$, so all second derivatives of $(g \bmod p)$ vanish on α. For X_i and X_j elements of $\{X,Y,Z\}$ we have,

$$\frac{\partial^2}{\partial X_i X_j}(g \bmod p) = 2\frac{\partial Q}{\partial X_i}\frac{\partial Q}{\partial X_j} + 2Q\frac{\partial Q}{\partial X_i X_j}.$$

Evaluating this on α and noting that $Q(\alpha) = 0$ gives us that

$$\frac{\partial Q}{\partial X_i}(\alpha)\frac{\partial Q}{\partial X_j}(\alpha) = 0.$$

Hence $\nabla Q(\alpha) = 0$. So $\alpha \in \mathcal{L}_1 \subseteq \mathcal{L}$. □

We give a rough bound on $\mathcal{L}$. What is important is that this bound does not depend on p. So even if p is very large we can still loop over $\mathcal{L}$ in our algorithm.

Lemma 5.7. *Let $g \in \mathbf{Z}[X,Y,Z]_4$ be a form, $p > 3$ a prime and $P \in \mathrm{GL}_3(\mathbf{Z})$ a matrix such that $\operatorname{diag}(1,p,p)$ is an improvement for $f := g \circ P$ at p. Let $\mathcal{L}$ be as above. Suppose that for all matrices $A \in \mathrm{GL}_3(\mathbf{Z})$ the matrix $A\operatorname{diag}(1,1,p)$ is not an improvement for g at p. It holds that $\#\mathcal{L} \leq 20$.*

Proof. We first give a bound for $\mathcal{L}_1$ and $\mathcal{L}_2$ separately. Then we add them together to form a (rough) bound on $\mathcal{L}$.

Bound on $\mathcal{L}_1$. We prove that $\#\mathcal{L}_1 \leq 12$. We first show that

$$\mathcal{L}_1 \subseteq \bigcup_{i \neq j} \{x \in \mathbf{P}^2(\mathbf{F}_p) \,:\, h_i(x) = 0 \text{ and } h_j(x) = 0\} \cup \bigcup_{i=1}^{n} \operatorname{sing}(h_i), \tag{6}$$

where for each index i the set $\operatorname{sing}(h_i)$ is the set of all singular points of h_i. Let $x \in \mathcal{L}_1$ be given. If x is a singular point for some h_i then the statement is clear. Suppose for all indices i that x is not a singular point of h_i. There is an index i such that $h_i(x) = 0$, for such an index we have that,

$$\nabla(\operatorname{rad}(g \bmod p))(x) = h_i(x)\nabla(\prod_{j \neq i} h_j(x)) + \nabla h_i(x) \prod_{j \neq i} h_j(x),$$

which gives us that

$$\nabla h_i(x) \prod_{j \neq i} h_j(x) = 0.$$

As $\nabla h_i(x) \neq 0$, there is an index j not equal to i such that $h_j(x) = 0$. This proves inclusion (6).

From inclusion (6) it follows that the size of $\mathcal{L}_1$ is bounded by

$$\sum_{i \neq j} \deg(h_i) \deg(h_j) + \sum_{i=1}^{n} \#\operatorname{sing}(h_i).$$

As $(g \bmod p)$ has degree 4 it follows that $4 = \sum_{i=1}^{n} e_i \deg(h_i)$. From this it follows that $\operatorname{rad}(g \bmod p)$ is either irreducible or if of one of the following forms

$$\begin{array}{lll} \text{(lin)}, & \text{(quad)}, & \\ \text{(lin)}\cdot\text{(lin)}, & \text{(quad)}\cdot\text{(lin)}, & \text{(cubic)}\cdot\text{(lin)}, \\ \text{(lin)}\cdot\text{(lin)}\cdot\text{(lin)}, & \text{(quad)}\cdot\text{(lin)}\cdot\text{(lin)}, & \\ \text{(lin)}\cdot\text{(lin)}\cdot\text{(lin)}\cdot\text{(lin)} & \text{or (quad)}\cdot\text{(quad)}. & \end{array}$$

We need to use some bound on the number of singular points of a homogeneous form in three variables. We use Bézout to give a rough bound. Claim: A non-zero irreducible homogeneous polynomial $f_d \in \mathbf{F}_p[X, Y, Z]_d$ for $d = 1, 2, 3, 4$ has at most $d(d-1)$ singular points. Proof of claim: Note that one of the derivatives of f_d has to be non-zero, otherwise f_d is zero. As f_d is irreducible it does not share a factor with this non-zero derivative. Hence, from Bézout it follows that f_d and this non-zero derivative have at most $d(d-1)$ points in common. As a singular point is a common point of f_d and all its derivatives there can be at most $d(d-1)$.

We calculate $d(d-1)$ for $d = 1, 2, 3, 4$,

d	1	2	3	4
$d(d-1)$	0	2	6	12

We then calculate these bound for every possible form of $\operatorname{rad}(g \bmod p)$. The results are shown in the following table.

	$\sum_{i=1}^{n} \#\operatorname{sing}(h_i)$ is less than or equal to	$\sum_{i \neq j} \deg(h_i)\deg(h_j)$ is equal to
(lin)·(lin)·(lin)·(lin)	0	6
(lin)·(lin)·(lin)	0	3
(lin)·(lin)	0	1
(lin)	0	0
(quad)	2	0
(quad)·(quad)	4	4
(quad)·(lin)	2	2
(quad)·(lin)·(lin)	2	5
(cubic)·(lin)	6	3
(quartic)	12	0

The size of $\mathcal{L}_1$ is bounded by the maximum of the sums of the two columns in the table above. Hence $\#\mathcal{L}_1 \leq 12$.

Bound on $\mathcal{L}_2$. We show that $\mathcal{L}_2$ has at most 8 elements. Note that $\#\mathcal{L}_2 \leq \sum_i \#\mathcal{L}_{2,i}$ where the sum is taken over all $i \in \{1, \ldots, n\}$ with $e_i > 1$ and $\deg(h_i) = 1$. Note that we have at most 2 terms in this sum.

Let $i \in \{1, \ldots, n\}$ be such that $e_i > 1$ and $\deg(h_i) = 1$. We show that $\#\mathcal{L}_{2,i} \leq 4$. It suffices to show that $\mathcal{L}^0_{2,i}$ has at most 4 elements. Note that $\mathcal{L}^0_{2,i}$ is the zero set of $\frac{g\circ\varphi}{p}$ for some parametrisation φ of some primitive form $l \in \mathbf{Z}[X,Y,Z]_1$. The form $(\frac{g\circ\varphi}{p} \bmod p)$ is a form of degree 4 in 2 variables. So we only have to show that $(\frac{g\circ\varphi}{p} \bmod p)$ is not the zero polynomial. Suppose that $\frac{g\circ\varphi}{p} \equiv 0 \pmod p$. Then $g \circ \varphi \equiv 0 \pmod{p^2}$, so from Lemma 5.4 it follows that $(l \bmod p^2) \mid (g \mod p^2)$. Per assumption we know that $(l^2 \bmod p) \mid (g \bmod p)$, but this contradicts Proposition 3.2 as we assumed no improvement of type $(0,0,1)$ is possible. So $\mathcal{L}^0_{2,i}$ contains at most 4 elements, thus so does $\mathcal{L}_{2,i}$.

We conclude that $\#\mathcal{L}_2 \leq 4 + 4 = 8$.

Bound on $\mathcal{L}$. As $\mathcal{L} = \mathcal{L}_1 \cup \mathcal{L}_2$ we conclude that $\#\mathcal{L} \leq 20$. □

5.3 Weight system $(0,1,3)$

Let $g \in \mathbf{Z}[X,Y,Z]_4$ be a form and p a prime. Suppose that for all $A \in \mathrm{GL}_3(\mathbf{Z})$ the matrix $A\,\mathrm{diag}(1,1,p)$ is not an improvement for g at p. Let $P \in \mathrm{GL}_3(\mathbf{Z})$ such that $\mathrm{diag}(1,p,p^3)$ is an improvement for $f := g \circ P$. Write $\alpha := (P(1,0,0) \bmod p)$. To apply Algorithm 3.18, we need a list $\mathcal{L} \subseteq \mathbf{P}^2(\mathbf{F}_p)$ of points such that $\alpha \in \mathcal{L}$. Algorithm 3.18 loops over the whole list $\mathcal{L}$, so it is important that $\mathcal{L}$ is not too big. In this section we give a method that gives a set $\mathcal{L}$ such that $\mathcal{L}$ contains at most 16 elements and such that $\alpha \in \mathcal{L}$.

For small p (< 5) we can take $\mathcal{L}$ to be equal to the set of all the singular points of $(g \bmod p)$ in $\mathbf{P}^2(\mathbf{F}_p)$. So suppose that p is big (≥ 5). As $(Z \bmod p) \mid (f \bmod p)$, it follows that $((Z \circ P^{-1}) \bmod p)$ divides $(g \bmod p)$. Define for every primitive linear form $l \in \mathbf{Z}[X,Y,Z]_1$ with $(l \bmod p) \mid (g \bmod p)$ the set $\mathcal{L}_0(l)$ as

$$\left\{(x \bmod p, y \bmod p) \in \mathbf{P}^1(\mathbf{F}_p) : \frac{g\circ\varphi_l}{p}(x,y) \equiv 0 \pmod p \text{ and } (\nabla g)(\varphi_l(x,y) \equiv 0 \pmod p)\right\},$$

where φ_l is a parametrisation of l. Now define $\mathcal{L} = \bigcup_{(l \bmod p)} \varphi_l(\mathcal{L}_0(l))$, where the union is taken over all linear factors $(l \bmod p)$ of $(g \bmod p)$ where we take l primitive.

Lemma 5.8. *Let $g \in \mathbf{Z}[X,Y,Z]_4$ be a form and $P \in \mathrm{GL}_3(\mathbf{Z})$ a matrix such that $P\,\mathrm{diag}(1,p,p^3)$ is an improvement for g at some prime $p > 3$. Assume that for all matrices $A \in \mathrm{GL}_3(\mathbf{Z})$ the matrix $A\,\mathrm{diag}(1,p,p)$ is not an improvement for g. Let $\mathcal{L}$ be the set as defined above. Then $\mathcal{L}$ has at most 16 elements and $\alpha \in \mathcal{L}$.*

Proof. Let $l \in \mathbf{Z}[X,Y,Z]_1$ be such that $l \equiv Z \circ P^{-1} \pmod p$ and let φ be a parametrisation of l. We show that $\alpha \in \varphi(\mathcal{L}_0(l))$. Write $b = l \circ P$ and $\psi = P^{-1}\varphi$ then $b \equiv Z \pmod p$. From Lemma 5.3 it follows that ψ is a parametrisation of b. As $b \equiv Z \pmod p$, it follows that there are $(s',t') \in \mathbf{Z}^2$ such that $\psi(s',t') \equiv (1,0,0) \pmod p$. As $\psi = P^{-1}\varphi$ we have that $\alpha = \varphi(s',t')$. We show that $(s',t') \in \mathcal{L}_0(l)$.

We know from Proposition 3.19 that α is a singular point for $(g \bmod p)$, so $(\nabla g)(\varphi(s',t')) \equiv 0 \pmod p$.

It follows from Equation (5) on page 17 that we may write

$$f \equiv XY^2Zc_1p + Y^3Zc_0 + Z^2h \pmod{p^2},$$

where for all indices i we have $c_i \in \mathbf{Z}$ and $h \in \mathbf{Z}[X,Y,Z]_2$. As $b \equiv Z \pmod p$, and as ψ is a parametrisation of b we may write $\psi = (\psi_1, \psi_2, p\psi_3)$ with ψ_1,ψ_2 and ψ_3 elements of $\mathbf{Z}[s,t]_1$. Then

$$f \circ \psi \equiv \psi_1\psi_2^2\psi_3c_1p^2 + \psi_2^3\psi_3pc_0 + p^2\psi_3^2 \cdot (h \circ \psi) \equiv \psi_2^3\psi_3pc_0 \pmod{p^2}.$$

So we see that

$$\frac{f\circ\psi}{p} \equiv \psi_2^2\psi_3c_0.$$

As $\psi_2(s',t') = 0$ we see that

$$\frac{f\circ\psi}{p}(s',t') \equiv 0 \pmod p.$$

Now we note that $f \circ \psi = g \circ \varphi$ so

$$\frac{g\circ\varphi}{p}(s',t') \equiv 0 \pmod p.$$

This shows that $\alpha \in \mathcal{L}$.

We now show that $\mathcal{L}$ has no more than 16 elements. As $\mathcal{L} = \bigcup_{(l \bmod p)} \varphi_l(\mathcal{L}_0(l))$, it suffices to show that for every linear factor $(l \bmod p)$ of $(g \bmod p)$ the set $\mathcal{L}_0(l)$ has at most 4 elements. As $(g \bmod p)$ is of degree 4, it can have at most 4 linear factors and hence $\mathcal{L}$ is bounded by 16.

So let $l \in \mathbf{Z}[X,Y,Z]_1$ be a primitive linear form such that $(l \bmod p)$ divides $(g \bmod p)$. (This is a different l then we used in the first part of this proof.) Note that $\mathcal{L}_0(l)$ is the intersection of the zero sets of forms of degree 3 and 4 in two variables. Thus it suffices to show that not all of these polynomials are zero.

Per assumption, there does not exist a matrix $A \in \mathrm{GL}_3(\mathbf{Z})$ such that $A\,\mathrm{diag}(1,1,p)$ is an improvement for g at p. It then follows from Proposition 3.2 that

$$(l^2 \bmod p) \nmid (g \bmod p) \quad \text{or} \quad (l \bmod p^2) \nmid \left(g \bmod p^2\right).$$

Assume first that $(l^2 \bmod p) \nmid (g \bmod p)$. As $(l \bmod p)$ divides $(g \bmod p)$ it follows from Lemma 5.5 that for some $v \in \{X,Y,Z\}$ we have that $(l \bmod p)$ does not divide$(\frac{\partial}{\partial v} g \bmod p)$. For such a v it follows from Lemma 5.4 that $\frac{\partial g}{\partial v}(\varphi) \not\equiv 0 \pmod p$.

Now assume that $(l \bmod p^2)$ does not divide $(g \bmod p^2)$. From Lemma 5.4 it now follows that $g \circ \varphi \not\equiv 0 \pmod{p^2}$. But as $g \circ \varphi \equiv 0 \pmod p$, it follows that $\frac{g\circ\varphi}{p} \not\equiv 0 \pmod p$.

So, $\mathcal{L}_0(l)$ is the intersection of the zero sets of forms in two variables of degree not more than 4. Thus $\#\mathcal{L}_0(l) \leq 4$.

As $(g \bmod p)$ has at most 4 linear factors it follows that $\mathcal{L}$ is bounded by 16. □

6 Final algorithm

Combining all previous sections we are able to state our Algorithm. To compute the discriminant of a form in $\mathbf{Z}[X,Y,Z]_4$ one could use the code of J. Sijsling [9, 7].

Algorithm 6.1: Final algorithm.

input : A form $g \in \mathbf{Z}[X,Y,Z]_4$ with coprime coefficients and non-zero discriminant

output: A form $h \in \mathbf{Z}[X,Y,Z]_4$ equivalent to g, such that for all forms $\hat{h} \in \mathbf{Z}[X,Y,Z]_4$ equivalent to h it holds that $|\Delta(\hat{h})| \geq |\Delta(h)|$.

1 **for** *every prime* p *dividing* $\Delta(g)$ **do**
  Try weight system $(0,0,1)$ as follows
2 $L \leftarrow$ the output of Algorithm 3.6 run with g and p
3 **if** L *contains a matrix* M **then**
4 $t \leftarrow$ the greatest common divisor of the coefficients of $g \circ M$
5 $g \leftarrow \frac{1}{t} g \circ M$ (M is an improvement!)
6 Go to step 2
  Try weight system $(0,1,1)$ as follows
7 **if** $p < 5$ **then**
8 $\mathcal{L} \leftarrow$ all triple points of $(g \bmod p)$
9 Go to line 11
10 Find the set $\mathcal{L}$ as described in section 5.2
11 $L \leftarrow$ the output of Algorithm 3.16 run with g, p and $\mathcal{L}$
12 **if** L *contains a matrix* M **then**
13 $t \leftarrow$ the greatest common divisor of the coefficients of $g \circ M$
14 $g \leftarrow \frac{1}{t} g \circ M$ (M is an improvement!)
15 Go to step 2
  Try weight system $(0,1,3)$
16 **if** $p < 5$ **then**
17 $\mathcal{L} \leftarrow$ all singular point of $(g \bmod p)$
18 Go to line 20
19 Find the set $\mathcal{L}$ as described in section 5.3
20 $L \leftarrow$ the output of Algorithm 3.18 run with g, p and $\mathcal{L}$
21 **if** L *contains a matrix* M **then**
22 $t \leftarrow$ the greatest common divisor of the coefficients of $g \circ M$
23 $g \leftarrow \frac{1}{t} g \circ M$ (M is an improvement!)
24 Go to step 2
25 **return** g

Proof. As the sets $\mathcal{L}$ on lines 11 and 20 are finite the called algorithms and **for** loops end in finite time. In lines 5, 14 and 23 the integer $\Delta(\frac{1}{t} g \circ M)$ has lower p-adic valuation than $\Delta(g)$. So every iteration to line 2

we treat a form that has smaller p-adic valuation of its discriminant. Since the p-adic valuation of a non-zero integer has a minimum (namely 0), eventually the algorithm will halt.

Let h be the output of our algorithm and let $\hat{h} \in \mathbf{Z}[X,Y,Z]_4$ be a form equivalent to h. Suppose that $|\Delta(\hat{h})| < |\Delta(h)|$. We show that our algorithm does not return h, which gives a contradiction since we assumed that h is the output.

There is a local improvement A for h at some prime p. We execute the steps after the first **for** loop with this prime p. It follows from Corollary 2.8 that there exists integral matrices $P \in \mathrm{GL}_3(\mathbf{Z})$, $Q \in \mathrm{GL}_3(\mathbf{Z}_{(p)})$ and $D \in \mathrm{GL}_3(\mathbf{Q})$ diagonal such that $A = PDQ$. Now from Proposition 2.9 it follows that PD is an improvement for h at p. Then it follows from Theorem 2.12 that one of the weight systems $(0,0,1)$, $(0,1,1)$ or $(0,1,3)$ is an improvement for $h \circ P$ at p.

Every time we find an improvement we loop back to step 2. So at some point we had to be in step 2 with $g \leftarrow h$.

First suppose that the weight system $(0,0,1)$ is an improvement for $h \circ P$ at p. Then Algorithm 3.6 returns a set of improvements. Hence the algorithm gets to step 5 and does not return h.

Next, suppose that the weight system $(0,1,1)$ is an improvement for $h \circ P$ at p. The set $\mathcal{L}$ contains $P(1,0,0)$ as seen in Section 5.2. Hence, Algorithm 3.16 returns a set of improvements. Thus we get to step 14 and do not return h.

Finally, suppose that the weight system $(0,1,3)$ is an improvement for $h \circ P$ at p. As shown in Section 5.3, the set $\mathcal{L}$ on line 20 contains $P(1,0,0)$. So Algorithm 3.18 returns an improvement, which means that we get to step 23 and hence do not return h. This finishes the proof. □

References

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[2] H. Cohen. *A course in computational algebraic number theory*. Springer, 1993.

[3] A-S. Elsenhans. Good models for cubic surfaces. Available at https://math.uni-paderborn.de/fileadmin/mathematik/AG-Computeralgebra/Preprints-elsenhans/red_5.pdf.

[4] W. Fulton. *Algebraic Curves*. 2008. Available at http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf.

[5] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, resultants, and multidimensional determinants*. Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, 1994.

[6] P. Kilicer, H. Labrande, R. Lercier, C. Ritzenthaler, J. Sijsling, and M. Streng. Plane quartics over $\mathbf{Q}$ with complex multiplication. *Acta Arithmetica*, 185(2):127–156, 2018.

[7] R. Lercier, C. Ritzenthaler, and J. Sijsling. Reconstructing plane quartics from their invariants. *Discrete & Computational Geometry*, 2018. Available at https://doi.org/10.1007/s00454-018-0047-4.

[8] M. Newman. *Integral Matrices*. Pure and applied mathematics : a series of monographs and textbooks. Academic Press, 1972.

[9] J. Sijsling. The file DixmierOhnoInvariants.m, 2016. Available at the GitHub page https://github.com/JRSijsling/quartic_reconstruction.

[10] P. Stevenhagen. *Algebra II*. 2017. Available (in Dutch) at http://websites.math.leidenuniv.nl/algebra/algebra2.pdf.

[11] M. Stoll. Reduction theory of point clusters in projective space. *Groups Geom. Dyn. 5, 553-565 (2011)*, 2009.