GOOD MODELS FOR CUBIC SURFACES

ANDREAS-STEPHAN ELSENHANS

Abstract. This article describes an algorithm for finding a model of a hypersurface with small coefficients. It is shown that the approach works in arbitrary dimension and degree. In the special case of a cubic surface it is completely explicit.

1. Introduction

In [EJ] J. Jahnel and the author constructed cubic surfaces by using explicit Galois descent and the hexahedral form. This leads to equations with big coefficients. The aim of this note is to explain a way to find an isomorphic surface with small coefficients. This isomorphism is an isomorphism of $\mathbb{Q}$-schemes. In general, the corresponding $\mathbb{Z}$-schemes are not isomorphic.

The construction of a good equation consists of two parts. In the first part one has to improve the model for the scheme over $\mathbb{Z}_p$ for each prime p of bad reduction. In an optimal situation, one can remove a bad prime completely. In the second part, one has to look at the infinite prime. This is classical known as reduction theory. It means to modify the embedding of the surface by operating with $\mathrm{Sl}_4(\mathbb{Z})$.

2. The finite places

In [K] J. Kollar discusses the problem of choosing good models in a very general way. We follow this approach but we focus on the arithmetic situation.

Let V be the hypersurface given by a homogeneous polynomial $f(x_0, \ldots, x_n) = 0$ in the projective space. Assuming that V is semi-stable leads to a least one nonzero invariant $I(f)$. Modifying f locally at the prime p changes this invariant by a power of p. We use this to control the finiteness of the algorithm.

More precisely, we construct a sequence of polynomials f_n with integral coefficients defining isomorphic schemes over $\mathbb{Q}$ such that $v_p(I(f_n))$ decreases. As I is a polynomial in the coefficients of f, this process terminates after finitely many steps.

[1] The author was partially suported by the Deutsche Forschungsgemeinschaft (DFG).

Remark 1. Recall from invariant theory that a smooth hypersurface of degree at least 3 is stable [MFK, Ch. IV, Proposition 4.2]. In this case one could choose the discriminant as the non-zero invariant.

The main tool for the description of the algorithm are weights.

Definition 2. Let $f(x_0, \dots, x_n)$ be a polynomial with integral coefficients. Denote by $\operatorname{mult}_p f(x_0, \dots, x_n)$ the smallest p-adic valuation of a coefficient of f.

Remark 3. Let f be a homogeneous polynomial of degree d with $\operatorname{mult}_p f(x_0, \dots, x_n) = 0$. Then $\operatorname{mult}_p f(px_0, \dots, px_n) = d$.

Let $M \in \operatorname{Mat}((n+1) \times (n+1), \mathbb{Z}) \cap \operatorname{Gl}_{n+1}(\mathbb{Q})$ be given such that $\det(M)$ is a power of p.

Then we can use M to modify the model. We get $g = p^{-e} f(Mx)$ with $e := \operatorname{mult}_p(f(Mx))$. The new equation $g(x_0, \dots, x_n) = 0$ is better if $v_p(I(g)) < v_p(I(f))$. This is equivalent to $e > \frac{v_p(\det(M)) \deg(f)}{n+1}$

Remark 4. Observe the following ambiguity. Suppose that the columns of M and M' define the same $\mathbb{Z}$-lattice. Then the resulting new models are equal (i.e. isomorphic as $\mathbb{Z}$-schemes).

Using the elementary divisor theorem, one can factor the matrix M into a product of $M_1 \in \operatorname{Gl}_{n+1}(\mathbb{Z})$ and a diagonal matrix M_2, whose entries are powers of p. The exponents of these diagonal entries are called a weight system. Without loss of generality the entries of M_2 are sorted.

Remark 5. One does not have to look at arbitrary weight systems here are some obvious restrictions:

- As the entries of M_2 are sorted the weights are sorted too.
- Replacing a weight system $(w_0, \dots, w_n)$ by a translated weight system $(c + w_0, \dots, c + w_n)$ does not affect the model. So we can assume $0 = w_0 \leq w_1 \leq \dots \leq w_n$.

All this can be interpreted in the language of affine Bruhat-Tits buildings.

Recall 6. The Bruhat-Tits building.

- The affine Bruhat-Tits building of type $\widetilde{A_{n+1}}$ for $\mathbb{Q}_p$ is a n-dimensional simplicial complex.
- The vertices are classes of $(n+1)$-dimensional lattices in $\mathbb{Q}_p^{n+1}$.
- The class of a lattice $L \subset \mathbb{Q}_p^{n+1}$ is $[L] := \{cL \mid c \in \mathbb{Q}_p^*\}$.
- Assume that the lattices $L_0, \dots, L_k$ satisfy $L_0 \supset L_1 \supset \dots \supset L_k \supset pL_0$. Then their classes form a k-simplex.
- Let $b_0, \dots, b_n$ be a basis of $\mathbb{Q}_p^{n+1}$. Then the classes of all lattices of the form $\mathbb{Z}_p p^{e_0} b_0 \oplus \dots \oplus \mathbb{Z}_p p^{e_n} b_n$ for $e_0, \dots, e_n \in \mathbb{Z}$ form a sub-complex called an apartment.

- The apartment corresponding to the standard basis is called the standard apartment.
- Any two simplices are contained in one apartment.

For a detailed description of buildings see, e.g., [B].

Remark 7. The factorization of the matrix M described above has the following interpretation. The matrix M_1 chooses the apartment containing the old and the new lattice. The matrix M_2 describes the position of the new lattice in the apartment.

Doing the reduction with a concrete equation consists of two steps. First one has to choose an apartment and then one has to choose weights, i.e., a lattice in the apartment. If we assume that we have already chosen the right apartment then the matrix M is diagonal.

Observation 8. Let f be a form of degree d and $n+1$ variables. The weight system $(0, w_1, \dots, w_n)$ improves our equation with respect to the standard apartment if and only if $f(x_0, p^{w_1}x_1, \dots, p^{w_n}x_n) \equiv 0 \pmod{p^k}$ for $k = \lfloor \frac{d}{n+1}(w_1 + \dots + w_n) \rfloor + 1$. Writing

$$f = \sum_{0 \leq i_1 \leq \dots \leq i_d \leq n} a_{i_1 \dots i_d} x_{i_1} \cdots x_{i_d}$$

we get the equivalent statement

$$p^{k - w_{i_1} - \dots - w_{i_d}} \mid a_{i_1 \dots i_d}$$

for each d-tuple $(i_1, \dots, i_d)$ such that $k - w_{i_1} - \dots - w_{i_d}$ is positive.

From this the following finiteness result is easily derived:

Proposition 9. *Let n and d be fixed. Then a finite set of weight systems W exists such that the following holds. A form f of degree d in $n+1$ variables can be improved if and only if it can be improved by using one of the weight systems of W.*

Proof. Without loss of generality the improvement takes place in the standard apartment.

A form of degree d and $n+1$ variables has $m := \binom{n+d}{d}$ coefficients. We identify the space of all forms with $\mathbb{Z}_p^m$.

A form can be improved with a given weight system w if and only if the divisibility conditions listed above are satisfied. This condition can be reformulated in terms of the p-adic valuation of the coefficients.

More precisely a form can be improved with the weight system w if and only if $v(a_i) \geq e_i(w)$. The $e_i(w)$ are non-negative integers depending on w and not on p. We have to show that the infinite union of all cones $C(e_1(w), \dots, e_m(w)) := \{a \in \mathbb{N}^m \mid a_i \geq e_i(w)\}$ has a finite sub-covering.

We show this purely geometric statement by induction on the dimension. Assume the the dimension is 1. Then the statement reduces to the fact that each non-empty subset of $\mathbb{N}$ has a smallest element.

Assume that the statement is proven in dimension $m-1$. We have to show that it is true in dimension m. We start with the cones $C(e), e \in E$. We project onto the first $m-1$ coordinates. By induction we find finitely many cones that cover the projection. We take arbitrary preimages $C(e_1), \ldots, C(e_l)$ of the cones that cover the projection. The union of the cones chosen in dimension m covers most of the union of all cones.

All missing points have the property that the last coordinate is smaller than $M := \max\{(e_j)_m : j = 1, \ldots, l\}$. As everything takes place in $\mathbb{N}^m$ the missing points are located in finitely many layers with last coordinate between 1 and M. Inspecting one layer we find the same kind of problem in dimension $m-1$. By induction hypothesis each layer leads to finitely many additional cones. □

Remark 10. This finiteness result proves the existence of an algorithm that constructs an optimal model for a given place.

The algorithm uses the fact that the Bruhat-Tits-building is locally finite. This ensures that only finitely many lattices exist which correspond to a given weight system.

So one gets the existence of a finite list of lattices that improve an arbitrary equation if it can be improved. Testing all these lattices either leads to a better equation or to the proof that no better equation exists.

Repeating this until no better model can be found on gets an algorithm that chooses a optimal one.

For semi-stable varieties this algorithm stops after finitely many steps.

Now we turn to a more concrete description of the necessary weight systems in the case of cubic surfaces. A proposition stated at the end of J. Kollar's paper claims the following.

Proposition 11. *Let $f(x_0, \ldots, x_3) = 0$ be a model of a cubic surface. Assume that this model can be improved. Then it can be improved with one of the following five weight systems*

$$(0,0,0,1),\ (0,0,1,1),\ (0,1,1,1),\ (0,1,2,2),\ (0,2,2,3)\,.$$

Proof. The proof has the following strategy:

Assuming that a given weight system with respect to the standard apartment leads to a better model, we show that one of the given five weight systems improves the model, too.

The $(0,0,0,1)$-case

The weight system $(0,0,0,1)$ improves the cubic equation $f(x_0, x_1, x_2, x_3) = 0$ if and only if all coefficients of the polynomial $f(x_0, x_1, x_2, px_3)$ are divisible by p. Equivalently the coefficients of $x_0^3, x_0^2x_1, x_0^2x_2, x_0x_1^2, x_0x_1x_2, x_0x_2^2, x_1^3, x_1^2x_3, x_1x_2^2, x_2^3$ in the original polynomial are divisible by p. All other weight systems which imply these divisibilities can be replaced by the weight system $(0, 0, 0, 1)$.

Claim: Assume that the sorted weight system $(0, w_1, w_2, w_3)$ improves our equation and satisfies the extra condition $w_1 + w_3 - 3w_2 \geq 0$. Then the weight system $(0, 0, 0, 1)$ improves the equation, too.

Check: We have to show that all monomials without x_3 have coefficients that are divisible by p. This is equivalent to $k - w_{i_1} - w_{i_2} - w_{i_3} \geq 1$ for $i_1, i_2, i_3 \in \{0, 1, 2\}$. Substituting $k = \left\lfloor \frac{3(w_1+w_2+w_3)}{4} \right\rfloor + 1$ the asserted inequality becomes $\frac{3}{4}(w_1 + w_2 + w_3) - w_{i_1} - w_{i_2} - w_{i_3} \geq 0$. As the weights are sorted it is enough to look at the case $i_1 = i_2 = i_3 = 2$. We get $\frac{3}{4}(w_1 + w_3) - \frac{9}{4}w_2 \geq 0$, which was assumed to hold.

The $(0, 1, 2, 2)$-case
Every sorted weight system $(0, w_1, w_2, w_3)$ which satisfies $w_1 + w_3 - 3w_2 \leq 0$, $w_1 \geq 1$, and $3w_1 - w_2 - w_3 \leq 0$ can be replaced by $(0, 1, 2, 2)$.

We have to show that the coefficient of $x_0^i x_1^{3-i}$ is divisible by p^{1+i}, that the coefficients of $x_0^2x_2$ and $x_0^2x_3$ is divisible by p^2, and finally that the coefficients of $x_0x_1x_2$ and $x_0x_1x_3$ are divisible by p.

As w_1 is assumed to be at least 1, the first statement reduces to $k - 3w_1 \geq 1$. The second requirement reduces to $k - w_3 \geq 2$ and the last condition is entailed by $k - w_1 - w_3 \geq 1$. Using $w_1 \geq 1$ we have to show $k - 3w_1 \geq 1$ and $k - w_1 - w_3 \geq 1$. The formula $k = \left\lfloor \frac{3(w_1+w_2+w_3)}{4} \right\rfloor + 1$ leads to the inequalities $\frac{3(w_2+w_3)}{4} - \frac{9}{4}w_1 \geq 0$ and $\frac{3}{4}w_2 - \frac{1}{4}w_1 - \frac{1}{4}w_3 \geq 0$, which are assumed to be true.

The $(0, 2, 2, 3)$-case
Every sorted weight system $(0, w_1, w_2, w_3)$ which satisfies $w_3 > w_2$, $3w_1 - w_2 - w_3 \geq 0$, and $w_3 \geq 3$ can be replaced by $(0, 2, 2, 3)$.

We have to show the following divisibilities

Monomial	Coefficient is divisible by
x_0^3	p^6
$x_0^2x_1, x_0^2x_2$	p^4
$x_0^2x_3$	p^3
$x_0x_1^2, x_0x_1x_2, x_0x_2^2$	p^2
$x_0x_1x_3, x_0x_2x_3$	p

These are entailed by the inequalities

$$\begin{aligned} k &\geq 6 \\ k - w_1, k - w_2 &\geq 4 \\ k - w_3 &\geq 3 \\ k - 2w_1, k - w_1 - w_2, k - 2w_2 &\geq 2 \\ k - w_1 - w_3, k - w_2 - w_3 &\geq 1\,. \end{aligned}$$

Using $w_3 > w_2 \geq w_1$ and the integrality of the w_i we reduce this system of inequalities to

$$\begin{aligned} k &\geq 6 \\ k - w_3 &\geq 3 \\ k - w_2 - w_3 &\geq 1\,. \end{aligned}$$

Note that our assumptions imply $w_2 \geq 2$ and $w_3 \geq 3$. Hence it remains to show $k - w_2 - w_3 \geq 1$. Substituting $k = \left\lfloor \frac{3(w_1+w_2+w_3)}{4} \right\rfloor + 1$ leads to the inequality $\frac{3}{4}w_1 - \frac{1}{4}w_2 - \frac{1}{4}w_3 \geq 0$ which was our assumption.

The $(0,1,1,1)$-case
Every sorted weight system $(0, w_1, w_2, w_3)$ which satisfies $3w_1 + 3w_2 - 5w_3 \geq 0$ can be replaced by $(0,1,1,1)$.

We have to show the following divisibilities

Monomial	Coefficient is divisible by
x_0^3	p^3
$x_0^2x_1, x_0^2x_2, x_0^2x_3$	p^2
$x_0x_1^2, x_0x_1x_2, x_0x_1x_3, x_0x_2^2, x_0x_2x_3, x_0x_3^2$	p

The resulting system of inequalities can be simplified to $k - 2w_3 \geq 1$ by using $1 \leq w_3 \geq w_2 \geq w_1$. The equality $k = \left\lfloor \frac{3(w_1+w_2+w_3)}{4} \right\rfloor + 1$ leads to the assumed inequality.

The $(0,0,1,1)$-case
Every sorted weight system $(0, w_1, w_2, w_3)$ which satisfies $-5w_1 + 3w_2 - w_3 \geq 0$ can be replaced by $(0,0,1,1)$.

We have to show the following divisibilities

Monomial	Coefficient is divisible by
$x_0^3, x_0^2x_1, x_0x_1^2, x_1^3$	p^2
$x_0^2x_2, x_0^2x_3, x_0x_1x_2, x_0x_1x_3, x_1^2x_2, x_1^2x_3$	p

The resulting system of inequalities reduces to $k - 3w_1 \geq 2$ and $k - 2w_1 - w_3 \geq 1$. Our assumption contradicts $w_1 = w_3$. So we can use $w_3 \geq w_1 + 1$. Only the inequality $k - 2w_1 - w_3 \geq 1$ is necessary.

Using $k = \left\lfloor \frac{3(w_1+w_2+w_3)}{4} \right\rfloor + 1$ we get $\frac{3}{4}w_2 - \frac{5}{4}w_1 - \frac{1}{4}w_3 \geq 0$. This is our assumption.

The general case

We have to show that a weight system $(0, w_1, w_2, w_3)$ with $0 \leq w_1 \leq w_2 \leq w_3$ can be replaced by one of the five given by J. Kollar.

If $w_1 = 0$ then $3w_2 - w_3$ is either ≥ 0 or < 0. So we are in the $(0,0,1,1)$ or the $(0,0,0,1)$ case.

If $w_3 = 1$ then we are in one of the three cases $(0,0,0,1)$, $(0,0,1,1)$, $(0,1,1,1)$. So we can assume $w_3 \geq 2$.

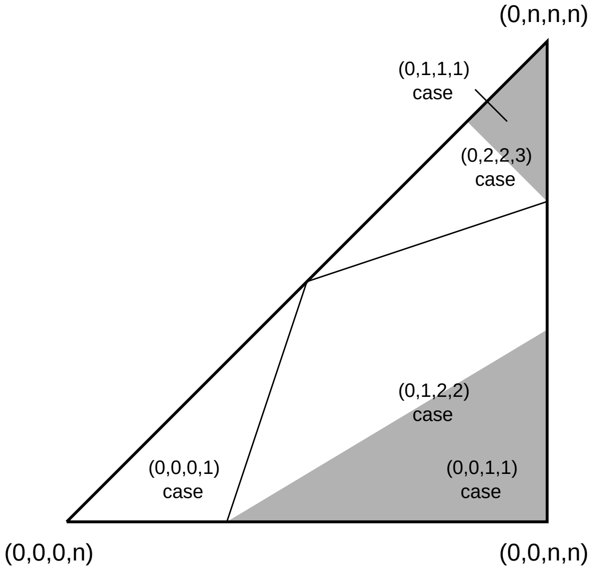
If $w_1 \geq 1$ and $w_3 = 2$ then we are in one of the cases $(0,1,1,2)$, $(0,1,2,2)$, or $(0,2,2,2)$. They are covered by the $(0,0,0,1)$, $(0,1,2,2)$, and $(0,1,1,1)$ cases.

Now we can assume $w_1 \geq 1$ and $w_3 \geq 3$. We test $w_1 + w_3 - 3w_2$. If this is not negative we are in the $(0,0,0,1)$-case. Otherwise we test $3w_1 - w_2 - w_3$. If this is not positive we are in the $(0,1,2,2)$ case.

It remains to treat the case $w_1 \geq 1$, $w_3 \geq 3$, and $3w_1 - w_2 - w_3 > 0$. This is the $(0,2,2,3)$-case if $w_3 > w_2$ holds.

The last possibility is $w_1 \geq 1$, $w_2 = w_3 \geq 3$, and $3w_1 - w_2 - w_3 > 0$. This is part of the $(0,1,1,1)$ case. □

As the main inequalities found are homogenous we can visualize the result by setting $w_3 = n$. Then the space of all weight systems is covered by the five cases as shown in the picture below. Note that the weight systems $(0,0,1,1)$ and $(0,1,1,1)$ are only necessary for very special cases at the boundary and for small w_3.



Covering of all weight-systems as shown in the proof

To get a practical algorithm one needs a strategy for choosing lattices which is better then an enumeration of all of them. We give a solution for this by a reduction modulo p method. The main idea behind this is the following. We have characterized the cases by divisibility conditions of the coefficients. Reduction modulo p leads to cubic surfaces with very few monomials. These are known to be singular. A detailed analysis of the singularities is the basis of the algorithm.

Proposition 12. *Let $f = 0$ be a model of a cubic surface. Then the following hold.*

- *An improvement with the weight system $(0, 0, 0, 1)$ is possible if and only if the reduction modulo p of f is reducible over $\mathbb{Z}/p\mathbb{Z}$.*
- *If the weight system $(0, 0, 1, 1)$ leads to an improvement then the reduction modulo p of $f = 0$ has at least a singular line.*

  For $p > 3$ the following holds. Let

  $$[t : u] \mapsto [g_0(t, u), g_1(t, u), g_2(t, u), g_3(t, u)]$$

  be the parameterization of an arbitrary lift of the singular line. An improvement is possible if and only if $f(g_0, g_1, g_2, g_3) \equiv 0$ holds modulo p^2.
- *A necessary condition that the weight system $(0, 1, 1, 1)$ leads to an improvement is that the reduction modulo p is a cone.*

  Further there exists a point P_0 that reduces to a singular point and satisfies $f(P_0) \equiv 0$ modulo p^3. If the cone has a unique apex then P_0 is a lift of this point.

Proof. Without loss of generality the improvement takes place in the standard apartment.

The weight system $(0, 0, 0, 1)$ works if and only if the coefficients of all monomials without x_3 are divisible by p. Equivalently x_3 is a linear factor of the reduction of f.

The possibility of an improvement with the weight system $(0, 0, 1, 1)$ leads to the following conditions

Monomial	Coefficient is divisible by
$x_0^3, x_0^2x_1, x_0x_1^2, x_1^3$	p^2
$x_0^2x_2, x_0^2x_3, x_0x_1x_2, x_0x_1x_3, x_1^2x_2, x_1^2x_3$	p

On the other hand let $h = 0$ be a cubic surface such that the reduction modulo p has the singular line $x_2 = x_3 = 0$. This is characterized by

$$p \mid h(x_0, x_1, 0, 0) \quad \text{and} \quad p \mid \left.\frac{\partial h}{\partial x_i}\right|_{x_2=x_3=0} .$$

A sufficient condition for this is that the coefficients of all monomials m with $\deg_{x_2}(m) + \deg_{x_3}(m) \leq 1$ are divisible by p (for $p > 3$ this is equivalent). These are the monomials listed in the table above.

It remains to look at the extra conditions given by the p^2 in the second line of the table. This means $p^2 \mid f(x_0, x_1, 0, 0)$. Which is the last statement given above. Note that for singular lines this condition is independent of the lift we choose.

Now we treat the weight system $(0, 1, 1, 1)$. This leads to

$$f(x_0, px_1, px_2, px_3) = f(1, 0, 0, 0)x_0^3 + px_0^2 l(x_1, x_2, x_3) + \\ p^2 x_0 q(x_1, x_2, x_3) + O(p^3)$$

with a linear form l and a quadratic form q. Using $p^3 | f(x_0, px_1, px_2, px_3)$ we get $p^3 | f(1, 0, 0, 0)$, $p^2 | l$, and $p | q$. This shows the claim. □

Proposition 13. *Let $f = 0$ be a model of a cubic surface. Assume that it can be improved with the weight system $(0, 1, 2, 2)$ or $(0, 2, 2, 3)$ with respect to the standard apartment. Then $[1 : 0 : 0 : 0]$ reduces to a singular point. Further $f(1, 0, 0, 0) \equiv 0$ holds at least modulo p^4.*

Proof. We can use the conditions $p^4 \mid f(x_0, px_1, px_2, p^2x_3)$ or $p^6 \mid f(x_0, p^2x_1, p^2x_2, p^3x_3)$. They imply the claim immediately. □

Remark 14. A deeper analysis of the singularities of the reduction modulo p shows the following.

In the $(0, 1, 2, 2)$-case the quadratic form of the local expansion in the singular point has rank at most 2. If it has rank 2 then this quadric is the union of two planes. The common line of the two planes is contained in the cubic surface. The singularity is of type A_3 or worse.

In the $(0, 2, 2, 3)$-case the quadratic form of the local expansion in the singular point has rank at most 1. This means the singularity is of type D_4 or worse.

We will not use these facts for our algorithm. But it seams possible to improve the algorithm by using them.

Algorithm 15. *Given a model of a cubic surface by $f = 0$ over $\mathbb{Q}$. This algorithm computes one model of this surface which is optimal at each finite place.*

The description starts at the top level. The subroutines follow afterwards.

i) *Check that $f = 0$ is at least semi-stable. Otherwise terminate the algorithm with an error-message. Output: "Unstable forms can not be treated."*

ii) *Calculate the GCD of the coefficients of f. Divide f by it.*

iii) *Compute all primes p of bad reduction.*

iv) *For each prime p of bad reduction repeat the following until no better model is found. If a better model is found start the computation for the next prime with this model.*

Try each of the five weight systems to improve the model. Use the order $(0, 0, 0, 1)$, $(0, 0, 1, 1)$, $(0, 1, 1, 1)$, $(0, 1, 2, 2)$, $(0, 2, 2, 3)$. If a better model is found then restart immediately with the first weight system and the new model.

v) *Return the last model model found as an optimal one.*

Try the weight system $(0,0,0,1)$

i) *Try to find a linear factor l of f in $(\mathbb{Z}/p\mathbb{Z})[x_0,x_1,x_2,x_3]$.*

ii) *If no factor is found terminate this subroutine.*

iii) *Compute the lattice generated by $p\mathbb{Z}^4$ and arbitrary lifts of three independent kernel vectors of l.*

iv) *Write a basis of this lattice into the columns of a matrix M.*

v) *Set $\tilde{f} := f(Mx)$. Let c be the GCD of the coefficients of $\tilde{f}$.*

vi) *return $\frac{1}{c}\tilde{f}$ as a better model.*

Try the weight system $(0,0,1,1)$

We assume that we are not in the $(0,0,0,1)$-case.

Compute the primary decomposition of the singular locus of the reduction of $f=0$ modulo p. For each line l found in the singular locus do the following.

i) *Choose two points $P_0, P_1 \in \mathbb{Z}^4$ that reduce to two different points on the singular line. Compute the lattice generated by P_0, P_1 and $p\mathbb{Z}^4$.*

ii) *Write a basis of this lattice into the columns of a matrix M.*

iii) *Set $\tilde{f} := f(Mx)$. Let c be the GCD of the coefficients of $\tilde{f}$.*

iv) *If $p^2 \mid c$ then return $\frac{1}{c}\tilde{f}$ as a better model.*

Try the weight systems $(0,1,1,1)$**,** $(0,1,2,2)$ **and** $(0,2,2,3)$

We assume that we are not in the $(0,0,0,1)$-case or the $(0,0,1,1)$-case.

i) *Compute the list L_1 of relevant singular points. (Use the subroutine below.)*

ii) *For each point S in L_1 do the following:*

a) *Compute the lattice generated by S and $p\mathbb{Z}^4$.*

b) *Write a basis of this lattice into the columns of the matrix M.*

c) *Set $\tilde{f} := f(Mx)$. Let c be the GCD of the coefficients of $\tilde{f}$.*

d) *Test $p^3 \mid c$.*

e) *If this divisibility condition is satisfied then return $\frac{1}{c}\tilde{f}$ as a better model.*

f) *Test $p^2 \mid c$.*

g) *If this divisibility condition is satisfied then try to complete for then weight systems $(0,1,2,2)$ or $(0,2,2,3)$ starting with the quotient $\frac{1}{c}\tilde{f}$.*

Search for relevant singular points

We assume that we are not in the $(0,0,0,1)$-case or the $(0,0,1,1)$-case.

i) *Compute the primary decomposition of the singular locus of the reduction of $f=0$ modulo p.*

ii) *Write all isolated points (defined over $\mathbb{Z}/p\mathbb{Z}$) found into a list L_1.*

iii) *For each line l (defined over $\mathbb{Z}/p\mathbb{Z}$) found in the singular locus do the following.*

a) *If $p \leq 3$ then write all rational points of the line into the list L_1.*

b) *If $p > 3$ compute a parameterization of an arbitrary lift of the line $[t : u] \mapsto [g_0(t,u) : g_1(t,u) : g_2(t,u) : g_3(t,u)]$. Solve $\frac{1}{p}f(g_0, g_1, g_2, g_3) \equiv 0 \pmod{p}$. (As we are not in the $(0,0,1,1)$-case this is not the zero equation.) Write $[g_0(t,u) : g_1(t,u) : g_2(t,u) : g_3(t,u)]$ for all solutions $[t : u]$ into the list L_1.*

iv) *For each Galois orbit of lines found compute the intersection of all these lines. If this leads to a point defined over $\mathbb{Z}/p\mathbb{Z}$ add it to the list L_1.*

v) *Return arbitrary representatives in $\mathbb{Z}^4$ of the points in L_1 as a list of relevant singular points.*

Try to complete for $(0,1,2,2)$ **and** $(0,2,2,3)$

Given an intermediate model $f = 0$ of a cubic surface.

i) *Factor the reduction of f modulo p.*

ii) *If f is irreducible then terminate with the error-message "This can not happen".*

iii) *If an irreducible quadratic factor q occurs then do the following. Compute the singular locus of $q = 0$. If exactly one line is found then treat this line as in the $(0,0,1,1)$-case. If this does not lead to a GCD of at least p^2 then no improvement is possible. Terminate the subroutine. Otherwise return the new model.*

iv) *For each linear factors l that occurs do the following:*

a) *Handle l as in the $(0,0,0,1)$ case. Denote the new model by $\tilde{f}$*

b) *If a GCD of at least p^2 occurs then return $\tilde{f}$ this as a new model.*

c) *Factor the reduction of $\tilde{f}$ modulo p. If a linear factor occurs then treat this once more as in the $(0,0,0,1)$-case. Return the resulting model as an improved one.*

v) *If no linear factor of f occurs multiply then terminate the subroutine.*

vi) *Treat the multiple factor as in the $(0,0,0,1)$-case. Call the resulting model $\tilde{f}$.*

vii) *The reduction of $\tilde{f}$ modulo p is irreducible. Search for a singular line in the reduction.*

viii) *If no singular line is found then terminate the subroutine.*

ix) *Treat this singular line as in the $(0,0,1,1)$-case.*

x) *If the GCD that arises during the computation is at least p^2 then return the result as the new model.*

xi) *If the GCD that arises during the computation is only p then denote the new model by g.*

xii) *Factor the reduction of g modulo p.*

xiii) *If a linear factor occurs multiply then treat this factor as in the* $(0,0,0,1)$*-case. If the GCD that arises during the computation is at least* p^2 *then return the new model as an improved one.*

xiv) *Return "no improvement is possible".*

Remark 16. In [H] Hilbert gave a classification of unstable cubic surfaces. This can be used to perform the first step.

Remark 17. Up to now the discussion of the $(0,1,2,2)$-case and the $(0,2,2,3)$-case led to a practical description of the first basis element modulo p. I.e., it is possible to change to the lattice generated by e_0, pe_1, pe_2, pe_3. The new coefficients become divisible by p^2. In order to explain the last subroutine of the algorithm let us inspect this intermediate model f_1. Note that f_1 can always be improved with the weight system $(0,0,0,1)$ by scaling the first basis element. This means we return to the original model f. That is why the reduction of f_1 is always reducible.

We have to analyze the conditions $p^2|f_1(x,y,pz,pw)$ and $p^4|f_1(x,py,pz,p^2w)$ in this situation.

In the first case we find

Monomial	Coefficient is divisible by
x^3, x^2y, xy^2, y^3	p^2
$x^2z, x^2w, xyz, xyw, y^2z, y^2w$	p

As a return to f is possible all monomials without x have coefficients divisible by p.

Consequently the reduction of f_1 has at most the monomials xz^2, xzw, xw^2. This shows that the reduction consists (geometrically) of three planes. If the three linear factors are defined over $\mathbb{Z}/p\mathbb{Z}$ then we have to choose the right linear factor and treat it as in the $(0,0,0,1)$-case. Then we do one more step with the weight system $(0,0,0,1)$. In the case that only one linear factor is defined over $\mathbb{Z}/p\mathbb{Z}$ we have to inspect the irreducible quadratic factor q. Then the scheme $q=0$ has a singular line. We treat it as in the $(0,0,1,1)$-case.

In the second case we find

Monomial	Coefficient is divisible by
x^3	p^4
x^2y, x^2z	p^3
x^2w, xy^2, xyz, xz^2	p^2
$xyw, xzw, y^3, y^2z, yz^2, z^3$	p

As a return to f is possible all monomials without x vanish in the reduction. Summarizing the reduction consists of only one monomial xw^2.

That means the reduction of f_1 has a multiple linear factor. We can treat it as in the $(0,0,0,1)$-case. If a GCD of at least p^2 occurs then we have an improved model. If this is not the case then we have to continue with this new intermediate model f_2.

It remains to do a step with the weight system $(0, 1, 1, 1)$. This leads to the following divisibilities:

Monomial	Coefficient is divisible by
x^3	p^3
x^2y, x^2z, x^2w	p^2
$xy^2, xyz, xyw, xz^2, xzw, xw^2$	p

Note that $f_2 = \frac{1}{p^3} f(x, py, pz, p^2w)$. This ensures the following additional divisibilities:

Monomial	Coefficient is divisible by
w^3	p^3
w^2y, w^2z	p^2
wz^2, wzy, wy^2, w^2x	p

Summarizing the reduction of f_2 has only the monomials y^3, y^2z, yz^2, z^3. If the reduction is reducible over $\mathbb{Z}/p\mathbb{Z}$ then we can treat a linear factor as in the $(0, 0, 0, 1)$-case. That means we do the same as in the $(0, 1, 2, 2)$-case and get a better model. This is a very special situation because we expected the weight system $(0, 2, 2, 3)$ and found that the weight system $(0, 1, 2, 2)$ works.

We have to handle irreducible f_2. We expect the weight system $(0, 1, 1, 1)$. But it is simpler to do one $(0, 1, 1, 0)$-step and one $(0, 0, 0, 1)$-step. This avoids a search for relevant singular points.

The set of possible monomials show that the reduction of $f_2 = 0$ consists (only geometrically) of three planes. They meet in a common line which is the singular locus of the reduction. Treating this line as in the $(0, 0, 1, 1)$ case leads to a model f_3. If a GCD of p^2 occurs in this step then we are done. But this is impossible as it would result in the weight system $(0, 2, 2, 2)$. (This can be replaced by $(0, 1, 1, 1)$.)

A final step for f_3 with the weight system $(0, 0, 0, 1)$ has to be done. It must lead to a GCD of at least p^2, otherwise no improvement is possible.

Remark 18. This approach can be described in the language of Bruhat-Tits buildings. We connect the start and the final lattice with a chain of 1-simplices.

Do not be confused with the notion of galleries and geodesics in Bruhat-Tits buildings. These are different objects.

3. The infinite Place

Let $f = 0$ be a cubic surface. Further assume that the model is locally optimal for every finite place p. It remains to choose a matrix $M \in \mathrm{Gl}_4(\mathbb{Z})$ such that the coefficients of $f(Mx)$ are small.

Naive approach. For a first try one could do the following:

i) Build up a list L of some matrices in $\mathrm{Gl}_4(\mathbb{Z})$. Ensure that these matrices form a generating system.

ii) If $f(Mx)$ is smaller than $f(x)$ for some M in L change to $f(Mx)$.

iii) Repeat the last step until no better equation is found.

The main problem of this approach is the selection of the list L. Experimentally we found that all matrices with at most two non-diagonal entries and all entries in $\{0, \pm 1\}$ suffice in most cases to find a good equation. Further on this is very slow. Next we describe a faster method with is based on a symbolic representation of the surface and the LLL-algorithm.

Proposition 19. *(Sylvester, Clebsch) Let $f = 0$ be a general cubic surface, then there exist five linear forms $l_1, \dots, l_5$ such that $f = l_1^3 + l_2^3 + l_3^3 + l_4^3 + l_5^3$. These linear forms are unique up to order and multiplication by third roots of unity. This is called the symbolic representation of f.*

Remark 20. For some very special cubic surfaces this statement does not hold. E.g. the diagonal cubic surface $x_0^3 + x_1^3 + x_2^3 + x_3^3 = 0$ has infinitely many such representations. For these surfaces the approach will not work.

Definition 21. Let $f = 0$ be a cubic surface. The kernel surface (sometimes called Hessian) is the quartic given by the equation

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

Proposition 22. *(Clebsch) Let $f = l_1^3 + l_2^3 + l_3^3 + l_4^3 + l_5^3$ be a general cubic surface. Choose coefficients $a_1, \dots, a_5$ and linear forms $k_1, \dots, k_5$ such that $k_1 + k_2 + k_3 + k_4 + k_5 = 0$ and $a_i k_i = l_i$. Then the singular points of the kernel surface of f are the points given by $k_{i_1} = 1, k_{i_2} = -1, k_{i_3} = 0, k_{i_4} = 0, k_{i_5} = 0$ for $\{i_1, i_2, i_3, i_4, i_5\} = \{1, 2, 3, 4, 5\}$.*

Remark 23. The symbolic representation of a cubic surface can be computed by inspecting the singular points of the kernel surface.

The main idea of the reduction algorithm is to do LLL-reduction with the linear forms of the symbolic representation.

Algorithm 24. *Let $f = 0$ be a general cubic surface this algorithm computes a reduction of f for the infinite place.*

i) *Set* $q = \det\left(\frac{\partial^2 f}{\partial x_i \partial x_j}\right)_{i,j}$.

ii) *Compute the singular points of* $q = 0$.

iii) *Compute $k_1, \dots, k_5$ by solving the linear system of equations for $k_1, \dots, k_5$ given by the singular points of q.*

iv) *Solve the linear system for the coefficients a_i.*

v) *Set $l_i := \sqrt[3]{a_i} k_i$ for $i = 1, \ldots, 5$.*

vi) *Define the hermitian form*
$h(x) = \|l_1(x)\|^2 + \|l_2(x)\|^2 + \|l_3(x)\|^2 + \|l_4(x)\|^2 + \|l_5(x)\|^2$

vii) *Use the LLL-algorithm to compute a matrix M whose columns are a reduced bases of $\mathbb{Z}^4$ with respect to h.*

viii) *Return $f(M^{-1}x)$ as reduced polynomial.*

Example 25. We start with the irreducible polynomial

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

Its Galois group is of order 72. Doing the explicit Galois descent as described in [EJ] naively leads to a cubic surface S_0 with coefficients having up to 43 digits. On the 27 lines of this surface operates a Galois group of order 144. S_0 has bad reduction at

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

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

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

S has bad reduction at

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

Modulo $p = 3, 5, 7, 13, 22436341$ the singularity is one point of type A_1. Modulo $p = 2$ the surface has one singular point of type A_1 and one of type A_3. Modulo 733 the surface degenerates to a cone over a smooth curve.

References

[B] Brown, K. S.: *Buildings,* Springer, New York 1998

[EJ] Elsenhans, A.-S. and Jahnel, J.: *Cubic surfaces with a Galois invariant double-six,* Preprint

[H] Hilbert, D.: *Über die vollen Invariantensysteme,* Math. Ann. **42** (1893), 313–373

[K] Kollar, J.: *Polynomials with integral coefficients, equivalent to a given polynomial,* Electron. Res. Announc. Amer. Math. Soc. **3** (1997), 17–27

[MFK] Mumford, D.; Fogarty, J.; Kirwan, F.: *Geometric invariant theory,* Springer, Berlin 1994