Experiments with general cubic surfaces

Andreas-Stephan Elsenhans and Jörg Jahnel

Universität Göttingen, Mathematisches Institut*
Bunsenstraße 3–5, D-37073 Göttingen, Germany
elsenhan@uni-math.gwdg.de, jahnel@uni-math.gwdg.de

Dedicated to Yuri Ivanovich Manin on the occasion of his 70th birthday

Summary. For general cubic surfaces, we test numerically the conjecture of Manin (in the refined form due to E. Peyre) about the asymptotics of points of bounded height on Fano varieties. We also study the behaviour of the height of the smallest rational point versus the Tamagawa type number introduced by Peyre.

1 Introduction

The arithmetic of cubic surfaces is a fascinating subject. To a large extent, it was initiated by the work of Yu. I. Manin, particularly by his fundamental and influential book on *Cubic Forms* [Ma].

In this article, we study the distribution of rational points on general cubic surfaces over $\mathbb{Q}$. The main problems are

- Existence of $\mathbb{Q}$-rational points,
- Asymptotics of $\mathbb{Q}$-rational points,
- The height of the smallest point.

Existence of rational points. Let V be an algebraic variety defined over $\mathbb{Q}$. Recall that the *Hasse principle* is said to hold for V if

$$V(\mathbb{Q}) = \emptyset \iff \exists\, \nu \in \mathrm{Val}(\mathbb{Q})\colon V(\mathbb{Q}_\nu) = \emptyset\,.$$

For quadrics in $\mathbf{P}^n_{\mathbb{Q}}$, the Hasse principle holds by the famous Theorem of Hasse-Minkowski. It is, however, well-known that for smooth cubic surfaces over $\mathbb{Q}$ the Hasse principle does not hold, in general. In all known examples, this is explained by the Brauer-Manin obstruction. (See section 2 for details.)

* The computer part of this work was executed on the Sun Fire V20z Servers of the Gauß Laboratory for Scientific Computing at the Göttingen Mathematical Institute. Both authors are grateful to Prof. Y. Tschinkel for the permission to use these machines as well as to the system administrators for their support.

Asymptotics of rational points. On the asymptotics of rational points of bounded height, there is the following famous conjecture due to Yu. I. Manin [FMT].

Conjecture 1 (Manin)**.** *Let V be an arbitrary Fano variety over $\mathbb{Q}$ and H be an anticanonical height on V. Then, there exist a dense, Zariski open subset $V^\circ \subseteq V$ and a constant C such that*

$$(*) \qquad \#\{x \in V^\circ(\mathbb{Q}) \mid \mathrm{H}(x) < B\} \sim CB \log^{\operatorname{rk}\operatorname{Pic}(V)-1} B$$

for $B \to \infty$.

Peyre's constant. Motivated by results obtained by the classical circle method, E. Peyre refined Manin's conjecture by a conjectural value for the leading coefficient C.

Let us explain this more precisely in the particular case that V is a smooth hypersurface in $\mathbf{P}^{d+1}_{\mathbb{Q}}$ defined by a polynomial $f \in \mathbb{Z}[X_0, \ldots, X_{d+1}]$. Assume that $\operatorname{rk}\operatorname{Pic}(V) = 1$ and suppose there is no Brauer-Manin obstruction on V. Then, Peyre's constant is equal to the Tamagawa type number τ given by $\tau := \prod\limits_{p \in \mathbb{P} \cup \{\infty\}} \tau_p$ where

$$\tau_p = \Big(1 - \frac{1}{p}\Big) \cdot \lim_{n \to \infty} \frac{\#\mathscr{V}(\mathbb{Z}/p^n\mathbb{Z})}{p^{dn}}$$

for p finite and

$$\tau_\infty = \frac{1}{2} \int\limits_{\substack{x \in [-1,1]^{d+2} \\ f(x)=0}} \frac{1}{\|(\operatorname{grad} f)(x)\|_2} \, dS \, .$$

Here, $\mathscr{V} \subset \mathbf{P}^{d+1}_{\mathbb{Z}}$ is the integral model of V defined by the polynomial f. dS denotes the usual hypersurface measure on the cone $C_V(\mathbb{R})$, considered as a hypersurface in $\mathbb{R}^{d+2}$.

Note that the constant τ is invariant under scaling. When we multiply f by a prime number p then τ_p gets multiplied by a factor of p. On the other hand, τ_∞ gets multiplied by a factor of $1/p$ and all the other factors remain unchanged.

Known cases. Conjecture 1 is established for smooth complete intersections of multidegree $d_1, \ldots, d_n$ in the case that the dimension of V is very large compared to $d_1, \ldots, d_n$ [Bi]. Further, it is proven for projective spaces and quadrics. Finally, there are a number of further special cases in which Manin's conjecture is known to be true. See, e.g., [Pe, sec. 4].

Recently, numerical evidence for Conjecture 1 has been presented in the case of the threefolds $V^e_{a,b}$ given by $ax^e = by^e + z^e + v^e + w^e$ in $\mathbf{P}^4_{\mathbb{Q}}$ for $e = 3$ and 4 [EJ1].

The smallest point. It would be desirable to have an a-priori upper bound for the height of the smallest $\mathbb{Q}$-rational point on V as this would allow to effectively decide whether $V(\mathbb{Q}) \neq \emptyset$ or not.

When V is a conic, Legendre's theorem on zeroes of ternary quadratic forms yields an effective bound for the smallest point. For quadrics of arbitrary dimension, the same is true by an observation due to J. W. S. Cassels [Ca]. Further, there is a theorem of C. L. Siegel [Sg, Satz 1] which provides a generalization to hypersurfaces defined by norm equations. This certainly includes some special cubic surfaces but, in general, no theoretical upper bound is known for the height of the smallest $\mathbb{Q}$-rational point on a cubic surface.

Remark 2. If one had an error term [S-D] for $(*)$ uniform over all cubic surfaces V of Picard rank 1 then this would imply that the height $\mathrm{m}(V)$ of the smallest $\mathbb{Q}$-rational point is always less than $\frac{C}{\tau(V)^\alpha}$ for certain constants $\alpha > 1$ and $C > 0$.

The investigations on quartic threefolds made in [EJ2] indicate that one might have even $\mathrm{m}(V) < \frac{C(\varepsilon)}{\tau(V)^{1+\varepsilon}}$ for any $\varepsilon > 0$. Assuming equidistribution, one would expect that the height of the smallest $\mathbb{Q}$-rational point on V should be even $\sim\frac{1}{\tau(V)}$. An inequality of the form $\mathrm{m}(V) < \frac{C}{\tau(V)}$ is, however, known to be wrong in a similar situation (cf. [EJ2, Theorem 2.2]).

The results. We consider two families of cubic surfaces which are produced by a random number generator. For each of these surfaces, we do the following.

i) We verify that the Galois group acting on the 27 lines is equal to $W(E_6)$.

ii) We compute E. Peyre's constant $\tau(V)$.

iii) Up to a certain bound for the anticanonical height, we count all $\mathbb{Q}$-rational points on the surface V.

Thereby, we establish the Hasse principle for each of the surfaces considered. Further, we test numerically the conjecture of Manin, in the refined form due to E. Peyre, on the asymptotics of points of bounded height. Finally, we study the behaviour of the height of the smallest $\mathbb{Q}$-rational point versus E. Peyre's constant. This means, we test the estimates formulated in Remark 2.

2 Background

27 lines. Recall that a non-singular cubic surface defined over $\overline{\mathbb{Q}}$ contains exactly 27 lines. The symmetries of the configuration of the 27 lines respecting the intersection pairing are given by the Weyl group $W(E_6)$ [Ma, Theorem 23.9.ii].

Fact 3. *Let V be a smooth cubic surface defined over $\mathbb{Q}$ and let K be the field of definition of the* 27 *lines on V. Then K is a Galois extension of $\mathbb{Q}$. The Galois group* $\mathrm{Gal}(K/\mathbb{Q})$ *is a subgroup of $W(E_6)$.*

Remark 4. $W(E_6)$ contains a subgroup U of index two which is isomorphic to the simple group of order 25 920. It is of Lie type $B_2(\mathbb{F}_3)$, i.e. $U \cong \Omega_5(\mathbb{F}_3) \subset \mathrm{SO}_5(\mathbb{F}_3)$.

Remark 5. The operation of $W(E_6)$ on the 27 lines gives rise to a transitive permutation representation $\iota\colon W(E_6) \to S_{27}$. It turns out that the image of ι is contained in the alternating group A_{27}. We will call an element $\sigma \in W(E_6)$ *even* if $\sigma \in U$ and *odd,* otherwise. This should not be confused with the sign of $\iota(\sigma) \in S_{27}$ which is always even.

The Brauer-Manin obstruction. For Fano varieties, all known obstructions against the Hasse principle are explained by the following observation.

Observation 6 (Manin)**.** *Let V be a non-singular variety over $\mathbb{Q}$. Choose an element $\alpha \in \mathrm{Br}(V)$ [Ma, Definition 41.3]. Then, any $\mathbb{Q}$-rational point $x \in V(\mathbb{Q})$ gives rise to an adelic point $(x_\nu)_\nu \in V(\mathbf{A}_\mathbb{Q})$ satisfying the condition*

$$\sum_{\nu \in \mathrm{Val}(\mathbb{Q})} \mathrm{inv}(\alpha|_{x_\nu}) = 0\,.$$

Here, $\mathrm{inv}\colon \mathrm{Br}(\mathbb{Q}_\nu) \to \mathbb{Q}/\mathbb{Z}$ *(respectively* $\mathrm{inv}\colon \mathrm{Br}(\mathbb{R}) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$*) denotes the canonical isomorphism.*

$\mathrm{inv}(\alpha|_{x_\nu})$ depends continuously on $x_\nu \in V(\mathbb{Q}_\nu)$. Further, Yu. I. Manin proved [Ma, Corollary 44.2.5] that, for each non-singular variety V over $\mathbb{Q}$, there exists a finite set $S \subset \mathrm{Val}(\mathbb{Q})$ such that $\mathrm{inv}(\alpha|_{x_\nu}) = 0$ for every $\alpha \in \mathrm{Br}(V)$, $\nu \notin S$, and $x_\nu \in V(\mathbb{Q}_\nu)$. This implies that the Brauer-Manin obstruction, if present, is an obstruction against the principle of weak approximation.

Denote by $\pi\colon V \to \mathrm{Spec}(\mathbb{Q})$ the structural map. It is obvious that altering $\alpha \in \mathrm{Br}(V)$ by some Brauer class $\pi^*\rho$ for $\rho \in \mathrm{Br}(\mathbb{Q})$ does not change the obstruction defined by α. By consequence, it is only the factor group $\mathrm{Br}(V)/\pi^*\mathrm{Br}(\mathbb{Q})$ which is relevant for the Brauer-Manin obstruction. The latter is canonically isomorphic to $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Pic}(V_{\overline{\mathbb{Q}}}))$ [Ma, Lemma 43.1.1]. In particular, if $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Pic}(V_{\overline{\mathbb{Q}}})) = 0$ then there is no Brauer-Manin obstruction on V.

For a smooth cubic surface V, the geometric Picard group $\mathrm{Pic}(V_{\overline{\mathbb{Q}}})$ is generated by the classes of the 27 lines on $V_{\overline{\mathbb{Q}}}$. Its first cohomology group can be described in terms of the Galois action on these lines. Indeed, there is a canonical isomorphism [Ma, Proposition 31.3]

$$(+) \qquad H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Pic}(V_{\overline{\mathbb{Q}}})) \cong \mathrm{Hom}((NF \cap F_0)/NF_0, \mathbb{Q}/\mathbb{Z}).$$

Here, $F \subset \mathrm{Div}(V_{\overline{\mathbb{Q}}})$ is the group generated by the 27 lines, $F_0 \subset F$ denotes the subgroup of principal divisors, and N is the norm map under the operation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/H$, H being the stabilizer of F.

Remark 7. Consider the particular case when the Galois group acts transitively on the 27 lines. Then, (+) shows that $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Pic}(V_{\overline{\mathbb{Q}}})) = 0$. In particular, there is no Brauer-Manin obstruction in this case.

It is expected that the Hasse principle holds for all cubic surfaces such that $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Pic}(V_{\overline{\mathbb{Q}}})) = 0$. (See [CS, Conjecture C].)

3 Computation of the Galois group

Let V be a smooth cubic surface defined over $\mathbb{Q}$ and let K be the field of definition of the 27 lines on V. By Fact 3, $K/\mathbb{Q}$ is a Galois extension and the Galois group $G := \mathrm{Gal}(K/\mathbb{Q})$ is a subgroup of $W(E_6)$. For general cubic surfaces, G is actually equal to $W(E_6)$. To verify this for particular examples, the following lemma is useful.

Lemma 8. *Let $H \subseteq W(E_6)$ be a subgroup which acts transitively on the 27 lines and contains an element of order five. Then, either H is the subgroup $U \subset W(E_6)$ of index two or $H = W(E_6)$.*

Proof. $H \cap U$ still acts transitively on the 27 lines and still contains an element of order five. Thus, we may suppose $H \subseteq U$.

Assume that $H \subsetneq U$. Denote by k the index of H in U. The natural action of U on the set of cosets U/H yields a permutation representation $i\colon U \to S_k$. As U is simple, i is necessarily injective. In particular, since $\#U \nmid 8!$, we see that $k > 8$. Let us consider the stabilizer $H' \subset H$ of one of the lines. As H acts transitively, it follows that $\#H' = \frac{\#H}{27} = \frac{\#U}{27 \cdot k} = \frac{960}{k}$. We distinguish two cases.

First case: $k > 16$. Then, $k \geq 20$ and $\#H' \leq 48$. This implies that the 5-Sylow subgroup is normal in H'. Its conjugate by some $\sigma \in H$ therefore depends only on $\overline{\sigma} \in H/H'$. By consequence, the number n of 5-Sylow subgroups in H is a divisor of $\#H/\#H' = 27$. Sylow's congruence $n \equiv 1 \pmod 5$ yields that $n = 1$.

Let $H_5 \subset H$ be the 5-Sylow subgroup. Then, $\iota(H_5) \subset S_{27}$ is generated by a product of disjoint 5-cycles leaving at least two lines fixed. It is, therefore, not normal in the transitive group $\iota(H)$. This is a contradiction.

Second case: $9 \leq k \leq 16$. We have $k \,|\, 960$. On the other hand, the assumption $5 \,|\, \#H$ implies $5 \nmid k$. This shows, there are only two possibilities, $k = 12$ and $k = 16$. As, in U, there is no subgroup of index eight or less, $H \subset U$ must be a maximal subgroup. In particular, the permutation representation $i\colon U \to S_k$ is primitive.

Primitive permutation representations of degree up to 20 have been classified already in the late 19th century. It is well known that no group of order 25 920 allows a faithful primitive permutation representation of degree 12 or 16 [Sm, Table 1]. □

Remark 9. The subgroups of the simple group U have been completely classified by L. E. Dickson [Di] in 1904. It would not be complicated to deduce the lemma from Dickson's list.

Let the smooth cubic surface V be given by a homogeneous equation $f = 0$ with integral coefficients. We want to compute the Galois group G.

An affine part of a general line ℓ can be described by four coefficients a, b, c, d via the parametrization

$$\ell\colon t \mapsto (1 : t : (a + bt) : (c + dt)).$$

ℓ is contained in S if and only if it intersects S in at least four points. This implies that

$$f(\ell(0)) = f(\ell(\infty)) = f(\ell(1)) = f(\ell(-1)) = 0$$

is a system of equations for a, b, c, d which encodes that ℓ is contained in S.

By a Gröbner base calculation in `SINGULAR`, we compute a univariate polynomial g of minimal degree belonging to the ideal generated by the equations. If g is of degree 27 then the splitting field of g is equal to the field K of definition of the 27 lines on V. We then use van der Waerden's criterion [PZ, Proposition 2.9.35]. More precisely, our algorithm works as follows.

Algorithm 10 (Verifying $G = W(E_6)$)**.** Given the equation $f = 0$ of a smooth cubic surface, this algorithm verifies $G = W(E_6)$.

i) Compute a univariate polynomial $0 \neq g \in \mathbb{Z}[d]$ of minimal degree such that

$$g \in (f(\ell(0)), f(\ell(\infty)), f(\ell(1)), f(\ell(-1))) \subset \mathbb{Q}[a, b, c, d]$$

where $\ell\colon t \mapsto (1 : t : (a + bt) : (c + dt))$.

If g is not of degree 27 then terminate with an error message. In this case, the coordinate system for the lines is not sufficiently general. If we are erroneously given a singular cubic surface then the algorithm will fail at this point.

ii) Factor g modulo all primes below a given limit. Ignore the primes dividing the leading coefficient of g.

iii) If one of the factors is multiple then go to the next prime immediately. Otherwise, check whether the decomposition type corresponds to one of the cases listed below,

$$A := \{(9, 9, 9)\}, \qquad B := \{(1, 1, 5, 5, 5, 5, 5), (2, 5, 5, 5, 10)\},$$
$$C := \{(1, 4, 4, 6, 12), (2, 5, 5, 5, 10), (1, 2, 8, 8, 8)\}.$$

iv) If each of the cases occurred for at least one of the primes then output the message “The Galois group is equal to $W(E_6)$.” and terminate.

Otherwise, output “Can not prove that the Galois group is equal to $W(E_6)$.”

Remark 11. The cases above are functioning as follows.

a) Case B shows that the order of the Galois group is divisible by five.

b) Cases A and B together guarantee that g is irreducible. Therefore, by Lemma 8, A and B prove that G contains the index two subgroup $U \subset W(E_6)$.

c) Case C is a selection of the most frequent odd conjugacy classes in $W(E_6)$.

Remark 12. One could replace cases B and C by their common element $(2, 5, 5, 5, 10)$. This would lead to a simpler but less efficient algorithm.

Remark 13. Actually, a decomposition type as considered in step iii) does not always represent a single conjugacy class in $W(E_6)$. Two elements $\iota(\sigma)$, $\iota(\sigma') \in S_{27}$ might be conjugate in S_{27} via a permutation $\tau \notin \iota(W(E_6))$.

For example, as is easily seen using `GAP`, the decomposition type $(3, 6, 6, 6, 6)$ falls into three conjugacy classes two of which are even and one is odd (cf. Remark 4). However, all the decomposition types searched for in Algorithm 10 do represent single conjugacy classes.

Remark 14. Since we expect $G = W(E_6)$, we can estimate the probability of each case by the Čebotarev density theorem. Case A has a probability of $\frac{1}{9}$. This is the lowest value among the three cases.

Remark 15. As we do not use the factors of $\overline{g}$ explicitly, it is enough to compute their degrees and to check that each of them occurs with multiplicity one. This means, we only have to compute $\gcd(\overline{g}(X), \overline{g}'(X))$ and $\gcd(\overline{g}(X), X^{p^d} - X)$ in $\mathbb{F}_p[X]$ for $d = 1, 2, \ldots, 13$ [Co, Algorithms 3.4.2 and 3.4.3].

4 Computation of Peyre's constant

The Euler product. We want to compute the product over all τ_p. For a finite place p, we have

$$\tau_p = \left(1 - \frac{1}{p}\right) \cdot \lim_{n \to \infty} \frac{V(\mathbb{Z}/p^n\mathbb{Z})}{p^{2n}} \,.$$

If the reduction $V_{\mathbb{F}_p}$ is smooth then the sequence under the limit is constant by virtue of Hensel's Lemma. Otherwise, it becomes stationary after finitely many steps.

We approximate the infinite product over all τ_p by the finite product taken over the primes less than 300. Numerical experiments show that the contributions of larger primes do not lead to a significant change. (Compare the values calculated for the concrete example in Section 6.)

The factor at the infinite place. We want to compute

$$\tau_\infty = \frac{1}{2} \int\limits_R \frac{1}{\|\operatorname{grad} f\|_2} \, dS$$

where the domain of integration is given by

$$R = \{(x, y, z, w) \in [-1, 1]^4 \mid f(x, y, z, w) = 0\} \,.$$

Here, dS denotes the usual hypersurface measure on R, considered as a hypersurface in $\mathbb{R}^4$. Thus, τ_∞ is given by a three-dimensional integral.

Since f is a homogeneous polynomial, we may reduce to an integral over the boundary of R which is a two-dimensional domain. In our particular case, we have $\deg f = 3$. Then, a direct computation leads to

$$\begin{aligned}\tau_\infty = & \int\limits_{R_0} \frac{1}{\|(\frac{\partial f}{\partial y}, \frac{\partial f}{\partial z}, \frac{\partial f}{\partial w})\|_2} \, dA + \int\limits_{R_1} \frac{1}{\|(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial z}, \frac{\partial f}{\partial w})\|_2} \, dA \\ & + \int\limits_{R_2} \frac{1}{\|(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial w})\|_2} \, dA + \int\limits_{R_3} \frac{1}{\|(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z})\|_2} \, dA\end{aligned}$$

where the domains of integration are

$$R_i = \{(x_0, x_1, x_2, x_3) \in [-1,1]^4 \mid x_i = 1 \text{ and } f(x_0, x_1, x_2, x_3) = 0\} .$$

dA denotes the two-dimensional hypersurface measure on R_i, considered as a hypersurface in $\mathbb{R}^3$.

We therefore have to integrate a smooth function over a compact part of a smooth two-dimensional submanifold in $\mathbb{R}^3$. To do this, we approximate the domain of integration by a triangular mesh.

Algorithm 16 (Generating a triangular mesh)**.** Given the equation $f = 0$ of a smooth surface in $\mathbb{R}^3$, this algorithm constructs a triangular mesh approximating the part of the surface which is contained in a given cube.

i) We split the cube into eight smaller cubes and iterate this procedure a predefined number of times, recursively. During recursion, we exclude those cubes which obviously do not intersect the manifold. To do this, we estimate $\|\text{grad}\, f\|_2$ on each cube.

ii) Then, each resulting cube is split into six simplices.

iii) For each edge of each simplex which intersects the manifold, we compute an approximation of the point of intersection. We use them as the vertices of the triangles to be constructed. This leads to a mesh consisting of one or two triangles per simplex.

The next step is to compute the contribution of each triangle $\varDelta_i$ to the integral. For this, we use some adaption of the midpoint rule. We approximate the integrand g by its value $g(C_i)$ at the barycenter C_i of the triangle. Note that this point usually lies outside the surface given by $f = 0$. Algorithm 16 guarantees only that the three vertices of each facet are contained in that surface.

The product $g(C_i)A(\varDelta_i)$ seems to be a reasonable approximation of the contribution of $\varDelta_i$ to the integral. We correct by an additional factor, the cosine of the angle between the normal vector of the triangle and the gradient vector $\text{grad}\, f$ at the barycenter C.

Remark 17. In our application, these correctional factors are close to 1 and seem to converge versus 1 when the number of recursions is growing. This is, however, not a priori clear. H. A. Schwarz's cylindrical surface [Sch] constitutes a famous example of a sequence of triangulations where the triangles become arbitrarily small and the factors are nevertheless necessary for correct integration.

We use the method described above to approximate the value of τ_∞. In Algorithm 16, we work with six recursions.

Remark 18. Our method of numerical integration is a combination of standard algorithms for 2.5-dimensional mesh generation and two dimensional integration which are described in the literature [Hb].

On a triangle, we integrate linear functions correctly. This indicates that the method should converge of second order. The facts that we work with the area of a linearized triangle and that the barycenters C_i are located in a certain distance from the manifold generate errors of the same order.

5 Numerical Data

The computations carried out. A general cubic surface is described by twenty coefficients. With current technology, it is impossible to study all cubic surfaces with coefficients below a given bound. For that reason, we decided to work with coefficient vectors provided by a random number generator. Our first sample consists of 20 000 surfaces with coefficients randomly chosen in the interval $[0 \ldots 50]$. The second sample consists of 20 000 surfaces with randomly chosen coefficients from the interval $[-100 \ldots 100]$.

These limits were, of course, chosen somewhat arbitrarily. There is, at least, some reason not to work with too large limits as this would lead to low values of τ. (The reader might want to compare [EJ2, Theorem 3.3.4] where this is rigorously proven in a different situation.) Low values of τ are undesirable as they require high search bounds in order to satisfactorily test Manin's conjecture.

We verified explicitly that each of the surfaces studied is smooth. For this, we inspected a Gröbner base of the ideal corresponding to the singular locus. The computations were done in `SINGULAR`.

Then, using Algorithm 10, we proved that, for each surface, the full Galois group $W(E_6)$ acts on the 27 lines. The largest prime used was 457. This means that all our examples are general from the Galois point of view. By consequence, their Picard ranks are equal to 1. Further, according to Remark 7, the Brauer-Manin obstruction is not present on any of the surfaces considered.

Almost as a byproduct, we verified that no two of the 40 000 surfaces are isomorphic. Actually, when running part ii) of Algorithm 10, we wrote the decomposition types found into a file. Primes at which the algorithm failed were labeled by a special marker. A program, written in `C`, ran in an iterated loop over all pairs of surfaces and looked for a prime at which the decomposition types differ. The largest prime needed to distinguish two surfaces was 73.

We counted all $\mathbb{Q}$-rational points of height less than 250 on the surfaces of the first sample. It turns out that, on two of these surfaces, there are no $\mathbb{Q}$-rational points occurring as the equation is unsolvable in $\mathbb{Q}_p$ for some small p. In this situation, Manin's conjecture is true, trivially. On each of the remaining surfaces, we found at least one $\mathbb{Q}$-rational point. 228 examples contained less than ten points. On the other hand, 1213 examples contained at least one hundred $\mathbb{Q}$-rational points. The largest number of points found was 335.

For the second sample, the search bound was 500. Again, on two of these surfaces, there are no $\mathbb{Q}$-rational points occurring as the equation is unsolvable in a certain $\mathbb{Q}_p$. There were 202 examples containing between one and nine points. 1857 examples contained at least one hundred $\mathbb{Q}$-rational points. The largest number of points found was 349.

To find the $\mathbb{Q}$-rational points, we used a 2-adic search method which works as follows. Let a cubic surface V be given. Then, in a first step, we determined on V all points defined over $\mathbb{Z}/512\mathbb{Z}$ (respectively $\mathbb{Z}/1024\mathbb{Z}$). Then, for each of the points found we checked which of its lifts to $\mathbf{P}^3(\mathbb{Z})$ actually lie on V. This leads to an $\mathrm{O}(B^3)$-algorithm which may be efficiently implemented in `C`.

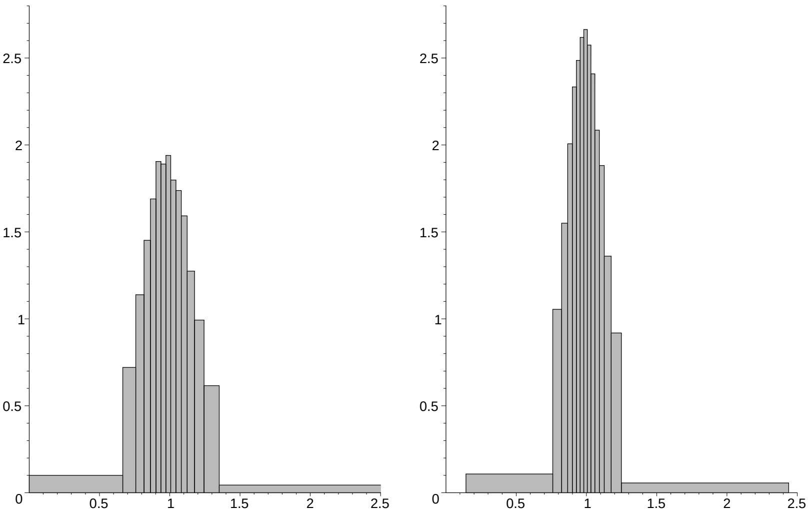
There are algorithms which are asymptotically faster, for example Elkies' method which is $\mathrm{O}(B^2)$ and implemented in `Magma`. A practical comparison shows, however, that Elkies' method is not yet faster for our relatively low search bounds.

Furthermore, using the method described in Section 4, we computed an approximation of Peyre's constant for each surface.

The density results. For each of the surfaces considered we calculated the quotient

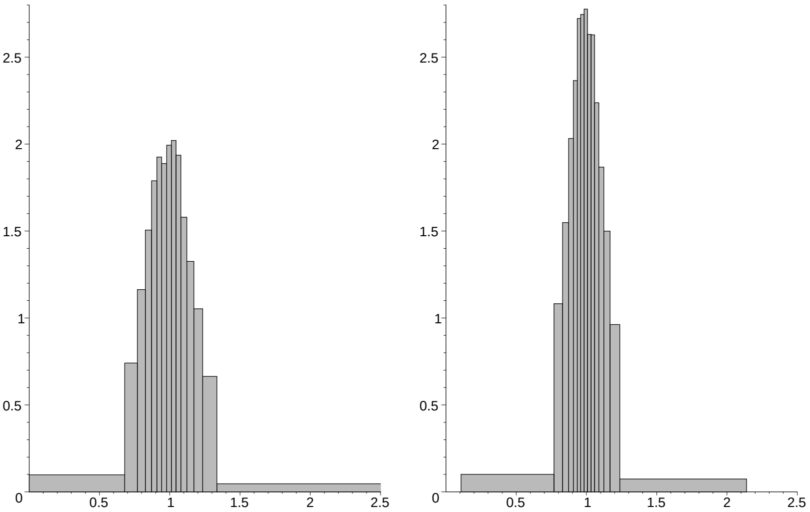
$$\#\{\,\text{points of height} < B \text{ found}\,\}\,/\,\#\{\,\text{points of height} < B \text{ expected}\,\}.$$

Let us visualize the distribution of the quotients by some histograms.



First sample, $B = 125$ First sample, $B = 250$

Fig. 1. Distribution of the quotients for the first sample



Second sample, $B = 250$ Second sample, $B = 500$

Fig. 2. Distribution of the quotients for the second sample

Some statistical parameters are as follows.

Table 1. Parameters of the distribution for the first sample

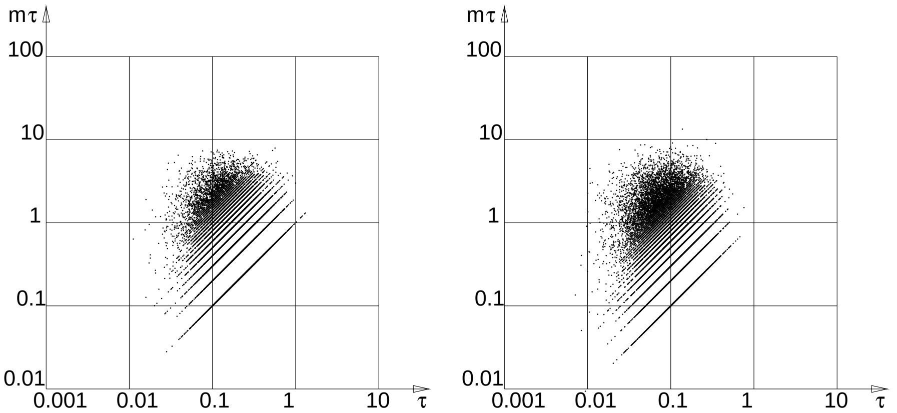
search bound	125	250
mean	0.999 93	0.998 87
standard deviation	0.235 58	0.169 25

Table 2. Parameters of the distribution for the second sample

search bound	250	500
mean	1.000 93	0.999 43
standard deviation	0.225 27	0.161 58

The results for the smallest point. For each of the surfaces in our samples, we determined the height $\mathrm{m}(V)$ of its smallest point. We visualize the behaviour of $\mathrm{m}(V)$ in the diagrams below.

At the first glance, it looks very natural to consider the distribution of the values of $\mathrm{m}(V)$ versus the Tamagawa type number $\tau(V)$. In view of the inequalities asked for in the introduction, it seems, however, to be better to make a slight modification and plot the product $\mathrm{m}(V)\tau(V)$ instead of $\mathrm{m}(V)$ itself.



First sample

Second sample

Fig. 3. The smallest height of a rational point versus the Tamagawa number

Conclusion. Our experiments suggest that, for general cubic surfaces V over $\mathbb{Q}$, the following assertions hold.

i) There are no obstructions against the Hasse principle.

ii) Manin's conjecture is true in the form refined by E. Peyre.

Further, it is apparent from the diagrams in Figure 3 that the experiment agrees with the expectation for the heights of the smallest points formulated in Remark 2, above. Indeed, for both samples, a line tangent to the top of the scatter plot, is nearly horizontal. This indicates that even the strong form of the estimate should be true, i.e. $\mathrm{m}(V) < \frac{C(\varepsilon)}{\tau(V)^{1+\varepsilon}}$ for any $\varepsilon > 0$.

Running Times. The largest portion of the running time was spent on the calculation of the Euler products. It took 20 days of CPU time to calculate all 40 000 Euler products for $p < 300$. For comparison, we estimated all the integrals, using six recursions, within 36 hours. Further, it took eight days to systematically search for all points of height less than 500 on the surfaces of the second sample. Search for points of height less than 250 on the surfaces of the first sample took only one day.

When running Algorithm 10, the lion's share of the time was used for the computation of the univariate degree 27 polynomials. This took approximately seven days of CPU time. In comparison with that, all other parts were negligible. It took only twelve minutes to ensure that all 40 000 surfaces are smooth. The `C` program verifying that no two of the surfaces are isomorphic to each other ran approximately 80 seconds.

6 A concrete example

The Example. Let us conclude the article by some results on the particular cubic surface V given by

$$x^3 + 2xy^2 + 11y^3 + 3xz^2 + 5y^2w + 7zw^2 = 0. \tag{$-$}$$

Example $(-)$ was not among the surfaces produced by the random number generator. Our intention is just to present the output of our algorithms in a specific (and not too artificial) example and, most notably, to show the intermediate results of Algorithm 10.

A Gröbner base calculation in `Magma` shows that V has bad reduction at $p = 2$, 3, 7, 23, and 22 359 013 270 232 677. The idea behind that calculation is the same as described above for the verification of smoothness. The only difference is that we consider Gröbner bases over $\mathbb{Z}$ instead of $\mathbb{Q}$.

The Galois group. The first step of Algorithm 10 works well on V, i.e. the polynomial g is indeed of degree 27. Its coefficients become rather large. The absolutely largest one is that of d^{13}. It is equal to 38 300 982 629 255 010. The leading coefficient of g is $5^3 \cdot 7^{12}$. We find case A at $p = 373$. The common decomposition type $(2, 5, 5, 5, 10)$ of the cases B and C occurs at $p = 19$, 31, 59, 61, 191, 199, and 223.

Consequently, V is an explicit example of a smooth cubic surface over $\mathbb{Q}$ admitting the property that the Galois group which acts on the 27 lines is equal to $W(E_6)$.

Remark 19. The first such examples have been constructed by T. Ekedahl [Ek, Theorem 2.1].

Remark 20. Our example $(-)$ is different from Ekedahl's. Indeed, in Ekedahl's examples, the Frobenius Frob_{11} acts on the 27 lines as an element of the conjugacy class $C_{15} \subset W(E_6)$ (in Sir P. Swinnerton-Dyer's numbering). In our case, however, the first two steps of Algorithm 10 show that Frob_{11} yields the decomposition type $(1,1,1,1,1,2,4,4,4,4,4)$. This corresponds to the class C_{18} [Ma, §31, Table 1]. Note that Ekedahl's examples, as well as ours, have good reduction at $p = 11$.

Computation of Peyre's constant. As an approximation of the Euler product, we get

$$\prod_{p<300} \tau_p \approx 0.729\,750.$$

Using the Lefschetz trace formula, we calculated all partial products of this particular Euler product up to $p < 40\,000$. The oscillations, we observed, remain in a distance of less than two percent. For example, we find

$$\prod_{p<40\,000} \tau_p \approx 0.731\,732.$$

For the factor at the infinite place, we get, using six recursions,

$$\tau_\infty \approx 1.786\,726.$$

We list several approximate values in the table below.

Table 3. Approximate values of τ_∞

recursions	3	4	5	6	7	8
approx. of τ_∞	1.780 729	1.785 147	1.786 453	**1.786 726**	1.786 800	1.786 820
Δ		0.004 418	0.001 306	0.000 273	0.000 074	0.000 020

The successive differences decline by a factor close to four from one step to the next. This conforms to the second order convergence expected for our method of numerical integration.

Altogether, E. Peyre's constant is approximately $\tau \approx 1.3074$.

Rational points. There are 345 $\mathbb{Q}$-rational points on V of height less than 250 and 693 $\mathbb{Q}$-rational points of height less than 500. The smallest points are $(0 : 0 : 1 : 0)$ and $(0 : 0 : 0 : 1)$. The smallest non-obvious point is $(1 : 2 : (-3) : (-2))$. A complete list of all $\mathbb{Q}$-rational points on V of height up to 20 looks as follows.

Table 4. Points on V of height ≤ 20

Point	Height
(0 : 0 : 0 : 1)	1
(0 : 0 : 1 : 0)	1
(1 : 2 : -3 : -2)	3
(3 : -2 : -3 : 2)	3
(0 : 7 : -6 : -7)	7
(0 : 4 : -3 : 8)	8
(5 : -5 : 0 : 8)	8
(2 : -8 : 8 : 7)	8
(10 : -5 : 0 : -1)	10
(0 : 5 : 0 : -11)	11
(8 : 6 : -11 : -8)	12
(12 : -6 : -4 : -3)	12
(9 : -12 : 9 : 10)	12
(4 : -6 : -13 : 2)	13
(5 : 5 : 0 : -14)	14
(10 : -14 : 12 : 11)	14
(0 : 7 : -16 : 7)	16
(16 : -8 : 3 : -4)	16
(6 : -9 : 16 : 3)	16
(12 : 7 : -6 : 17)	17
(14 : -9 : -2 : 17)	17
(6 : -3 : -18 : 7)	18
(9 : -6 : -1 : 18)	18
(3 : 6 : -19 : -6)	19
(8 : 7 : -4 : 19)	19

The field of definition of the 27 lines. Having done the Gröbner base calculation in Algorithm 10.i), the 27 lines may be computed at high precision. This allows to find the 45 triangles on V, explicitly. We calculated a degree 45 resolvent G of the degree 27 polynomial g the zeroes of which are all the sums $a_{i_1} + a_{i_2} + a_{i_3}$ for $\ell_{i_1}, \ell_{i_2}, \ell_{i_3}$ representing three lines which form a triangle. Here, $\ell_i \colon t \mapsto (1 : t : (a_i + b_i t) : (c_i + d_i t))$ denote parametrizations of the 27 lines. As $G \in \mathbb{Z}[X]$, our floating point calculation is in fact exact.

Proposition 21. *The unique quadratic subfield in the field K of definition of the* 27 *lines on V is* $\mathbb{Q}(\sqrt{-23 \cdot 22\,359\,013\,270\,232\,677})$.

Proof. K is unramified at all places of good reduction of V. This leaves us with only $2^6 - 1 = 63$ possibilities for the quadratic subfield $\mathbb{Q}(\sqrt{d})$. To exclude 62 of them is algorithmically easy.

Indeed, for a good prime p, there is a way to compute $\left(\frac{d}{p}\right)$ without knowledge of d. We factor the degree 45 resolvent G modulo p. If p divides the leading coefficient or there are multiple factors then we get no answer. Otherwise, $\left(\frac{d}{p}\right) = \pm 1$ depending on whether the decomposition type found is even or odd in S_{45}.

It turns out that it is sufficient to do this for $p = 13$, 17, 19, 29, 31, and 53. □

Proposition 22. *The field extension $K/\mathbb{Q}$ is ramified exactly at $p = 2$, 3, 7, 23, and* $22\,359\,013\,270\,232\,677$.

Proof. It remains to verify ramification at $p = 2$, 3, and 7. For that, we computed in `Magma` the p-adic factorization of g. The decomposition types are $(3, 24)$ for $p = 2$ and 3 and $(1, 1, 1, 4, 4, 4, 4, 8)$ for $p = 7$.

Let Z_p be the decomposition field of p. If p were unramified then $\mathrm{Gal}(K/Z_p)$ would be a cyclic group, i.e. $\mathrm{Gal}(K/Z_p) = \langle\sigma\rangle$ for some $\sigma \in W(E_6)$. On the other hand, on the 27 lines, the orbit structure under the operation of $\mathrm{Gal}(K/Z_p)$ is the same as under the operation of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. There is, however, no element in $W(E_6)$ which yields the decomposition type $(3, 24)$ or $(1, 1, 1, 4, 4, 4, 4, 8)$ [Ma, §31, Table 1]. □

Remark 23. This shows that there is no integral model of V which is smooth over $p = 2$, 3, 7, 23, or 22 359 013 270 232 677.

References

[Bi] Birch, B. J.: *Forms in many variables,* Proc. Roy. Soc. Ser. A **265** (1961/1962), 245–263

[Ca] Cassels, J. W. S.: *Bounds for the least solutions of homogeneous quadratic equations,* Proc. Cambridge Philos. Soc. **51** (1955), 262–264

[Co] Cohen, H.: *A course in computational algebraic number theory,* Springer, Berlin, Heidelberg 1993

[CS] Colliot-Thélène, J.-L. and Sansuc, J.-J.: *On the Chow groups of certain rational surfaces: A sequel to a paper of S. Bloch,* Duke Math. J. **48** (1981), 421–447

[Di] Dickson, L. E.: *Determination of all the subgroups of the known simple group of order* 25 920, Trans. Amer. Math. Soc. **5** (1904), 126–166

[Ek] Ekedahl, T.: *An effective version of Hilbert's irreducibility theorem,* in: Séminaire de Théorie des Nombres, Paris 1988–1989, Progr. Math. 91, Birkhäuser, Boston 1990, 241–249

[EJ1] Elsenhans, A.-S. and Jahnel, J.: *The Asymptotics of Points of Bounded Height on Diagonal Cubic and Quartic Threefolds,* in: Algorithmic number theory, Lecture Notes in Computer Science 4076, Springer, Berlin 2006, 317–332

[EJ2] Elsenhans, A.-S. and Jahnel, J.: *On the smallest point on a diagonal quartic threefold,* J. Ramanujan Math. Soc. **22** (2007), 189–204

[FMT] Franke, J., Manin, Y. I., and Tschinkel, Y.: *Rational points of bounded height on Fano varieties,* Invent. Math. **95** (1989), 421–435

[Hb] *Handbook of numerical analysis,* edited by P. G. Ciarlet and J. L. Lions, Vols. II–IV, North-Holland Publishing Co., Amsterdam 1991–1996

[He] Hermann, G.: *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale,* Math. Ann. **95** (1926), 736–788

[Ma] Manin, Yu. I.: *Cubic forms, algebra, geometry, arithmetic,* North-Holland Publishing Co. and American Elsevier Publishing Co., Amsterdam, London, and New York 1974

[Pe] Peyre, E.: *Points de hauteur bornée et géométrie des variétés (d'après Y. Manin et al.),* Séminaire Bourbaki 2000/2001, Astérisque **282** (2002), 323–344

[PZ] Pohst, M. and Zassenhaus, H.: *Algorithmic algebraic number theory,* Cambridge University Press, Cambridge 1989

[Sch] Schwarz, H. A.: *Sur une définition erronée de l'aire d'une surface courbe,* Communication faite à M. Charles Hermite, 1881–82, in: Gesammelte Mathematische Abhandlungen, Zweiter Band, Springer, Berlin 1890, 309–311

[Sg] Siegel, C. L.: *Normen algebraischer Zahlen,* Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl. II **1973** (1973), 197–215

[Sm] Sims, C. C.: *Computational methods in the study of permutation groups,* in: Computational Problems in Abstract Algebra (Proc. Conf., Oxford 1967), Pergamon, Oxford 1970, 169–183

[S-D] Swinnerton-Dyer, Sir P.: *Counting points on cubic surfaces II,* in: Geometric methods in algebra and number theory, Progr. Math. 235, Birkhäuser, Boston 2005, 303–309