

Algebra & Number Theory

Volume 7

2013

No. 6

**Weak approximation for cubic hypersurfaces of
large dimension**

Mike Swarbrick Jones



Weak approximation for cubic hypersurfaces of large dimension

Mike Swarbrick Jones

We address the problem of weak approximation for general cubic hypersurfaces defined over number fields with arbitrary singular locus. In particular, weak approximation is established for the smooth locus of projective, geometrically integral, nonconical cubic hypersurfaces of dimension at least 17. The proof utilises the Hardy–Littlewood circle method and the fibration method.

1. Introduction

Let k be an algebraic number field. The possible existence and structure of k -rational points on hypersurfaces defined over k is a major theme in number theory and arithmetic geometry. Let $X \subset \mathbb{P}_k^{n-1}$ be a variety defined over k . Given a place ν of k , define k_ν to be the completion with respect to that place. If X is smooth, recall that *weak approximation* holds for X if $X(k) \neq \emptyset$ and the image of the diagonal embedding

$$X(k) \rightarrow \prod_{\nu \in S} X(k_\nu)$$

is dense for any finite set of places S . Given a possibly singular X , we shall consider weak approximation for X_{smooth} , the smooth locus of X .

We say that X is k -rational if there is a k -birational map $\mathbb{P}_k^{n-1} \dashrightarrow X$. Weak approximation is a birational invariant of smooth integral varieties, and since weak approximation holds on \mathbb{P}_k^m for any positive integer m , it must hold for any smooth k -rational variety.

A classical observation is that a quadric k -hypersurface Q with a nonsingular k -point will be k -rational, provided it is geometrically integral. Essentially this is because we can parameterise the surface by lines through the k -point. In this case, the smooth locus of the quadric satisfies weak approximation. The Hasse–Minkowski theorem implies that $Q_{\text{smooth}}(k) \neq \emptyset \iff Q_{\text{smooth}}(k_\nu) \neq \emptyset$ for all places ν of k .

MSC2010: primary 11G35; secondary 11D25, 11D72, 11P55, 14G25.

Keywords: cubic hypersurfaces, weak approximation, local-global principles, fibration method, circle method, many variables.

For larger degree hypersurfaces, relatively little is known. The emergence of counterexamples to weak approximation, even when rational points are present, is an indication that the situation is much more complex. For instance, with $k = \mathbb{Q}$ we have a cubic surface from [Swinnerton-Dyer 1962],

$$x_1(x_2^2 + x_3^2) = (4x_4 - 7x_1)(x_4^2 - 2x_1^2). \quad (1-1)$$

Ignoring the subvariety $x_1 = x_4 = 0$, this has two components over the reals: one with $x_4/x_1 \geq 7/4$, which contains infinitely many rational points, and the other with $|x_4/x_1| \leq \sqrt{2}$, which contains none. Clearly then this fails weak approximation. This counterexample can be accounted for by the *Brauer–Manin obstruction*. A conjecture of Colliot-Thélène [2003] states that this will be the only such obstruction for rationally connected varieties such as cubic hypersurfaces of dimension at least 2.

Suppose (once and for all) that $Y \subset \mathbb{P}_k^{n-1}$ is a geometrically integral, nonconical cubic hypersurface given by the zero locus of a cubic form $C \in k[x_1, \dots, x_n]$. The Brauer group of Y_{smooth} will be trivial if its dimension is at least 3, and the codimension of the singular locus is at least 4 (see the appendix by Colliot-Thélène in [Browning 2010]). Thus, we expect that these assumptions, together with $Y_{smooth}(k) \neq \emptyset$, imply that weak approximation holds for Y_{smooth} .

We should note at this point that $Y(k) \neq \emptyset$ for $n \geq 16$ by the Corollary in [Pleasants 1975]. Furthermore, $Y(K) \neq \emptyset \implies Y_{smooth}(K) \neq \emptyset$ for any field K , for example, by [Kollár 2002, Theorem 2.3], and so the Hasse principle holds on Y_{smooth} as soon as $n \geq 16$.

Let us now consider a few cases where weak approximation for Y_{smooth} is known. We shall assume that $Y_{smooth}(k_\nu) \neq \emptyset$ for all ν since otherwise the matter is trivial (this is in fact guaranteed if $n \geq 10$; see, for example, [Birch and Lewis 1960]). First a classical remark: if $Y_{sing}(k) \neq \emptyset$, where Y_{sing} is the singular locus, then we can parameterise Y by means of lines through a rational singular point, so Y is k -rational. If Y contains two conjugate singular points and $n \geq 7$, it follows from work of Harari [1995, §5.1; 1994]. If Y contains three conjugate singular points, it is known for $n = 4$ [Coray 1976, Corollary 2; Coray and Tsfasman 1988, Theorem A] and for $n \geq 6$ [Colliot-Thélène and Salberger 1989], but counterexamples exist for $n = 5$ [ibid., Section 8]. If $n \geq 5$ and Y is smooth and contains a k -rational line, then it follows from §5.2.2 of [Harari 1995]. Finally, Corollary 2 of [Skinner 1997] shows that if Y is smooth, $n \geq 17$ is sufficient.

Note that all the results mentioned so far rely fundamentally on the shape of the singular locus of Y , either that it is empty or contains some arithmetic structure. The aim of this paper is to consider general cubic hypersurfaces Y with arbitrary singular locus and to obtain a reasonable lower bound on the dimension required to guarantee that Y_{smooth} satisfies weak approximation. Our main result is the following:

Theorem A. *Let $Y \subset \mathbb{P}_k^{n-1}$ be a geometrically integral, nonconical cubic hypersurface defined over k . If $n \geq 19$, then Y_{smooth} satisfies weak approximation.*

In a qualitative sense, this result is best possible in that the geometrically integral and nonconical assumptions cannot be eliminated. For example, we could consider the union of a line and a quadric having no nonsingular rational points, or we could take a cone over the surface (1-1).

2. Structure of the proof

Theorem A is related to the result of Skinner [1997, Corollary 2], which was obtained using the Hardy–Littlewood circle method. This is advantageous when the dimension of the singular locus is small. The circle method can also be an effective tool when the equations involved have large ‘ h -invariant’. This concept was originally introduced by Davenport and Lewis [1964].

Given a cubic form C , define the h -invariant of C , $h = h_k(C)$, as follows: h is the smallest positive integer such that $C(\mathbf{x})$ is expressible identically as

$$L_1(\mathbf{x})Q_1(\mathbf{x}) + \cdots + L_h(\mathbf{x})Q_h(\mathbf{x}), \quad (2-1)$$

where L_i and Q_i are linear and quadratic forms, respectively, with coefficients in k . Similarly, for the cubic hypersurface Y , we shall define $h_k(Y)$ to mean the h -invariant of the underlying cubic form. Finally, for a cubic polynomial f , we define $h_k(f)$ to be the h -invariant of the homogeneous cubic part of the polynomial. Clearly it is an invariant with respect to nonsingular linear transformations on \mathbf{x} over k . Also note that $h_k(Y) \leq n$ with equality if and only if $Y(k) = \emptyset$. Furthermore, if $n \geq h_k(Y) + r + 1$, there is a k -rational r -plane contained in Y given by $L_i = 0$ in (2-1).

Our strategy is to show weak approximation for two classes of cubics, the union of which contains all of those considered in **Theorem A**. The first class is cubics for which the h -invariant is sufficiently large.

Lemma 1. *Suppose we have a geometrically integral, nonconical cubic hypersurface Y defined over k . If $h_k(Y) \geq 16$, then Y_{smooth} satisfies weak approximation.*

To prove this, we take a cue from the concluding remarks of [Skinner 1997] and note that to find k -rational points that are p -adically close to a p -adic point, it is sufficient to find *integer* points that are in specific classes modulo p^t for some integer t ; this is equivalent to finding integral solutions to a cubic polynomial f , where the cubic part has the same h -invariant as the original cubic form. For large h , this problem is tailor-made for the circle method. Indeed, we will use a mild generalisation of a previous result of Pleasants [1975] that obtains an asymptotic expression for the number of integral solutions to f in an expanding region under the assumption that $h_k(f) \geq 16$.

The second class of cubic hypersurfaces we consider are those for which the dimension is somewhat larger than the h -invariant.

Lemma 2. *Suppose we have a geometrically integral, nonconical cubic hypersurface Y defined over k . If $n \geq h_k(Y) + 4$, then Y_{smooth} satisfies weak approximation.*

This is based on the fibration method (see, for example, [Colliot-Thélène 2003] for a more general description), which reduces the question to proving weak approximation for the fibres of a particular map involving Y . Thanks to the assumptions of the lemma, the fibres in question are quadrics of dimension at least 3. As noted in the introduction, a quadric Q will satisfy weak approximation if $Q_{smooth}(k_\nu) \neq \emptyset$ for each place ν of k . A well known theorem of Hasse [1923] tells us that this holds if the underlying quadratic form has rank at least 5 and $Q_{smooth}(k_\nu) \neq \emptyset$ for each real place ν . We must then find conditions on Y under which we can assume that for a generic fibre Q , this is the case. This is achieved using an elementary argument.

Lemmas 1 and 2 immediately give Theorem A.

3. Proof of Lemma 1

First we introduce some notation. Let k be of degree d over \mathbb{Q} , and let \mathfrak{o} be the ring of integers of k with \mathbb{Z} -basis $\omega_1, \dots, \omega_d$. Let \mathfrak{m} be an integral ideal of \mathfrak{o} with \mathbb{Z} -basis τ_1, \dots, τ_d .

Define $\sigma_1, \dots, \sigma_{d_1}$ to be the distinct real embeddings of k and $\sigma_{d_1+1}, \dots, \sigma_{d_1+2d_2}$ the distinct complex embeddings such that σ_{d_1+i} is conjugate to $\sigma_{d_1+d_2+i}$. Put k_i to be the completion of k with respect to the embedding σ_i for $i = 1, \dots, d_1 + d_2$.

Define V to be the commutative \mathbb{R} -algebra $\bigoplus_{i=1}^{d_1+d_2} k_i \cong k \otimes_{\mathbb{Q}} \mathbb{R}$ that has dimension d . For an element $x \in V$, we write $\pi_i(x)$ for its projection onto the i -th summand (so $x = \bigoplus \pi_i(x)$). There is a canonical embedding of k into V given by $\alpha \rightarrow \bigoplus \sigma_i(\alpha)$, and we identify k with its image in V . Under this image, \mathfrak{m} forms a lattice in V , and τ_1, \dots, τ_d form a real basis for V .

We define a distance function $|\cdot|_\tau$ on V as follows:

$$|x|_\tau = |x_1 \tau_1 + \dots + x_d \tau_d|_\tau = \max_i |x_i|.$$

This extends to V^n in the obvious way: if $\mathbf{x} = (x^{(1)}, \dots, x^{(n)}) \in V^n$, then

$$|\mathbf{x}|_\tau = \max_j |x^{(j)}|_\tau.$$

We note that there will be some constant c , dependent only on k and the choice of basis τ_1, \dots, τ_d , such that

$$|\pi_i(x)| \leq c|x|_\tau \tag{3-1}$$

for all $x \in V$ and $1 \leq i \leq d_1 + d_2$ (since each π_i is linear, this is clear).

For any point $\mathbf{b} \in V^n$, let $\mathfrak{B}(\mathbf{b})$ be the box

$$\mathfrak{B}(\mathbf{b}) = \{ \mathbf{x} \in V^n : |\mathbf{x} - \mathbf{b}|_\tau < \rho/2 \}, \quad (3-2)$$

where ρ will always be a real number $0 < \rho < 1$.

For any set $\mathcal{A} \subset V^n$ and positive real number P , we define $P\mathcal{A}$ to be the set $\{ \mathbf{x} \in V^n : P^{-1}\mathbf{x} \in \mathcal{A} \}$. Given a polynomial $\psi(x_1, \dots, x_n)$ defined over k , we shall be interested in the quantity

$$\mathcal{N}_{\psi, \mathcal{A}, \mathfrak{m}}(P) = \#\{ \mathbf{x} \in P\mathcal{A} \cap \mathfrak{m}^n : \psi(\mathbf{x}) = 0 \}$$

and its asymptotic behaviour as $P \rightarrow \infty$.

We can now state the generalisation of the main theorem of [Pleasants 1975] we shall use.

Lemma 3 (Pleasants). *Let \mathfrak{m} be an integral ideal of \mathfrak{o} , and let $f(\mathbf{x})$ be a cubic polynomial over k with homogeneous cubic part $C(\mathbf{x})$ that is not the cube of a linear form. Suppose that $h_k(f) \geq 16$ and that for every integral ideal \mathfrak{a} of \mathfrak{o} , the congruence*

$$f(\mathbf{x}) \equiv 0 \pmod{\mathfrak{a}} \quad (3-3)$$

has nonsingular solutions in \mathfrak{m}^n . Also, let $\xi_0 = \bigoplus_{i=1}^{d_1+d_2} \xi_i$, where each $\xi_i \in \pi_i(V)^n$ is a nonsingular solution to $C(\mathbf{x}) = 0$. Then there exists a set $\mathfrak{X} \subset V^n$ containing ξ_0 and a real constant $c_{f, \mathfrak{X}, \mathfrak{m}} > 0$ such that

$$\mathcal{N}_{f, \mathfrak{X}, \mathfrak{m}}(P) = c_{f, \mathfrak{X}, \mathfrak{m}} P^{(n-3)d} + o(P^{(n-3)d}).$$

Proof. In the case where $\mathfrak{m} = \mathfrak{o}$, this is equivalent to Lemmas 6.1, 7.1, 7.2, and 7.4 of [Pleasants 1975], which were proved using the circle method. However, all the arguments go through unchanged to prove the generalisation. Indeed, if one just changes the words ‘integral points’ to ‘elements of \mathfrak{m} ’ and ‘ $\omega_1, \dots, \omega_d$ ’ to ‘ τ_1, \dots, τ_d ’ in the relevant places, essentially all the arguments work verbatim in the same way. In terms of the circle method, the commutative algebra V does not behave differently whether \mathfrak{m} is the ring of integers or an arbitrary integral ideal, and the nontrivial algebraic number theory results required [Pleasants 1975, Section 4] were not specific to \mathfrak{o} . \square

It is straightforward to show that a suitable ξ_0 exists, for example, the argument following [Pleasants 1975, Lemma 7.2]. Thus, Lemma 3 shows that any such cubic polynomial has infinitely many solutions in \mathfrak{m}^n .

We now prove Lemma 1. Recall Y is the hypersurface associated to a rational cubic form C with $h_k(C) \geq 16$. As noted in the introduction, since Y is not a cone and C has at least ten variables, the congruences (3-3) have nonsingular solutions in \mathfrak{o}^n for all ideals \mathfrak{a} . Then it is clear upon taking $\mathfrak{m} = \mathfrak{o}$ in Lemma 3 that $Y(k) \neq \emptyset$. Furthermore, this implies that $Y_{\text{smooth}}(k) \neq \emptyset$ as in the introduction. Suppose

we are given $\varepsilon > 0$, any finite set of places S , and any set of nonsingular points $\{\mathbf{x}_\nu = (x_\nu^{(1)}, \dots, x_\nu^{(n)}) \in Y_{smooth}(k_\nu) : \nu \in S\}$. To show that weak approximation holds for Y_{smooth} , it suffices to show there exists a point $\mathbf{x} = (x^{(1)}, \dots, x^{(n)}) \in Y_{smooth}(k)$ such that $|x^{(i)} - x_\nu^{(i)}|_\nu < \varepsilon$ for each i and every $\nu \in S$ (where $|\cdot|_\nu$ is the valuation with respect to ν). We follow the line of argument of [Skinner 1997, Section 5].

Let $\varepsilon < 1$, S , and $\{\mathbf{x}_\nu\}_{\nu \in S}$ be given. Write $S = S_\infty \cup S_f$, where S_∞ consists of infinite places and S_f consists of finite places. Without loss of generality, we can assume that S_∞ consists of all the infinite places of k since there are only finitely many of them and $Y_{smooth}(k_\nu) \supset Y_{smooth}(k) \neq \emptyset$ for all ν . We may also assume that $\text{ord}_\nu(x_\nu^{(i)}) \geq 0$ for every i and every $\nu \in S_f$.

We can find $\mathbf{a} = (a^{(1)}, \dots, a^{(n)}) \in \mathfrak{o}^n$ such that $|a^{(i)} - x_\nu^{(i)}|_\nu < \varepsilon/3$ for all i and $\nu \in S_f$ (by the Chinese remainder theorem). Let

$$r_\nu = \min_i \text{ord}_\nu\{a^{(i)} - x_\nu^{(i)}\},$$

and let \mathfrak{p}_ν be the prime ideal corresponding to ν . Put

$$\mathfrak{m} = \prod_{\nu \in S_f} \mathfrak{p}_\nu^{r_\nu}.$$

Consider $f(\mathbf{x}) = C(\mathbf{x} + \mathbf{a})$, a cubic polynomial defined over k . Let t be a positive integer. Choose $D \equiv 1 \pmod{\mathfrak{m}^t}$ to be a positive integer such that

$$D > \frac{2c}{\varepsilon}$$

with c as in (3-1). For each infinite place ν , let

$$\mathbf{r}_\nu = D\mathbf{x}_\nu.$$

Put

$$\boldsymbol{\zeta}_0 = \bigoplus_{i=1}^{d_1+d_2} \mathbf{r}_{\nu_i} \in V^n,$$

where ν_i is the infinite place corresponding to the embedding σ_i . Note that $\boldsymbol{\zeta}_0$ satisfies the conditions of Lemma 3. Take a set \mathfrak{R} as in Lemma 3 centred at $\boldsymbol{\zeta}_0$. In [Pleasants 1975], the region \mathfrak{R} is essentially a box-like shape, and the only extra condition it needs to have is that it is sufficiently small. Therefore, we can take its ‘diameter’ with respect to $|\cdot|_\tau$ to be as small as we like, and we can assume it is contained inside a box of side length $\rho < 1$ as in (3-2).

We consider the congruence conditions (3-3). For any finite place $\nu \notin S_f$, we have $\sigma_\nu = \mathfrak{m}_\nu$, and so any point in $Y_{smooth}(k_\nu)$ will give rise to a nonsingular solution in \mathfrak{m}_ν^n of $f(\mathbf{x}) = 0$. On the other hand, if $\nu \in S_f$, then $\mathbf{x}_\nu - \mathbf{a} \in \mathfrak{m}_\nu^n$ is a nonsingular

solution to $f(\mathbf{x}) = 0$. Thus, the conditions hold for all integral ideals \mathfrak{a} in k by the Chinese remainder theorem.

Finally, we note that the cubic part of f is just C and $h_k(C) \geq 16$. Thus, the conditions for [Lemma 3](#) are met, so for a sufficiently large integer $P \equiv 1 \pmod{\mathfrak{m}^t}$, there exists a point $\mathbf{y} \in \mathfrak{m}^n \cap P\mathfrak{A}$ that is a zero of f , and thus, $\mathbf{z} = \mathbf{y} + \mathfrak{a}$ is a zero of C . Also, since we can have arbitrarily many such points, we can choose one such that $\mathbf{z} \neq \mathbf{0}$. We now fix our point \mathbf{x} to be $\mathbf{z}/(DP)$.

For $\nu \in S_\infty$ we have

$$|DPx_\nu^{(i)} - y^{(i)}|_\nu \leq \rho cP < cP,$$

whence

$$\begin{aligned} |x_\nu^{(i)} - x^{(i)}|_\nu &= \left| x_\nu^{(i)} - \frac{z^{(i)}}{DP} \right|_\nu \\ &\leq \left| x_\nu^{(i)} - \frac{y^{(i)}}{DP} \right|_\nu + \frac{|a^{(i)}|_\nu}{DP} \\ &\leq \frac{c}{D} + \frac{|a^{(i)}|_\nu}{DP} < \varepsilon \end{aligned}$$

for P sufficiently large.

For every $\nu \in S_f$ and when $DP \equiv 1 \pmod{\mathfrak{m}^t}$ for sufficiently large t , we have

$$\begin{aligned} |x_\nu^{(i)} - x^{(i)}|_\nu &= \left| x_\nu^{(i)} - \frac{z^{(i)}}{DP} \right|_\nu \\ &\leq |x_\nu^{(i)} - z^{(i)}|_\nu + \frac{|DP-1|_\nu}{|DP|_\nu} |z^{(i)}|_\nu \\ &\leq |x_\nu^{(i)} - z^{(i)}|_\nu + 2^{-t} \\ &= |(z^{(i)} - a^{(i)}) - (x_\nu^{(i)} - a^{(i)})|_\nu + 2^{-t} \\ &\leq \frac{2}{3}\varepsilon + 2^{-t} < \varepsilon. \end{aligned}$$

Finally, we note that by taking ε sufficiently small, we can make \mathbf{x} be arbitrarily close to a nonsingular point on $Y(k_\nu)$ for each $\nu \in S$. In this way, we may clearly assume that $\mathbf{x} \in Y_{smooth}(k)$. This proves [Lemma 1](#). \square

4. Proof of [Lemma 2](#)

Throughout this section, we shall suppose that $h = h_k(Y)$ and that $n \geq h + 4$. In fact, for simplification, we shall only consider the case $n = h + 4$, other cases being handled similarly. After a change of variables if necessary, we can express the cubic form C in terms of variables $(\mathbf{x}, \mathbf{y}) = (x_1, \dots, x_4, y_1, \dots, y_h)$ as follows:

$$\begin{aligned} Y : C(\mathbf{x}, \mathbf{y}) &= y_1 Q_1(x_1, \dots, x_4, y_1, \dots, y_h) + \dots \\ &\quad + y_h Q_h(x_1, \dots, x_4, y_1, \dots, y_h) = 0, \end{aligned}$$

where the Q_i are quadratic forms defined over k . Clearly $Y(k) \neq \emptyset$ since $h < n$, so $Y_{smooth}(k) \neq \emptyset$ as in the introduction.

Consider the three-dimensional linear space L given by $y_1 = \dots = y_h = 0$. Take the blow-up W of Y along L . Let z_1, \dots, z_h be coordinates for \mathbb{A}_k^h . Then the variety given by the vanishing of C and $y_i z_j - y_j z_i$ for all $i, j \in \{1, \dots, h\}$ is $L \cup W$. Our plan is to prove weak approximation for W_{smooth} , which, by birationality, will prove it for Y_{smooth} .

Let $\pi : W \rightarrow \mathbb{A}_k^h$ be the projection $(\mathbf{x}, \mathbf{y}, \mathbf{z}) \mapsto \mathbf{z}$. The generic fibres of this map are quadrics in \mathbb{P}_k^4 . Abusing our notation slightly, suppose that for $\mathbf{y} \in \mathbb{A}_k^h \setminus \{\mathbf{0}\}$, the fibre of W/\mathbb{A}_k^h at the point \mathbf{y} is given by the quadric

$$X_{\mathbf{y}} : Q_{\mathbf{y}}(\mathbf{x}, t) = 0. \tag{4-1}$$

Then we see that

$$Q_{\mathbf{y}}(\mathbf{x}, t) = C(\mathbf{x}, \mathbf{y}t). \tag{4-2}$$

For an alternative description of the fibres, consider a generic four-dimensional linear space L_4 that contains L . Then this cuts out on Y the union of L and one such quadric Q .

We now quote a simple case of the fibration method, which is given in the paper of Colliot-Thélène, Sansuc, and Swinnerton-Dyer [1987]. To avoid confusion, we say that a *generic fibre* of a fibration Z/X , for varieties X and Z , is one where the image lies in some Zariski dense open subset $X' \subset X$.

Lemma 4. *Let X be a smooth geometrically integral variety such that $X(k) \neq \emptyset$ and X satisfies weak approximation. Let Z/X be a fibration such that the generic fibre is a smooth quadric of dimension at least 3. Then weak approximation holds for any smooth model of Z .*

Proof. This is essentially [Colliot-Thélène et al. 1987, Proposition 3.9] with the caveat that only the generic fibre is smooth. This amounts to trivial changes in the argument that we will not discuss here. □

We may write

$$Y : C(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^h y_i Q_i(\mathbf{x}) + 2 \sum_{j=1}^4 x_j q_j(\mathbf{y}) + c(\mathbf{y}),$$

where Q_i and q_j are quadratic forms and c is a cubic form. Then by (4-2), $Q_{\mathbf{y}}$ takes the form

$$Q_{\mathbf{y}}(\mathbf{x}, t) = \sum_{i=1}^h y_i Q_i(\mathbf{x}) + 2 \sum_{j=1}^4 x_j q_j(\mathbf{y})t + c(\mathbf{y})t^2. \tag{4-3}$$

We rewrite this in terms of a 5×5 matrix $A = A(\mathbf{y})$ defined by

$$Q_{\mathbf{y}}(\mathbf{x}, t) = (\mathbf{x}, t)^T A(\mathbf{x}, t).$$

Also we consider the 4×4 submatrices M_i given by $Q_i(\mathbf{x}) = \mathbf{x}^T M_i \mathbf{x}$.

By (4-3), A must take the shape

$$A(\mathbf{y}) = \left(\begin{array}{ccc|c} & & & q_1(\mathbf{y}) \\ & \sum_i y_i M_i & & \vdots \\ & & & q_4(\mathbf{y}) \\ \hline q_1(\mathbf{y}) & \cdots & q_4(\mathbf{y}) & c(\mathbf{y}) \end{array} \right). \quad (4-4)$$

Now we can reduce [Lemma 2](#) to the following:

Lemma 5. *Suppose Y is as in [Lemma 2](#). For $\mathbf{y} \in \mathbb{A}_k^h$, we define $A(\mathbf{y})$ as in (4-4). Either $A(\mathbf{y})$ is generically of full rank, or $Y_{\text{sing}}(k) \neq \emptyset$.*

If $A(\mathbf{y})$ is generically of full rank at least 5, then $Q_{\mathbf{y}}$ is generically smooth and of dimension at least 3, so we apply [Lemma 4](#) with $Z = W$ and $X = \mathbb{A}_k^h$ to prove weak approximation for W_{smooth} and hence Y_{smooth} . In the alternative, $Y_{\text{sing}}(k) \neq \emptyset$, which is sufficient for weak approximation as noted in the introduction.

We now establish [Lemma 5](#). Note that the equation $\det[A(\mathbf{y})] = 0$ defines an algebraic set, \mathcal{A} say, in \mathbb{A}_k^h , so if $A(\mathbf{y})$ is not generically of full rank, then $\det[A(\mathbf{y})] = 0$ identically in \mathbf{y} .

We examine the leading 4×4 submatrix $M = M(\mathbf{y}) = \sum_i y_i M_i$.

Lemma 6. *Let M_1, \dots, M_h be $m \times m$ symmetric matrices defined over an arbitrary field k with $\text{char}(k) \neq 2$. For $(y_1, \dots, y_h) \in k^h$, put $M(y_1, \dots, y_h) = \sum_i y_i M_i$. Either there exists a vector $v \in \mathbb{A}_k^m$ such that $v^T M_i v = 0$ for each $1 \leq i \leq h$, or the polynomial $\det[M(\mathbf{y})]$ is not identically zero in \mathbf{y} .*

Proof. This is essentially contained in [[Colliot-Thélène et al. 1987](#), Lemma 1.14], which deals with the case $h = 2$, but there are enough changes to warrant giving detail. We proceed by induction. Suppose that $\det[M(\mathbf{y})] = 0$ identically. If $h = 1$, then the lemma follows from the fact that $\det(M_1) = 0$ implies that M_1 has a nonzero null space. Now assume that $h \geq 2$ and that the lemma is true for smaller values of h . If $M_1 = \dots = M_h = 0$, then the lemma is obvious. So we assume that $M_1 \neq 0$. Inserting $\mathbf{y} = (1, 0, \dots, 0)$, we see that $\det(M_1) = 0$. Since $\text{char}(k) \neq 2$, we can choose a basis v_1, \dots, v_m of \mathbb{A}_k^m such that $M_1 = \text{diag}(a_1, \dots, a_r, 0, \dots, 0)$ with each $a_i \neq 0$ for some $0 < r < m$. Let M'_2, \dots, M'_h be the $(m-r) \times (m-r)$ symmetric matrices corresponding to the basis elements v_{r+1}, \dots, v_m . Then for fixed y_2, \dots, y_h , the coefficient of y_1^r in $\det[M(\mathbf{y})]$ is $a_1 \cdots a_r \det[\sum_{i=2}^h y_i M'_i]$. Hence, by assumption this must vanish identically. By the induction hypothesis, this implies that there is a nonzero vector $w = (b_{r+1}, \dots, b_m) \in \mathbb{A}^{m-r}$ such that $w^t M'_i w = 0$ for $2 \leq i \leq h$. Then $v = (0, \dots, 0, b_{r+1}, \dots, b_m)$ satisfies $v^T M_i v = 0$ for $1 \leq i \leq h$. \square

Now we prove [Lemma 5](#). First suppose that $\det[M(\mathbf{y})]$ is identically zero. Then we apply the previous lemma with $m = 4$ to show that there is a nonzero $v \in \mathbb{A}_k^h$ such that $v^T M_i v = 0$ for $1 \leq i \leq h$, i.e., $Q_i(v) = 0$. We can assume after a change of variables that this vector is $(1, 0, 0, 0)$. Now note that this implies there is no x_1^2 term in any of the Q_i . This implies that all terms in $C(\mathbf{x}, \mathbf{y})$ are at most linear in x_1 . But then $Y_{\text{sing}}(k) \neq \emptyset$ since it contains the point $(1, 0, \dots, 0)$, so we are done.

Next, we suppose that $\det[M(\mathbf{y})]$ is not identically zero. In particular, after a change of variables involving only y_1, \dots, y_h , we can assume that it is not zero at $(1, 0, \dots, 0)$, so $\det(M_1) \neq 0$. Now applying another change of variables involving only x_1, \dots, x_4 , we can assume that $M_1 = \text{diag}(a_1, \dots, a_4)$ with $a_j \in k^\times$.

We write

$$q_j(\mathbf{y}) = 2d_j y_1^2 + \dots \quad \text{for } 1 \leq j \leq 4$$

and

$$c(\mathbf{y}) = e y_1^3 + y_1^2 L(y_2, \dots, y_h) + \dots,$$

with L a linear form defined over k .

Assume that $\det[A(\mathbf{y})]$ is identically zero. Now

$$\begin{aligned} C(\mathbf{x}, y_1, 0, \dots, 0) &= y_1 \left(\sum_{j=1}^4 a_j x_j^2 \right) + \sum_{j=1}^4 2d_j x_j y_1^2 + e y_1^3 \\ &= y_1 \sum_{j=1}^4 a_j \left(\sum_{j=1}^4 x_j + \frac{d_j}{a_j} y_1 \right)^2 + e' y_1^3 \end{aligned}$$

for some $e' \in k$. The invertible linear change of variables $x'_j = x_j + (d_j/a_j)y_1$ shows that we can assume that each $d_j = 0$. The coefficient of y_1^7 in $\det[A(\mathbf{y})]$ is $a_1 \cdots a_4 e$, which must be zero; hence, $e = 0$. The coefficient of y_1^6 in $\det[A(\mathbf{y})]$ is $a_1 \cdots a_4 L(y_2, \dots, y_h)$, which is also identically zero in y_2, \dots, y_h ; hence, $L = 0$. Now we see that all terms in C are at most linear in y_1 ; consequently, the point $(\mathbf{x}_0, \mathbf{y}_0) = (0, 0, 0, 0; 1, 0, \dots, 0)$ lies in $Y_{\text{sing}}(k)$, completing the proof of the lemma. □

Acknowledgements

I am indebted to Professor Colliot-Thélène and Professor Leep for numerous remarks on an earlier version of this paper. These ultimately led to a substantially improved version of [Lemma 2](#), and hence [Theorem A](#), as well as streamlining the proof of this lemma. I would also like to thank my supervisor Tim Browning for suggesting the original problem and for his excellent supervision over the course of the project. Finally, I am grateful to Dan Loughran for several useful discussions.

References

- [Birch and Lewis 1960] B. J. Birch and D. J. Lewis, “ p -adic forms”, *J. Indian Math. Soc. (N.S.)* **23** (1960), 11–32. [MR 23 #A859](#) [Zbl 0096.02503](#)
- [Browning 2010] T. D. Browning, “Rational points on cubic hypersurfaces that split off a form”, *Compos. Math.* **146**:4 (2010), 853–885. [MR 2012g:11178](#) [Zbl 1198.14021](#)
- [Colliot-Thélène 2003] J.-L. Colliot-Thélène, “Points rationnels sur les fibrations”, pp. 171–221 in *Higher dimensional varieties and rational points* (Budapest, 2001), edited by K. Böröczky, Jr. et al., Bolyai Soc. Math. Stud. **12**, Springer, Berlin, 2003. In French. [MR 2005a:14027](#) [Zbl 1077.14029](#)
- [Colliot-Thélène and Salberger 1989] J.-L. Colliot-Thélène and P. Salberger, “Arithmetic on some singular cubic hypersurfaces”, *Proc. London Math. Soc. (3)* **58**:3 (1989), 519–549. [MR 90e:11091](#) [Zbl 0638.14011](#)
- [Colliot-Thélène et al. 1987] J.-L. Colliot-Thélène, J.-J. Sansuc, and P. Swinnerton-Dyer, “Intersections of two quadrics and Châtelet surfaces. I”, *J. Reine Angew. Math.* **373** (1987), 37–107. [MR 88m:11045a](#) [Zbl 0622.14029](#)
- [Coray 1976] D. F. Coray, “Arithmetic on singular cubic surfaces”, *Compositio Math.* **33**:1 (1976), 55–67. [MR 55 #5636](#) [Zbl 0337.14028](#)
- [Coray and Tsfasman 1988] D. F. Coray and M. A. Tsfasman, “Arithmetic on singular Del Pezzo surfaces”, *Proc. London Math. Soc. (3)* **57**:1 (1988), 25–87. [MR 89f:11083](#) [Zbl 0653.14018](#)
- [Davenport and Lewis 1964] H. Davenport and D. J. Lewis, “Non-homogeneous cubic equations”, *J. London Math. Soc.* **39** (1964), 657–671. [MR 29 #4731](#) [Zbl 0125.02402](#)
- [Harari 1994] D. Harari, “Méthode des fibrations et obstruction de Manin”, *Duke Math. J.* **75**:1 (1994), 221–260. In French. [MR 95j:11056](#) [Zbl 0847.14001](#)
- [Harari 1995] D. Harari, “Principe de Hasse et approximation faible sur certaines hypersurfaces”, *Ann. Fac. Sci. Toulouse Math. (6)* **4**:4 (1995), 731–762. In French. [MR 99c:11080](#) [Zbl 0870.14014](#)
- [Hasse 1923] H. Hasse, “Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper.”, *J. für Math.* **153** (1923), 113–130. In German. [Zbl 49.0114.01](#)
- [Kollár 2002] J. Kollár, “Unirationality of cubic hypersurfaces”, *J. Inst. Math. Jussieu* **1**:3 (2002), 467–476. [MR 2003m:14082](#) [Zbl 1077.14556](#)
- [Pleasant 1975] P. A. B. Pleasants, “Cubic polynomials over algebraic number fields”, *J. Number Theory* **7**:3 (1975), 310–344. [MR 56 #11895](#) [Zbl 0328.12003](#)
- [Skinner 1997] C. M. Skinner, “Forms over number fields and weak approximation”, *Compositio Math.* **106**:1 (1997), 11–29. [MR 98b:14021](#) [Zbl 0892.11014](#)
- [Swinnerton-Dyer 1962] H. P. F. Swinnerton-Dyer, “Two special cubic surfaces”, *Mathematika* **9** (1962), 54–56. [MR 25 #3413](#) [Zbl 0103.38302](#)

Communicated by Jean-Louis Colliot-Thélène

Received 2011-10-25

Revised 2012-07-24

Accepted 2012-09-07

mampsj@bristol.ac.uk

School of Mathematics, University of Bristol,
University Walk, Bristol BS8 1TW, United Kingdom

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Georgia Benkart	University of Wisconsin, Madison, USA	Susan Montgomery	University of Southern California, USA
Dave Benson	University of Aberdeen, Scotland	Shigefumi Mori	RIMS, Kyoto University, Japan
Richard E. Borcherds	University of California, Berkeley, USA	Raman Parimala	Emory University, USA
John H. Coates	University of Cambridge, UK	Jonathan Pila	University of Oxford, UK
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Victor Reiner	University of Minnesota, USA
Brian D. Conrad	University of Michigan, USA	Karl Rubin	University of California, Irvine, USA
Hélène Esnault	Freie Universität Berlin, Germany	Peter Sarnak	Princeton University, USA
Hubert Flenner	Ruhr-Universität, Germany	Joseph H. Silverman	Brown University, USA
Edward Frenkel	University of California, Berkeley, USA	Michael Singer	North Carolina State University, USA
Andrew Granville	Université de Montréal, Canada	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Joseph Gubeladze	San Francisco State University, USA	J. Toby Stafford	University of Michigan, USA
Ehud Hrushovski	Hebrew University, Israel	Bernd Sturmfels	University of California, Berkeley, USA
Craig Huneke	University of Virginia, USA	Richard Taylor	Harvard University, USA
Mikhail Kapranov	Yale University, USA	Ravi Vakil	Stanford University, USA
Yujiro Kawamata	University of Tokyo, Japan	Michel van den Bergh	Hasselt University, Belgium
János Kollár	Princeton University, USA	Marie-France Vignéras	Université Paris VII, France
Yuri Manin	Northwestern University, USA	Kei-Ichi Watanabe	Nihon University, Japan
Barry Mazur	Harvard University, USA	Efim Zelmanov	University of California, San Diego, USA
Philippe Michel	École Polytechnique Fédérale de Lausanne		

PRODUCTION

production@msp.org

Silvio Levy, Scientific Editor

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2013 is US \$200/year for the electronic version, and \$350/year (+\$40, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW[®] from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**

nonprofit scientific publishing

<http://msp.org/>

© 2013 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 7 No. 6 2013

On the discrete logarithm problem in elliptic curves II	1281
CLAUS DIEM	
Identifying Frobenius elements in Galois groups	1325
TIM DOKCHITSER and VLADIMIR DOKCHITSER	
Weak approximation for cubic hypersurfaces of large dimension	1353
MIKE SWARBRICK JONES	
The Picard crossed module of a braided tensor category	1365
ALEXEI DAVYDOV and DMITRI NIKSHYCH	
A Gross–Zagier formula for quaternion algebras over totally real fields	1405
EYAL Z. GOREN and KRISTIN E. LAUTER	
Counting rational points over number fields on a singular cubic surface	1451
CHRISTOPHER FREI	
On the ample cone of a rational surface with an anticanonical cycle	1481
ROBERT FRIEDMAN	
Commuting involutions of Lie algebras, commuting varieties, and simple Jordan algebras	1505
DMITRI I. PANYUSHEV	