ACTA ARITHMETICA
110.2 (2003)

Pairs of cubic forms in many variables

by

Rainer Dietmann (Stuttgart) and
Trevor D. Wooley (Ann Arbor, MI)

1. Introduction. A celebrated theorem of Birch [1] asserts that a system of homogeneous polynomials, with rational coefficients from a number field K, has a non-trivial rational zero provided only that these polynomials are of odd degree, and the system has sufficiently many variables in terms of the number and degrees of these polynomials. The condition that the degrees be odd can be omitted if one substitutes a $\mathfrak{p}$-adic field for K (see Brauer [4]), and similarly if one instead substitutes a purely imaginary field for K (see Peck [17]). Much effort has been expended on the task of quantifying the condition that there be "sufficiently many variables". Linear algebra applies, of course, when the forms all have degree one. Davenport [6] showed that 16 variables suffice for a single cubic form defined over $\mathbb{Q}$, and the same conclusion was subsequently established in any number field by Pleasants [18]. Meanwhile, Lewis [13] had shown rather earlier that 10 variables suffice to solve a homogeneous cubic equation in any $\mathfrak{p}$-adic field. It seems fair to say that the current state of knowledge for larger systems of odd degree, and for systems involving polynomials of larger degrees, remains highly unsatisfactory. In this note we consider pairs of homogeneous cubic equations, arguably the simplest situation that remains without a satisfactory solution. Our new conclusions go beyond those obtained previously by the second author (see [21, 22]) and, as with this previous work, have relevance also for the existence of rational linear spaces on cubic hypersurfaces.

We require some notation in order to discuss our conclusions. When K is a field, and r and m are non-negative integers, let $\gamma_K(r;m)$ denote the

2000 *Mathematics Subject Classification*: 11D72, 11E76.
Key words and phrases: Diophantine equations, rational points.
Research of the second author supported in part by NSF grant DMS-9970440, by the Department of Mathematics at Harvard University, and by the Max Planck Institute for Mathematics in Bonn. The authors are grateful to the CIRM in Luminy for fostering the discussions that led to the production of this paper.

least integer (if any such integer exists) with the property that whenever $s > \gamma_K(r;m)$, and $f_i(\mathbf{x}) \in K[x_1,\dots,x_s]$ $(1 \le i \le r)$ are cubic forms, then the system of equations $f_i(\mathbf{x}) = 0$ $(1 \le i \le r)$ possesses a solution set which contains a linear subspace of K^s with projective dimension m. If no such integer exists, define $\gamma_K(r;m)$ to be ∞. We abbreviate $\gamma_K(r;0)$ to $\gamma_K(r)$, and $\gamma_K(1;0)$ to γ_K. In §2 we establish the upper bounds recorded in the following two theorems.

THEOREM 1. *Let p be a rational prime, and suppose that F is an algebraic extension of $\mathbb{Q}_p$ (possibly $\mathbb{Q}_p$ itself).*

(a) *Define δ_m for $m \ge 0$ by taking $\delta_0 = 18$, $\delta_2 = 18$, and*

$$\delta_m = \begin{cases} 16 & \text{when } 2 \mid m \text{ and } m \ne 0, 2, \\ 20 & \text{when } 2 \nmid m. \end{cases}$$

Then for each non-negative integer m, one has

$$\gamma_F(1;m) \le \tfrac{1}{2}(5m^2 + 19m + \delta_m).$$

(b) *Define ε_m for $m \ge 0$ by taking*

$$\varepsilon_m = \begin{cases} 18 & \text{when } 3 \mid m, \\ 26 & \text{when } 3 \nmid m. \end{cases}$$

Then whenever the field of residue classes of F has odd cardinality q with $q \ge 5$, one has

$$\gamma_F(1;m) \le \tfrac{1}{2}(5m^2 + 17m + \varepsilon_m).$$

(c) *Define κ_m for $m \ge 0$ by taking $\kappa_0 = 18$, $\kappa_2 = 30$, $\kappa_3 = 28$, $\kappa_6 = 22$, and*

$$\kappa_m = \begin{cases} 16 & \text{when } 3 \mid m \text{ and } m \ne 0, 3, 6, \\ 24 & \text{when } 3 \nmid m \text{ and } m \ne 2. \end{cases}$$

Then whenever the field of residue classes of F has odd cardinality q with $q \ge 11$, one has

$$\gamma_F(1;m) \le \tfrac{1}{2}(5m^2 + 15m + \kappa_m).$$

The bounds recorded in Theorem 1 may be compared with that presented in Theorem 2(a) of Wooley [21], which shows that whenever F is an algebraic extension of $\mathbb{Q}_p$, then

$$\gamma_F(1;m) \le \tfrac{1}{2}(5m^2 + 21m + \zeta_m),$$

where ζ_m is 18 or 22 according to whether m is even or odd. See the end of §2 for a discussion concerning the extent to which the conditions $q \ge 5$ and $q \ge 11$, in Theorems 1(b) and (c), respectively, are justified by available literature.

THEOREM 2. *Let L be an algebraic extension of $\mathbb{Q}$ (possibly $\mathbb{Q}$ itself).*

(a) *Define η_m to be 30 or 34 according to whether m is even or odd. Then for each non-negative integer m, one has*

$$\gamma_L(1;m) \le \tfrac{1}{2}(5m^2 + 33m + \eta_m).$$

(b) *Define θ_m by taking $\theta_0 = 30$, $\theta_2 = 30$, and*

$$\theta_m = \begin{cases} 28 & \text{when } 2 \mid m \text{ and } m \ne 0, 2, \\ 32 & \text{when } 2 \nmid m. \end{cases}$$

Then whenever L is a purely imaginary field extension of $\mathbb{Q}$, one has

$$\gamma_L(1;m) \le \tfrac{1}{2}(5m^2 + 31m + \theta_m).$$

For comparison, Theorem 2(b) of Wooley [21] demonstrates that

$$\gamma_L(1;m) \le \tfrac{1}{2}(5m^2 + 37m + 30).$$

The conclusion of Theorem 2(a) above is superior to the latter bound for $m > 1$. When $m = 1$, these bounds coincide. In particular, any cubic hypersurface defined over $\mathbb{Q}$, of projective dimension at least 35, necessarily contains a rational line.

By combining the conclusions of Theorems 1 and 2 with a consequence of earlier work of the second author (see [22]), one obtains new bounds for the number of variables required to guarantee the existence of a non-trivial zero to a pair of homogeneous cubic equations. In §3 we establish the following conclusions.

THEOREM 3. *Let p be a rational prime, and suppose that F is an algebraic extension of $\mathbb{Q}_p$ (possibly $\mathbb{Q}_p$ itself).*

(a) *For all such fields F, one has $\gamma_F(2) \le 298$.*

(b) *Provided that F is not an extension of $\mathbb{Q}_2$ with degree exceeding 1, and not a completely ramified extension of $\mathbb{Q}_3$, then $\gamma_F(2) \le 288$.*

(c) *Suppose that F is not an extension of $\mathbb{Q}_2$ with degree exceeding 1, not $\mathbb{Q}_7$, not a completely ramified extension of $\mathbb{Q}_3$, $\mathbb{Q}_5$ or $\mathbb{Q}_7$, and not a completely ramified extension of an inert quadratic extension of $\mathbb{Q}_3$. Then $\gamma_F(2) \le 278$.*

(d) *One has*

$$\gamma_{\mathbb{Q}_p}(2) \le \begin{cases} 150 & \text{when } p \equiv 2 \pmod 3, \\ 233 & \text{when } p = 3. \end{cases}$$

Earlier work of Leep and Schmidt [12, equation (3.16p)] had established the bound $\gamma_{\mathbb{Q}_p}(2) \le 320$, this having been improved and generalised in Wooley [21] to obtain $\gamma_F(2) \le 308$ for any field extension F of $\mathbb{Q}_p$. Of course, by combining the conclusions of parts (b) and (d) of Theorem 3, we

now have $\gamma_{\mathbb{Q}_p}(2) \leq 288$ for every prime p. Moreover, in view of Theorem 3(c), one has $\gamma_{\mathbb{Q}_p}(2) \leq 278$, except possibly when $p = 7$.

THEOREM 4. *Let L be any field extension of $\mathbb{Q}$ (possibly $\mathbb{Q}$ itself).*

(a) *For all such fields L, one has $\gamma_L(2) \leq 827$.*

(b) *When L is a purely imaginary field extension of $\mathbb{Q}$, one has $\gamma_L(2) \leq 811$.*

By way of comparison, part (b) of Corollary 1 to Theorem 2 in Wooley [21] establishes the upper bound $\gamma_L(2) \leq 855$ for any field extension L of $\mathbb{Q}$, this in turn representing an improvement on Schmidt's earlier estimate $\gamma_{\mathbb{Q}}(2) \leq 5139$ (see [19]).

With the exception of part (d) of Theorem 3, our proofs of the above conclusions depend for their success on the modification of a beautiful observation of Lewis (see [14]). Suppose that a K-rational cubic hypersurface $\mathcal{C}$ contains a K-rational linear space $\mathcal{L}$ of dimension d, say $\mathcal{L} = \text{span}\{\mathbf{v}_1, \dots, \mathbf{v}_d\}$. Suppose also that one is able to find a vector $\mathbf{w}$, linearly independent of $\{\mathbf{v}_1, \dots, \mathbf{v}_d\}$, and lying in a quadratic extension L of K, with the property that $\mathcal{W} = \text{span}\{\mathbf{v}_1, \dots, \mathbf{v}_d, \mathbf{w}\}$ is contained in $\mathcal{C}$. Under such circumstances, Lewis observes that $\mathcal{C}$ necessarily contains a K-rational linear space of dimension $d + 1$. Thus, given a linear space in $\mathcal{C}$ partially defined in the quadratic extension L, one is able to construct a corresponding linear space defined completely in K. The main innovation of the present paper is to make an inspired choice for the quadratic extension L, so as to save additional variables over the previous explicit version of Lewis's argument as described in Wooley [21].

Since the argument of Lewis underlying the above observation is purely algebraic, and as far as we are aware, no conceptual argument is available in the literature, we now describe a geometric argument that justifies Lewis's observation. We begin by recalling the classical zero-dimensional version. Suppose that a K-rational cubic hypersurface $\mathcal{C}$ contains a point $\mathbf{x}$ defined in a quadratic extension L of K. It is possible that $\mathbf{x}$ is already a K-rational point when considered projectively, in which case $\mathcal{C}$ contains a K-rational point. Otherwise, the conjugate $\mathbf{x}^*$ of $\mathbf{x}$ is an L-rational point of $\mathcal{C}$ distinct from $\mathbf{x}$. The line $\mathcal{L}$ passing through $\mathbf{x}$ and $\mathbf{x}^*$ is fixed under conjugation, and is either contained in $\mathcal{C}$, or else necessarily intersects $\mathcal{C}$ in a third point $\mathbf{y}$, by Bezout's theorem, and moreover $\mathbf{y}$ is fixed under conjugation. In any case, therefore, $\mathcal{C}$ contains a K-rational point. Suppose next that the hypotheses described in the previous paragraph hold. It is possible that, considered projectively, the space $\mathcal{W}$ is already K-rational, in which case $\mathcal{C}$ contains a K-rational linear space of dimension $d + 1$. Otherwise, the linear space $\mathcal{W}$ and its conjugate $\mathcal{W}^* = \text{span}\{\mathbf{v}_1, \dots, \mathbf{v}_d, \mathbf{w}^*\}$ are distinct. The linear space $\mathcal{X} = \text{span}\{\mathbf{v}_1, \dots, \mathbf{v}_d, \mathbf{w}, \mathbf{w}^*\}$ is fixed under conjugation, has dimension $d+2$,

and contains the linear spaces $\mathcal{W}$ and $\mathcal{W}^*$. By intersection theory, therefore (see Theorem 7.7 of Hartshorne [10]), the linear space $\mathcal{X}$ is either contained in $\mathcal{C}$, or else necessarily intersects $\mathcal{C}$ in a third linear space $\mathcal{Y}$ of dimension $d+1$, and moreover $\mathcal{Y}$ is fixed under conjugation. In any case, therefore, the cubic hypersurface $\mathcal{C}$ contains a K-rational linear space of dimension $d+1$.

The authors thank the referee for useful comments.

2. Linear spaces on cubic hypersurfaces. Our proofs of Theorems 1 and 2 rest on a technical lemma devoted to the existence of certain linear spaces on the intersection of quadratic hypersurfaces. In order to describe the latter lemma, we must introduce some notation. When K is a field, and r and m are non-negative integers, let $\beta_K(r;m)$ denote the least integer (if any such integer exists) with the property that whenever $s > \beta_K(r;m)$, and $g_i(\mathbf{x}) \in K[x_1,\dots,x_s]$ $(1 \le i \le r)$ are quadratic forms, then the system of equations $g_i(\mathbf{x}) = 0$ $(1 \le i \le r)$ possesses a solution set that contains a linear subspace of K^s with projective dimension m. If no such integer exists, define $\beta_K(r;m)$ to be ∞. Define similarly the integer $\beta_K^*(r;m)$ by taking

$$\beta_K^*(r;m) = \inf_L \beta_L(r;m),$$

where the infimum is taken over all quadratic extensions L of K. Also, when K is an extension of a p-adic field for some prime p, we define the integer $\beta_K^0(r;m)$ by taking

$$\beta_K^0(r;m) = \inf_M \beta_M(r;m),$$

where the infimum is taken over all (inert) quadratic extensions M of K, wherein $M = K(\sqrt{d})$ for some valuation unit d in K. Finally, we note that although the bulk of our account makes use of the language of projective geometry, it occasionally simplifies our discussion to make use of corresponding affine language. Such expedience should pose no difficulties even for those readers less familiar with geometry.

We begin with an auxiliary lemma that might be considered to be a variant of Proposition 2.2 of Leep [11].

LEMMA 2.1. *Suppose that r and m are positive integers.*

(a) *For any field F, one has*

$$\beta_F^*(r;m) \le \max\{\beta_F(r;0) + (m-1)(r+1), \beta_F(r-1;0) + m(r+1) + r\}.$$

(b) *Suppose that F is a field extension of $\mathbb{Q}_p$, for some prime p. Then*

$$\beta_F^0(r;m) \le \max\{\beta_F(r;0) + (m-1)(r+1), \beta_F(r-1;0) + m(r+1) + 2r\}.$$

Proof. There is no loss of generality in supposing that $\beta_F(r;m)$ is finite. Suppose that

$$s > \beta_F(r;0) + (m-1)(r+1) \tag{2.1}$$

and that with $k = 1$ or 2,

$$s > \beta_F(r-1;0) + m(r+1) + kr. \tag{2.2}$$

Let $g_1, \dots, g_r \in F[x_1, \dots, x_s]$ be quadratic forms. Then in view of Corollary 2.4(ii) of Leep [11], the lower bound (2.1) suffices to ensure that the polynomials $g_i(\mathbf{x})$ $(1 \le i \le r)$ vanish simultaneously on an F-rational linear space of affine dimension m. Let $\mathbf{e}_1, \dots, \mathbf{e}_m$ be a basis for the latter subspace. We may extend this basis to a new basis $\mathbf{e}_1, \dots, \mathbf{e}_s$ for the whole space F^s. Write

$$\mathbf{x} = y_1\mathbf{e}_1 + \dots + y_m\mathbf{e}_m + z_1\mathbf{e}_{m+1} + \dots + z_{s-m}\mathbf{e}_s,$$

and substitute into the system $g_i(\mathbf{x}) = 0$ $(1 \le i \le r)$. We now obtain a system of equations

$$\sum_{i=1}^{m} h_{ij}(\mathbf{z})y_i + q_j(\mathbf{z}) = 0 \quad (1 \le j \le r), \tag{2.3}$$

with $h_{ij}(\mathbf{z}) \in F[\mathbf{z}]$ $(1 \le i \le m,\ 1 \le j \le r)$ linear forms, and with $q_j(\mathbf{z}) \in F[\mathbf{z}]$ $(1 \le j \le r)$ quadratic forms. The aforementioned linear forms vanish simultaneously on an F-rational linear subspace $\mathcal{U}$ of affine dimension $t \ge (s-m) - rm$. Let $\widehat{e}_1, \dots, \widehat{e}_t$ be a basis for $\mathcal{U}$, write $\mathbf{z} = w_1\widehat{e}_1 + \dots + w_t\widehat{e}_t$, and substitute into (2.3). We obtain a new system of equations

$$Q_j(\mathbf{w}) = 0 \quad (1 \le j \le r), \tag{2.4}$$

with $Q_j(\mathbf{w}) \in F[\mathbf{w}]$ $(1 \le j \le r)$ quadratic forms. We seek now to obtain a non-trivial solution of the system (2.4) over some quadratic extension L of F (or, respectively, some inert quadratic extension L of F). Given any such solution, it follows from the above argument that there exists an associated vector $\mathbf{e}_0 \in L^s$, linearly independent of $\mathbf{e}_1, \dots, \mathbf{e}_m$, such that whenever $y_0, \dots, y_m \in L$, the vector $\mathbf{x} = y_0\mathbf{e}_0 + \dots + y_m\mathbf{e}_m$ satisfies the system $g_i(\mathbf{x}) = 0$ $(1 \le i \le r)$. In particular, the latter system possesses a solution set that contains a linear subspace of L^s with projective dimension m. The first conclusion of the lemma therefore follows on checking that a quadratic extension L of F exists for which, with $k = 1$, one has

$$t > \beta_L(r;0), \tag{2.5}$$

and the second conclusion follows on demonstrating that when $k = 2$, then the lower bound (2.5) holds for some inert quadratic extension L of F.

In order to verify that (2.5) holds whenever (2.2) is satisfied in the respective cases, we consider a system (2.4) as above. An application of Corollary 2.4(ii) of Leep [11] establishes that whenever

$$t > \beta_F(r-1;0) + kr, \tag{2.6}$$

as is guaranteed by the lower bound (2.2), then the system of equations $Q_j(\mathbf{w}) = 0$ $(1 \le j \le r-1)$ possesses a solution set that contains a linear

subspace of F^s with affine dimension $k+1$. Let $\widetilde{e}_0, \dots, \widetilde{e}_k$ be a basis for this linear space, write $\mathbf{w} = v_0\widetilde{e}_0 + \dots + v_k\widetilde{e}_k$, and substitute into (2.4). The latter system of equations now simplifies to the shape

$$Q_r(v_0\widetilde{e}_0 + \dots + v_k\widetilde{e}_k) = 0.$$

Here we note that $Q_r(v_0\widetilde{e}_0 + \dots + v_k\widetilde{e}_k)$ is a quadratic form $R(\mathbf{v}) \in F[v_0, \dots \dots, v_k]$, say.

Consider first the situation in which $k = 1$. Here it is possible that R already possesses a non-trivial F-rational solution. If such is not the case, we take L to be the splitting field of the quadratic polynomial $R(T, 1)$, and then observe that $R(v_0, v_1)$ trivially possesses a non-trivial zero over the quadratic extension L of F. In either case, therefore, we find that the lower bound (2.6), with $k = 1$, suffices to establish (2.5) for some quadratic extension L of F. The first conclusion of the lemma now follows immediately, according to our previous discussion.

Suppose next that $k = 2$, and that F is a field extension of $\mathbb{Q}_p$ for some prime p. It is again possible that R already possesses a non-trivial F-rational zero. If not, by diagonalising R, we find that there exist linear forms $l_1, l_2, l_3 \in F[\mathbf{v}]$, and non-zero elements $D, a_1, a_2, a_3 \in F$, such that

$$R(\mathbf{v}) = D(a_1 l_1(\mathbf{v})^2 + a_2 l_2(\mathbf{v})^2 + a_3 l_3(\mathbf{v})^2).$$

Plainly, moreover, we may make a choice for D, $\mathbf{a}$, $\mathbf{l}$ in which two at least of a_1, a_2, a_3 are valuation units. By relabelling variables, therefore, we may suppose that a_1 and a_2 are valuation units. Then on setting $L = F(\sqrt{-a_2/a_1})$, it is apparent that the equation

$$R(\mathbf{v}) = D(a_1(l_1(\mathbf{v})^2 - (\sqrt{-a_2/a_1}\, l_2(\mathbf{v}))^2) + a_3 l_3(\mathbf{v})^2) = 0$$

possesses a non-trivial L-rational solution. Moreover, one has $L = F(\sqrt{d})$ with d a valuation unit of F. Thus we conclude that in either case here, the lower bound (2.6), with $k = 2$, suffices to establish (2.5) for some inert quadratic extension L of F. The second conclusion of the lemma now follows as before, and this completes the proof of the lemma.

The procedure for constructing F-rational linear spaces on cubic hypersurfaces through the use of suitable quadratic extensions of F now follows closely the argument of §2 of Wooley [21], this itself paralleling earlier work of Lewis [14], and indeed we suppress the bulk of the details. We begin with some notation. Let K be a field, and suppose that $f(\mathbf{x}) \in K[x_1, \dots, x_s]$ is a cubic form. Then for suitable coefficients $c_{ijk} \in K$, we can write $f(\mathbf{x})$ in the shape

$$f(\mathbf{x}) = \sum_{1 \le i \le j \le k \le s} c_{ijk} x_i x_j x_k,$$

and define the trilinear form $T(\mathbf{x},\mathbf{y},\mathbf{z})$ associated with f by

$$T(\mathbf{x},\mathbf{y},\mathbf{z}) = \sum_{1\le i\le j\le k\le s} c_{ijk}x_iy_jz_k.$$

We then define the polar forms f_{21}, f_{12} and f_{111} associated with f by

$$f_{21} = T(\mathbf{x},\mathbf{x},\mathbf{y}) + T(\mathbf{x},\mathbf{y},\mathbf{x}) + T(\mathbf{y},\mathbf{x},\mathbf{x}), \quad f_{12}(\mathbf{x},\mathbf{y}) = f_{21}(\mathbf{y},\mathbf{x}),$$
$$f_{111}(\mathbf{x},\mathbf{y},\mathbf{z}) = T(\mathbf{x},\mathbf{y},\mathbf{z}) + T(\mathbf{x},\mathbf{z},\mathbf{y}) + T(\mathbf{y},\mathbf{z},\mathbf{x}) + T(\mathbf{y},\mathbf{x},\mathbf{z}) + T(\mathbf{z},\mathbf{x},\mathbf{y}) + T(\mathbf{z},\mathbf{y},\mathbf{x}).$$

Finally, we define $\gamma_K^* = \sup_L \gamma_L$, where the supremum is taken over all quadratic extensions L of K, and $\gamma_K^0 = \sup_M \gamma_M$, where the supremum is taken over all (inert) quadratic extensions M of K, wherein $M = K(\sqrt{d})$ for some valuation unit d in K.

LEMMA 2.2. *Let m be a positive integer.*

(a) *Whenever F is a field with characteristic not equal to 2,*

$$\gamma_F(1;m) \le \tfrac{1}{2}m(m+3) + \beta_F^*(m;\gamma_F^*).$$

(b) *Suppose that F is a field extension of $\mathbb{Q}_p$, for some prime p. Then*

$$\gamma_F(1;m) \le \tfrac{1}{2}m(m+3) + \beta_F^0(m;\gamma_F^0).$$

We remark that the hypothesis on the characteristic of F in the statement of Lemma 2.2(a) is surely superfluous, and can be deleted by working along the lines of our geometric sketch in §1.

Proof of Lemma 2.2. Suppose that the conclusion of the lemma holds when $m = n-1$, where n is some positive integer. Write $+$ for either $*$ or 0 in our notation involving β_F and γ_F. If γ_F^+ and $\beta_F^+(m;\gamma_F^+)$ are not both finite, then the conclusions of the lemma are vacuous, so we may suppose henceforth that both are finite. We aim to show that whenever s is an integer with

$$s > \tfrac{1}{2}n(n+3) + \beta_F^+(n;\gamma_F^+), \tag{2.7}$$

and $f(\mathbf{x}) \in F[x_1,\dots,x_s]$ is a cubic form, then the equation $f(\mathbf{x}) = 0$ possesses a solution set that contains an F-rational linear space of projective dimension n. The full conclusion of the lemma will then follow by induction.

Suppose that L is a quadratic extension of F, so that the hypotheses of the lemma ensure that $L = F(\sqrt{d})$ for some $d \in F$. If $f(\mathbf{x})$ possesses a non-trivial L-rational zero, then it follows from Lemma 2.1 of Wooley [21] (which is essentially Lemma D of Lewis [14]) that $f(\mathbf{x})$ possesses a non-trivial F-rational zero. Thus it follows that $\gamma_F \le \gamma_F^+$. But when $n = 0$ one has $\beta_F^+(n;\gamma_F^+) = \gamma_F^+$, and so whenever (2.7) holds we have $s > \gamma_F^+ \ge \gamma_F$, whence f has a non-trivial F-rational zero. This establishes the conclusions of the lemma for $m = 0$.

Suppose next that the conclusions of the lemma hold for $m = n-1$, and that s satisfies (2.7). Then there exist linearly independent zeros $\mathbf{v}_1, \dots, \mathbf{v}_n \in F^s$ with the property that for each $t_1, \dots, t_n$, the equation

$$f(t_1\mathbf{v}_1 + \dots + t_n\mathbf{v}_n) = 0$$

holds. We may choose elements $\mathbf{e}_1, \dots, \mathbf{e}_{s-n} \in F^s$ so that the $\mathbf{e}_i$ and $\mathbf{v}_j$ together form a basis for F^s. Write $\mathbf{x} = u_1\mathbf{e}_1 + \dots + u_{s-n}\mathbf{e}_{s-n}$, and substitute into the system

$$f(\mathbf{x}) = f_{12}(\mathbf{v}_i, \mathbf{x}) = f_{21}(\mathbf{v}_i, \mathbf{x}) = f_{111}(\mathbf{v}_i, \mathbf{v}_j, \mathbf{x}) = 0 \quad (1 \le i, j \le n). \tag{2.8}$$

Then we obtain a system of homogeneous equations in $\mathbf{u}$, one cubic, n quadratic and (by symmetry) $\frac{1}{2}n(n+1)$ linear, all with F-rational coefficients. We seek to find a quadratic extension L of F, in part (b) of the lemma subject to the inertness hypothesis, with the property that the system (2.8) possesses a non-trivial L-rational solution. Such a solution is necessarily linearly independent of $\mathbf{v}_1, \dots, \mathbf{v}_n$. Moreover, on recalling that $L = F(\sqrt{d})$ for some $d \in F$, we find that the hypotheses of Lemma 2.2 of Wooley [21] are satisfied. Consequently, we deduce that f possesses an F-rational linear space of zeros of projective dimension n, thereby establishing the conclusions of the lemma for $m = n$. The entire conclusion of the lemma thus follows by induction.

In the linear space spanned by the $\mathbf{e}_i$, the system of $\frac{1}{2}n(n+1)$ linear equations vanish on an F-rational subspace of affine dimension $s-n-\frac{1}{2}n(n+1)$. Let $\mathbf{g}_1, \dots, \mathbf{g}_r$ be a basis for the latter subspace, write $\mathbf{x} = y_1\mathbf{g}_1 + \dots + y_r\mathbf{g}_r$, and substitute into (2.8). We now obtain a system of homogeneous equations, one cubic and n quadratic, with F-rational coefficients, and having r variables. In view of (2.7), moreover, one has $r = s - \frac{1}{2}n(n+3) > \beta_F^+(n; \gamma_F^+)$. Thus there exists a quadratic extension L of F (subject to the inertness hypothesis in part (b) of the lemma) with the property that the aforementioned system of quadratic equations necessarily vanish on an L-rational subspace of projective dimension γ_F^+. Let $\mathbf{h}_0, \dots, \mathbf{h}_{\gamma_F^+}$ be a basis for the latter subspace, write $\mathbf{x} = z_0\mathbf{h}_0 + \dots + z_{\gamma_F^+}\mathbf{h}_{\gamma_F^+}$, and substitute into (2.8). Now the system becomes a single homogeneous cubic equation with L-rational coefficients, and having $\gamma_F^+ + 1 > \gamma_L$ variables. It follows that this cubic equation possesses a non-trivial L-rational solution, whence (2.8) likewise possesses an L-rational solution, linearly independent of $\mathbf{v}_1, \dots, \mathbf{v}_n$. This establishes the conclusions of the lemma when $m = n$, and, as already discussed, the lemma now follows by induction.

The proofs of Theorems 1 and 2 are now easily completed by making use of estimates for γ_F and $\beta_F(r; 0)$ available from the literature. We begin with Theorem 1, and suppose that F is a field extension of $\mathbb{Q}_p$ for some prime p. We note that there is no loss of generality in supposing throughout that F

is a finite extension of $\mathbb{Q}_p$, since the coefficients of any implicit equations necessarily lie in a finite field extension, $\widetilde{F}$, and we may work exclusively in $\widetilde{F}$ in the ensuing discussion. We recall first that Lewis [13] has established that whenever F is a field of the above type, then $\gamma_F = 9$ (see Mordell [16] for a discussion of the lower bound $\gamma_F \geq 9$, and Dem'yanov [8] for the case $p \neq 3$). This conclusion implies, of course, that $\gamma_F^* = 9$ and $\gamma_F^0 = 9$. Also, for the same class of fields F, it follows from work of Dem'yanov [9] that $\beta_F(2;0) = 8$ (see also Birch, Lewis and Murphy [3] for a simple proof of this conclusion). Under the additional hypothesis that the field of residue classes of F has odd cardinality q with $q \geq 11$, work of Schuur [20] (improving on earlier work of Birch and Lewis [2]) shows that $\beta_F(3;0) = 12$. Employing the last two conclusions together with Theorem 1 of Martin [15], we find that whenever F is a field extension of $\mathbb{Q}_p$ for some prime p, then

$$\beta_F(r;0) \leq 2r^2 + \delta_r, \tag{2.9}$$

where δ_r is 0 or 2 according to whether r is even or odd. With the additional hypothesis that the field of residue classes of F has odd cardinality q with $q \geq 11$, we find similarly that

$$\beta_F(r;0) \leq 2r^2 - 2r + \varepsilon_r, \tag{2.10}$$

where ε_r is 0 or 4 according to whether $3 \mid r$ or $3 \nmid r$.

Substituting (2.9) into Lemma 2.1(a), and then inserting the ensuing conclusion into the bound provided by Lemma 2.2(a), we deduce that whenever F is a field extension of $\mathbb{Q}_p$ for some prime p, then for $m \geq 1$,

$$\begin{aligned}\gamma_F(1;m) &\leq \tfrac{1}{2}m(m+3) + (\gamma_F^* - 1)(m+1)\\ &\quad + \max\{\beta_F(m;0), \beta_F(m-1;0) + 2m + 1\}\\ &\leq \tfrac{1}{2}(m^2 + 19m + 16) + \max\{2m^2 + \delta_m, 2m^2 - 2m + 3 + \delta_{m-1}\}.\end{aligned}$$

Following a modicum of computation, one finds that $\gamma_F(1;2) \leq 38$, and that when $m \geq 1$ and $m \neq 2$, one has

$$\gamma_F(1;m) \leq \tfrac{1}{2}(5m^2 + 19m + 16 + 2\delta_m).$$

This completes the proof of part (a) of Theorem 1.

Suppose next that F is a field extension of $\mathbb{Q}_p$ for some prime p, and that the field of residue classes of F has odd cardinality q, with $q > 3$. It follows that any field extension L of F for which $L = F(\sqrt{d})$, for some valuation unit d of F, satisfies the property that its field of residue classes has cardinality at least $pq \geq 25$. Thus the hypotheses required to apply (2.10) (with F replaced by L) hold, and we may conclude from Corollary 2.4 of Leep [11] that there is such a field extension L of F for which

$$\beta_F^0(r;m) \leq \beta_L(r;m) \leq 2r^2 - 2r + \varepsilon_r + m(r+1).$$

We substitute the latter upper bound into the conclusion of Lemma 2.2(b), and thus obtain the estimate

$$\gamma_F(1;m) \le \tfrac{1}{2}m(m+3) + \beta_F^0(m;9) \le \tfrac{1}{2}(5m^2+17m+18+2\varepsilon_m).$$

The conclusion of part (b) of Theorem 1 follows on noting that the only field extensions F of $\mathbb{Q}_p$ excluded by the above hypotheses are those having field of residue classes of cardinality 2^s ($s \ge 1$) or 3.

Finally, suppose that F is a field extension of $\mathbb{Q}_p$ for some prime p, and that the field of residue classes of F has odd cardinality q, with $q \ge 11$. The hypotheses required to apply (2.10) now hold. We substitute the latter inequality into Lemma 2.1(b), and then insert the consequent upper bound into the conclusion of Lemma 2.2(b), thus obtaining the estimate

$$\begin{aligned}\gamma_F(1;m) &\le \tfrac{1}{2}m(m+3) + (\gamma_F^0 - 1)(m+1)\\ &\quad + \max\{\beta_F(m;0), \beta_F(m-1;0) + 3m + 1\}\\ &\le \tfrac{1}{2}(m^2+19m+16)\\ &\quad + \max\{2m^2 - 2m + \varepsilon_m, 2m^2 - 3m + 5 + \varepsilon_{m-1}\}.\end{aligned}$$

A little computation now leads to the conclusion that when $m \ge 1$, one has

$$\gamma_F(1;m) \le \begin{cases} \tfrac{1}{2}(5m^2+13m+26+2\varepsilon_{m-1}) & \text{when } m = 2, 3, 6,\\ \tfrac{1}{2}(5m^2+15m+16+2\varepsilon_m) & \text{otherwise.}\end{cases}$$

The conclusion of part (c) of Theorem 1 follows on noting that the only field extensions F of $\mathbb{Q}_p$ excluded by the above hypotheses are those having field of residue classes of cardinality 2^s ($s \ge 1$), 3, 5, 7 or 9. This completes the proof of Theorem 1.

We now turn to the proof of Theorem 2. Suppose that L is any purely imaginary field extension of $\mathbb{Q}$. Again, there is no loss of generality in supposing throughout that L is a finite extension of $\mathbb{Q}$. Then by Corollary 10.4 of Colliot-Thélène, Sansuc and Swinnerton-Dyer [5], one has $\beta_L(2;0) = 8$. In this instance, Theorem 1 of Martin [15] together with Corollary 2.4 of Leep [11] leads to the upper bound

$$\beta_L(r;m) \le 2r^2 + \delta_r + m(r+1). \tag{2.11}$$

We recall also that, under the same hypotheses on L, one has the upper bound $\gamma_L \le 15$ from Pleasants [18].

First consider an algebraic extension K of $\mathbb{Q}$, and let $f(\mathbf{x}) \in K[\mathbf{x}]$ be a cubic form. Let $\widetilde{K}$ be the finite field extension of $\mathbb{Q}$ containing the coefficients of f. If $\sqrt{-1} \in \widetilde{K}$, then we take d to be any element of $\widetilde{K}$ with $\sqrt{d} \notin \widetilde{K}$. Otherwise we take $d = -1$. Write $L = \widetilde{K}(\sqrt{d})$. Then in either case we have $\sqrt{-1} \in L$, and so L is purely imaginary. Consequently, Theorem 1 of Wooley

[21], in combination with (2.11) and the bound $\gamma_L \le 15$, yields

$$\begin{aligned}\gamma_K(1;m) &\le \tfrac{1}{2}m(m+3) + \beta_L(m;\gamma_L)\\ &\le \tfrac{1}{2}m(m+3) + 2m^2 + \delta_m + 15(m+1).\end{aligned}$$

The conclusion of part (a) of Theorem 2 follows immediately.

Suppose next that L is a purely imaginary field extension of $\mathbb{Q}$. We now apply (2.11) (with $m = 0$) together with Lemma 2.1(a) and Lemma 2.2(a), deducing from the bound $\gamma_L^* \le 15$ that for $m \ge 1$, one has

$$\begin{aligned}\gamma_L(1;m) &\le \tfrac{1}{2}m(m+3) + (\gamma_L^* - 1)(m+1)\\ &\quad + \max\{\beta_L(m;0), \beta_L(m-1;0) + 2m + 1\}\\ &\le \tfrac{1}{2}(m^2 + 31m + 28) + \max\{2m^2 + \delta_m, 2m^2 - 2m + 3 + \delta_{m-1}\}.\end{aligned}$$

A moment of reflection reveals that $\gamma_L(1;2) \le 56$, and that when $m \ge 1$ and $m \ne 2$, one has

$$\gamma_L(1;m) \le \tfrac{1}{2}(5m^2 + 31m + 28 + 2\delta_m).$$

This completes the proof of part (b) of Theorem 2.

A comment is in order concerning our use of Schuur's conclusion that whenever F is a field extension of $\mathbb{Q}_p$, for which the field of residue classes has cardinality $q \ge 11$, then $\beta_F(3;0) = 12$. In point of fact, Schuur [20] only explains that such a conclusion is attainable. The weaker conclusion that $\beta_F(3;0) = 12$ for $q \ge 49$, proved in full between the papers of Birch and Lewis [2] and Schuur [20], suffices to establish the conclusion of Theorem 1(b) with the exception of certain fields F arising as field extensions of $\mathbb{Q}_2$, $\mathbb{Q}_3$ and $\mathbb{Q}_5$. However, as will be evident from §3 below, the primary application of these bounds in the proof of Theorem 3 is unaffected by the exclusion of such fields from Theorem 1(b).

3. Pairs of homogeneous cubic equations. The conclusions of Theorem 3(a)–(c) and Theorem 4 follow immediately from Theorems 1 and 2 on noting that, from the argument of the proof of Lemma 2.2, for example, one has for any field F,

$$\gamma_F(2) \le \gamma_F(1;\gamma_F).$$

Thus, in view of the aforementioned bound of Lewis [13], it follows that whenever F is a field extension of $\mathbb{Q}_p$, then from Theorem 1(a),

$$\gamma_F(2) \le \gamma_F(1;9) \le 298.$$

When, furthermore, the field of residue classes of F has cardinality $q > 3$, then from Theorem 1(b),

$$\gamma_F(2) \le \gamma_F(1;9) \le 288.$$

Subject to the condition that the field of residue classes of F has cardinality $q \geq 11$, we find from Theorem 1(c) that

$$\gamma_F(2) \leq \gamma_F(1;9) \leq 278.$$

On recalling the work of Pleasants [18], on the other hand, it follows that whenever K is a field extension of $\mathbb{Q}$, then from Theorem 2(a),

$$\gamma_K(2) \leq \gamma_K(1;15) \leq 827.$$

When, moreover, the field L is purely imaginary, then from Theorem 2(b) one obtains

$$\gamma_L(2) \leq \gamma_L(1;15) \leq 811.$$

It remains only to establish Theorem 3(d), that is, to estimate $\gamma_{\mathbb{Q}_p}(2)$ when $p = 3$ or $p \equiv 2 \pmod 3$. In these circumstances we make use of the diagonalisation procedures of §3(d) of Wooley [22]. Write $\phi = \phi(\mathbb{Q}_p)$ for the smallest positive integer with the property that whenever $s > \phi(\mathbb{Q}_p)$, then whenever $a_1, \dots, a_s \in \mathbb{Q}_p$, the equation

$$a_1x_1^3 + \dots + a_sx_s^3 = 0 \tag{3.1}$$

possesses a non-trivial p-adic solution. From the argument of the proof of Lemma 3.1 of [22], it follows that $\gamma_{\mathbb{Q}_p}(2)$ is bounded above by the least number t satisfying the property that whenever $s > t - \phi$, then any system of homogeneous equations, one cubic, 2ϕ quadratic, and $\phi(\phi+1)$ linear, with coefficients in $\mathbb{Q}_p$ and having s variables, necessarily possesses a non-trivial p-adic solution. But as in the argument of the proof of Lemma 2.2 above, it is straightforward to show that

$$t \leq \phi(\phi + 2) + \beta_{\mathbb{Q}_p}(2\phi; \gamma_{\mathbb{Q}_p}),$$

whence, by the argument leading to (2.11), together with Lewis's conclusion $\gamma_{\mathbb{Q}_p} = 9$, one finds that

$$\gamma_{\mathbb{Q}_p}(2) \leq \phi(\phi + 2) + 2(2\phi)^2 + (2\phi + 1)\gamma_{\mathbb{Q}_p} = 9\phi^2 + 20\phi + 9. \tag{3.2}$$

When $p \equiv 2 \pmod 3$, one has $\phi = 3$ (see, for example, §3 of [22]), and under such circumstances we conclude that $\gamma_{\mathbb{Q}_p}(2) \leq 150$.

It remains to consider $\gamma_{\mathbb{Q}_3}(2)$, and here we point out an oversight in §3 of [22], where it is stated that $\phi(\mathbb{Q}_3) = 3$. Whenever $\mathbf{x}$ satisfies the congruence

$$x_1^3 + 2x_2^3 + 4x_3^3 + 9x_4^3 \equiv 0 \pmod{27},$$

it is apparent that $\mathbf{x} \equiv \mathbf{0} \pmod 3$, and thus we see that the polynomial $x_1^3 + 2x_2^3 + 4x_3^3 + 9x_4^3$ has only the trivial 3-adic zero $\mathbf{x} = \mathbf{0}$. In particular, it is clear that $\phi(\mathbb{Q}_3) \geq 4$.

Let $a_1, \dots, a_s$ be non-zero elements of $\mathbb{Q}_3$, and consider the diagonal equation (3.1). On applying the normalisation procedure of Davenport and Lewis [7] to this equation, with $s = 5$, we find that (3.1) possesses a non-trivial 3-adic solution if and only if an associated equation

$$b_1 x_1^3 + \dots + b_s x_s^3 = 0 \tag{3.3}$$

possesses a non-trivial solution, and here we may suppose that $b_i \in \mathbb{Z}_3$ $(1 \le i \le s)$, that $3 \nmid b_i$ for $1 \le i \le \lceil s/3 \rceil = 2$, and that $3^2 \nmid b_j$ for $1 \le j \le \lceil 2s/3 \rceil = 4$. Relabel variables so that the power of 3 dividing b_i increases (not necessarily monotonically) as i increases. We may suppose, moreover, that $b_1 = 1$. We aim to show that the congruence

$$b_1 x_1^3 + \dots + b_s x_s^3 \equiv 0 \pmod 9 \tag{3.4}$$

possesses a solution with $3 \nmid b_i x_i$ for some i. From this, a variant of Hensel's lemma guarantees the existence of a 3-adic solution. But on noting that

$$b_i(-x_i)^3 \equiv (9 - b_i) x_i^3 \pmod 9,$$

we see that when the congruence

$$b_1 x_1^3 + b_2 x_2^3 \equiv 0 \pmod 9$$

fails to possess a non-trivial solution, then we may suppose that (b_1, b_2) is either $(1, 2)$ or $(1, 4)$. By multiplying through by 2, moreover, the latter case is subsumed by the former. But if $b_1 = 1$ and $b_2 = 2$, and the congruence

$$x_1^3 + 2x_2^3 + b_3 x_3^3 \equiv 0 \pmod 9$$

fails to possess a solution with $3 \nmid b_i x_i$ for some i with $1 \le i \le 3$, then b_3 cannot be 3 or 6 modulo 9, and hence there is no loss in supposing that $b_3 = 4$. Next, if $(b_1, b_2, b_3) = (1, 2, 4)$, and the congruence

$$x_1^3 + 2x_2^3 + 4x_3^3 + b_4 x_4^3 \equiv 0 \pmod 9$$

fails to possess a solution with $3 \nmid b_i x_i$ for some i with $1 \le i \le 4$, then necessarily $9 \mid b_4$, and this contradicts our earlier observation that without loss, we have $3^2 \nmid b_j$ for $1 \le j \le 4$. Then we are forced to conclude that (3.4) does indeed possess a solution with $3 \nmid b_i x_i$ for some i, whence (3.3) possesses a non-trivial 3-adic solution.

The above discussion shows that $\phi(\mathbb{Q}_3) = 4$, so that in view of (3.2), one finds that $\gamma_{\mathbb{Q}_3}(2) \le 233$. This completes the proof of Theorem 3(d).

In view of the above correction to §3 of [22], it may be worth noting that the conclusion of Lemma 3.1 of [22] should be replaced in the case $p = 3$ by

the upper bound

$$v_{3,r}(\mathbb{Q}_3) \le 8r^4 + \frac{64}{3}\,r^3 + 13r^2 + \frac{11}{3}\,r,$$

where, in the notation of this paper, one has $v_{3,r}(\mathbb{Q}_3) = \gamma_{\mathbb{Q}_3}(r)$.

References

[1] B. J. Birch, *Homogeneous forms of odd degree in a large number of variables*, Mathematika 4 (1957), 102–105.

[2] B. J. Birch and D. J. Lewis, *Systems of three quadratic forms*, Acta Arith. 10 (1965), 423–442.

[3] B. J. Birch, D. J. Lewis and T. G. Murphy, *Simultaneous quadratic forms*, Amer. J. Math. 84 (1962), 110–115.

[4] R. Brauer, *A note on systems of homogeneous algebraic equations*, Bull. Amer. Math. Soc. 51 (1945), 749–755.

[5] J.-L. Colliot-Thélène, J.-J. Sansuc and H. P. F. Swinnerton-Dyer, *Intersections of two quadrics and Châtelet surfaces. II*, J. Reine Angew. Math. 374 (1987), 72–168.

[6] H. Davenport, *Cubic forms in* 16 *variables*, Proc. Roy. Soc. Ser. A 272 (1963), 285–303.

[7] H. Davenport and D. J. Lewis, *Homogeneous additive equations*, ibid. 274 (1963), 443–460.

[8] V. B. Dem'yanov, *On cubic forms in discretely normed fields*, Dokl. Akad. Nauk SSSR 74 (1950), 889–891 (in Russian).

[9] —, *Pairs of quadratic forms over a complete field with discrete norm with a finite field of residue classes*, Izv. Akad. Nauk SSSR Ser. Mat. 20 (1956), 307–324 (in Russian).

[10] R. Hartshorne, *Algebraic Geometry*, Springer, New York, 1977.

[11] D. B. Leep, *Systems of quadratic forms*, J. Reine Angew. Math. 350 (1984), 109–116.

[12] D. B. Leep and W. M. Schmidt, *Systems of homogeneous equations*, Invent. Math. 71 (1983), 539–549.

[13] D. J. Lewis, *Cubic homogeneous polynomials over* $\mathfrak{p}$*-adic number fields*, Ann. of Math. 56 (1952), 473–478.

[14] —, *Cubic forms over algebraic number fields*, Mathematika 4 (1957), 97–101.

[15] G. Martin, *Solubility of systems of quadratic forms*, Bull. London Math. Soc. 29 (1997), 385–388.

[16] L. J. Mordell, *A remark on indeterminate forms in several variables*, J. London Math. Soc. 12 (1937), 127–129.

[17] L. G. Peck, *Diophantine equations in algebraic number fields*, Amer. J. Math. 71 (1949), 387–402.

[18] P. A. B. Pleasants, *Cubic polynomials over algebraic number fields*, J. Number Theory 7 (1975), 310–344.

[19] W. M. Schmidt, *On cubic polynomials IV. Systems of rational equations*, Monatsh. Math. 93 (1982), 329–348.

[20] S. E. Schuur, *On systems of three quadratic forms*, Acta Arith. 36 (1980), 315–322.

[21] T. D. Wooley, *Linear spaces on cubic hypersurfaces, and pairs of homogeneous cubic equations*, Bull. London Math. Soc. 29 (1997), 556–562.
[22] —, *On the local solubility of diophantine systems*, Compositio Math. 111 (1998), 149–165.

Mathematisches Institut A
Universität Stuttgart
Postfach 80 11 40
D-70511 Stuttgart, Germany
E-mail: dietmarr@mathematik.uni-stuttgart.de

Department of Mathematics
University of Michigan
East Hall, 525 East University Avenue
Ann Arbor, MI 48109-1109, U.S.A.
E-mail: wooley@math.lsa.umich.edu

Current address:
Max Planck Institut für Mathematik
Postfach 7280
D-53072 Bonn, Germany

Received on 25.2.2002
and in revised form on 29.7.2002 (4234)