DIOPHANTINE PROBLEMS IN MANY VARIABLES: THE ROLE OF ADDITIVE NUMBER THEORY

Trevor D. Wooley*

Abstract. We provide an account of the current state of knowledge concerning diophantine problems in many variables, paying attention in particular to the fundamental role played by additive number theory in establishing a large part of this body of knowledge. We describe recent explicit versions of the theorems of Brauer and Birch concerning the solubility of systems of forms in many variables, and establish an explicit version of Birch's Theorem in algebraic extensions of $\mathbb{Q}$. Finally, we consider the implications of recent progress on explicit versions of Brauer's Theorem for problems concerning the solubility of systems of forms in solvable extensions, such as Hilbert's resolvant problem.

1. Introduction

The purpose of this paper is to provide an overview of the current state of knowledge concerning diophantine problems in many variables, and in particular to describe the fundamental role played by additive number theory in establishing a great part of this body of knowledge. Diophantine problems in few variables have attracted the enthusiastic attention of number theorists for millenia, and indeed the recent work of Wiles [81] concerning Fermat's Last Theorem has even attracted the attention of the mass media. Exercising considerable literary hyperbole, one might describe the current state of knowledge concerning diophantine problems as resembling the European view of the world towards the end of the 16^{th} Century. Thus, while a scientific renaissance flourished within Europe itself, knowledge concerning much of the globe consisted of little more than wild speculation based on the exotic tales brought back by adventurous explorers. In a similar fashion, the past half century has delivered a remarkable level of understanding of the arithmetic of curves, and this in turn has provided reasonably satisfactory knowledge concerning the solubility of diophantine equations in 2 or 3 variables. In contrast, the solubility of diophantine equations in many variables is a wild frontier with, for the most part, only sketchy knowledge and speculative conjectures. Hopefully, rather than be deterred by the relative lack of knowledge in the latter area, readers will

1991 *Mathematics Subject Classification.* 11D72, 11G25, 11E76, (11E95, 14G20, 20D10).

Key words and phrases. Diophantine problems, local solubility, diophantine equations, forms in many variables, p-adic fields, solvable extensions, Hilbert's resolvant problem.

*Packard Fellow and supported in part by NSF grant DMS-9622773. This paper was completed while the author was enjoying the hospitality of the Department of Mathematics at Princeton University.

be tempted by the ripping yarns recounted herein to themselves become explorers of this vast untamed territory.

Before proceeding further we pause to more carefully describe the type of diophantine problems central to this paper. Usually we will be interested in the solubility of a system of polynomial equations or inequalities over the rational integers $\mathbb{Z}$ or field of rational numbers $\mathbb{Q}$, but sometimes we will consider such problems over more general fields. As intimated above, one may loosely divide such diophantine problems into two types.

(i) Diophantine problems in few variables. Consider a homogeneous polynomial $p(\mathbf{x}) \in \mathbb{Z}[x_1, x_2, x_3]$ of degree d. When d is large, one might expect there to be few, if any, primitive solutions of the equation $p(\mathbf{x}) = 0$ with $\mathbf{x} \in \mathbb{Z}^3 \setminus \{\mathbf{0}\}$, for the values taken by the polynomial $p(\mathbf{x})$ are naively expected to be sparse amongst the set of all integers. The corresponding set of complex zeros of $p(\mathbf{x})$ may be considered geometrically as a projective plane curve $\mathcal{C}$, and so the problem of determining the integral zeros of $p(\mathbf{x})$ is equivalent to finding the rational points of $\mathcal{C}$, a problem of fundamental interest in arithmetic geometry. The general expectation in these problems is that such polynomials should have few primitive integral zeros other than the "obvious" ones. By way of illustration, Wiles [81] has resolved Fermat's notorious conjecture by completing a program of investigation to show that when $n \geq 3$, the equation $x^n + y^n = z^n$ has only the "obvious" integral solutions satisfying $xyz = 0$. In a more general setting, and somewhat earlier, Faltings [29] resolved Mordell's Conjecture by showing that when the curve $\mathcal{C}$ defined above has genus exceeding 1, then $\mathcal{C}$ has at most finitely many rational points, whence the underlying equation has only finitely many primitive integral solutions. In another rather older direction, when $f(x, y) \in \mathbb{Z}[x, y]$ is a homogeneous polynomial of degree $d \geq 2$ and n is a natural number, the investigation of the integral solutions of the Thue equation $f(x, y) = n$ is fundamental to a whole branch of the theory of diophantine approximations (see, for example, Schmidt [66]). We spend no more space here on this class of diophantine problems, but rather direct the reader to browse the literature wherein papers on this topic proliferate in copious quantities.

(ii) Diophantine problems in many variables. Rather than investigate polynomials which are expected to have few if any integral zeros, one may seek instead to show that a given polynomial has many primitive integral zeros. Consider a homogeneous polynomial $F(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_s]$ of degree d. It is a remarkable fact that when d is odd and s is sufficiently large compared to d, there are infinitely many primitive integral zeros of $F(\mathbf{x})$ (see Birch [8]). In consequence, the philosophy underlying investigations concerning the solubility of diophantine equations in many variables takes on an entirely different flavour to the work sketched above. For the purpose of exposition, we characterise two basic problems in this area as follows.

Problem (a). *Existence of solutions.* How large must s be in terms of d so that there exists $\mathbf{x} \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$ such that $F(\mathbf{x}) = 0$?

Problem (b). *Density of solutions.* How small can κ be in terms of s and d so

that for each large real number B, one has

$$\mathrm{card}(\{\mathbf{x} \in [-B,B]^s \cap \mathbb{Z}^s \ : \ F(\mathbf{x}) = 0\}) \gg B^{s-\kappa}. \tag{1.1}$$

Here, as is usual in analytic number theory, we write $f(t) \gg g(t)$ when for some positive constant c one has $|f(t)/g(t)| > c$ for all t under consideration. Also, we write $f(t) \ll g(t)$ when $g(t) \gg f(t)$.

Fortified with a mild dose of optimism, one might expect that as soon as s is sufficiently large in terms of d, the number of zeros counted by the left hand side of (1.1) should be asymptotic to a suitable product of densities of real solutions and p-adic solutions. In most situations, the truth of such an expectation would imply the validity of the lower bound (1.1) with $\kappa = d$.

Although we restrict attention in this paper primarily to the problems (a) and (b) above, we remark that there are natural generalisations of the latter problems to questions involving inequalities, and the methods described herein can be adapted (with substantial modification) to handle such questions. Consider, for example, the following problem.

Problem (c). *Small values of polynomials.* Consider a homogeneous polynomial $G(\mathbf{x}) \in \mathbb{R}[x_1, \dots, x_s]$ of degree d. How large must s be in terms of d so that given $\varepsilon > 0$, there are infinitely many $\mathbf{x} \in \mathbb{Z}^s$ such that $|G(x_1, \dots, x_s)| < \varepsilon$?

Even the simplest cases of the latter problem appear to be formidably difficult. It is a beautiful theorem of Schmidt [58] that when $G(\mathbf{x}) \in \mathbb{R}[x_1, \dots, x_s]$ is a homogeneous polynomial of odd degree d, there exists an integer $s_0(d)$ such that whenever $s > s_0(d)$ and $\varepsilon > 0$, then there are infinitely many integral solutions of the inequality $|G(\mathbf{x})| < \varepsilon$. At present the only explicit estimate available for $s_0(d)$ is that due to Pitman [53] in the special case where $d = 3$, namely $s_0(3) \leq (1314)^{256} - 2$. Little seems to be known concerning lower bounds on permissible values of $s_0(d)$. For what is known on this and related problems, see Schmidt [63], Baker [6] and Lewis [47].

2. Some simple constraints and observations

Before embarking for more technical territory, we pause to discuss some obvious constraints within the problems (a) and (b) above. In keeping with our initial tack in the introduction, we confine ourselves for the moment to considering single equations, our observations generalising easily to systems of equations.

(i) Real solubility. Plainly, a *definite* polynomial such as $x_1^{2k} + \cdots + x_s^{2k}$ ($k \in \mathbb{N}$) has only the trivial zero $\mathbf{x} = \mathbf{0}$, no matter how large s may be. On the other hand, every homogeneous polynomial $F(\mathbf{x}) \in \mathbb{Z}[x_1, \dots, x_s]$ of odd degree is indefinite, and necessarily possesses a non-trivial real zero (we leave this as a simple exercise to the reader). We therefore pay particular attention to polynomials of odd degree without further apology.

(ii) p-adic solubility. Since a somewhat detailed discussion at this point is useful in motivating a later argument (see the proof of Theorem 6.2 below), we will be more

precise temporarily than would otherwise be warranted by present circumstances. Let d be an integer exceeding 1, let p be a prime number, and write $\mathbb{F}_p$ for the field of p elements. There is a field extension K of $\mathbb{F}_p$ of degree d. Let $\omega_1, \dots, \omega_d$ be a basis for $K/\mathbb{F}_p$, and consider the norm form $\overline{N}(\mathbf{x}) = N_{K/\mathbb{F}_p}(\omega_1 x_1 + \cdots + \omega_d x_d)$ defined to be the determinant of the linear transformation in K determined by multiplication by $\omega_1 x_1 + \cdots + \omega_d x_d$. When $\boldsymbol{\alpha} \in \mathbb{F}_p^d$ and $\alpha = \alpha_1\omega_1 + \cdots + \alpha_d\omega_d$, we write $\overline{N}(\alpha) = \overline{N}(\boldsymbol{\alpha})$. Plainly $\overline{N}(\mathbf{x})$ is a polynomial of degree d with $\mathbb{F}_p$-rational coefficients. It is easily verified, moreover, that whenever $\alpha, \beta \in K$, one has $\overline{N}(\alpha)\overline{N}(\beta) = \overline{N}(\alpha\beta)$. Consequently, whenever $\boldsymbol{\alpha} \in \mathbb{F}_p^d \setminus \{\mathbf{0}\}$, and $\alpha = \alpha_1\omega_1 + \cdots + \alpha_d\omega_d$, then necessarily one has $\overline{N}(\alpha)\overline{N}(1/\alpha) = 1$, whence $\overline{N}(\boldsymbol{\alpha}) = \overline{N}(\alpha) \neq 0$. So the only zero in $\mathbb{F}_p^d$ of $\overline{N}(\mathbf{x})$ is the trivial one. Identifying now the polynomial $\overline{N}(\mathbf{x})$ with a corresponding polynomial $N(\mathbf{x})$ having integer coefficients, whose reduction modulo p coincides with $\overline{N}(\mathbf{x})$ in the obvious sense, it follows that the polynomial

$$F(\mathbf{x}) = N(x_1, \dots, x_d) + pN(x_{d+1}, \dots, x_{2d}) + \dots + p^{d-1}N(x_{d^2-d+1}, \dots, x_{d^2}) \tag{2.1}$$

has only the trivial zero $\mathbf{x} = \mathbf{0}$ over $\mathbb{Q}_p$. For whenever this polynomial is divisible by p, it follows from the above argument that $p|x_i$ for $1 \le i \le d$. On substituting and dividing by p, an obvious induction shows that when $\mathbf{x}$ is a zero of $F(\mathbf{x})$, then $p^r|x_i$ $(1 \le i \le d^2)$ for every $r \in \mathbb{N}$. In particular, there exist forms $F(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}]$ of odd degree d in as many as d^2 variables which fail to possess non-trivial integral zeros.

(iii) Hybrid examples. Motivated by an example described by Swinnerton-Dyer, one may construct hybrid examples less trivial than those above. For example, Cassels and Guy [18] have shown that the equation $5x^3 + 12y^3 - 9z^3 - 10t^3 = 0$ has no non-trivial integral solutions, despite having non-trivial real and p-adic solutions, for every prime p. Consequently the sextic polynomial

$$5(x_1^2 + \cdots + x_s^2)^3 + 12(y_1^2 + \cdots + y_s^2)^3 - 9(z_1^2 + \cdots + z_s^2)^3 - 10(t_1^2 + \cdots + t_s^2)^3$$

has non-trivial real and p-adic zeros, for every prime p, but has no non-trivial integral zeros, no matter how large s may be.

While problem (b) is considerably more subtle than that concerning the mere existence of solutions, the discussion of example (ii) above is nonetheless instructive.

(iv) Density of solutions. Suppose that $F(\mathbf{x}) \in \mathbb{Z}[x_1, \dots, x_s]$ is a homogeneous polynomial of odd degree d, and suppose that $F(\mathbf{x})$ possesses non-trivial p-adic zeros for every prime p. One may naively expect that when B is large, as we vary $(x_1, \dots, x_s)$ through the box $[-B, B]^s$, one should find that almost every integer in the convex hull of the set $F([-B, B]^s)$ should receive its fair share of representations. Given this weak probabilistic heuristic, it is to be expected that for a suitable positive real number β, one should have

$$\operatorname{card}(\{\mathbf{x} \in [-B, B]^s \cap \mathbb{Z}^s \ : \ F(\mathbf{x}) = 0\}) \gg \frac{\operatorname{card}([-B, B]^s \cap \mathbb{Z}^s)}{\operatorname{card}([-\beta B^d, \beta B^d] \cap \mathbb{Z})} \gg B^{s-d}. \tag{2.2}$$

This lower bound is consistent with the expectation that the number of integral zeros of $F(\mathbf{x})$ in the box $[-B,B]^s$ should be asymptotic to a product of local densities. However, the above heursitic may be far from the truth when the form $F(\mathbf{x})$ is degenerate. Consider, for example, any large natural number s, an odd integer d, and linear polynomials $L_i(\mathbf{x}) \in \mathbb{Z}[x_1,\dots,x_s]$ $(1 \le i \le d^2)$ linearly independent over $\mathbb{Q}$. Recalling the example (2.1) above, we define

$$G(\mathbf{x}) = F(L_1(\mathbf{x}),\dots,L_{d^2}(\mathbf{x})).$$

Then by the argument of example (ii), it follows that whenever $G(\mathbf{x}) = 0$ one necessarily has $L_i(\mathbf{x}) = 0$ $(1 \le i \le d^2)$, and hence the linear independence of the $L_i(\mathbf{x})$ forces us to conclude that

$$\mathrm{card}(\{\mathbf{x} \in [-B,B]^s \cap \mathbb{Z}^s \ : \ G(\mathbf{x}) = 0\}) \ll B^{s-d^2}.$$

We stress that such is the case no matter how large s may be, and when $d > 1$ this estimate sharply contradicts the lower bound (2.2).

We remark that in the current state of knowledge, it remains possible that the following conjecture is true.

Conjecture. *Let s and d be natural numbers with d odd and $s > d^2$. Suppose that $F(\mathbf{x}) \in \mathbb{Z}[x_1,\dots,x_s]$ is a homogeneous polynomial of degree d. Then when B is large, one has*

$$\mathit{card}(\{\mathbf{x} \in [-B,B]^s \cap \mathbb{Z}^s \ : \ F(\mathbf{x}) = 0\}) \gg B^{s-d^2}.$$

Similarly, let s and $d_1,\dots,d_r$ be natural numbers with d_i odd $(1 \le i \le r)$ and $s > d_1^2 + \cdots + d_r^2$. Suppose that $F_i(\mathbf{x}) \in \mathbb{Z}[x_1,\dots,x_s]$ $(1 \le i \le r)$ is a homogeneous polynomial of degree d_i $(1 \le i \le r)$. Then one might conjecture that

$$\mathrm{card}(\{\mathbf{x} \in [-B,B]^s \cap \mathbb{Z}^s \ : \ F_1(\mathbf{x}) = \dots = F_r(\mathbf{x}) = 0\}) \gg B^{s-d_1^2-\cdots-d_r^2}.$$

3. Approaches to these problems

Except in a few isolated instances, we currently have only two approaches to the problems (a) and (b) above which are guaranteed to achieve some measure of success. While methods from arithmetic geometry and ergodic theory are applicable to special examples (see, for example, Batyrev and Manin [7], Lang [38] and Duke, Rudnick and Sarnak [28]), the applicability of such methods requires detailed knowledge of the geometry and algebraic structure of the examples under consideration. In contrast, the methods we highlight herein are applicable in considerable generality, and make use of only the weakest properties of the underlying polynomials.

(i) Elementary diagonalisation methods. There is a vast body of knowledge available concerning the solubility of additive diophantine equations of the shape

$$a_1y_1^k + \cdots + a_ty_t^k = 0, \tag{3.1}$$

where the a_i are fixed integers (see, for example, Vaughan [79] and Davenport [22]). Owing to their diagonal structure, such equations are particularly amenable to methods involving exponential sums and the Hardy-Littlewood method. Thus, given a homogeneous polynomial $F(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_s]$ of odd degree d, one may attempt an attack on problem (a) by seeking linear polynomials $L_i(\mathbf{y}) = a_{i1}y_1 + \cdots + a_{it}y_t$ $(1 \le i \le s)$ with $a_{ij} \in \mathbb{Z}$ $(1 \le i \le s, 1 \le j \le t)$, satisfying the property that the equation

$$F(L_1(\mathbf{y}), \ldots, L_s(\mathbf{y})) = 0$$

takes the shape (3.1). Since polynomials of degree exceeding 2 do not, in general, diagonalise under a non-singular substitution, one expects that s need be much larger than t in order that this strategy should stand a chance of success. This approach has been successfully exploited by Brauer [14] and Birch [8] to establish two remarkable theorems about which we will say much more in due course.

Theorem 3.1 (Brauer). *Let d be a natural number. Then there is a number $s_1(d)$ such that whenever p is a prime number and $s > s_1(d)$, and $F(\mathbf{x}) \in \mathbb{Q}_p[x_1, \ldots, x_s]$ is homogeneous of degree d, then the equation $F(\mathbf{x}) = 0$ possesses a solution $\mathbf{x} \in \mathbb{Q}_p^s \setminus \{\mathbf{0}\}$.*

Theorem 3.2 (Birch). *Let d be an odd integer. Then there is a number $s_2(d)$ such that whenever $s > s_2(d)$ and $F(\mathbf{x}) \in \mathbb{Q}[x_1, \ldots, x_s]$ is homogeneous of degree d, then it follows that the equation $F(\mathbf{x}) = 0$ possesses a solution $\mathbf{x} \in \mathbb{Q}^s \setminus \{\mathbf{0}\}$.*

While these theorems in some sense provide a solution of problem (a) above, neither Brauer nor Birch explicitly computed the dependence of $s_1(d)$ and $s_2(d)$ on d, and with good reason! The arguments used in establishing these theorems involve complicated inductions which lead to bounds so large that they are aptly described by Birch's sarcastic phrase "not even astronomical".

(ii) The Hardy-Littlewood method. Various versions of the Hardy-Littlewood method have been developed in order to discuss the problems (a) and (b) above. All of these versions have rather serious limitations which restrict their use somewhat, and thus we will avoid describing such methods in detail within this paper. Two results typify the kind of conclusions available within this circle of ideas.

Theorem 3.3 (Birch). *Let $F(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_s]$ be homogeneous of degree d, and suppose that the variety defined by the equation $F(\mathbf{x}) = 0$ has a singular locus of dimension at most D. Then whenever $s - D > (d-1)2^d$, one has*

$$card(\{\mathbf{x} \in [-B, B]^s \cap \mathbb{Z}^s \ : \ F(\mathbf{x}) = 0\}) \sim CB^{s-d},$$

where C denotes the "product of local densities" within the box $[-B, B]^s$.

Here, in order to save space, we avoid explaining precisely what "product of local densities" means, and instead note merely that this number is positive and uniformly

bounded away from 0 whenever the equation $F(\mathbf{x}) = 0$ possesses non-singular real and p-adic solutions for every prime p. In such a situation, it follows from Birch's Theorem that the equation $F(\mathbf{x}) = 0$ possesses infinitely many primitive integral solutions. The difficulty in applying this result of Birch [10] to resolve the problem (a) satisfactorily lies in our failure to adequately understand singular loci. It seems likely that whenever a variety defined as the set of zeros of a polynomial $F(\mathbf{x})$ possesses a singular locus of extremely large dimension, then necessarily that locus contains a subvariety defined by a system of rational equations of small degree. If such were known, then one could apply an inductive procedure in order to infer the existence of non-trivial integral solutions. Presently, however, we do not even understand the singular loci of cubic polynomials in any generality.

There is a second rather general approach due to Schmidt [65]. In order to describe this method, we require some notation. When $F(\mathbf{x}) \in \mathbb{Q}[x_1, \dots, x_s]$ is a form of degree $d > 1$, write $h(F)$ for the least number h such that F may be written in the form

$$F = A_1B_1 + A_2B_2 + \cdots + A_hB_h,$$

with A_i, B_i forms in $\mathbb{Q}[\mathbf{x}]$ of positive degree $(1 \le i \le h)$. There is an analogous concept for systems of forms which we avoid describing in the interest of saving space.

Theorem 3.4 (Schmidt). *Let d be an integer exceeding 1, and write $\chi(d) = d^2 2^{4d} d!$. Let $F(\mathbf{x}) \in \mathbb{Z}[x_1, \dots, x_s]$ be homogeneous of degree d, and suppose that $h(F) \ge \chi(d)$. Then one has*

$$\mathit{card}(\{\mathbf{x} \in [-B, B]^s \cap \mathbb{Z}^s \ : \ F(\mathbf{x}) = 0\}) \sim CB^{s-d},$$

where C denotes the "product of local densities" within the box $[-B, B]^s$.

While the integer $h(F)$ associated with a form F may be difficult to compute for a specific example, Schmidt's approach has the advantage of leading naturally to an inductive strategy for solving an equation. For suppose that the form $F(\mathbf{x}) \in \mathbb{Z}[x_1, \dots, x_s]$ has odd degree d, and possesses non-singular real and p-adic solutions for every prime p. Then if $h(F) \ge d^2 2^{4d} d!$, it follows from Theorem 3.4 that the equation $F(\mathbf{x}) = 0$ possesses infinitely many primitive integral solutions. Otherwise we may write

$$F(\mathbf{x}) = A_1(\mathbf{x})B_1(\mathbf{x}) + \cdots + A_h(\mathbf{x})B_h(\mathbf{x})$$

with $h < d^2 2^{4d} d!$, and with $A_1(\mathbf{x}), \dots, A_h(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}]$ homogeneous of odd degree at most $d-2$. Thus, provided that we can solve the system $A_i(\mathbf{x}) = 0$ $(1 \le i \le h)$, then again we obtain a non-trivial integral solution of the equation $F(\mathbf{x}) = 0$. Moreover, all of the equations occurring in the latter system have degree smaller than that of $F(\mathbf{x})$. We may now, therefore, apply the analogue of Theorem 3.4 for systems of polynomials, and with sufficiently many variables we will either solve the system, or again reduce the degrees of the equations occurring therein. Unfortunately, the number of variables required to establish the existence of solutions using this approach is "not even astronomical" in size, and indeed Birch's elementary approach may be fashioned to do better in this respect.

For more restricted variants of the Hardy-Littlewood method applicable to the solubility of systems of equations in many variables, see also Tartakovsky [76], Davenport [20], [21], [23], Pleasants [54], Schmidt [62], Heath-Brown [33], Hooley [34], [35], [36], Skinner [73], [75] and Vaughan and Wooley [80].

4. Some notation

In order to navigate further our discussion of the problem (a), we require some notation. Despite the unpleasant appearance of this notation, it is best simply to introduce it in the most general form in one clean sweep.

Definition 4.1. *Given an r-tuple of polynomials*

$$\mathbf{F} = (F_1, \dots, F_r)$$

with coefficients in a field k, denote by $\nu(\mathbf{F})$ the number of variables appearing explicitly in $\mathbf{F}$.

We are interested in solution sets, over a field k, of systems of homogeneous polynomial equations with coefficients in k. When such a set contains a linear subspace of the ambient space, we define its dimension to be that when considered as a projective space.

Definition 4.2. *Let k be a field. Denote by $\mathcal{G}_d^{(m)}(r_d, \dots, r_1; k)$ the set of $(r_d + \cdots + r_1)$-tuples of homogeneous polynomials, of which r_i have degree i for $1 \le i \le d$, with coefficients in k, which possess no linear space of solutions of dimension m over k. We define $V_d^{(m)}(\mathbf{r}) = V_d^{(m)}(r_d, \dots, r_1; k)$ by*

$$V_d^{(m)}(r_d, \dots, r_1; k) = \sup_{\mathbf{h} \in \mathcal{G}_d^{(m)}(r_d, \dots, r_1; k)} \nu(\mathbf{h}).$$

We abbreviate $V_d^{(m)}(r, 0, \dots, 0; k)$ to $v_{d,r}^{(m)}(k)$, and similarly $v_{d,r}^{(0)}(k)$ to $v_{d,r}(k)$, and $v_{d,1}^{(m)}(k)$ to $v_d^{(m)}(k)$, and $v_d^{(0)}(k)$ to $v_d(k)$.

Notice that this definition simply tells us how many variables we require in order to solve an arbitrary implicit system of equations.

Examples.

(i). We have $v_{1,r}(k) = r$, by familiar linear algebra. In other words, in any field k a system of r linear forms with k-rational coefficients, in $r + 1$ or more variables, necessarily possesses a non-trivial k-rational solution. Moreover, there exist systems of r linear forms in r variables which possess only trivial solutions.

(ii). For any prime number p, it follows from the classical theory of quadratic forms that $v_2(\mathbb{Q}_p) = 4$. In other words, any quadratic form with p-adic coefficients in 5 or more variables possesses a non-trivial p-adic solution. Moreover, in view of examples of the type (2.1) above, there are quadratic forms in 4 variables which possess only the trivial p-adic solution.

(iii). We have $v_2(\mathbb{Q}) = +\infty$, because any definite quadratic form has only the trivial zero over $\mathbb{Q}$, no matter how many variables it might have.

The simplest forms of degree d to investigate are diagonal forms of the shape

$$a_1x_1^d + \cdots + a_sx_s^d. \tag{4.1}$$

Definition 4.3. *When k is a field, denote by $\mathcal{D}_{d,r}(k)$ the set of r-tuples of diagonal forms of degree d, with coefficents in a field k, which possess no non-trivial zeros over k. Define*

$$\phi_{d,r}(k) = \sup_{\mathbf{f}\in\mathcal{D}_{d,r}(k)} \nu(\mathbf{f}).$$

We abbreviate $\phi_{d,1}(k)$ to $\phi_d(k)$.

Note that whenever $s > \phi_d(k)$ and $a_i \in k$ $(1 \le i \le s)$, then the polynomial (4.1) possesses a non-trivial k-rational zero.

5. Brauer's method

Equipped with the notation of the previous section, we may restate a quite general version of problem (a) as follows.

Problem (A). *Existence of solutions.* Given a field k, a natural number d, and non-negative integers $r_1, \dots, r_d$ and m, find an upper bound for $V_d^{(m)}(r_d, \dots, r_1; k)$.

The methods of Brauer [14] alluded to above in connection with Theorem 3.1 may be applied to provide an elegantly simple solution of problem (A).

Theorem 5.1 (Brauer). *Let k be a field, and suppose that for $i \ge 2$ one has $\phi_i(k) < \infty$. Then for each natural number d and for all non-negative integers $r_1, \dots, r_d$ and m, one has*

$$V_d^{(m)}(r_d, \dots, r_1; k) < \infty.$$

It has been known since at least the early part of this century that for every prime number p one has $\phi_d(\mathbb{Q}_p) < \infty$, and thus we see that Theorem 3.1 is an immediate corollary of Theorem 5.1. Unfortunately, since $\phi_t(\mathbb{Q}) = +\infty$ whenever t is even, Theorem 5.1 does not yield insight into bounds for $v_d(\mathbb{Q})$.

As indicated in §3, the method of proof of Theorem 5.1 is a complicated induction, so highly iterative that for decades it was thought that any explicit estimate arising from such methods would surely be too large to be sensibly written down. It was therefore a surpise when Leep and Schmidt [42] were able to obtain a "reasonable" bound by employing a clever variant of Brauer's original method. When p is a prime number and $k = \mathbb{Q}_p$, the conclusions of Leep and Schmidt [42] may be stated reasonably cleanly as follows.

Theorem 5.2 (Leep and Schmidt). *Let p be a prime number, and let d be a natural number. Then for each positive number ε, one has*

$$v_d(\mathbb{Q}_p) \ll_\varepsilon e^{(d!)^2(1+\varepsilon)^d}.$$

Further, when r is a natural number,

$$v_{d,r}(\mathbb{Q}_p) \le \left(\frac{v_2}{2}\right)\left(\frac{v_3}{2}\right)^2 \dots \left(\frac{v_d}{2}\right)^{2^{d-2}} r^{2^{d-1}} \left(1 + O(r^{-1})\right).$$

We will return momentarily to the topic of explicit versions of Brauer's Theorem. In order to better explain the ideas involved in subsequent developments, however, it seems appropriate at this stage to sketch a proof of Theorem 5.1. Let k be a field, and suppose that $\phi_i(k) < \infty$ for $i \ge 2$. When $D \ge 1$, we form the inductive hypothesis that for all non-negative integers $r_D, \dots, r_1$ and m, one has

$$V_D^{(m)}(r_D, \dots, r_1; k) < \infty. \tag{5.1}$$

The hypothesis (5.1) is immediate from linear algebra when $D = 1$. We suppose that $d \ge 2$ and that (5.1) holds for all m and $\mathbf{r}$ when $D = d - 1$, and then aim to establish (5.1) for all m and $\mathbf{r}$ when $D = d$.

We start with some simplifications, observing first that for all m and $\mathbf{r}$, one has

$$V_d^{(m)}(r_d, \dots, r_1; k) \le v_{d,r_d}^{(v)}(k), \tag{5.2}$$

where $v = V_{d-1}^{(m)}(r_{d-1}, \dots, r_1; k)$. For given any system of r_j forms of degree j $(1 \le j \le d)$ in more than $v_{d,r_d}^{(v)}(k)$ variables, the subsystem of r_d forms of degree d possesses a v-dimensional linear space of k-rational zeros. Writing down a basis for this linear space, and substituting into the remaining forms, we obtain a system of r_i forms of degree i $(1 \le i \le d-1)$ in $v+1$ variables, and by the definition of $V_{d-1}^{(m)}(\mathbf{r}; k)$, this system possesses an m-dimensional linear space of k-rational zeros. The upper bound (5.2) is immediate. Moreover, a similar argument shows that whenever $r \ge 2$, one has

$$v_{d,r}^{(m)}(k) \le v_d^{(w)}(k), \tag{5.3}$$

where $w = v_{d,r-1}^{(m)}(k)$. We therefore deduce that in order to establish (5.1), it suffices to show that $v_d^{(m)}(k) < \infty$ for each m.

Next we indicate how to diagonalise a form. We claim that for each natural number t, there is an integer $n(t)$, depending at most on k and t, such that whenever $s > n(t)$ and $F(\mathbf{x}) \in k[x_1, \dots, x_s]$ is a form of degree d, then there exist linearly independent k-rational points $\mathbf{y}_1, \dots, \mathbf{y}_t$ with the property that for every $z_1, \dots, z_t$ in k one has

$$F(z_1\mathbf{y}_1 + \cdots + z_t\mathbf{y}_t) = F(\mathbf{y}_1)z_1^d + \cdots + F(\mathbf{y}_t)z_t^d. \tag{5.4}$$

In other words, the polynomial $F(\mathbf{x})$ may be reduced non-trivially to a diagonal form in at least t variables. When $t = 1$ this claim is trivial, so we suppose that $t \ge 1$ and that $\mathbf{y}_1, \dots, \mathbf{y}_t$ satisfy (5.4). Write $\mathbf{u} = z_1\mathbf{y}_1 + \cdots + z_t\mathbf{y}_t$, and consider a point $\mathbf{v} \in k^s$ linearly independent of $\mathbf{y}_1, \dots, \mathbf{y}_t$. Then for every t and w in k one has

$$F(t\mathbf{u} + w\mathbf{v}) = t^d F(\mathbf{u}) + w^d F(\mathbf{v}) + \sum_{i=1}^{d-1} t^i w^{d-i} G_i(\mathbf{u}, \mathbf{v}), \tag{5.5}$$

where the polynomials $G_i(\mathbf{u},\mathbf{v}) \in k[\mathbf{u},\mathbf{v}]$ are homogeneous of degree i in terms of $\mathbf{u}$, and of degree $d-i$ in terms of $\mathbf{v}$. When $t=1$, so that $\mathbf{u}=z_1\mathbf{y}_1$, the system of equations $G_i(\mathbf{u},\mathbf{v})=0$ $(1 \le i \le d-1)$ is equivalent to a system of homogeneous equations in $\mathbf{v}$ of respective degrees $1,2,\dots,d-1$. On recalling that we are choosing $\mathbf{v}$ to be linearly independent of $\mathbf{y}_1$, it follows that whenever $s-1 > V_{d-1}^{(0)}(1,1,\dots,1;k)$, then the latter system possesses a non-trivial k-rational solution. From (5.5) we therefore deduce that the polynomial $F(\mathbf{x})$ may be reduced non-trivially to a diagonal form in at least $t+1$ variables. When $t>1$, we may adopt a similar strategy, examining separately the coefficients of each term of the shape $z_1^{i_1}\dots z_t^{i_t}$, although we emphasise that the number of equations needing to be solved will increase with t. Thus it follows that whenever both $n(t)$ and $V_{d-1}^{(0)}(\mathbf{r};k)$ are finite, for each $\mathbf{r}$, then one has that $n(t+1)$ is finite. Our claim that $n(t)<\infty$ for each t therefore follows by induction.

Consider next a form $F(\mathbf{x}) \in k[x_1,\dots,x_s]$ with $s > n(t)$, where $t=(m+1)\psi$ and $\psi=\phi_d(k)+1$. By the above argument the polynomial $F(\mathbf{x})$ diagonalises via a substitution $\mathbf{x}=z_1\mathbf{y}_1+\cdots+z_t\mathbf{y}_t$ to the shape $F(\mathbf{x})=a_1z_1^d+\cdots+a_tz_t^d$. But the variables in the latter form may plainly be partitioned into $m+1$ sets each containing ψ variables, and moreover, with the diagonal form underlying each set possessing a non-trivial k-rational zero. Thus it follows that the equation $F(\mathbf{x})=0$ has a k-rational linear space of solutions of dimension m, and hence $v_d^{(m)}(k) \le n(t) < \infty$. In view of (5.2) and (5.3), we may conclude that (5.1) holds with $D=d$, and so our induction is complete.

A cursory examination reveals that the bounds stemming from the above argument will involve highly iterated exponential functions of unpleasant type. In order to establish the respectable bounds embodied in Theorem 5.2, Leep and Schmidt [42] required three new ingredients. First, an efficient new inductive approach is used to generate linear spaces of k-rational solutions to systems of equations, thereby replacing the simplifying bounds (5.2) and (5.3) by ones considerably less wasteful. The idea is to make use of the existence of a linear space of k-rational solutions, via a change of variables, in order to simplify the shape of the equations under consideration, and thence make easier the task of finding a larger linear space of k-rational solutions. By making use of the bound $v_{d,r}(k) \le v_{d,r-1}^{(w)}(k)$, with $w=v_d(k)$, this idea also enables one to bound $v_{d,r}^{(m)}(k)$ simply in terms of $v_j(k)$ $(1 \le j \le d)$. Second, Leep and Schmidt diagonalise whole systems of forms simultaneously, rather than just a single form. Then by making use of estimates of Davenport and Lewis [25] for $\phi_{d,r}(\mathbb{Q}_p)$, Leep and Schmidt are able to remove another of the highly iterated inductions from the above argument. Thirdly, and this ingredient should not be underestimated, Leep and Schmidt were brave enough to push the project through to completion! By developing further the theory of simultaneous additive equations, Schmidt [64] was subsequently able to improve the bounds recorded in Theorem 5.2 somewhat, showing that for every prime p and natural number d, one has $v_d(\mathbb{Q}_p)=o(e^{2^d d!})$.

The author recently found that the Leep-Schmidt approach to Brauer's method could be improved further (see Wooley [84]). The key idea is to generate a linear

space of k-rational solutions to all but one equation of a system via the Leep-Schmidt process, and at the same time diagonalise the final equation with little additional cost. This amputates another of the iterated inductive steps from the process described above. In addition to providing sharper bounds, this new method offers greater flexibility in its application than that of Leep and Schmidt, for it depends only on the theory of a single additive equation. The latter is by now rather well understood in almost any respectable field. We illustrate the conclusions stemming from these ideas with the following theorem.

Theorem 5.3 (Wooley). *Let m, d and r be non-negative integers with $d \geq 2$ and $r \geq 1$. Write ϕ_i for $\phi_i(k)$ $(2 \leq i \leq d)$. Then whenever k is a field for which $\phi_i < \infty$ $(2 \leq i \leq d)$, one has*

$$v_{d,r}^{(m)}(k) \leq 2(r^2\phi_d + mr)^{2^{d-2}} \prod_{i=2}^{d-1} (\phi_i + 1)^{2^{i-2}}.$$

The conclusion of Theorem 5.3 improves on that of Theorem 5.2 whenever ϕ_j is significantly smaller than v_j $(2 \leq j \leq d)$. Given that we no so much about ϕ_j and little concerning bounds for v_j, the reader will anticipate numerous painless corollaries.

Corollary 1. *Let d be an integer with $d \geq 2$, and let r be a natural number. Then for each prime number p one has $v_{d,r}(\mathbb{Q}_p) \leq (rd^2)^{2^{d-1}}$, and in particular, one has $v_d(\mathbb{Q}_p) \leq d^{2^d}$.*

This follows from Theorem 5.3 via the bound $\phi_d(\mathbb{Q}_p) \leq d^2$ of Davenport and Lewis [24].

Corollary 2. *Let d be an integer with $d \geq 2$, let r be a natural number, and let p be a prime number. Then whenever K is an algebraic extension of $\mathbb{Q}_p$, one has*

$$v_{d,r}(K) \leq r^{2^{d-1}} e^{2^{d+2}(\log d)^2}.$$

Whenever one has a system of equations with coefficients from an algebraic extension of $\mathbb{Q}_p$, these coefficients must all lie in some finite extension K' of $\mathbb{Q}_p$. Thus Corollary 2 follows from Theorem 5.3 via the bound

$$\phi_d(K') \leq d((d+1)^{\max\{2\log d/\log p, 1\}} - 1)$$

of Skinner [74].

It transpires that in purely imaginary field extensions L of $\mathbb{Q}$, the archimedean local solubility condition is automatically satisfied. Consequently, on deriving a bound on $\phi_d(L)$ from work of Siegel [71], [72] and Birch [9], we are able to derive an explicit version of a theorem of Peck [52].

Corollary 3. *Let d be an integer with $d \geq 2$, let r be a natural number, and let L be a purely imaginary field extension of $\mathbb{Q}$. Then $v_{d,r}(L) \leq r^{2^{d-1}} e^{2^d d}$.*

The situation in which Brauer's methods may be expected to be most effective is that in which equations of the shape $ax^d + by^d = 0$ necessarily possess non-trivial solutions. This brings us to the topic of radical solutions of polynomials, an area distinguished since Medieval times and invigorated by the celebrated work of Galois. Such a topic deserves a digression to itself.

6. Solving equations in solvable extensions

Consider a countable field k of characteristic zero, such as $\mathbb{Q}$. We remark that these hypotheses are more a matter of convenience than an essential requirement, the corresponding theory in positive characteristic containing several technical complications. We define the *radical closure* $k^{\rm rad}$ of k as follows. Let $\overline{k}$ denote the algebraic closure of k. Also, let S denote the set of all elements α of $\overline{k}$ for which the field extension $k(\alpha)/k$ is solvable. Since $\overline{k}$ is countable, so too must be S, so that we may write $S = \{\alpha_1, \alpha_2, \dots\}$. We then define

$$k^{\rm rad} = \bigcup_{n=1}^{\infty} k(\alpha_1, \dots, \alpha_n).$$

The reader will readily verify that $k^{\rm rad}$ satisfies all of the axioms for a field, and moreover, whenever $\alpha \in k^{\rm rad}$ one has that $k(\alpha)$ is a solvable extension of k, whence α is radical.

The classical theory of equations shows that polynomial equations of the shape

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0 \tag{6.1}$$

are solvable over $k^{\rm rad}$ when $n = 2, 3, 4$. Meanwhile, a celebrated consequence of Galois theory shows that when $k = \mathbb{Q}$, for each n with $n \ge 5$ such equations exist with no radical solutions (the only solutions are "irradical"). By homogenising the equation (6.1), therefore, we find that for every countable field k one has $v_d(k^{\rm rad}) = 1$ when $d = 2, 3, 4$, but that $v_d(\mathbb{Q}^{\rm rad}) \ge 2$ whenever $d \ge 5$. This classical problem naturally leads one, therefore, to consider upper bounds for $v_d(k^{\rm rad})$ in general. Since, when $a, b \in k^{\rm rad}$, the equation $ax^d + by^d = 0$ is always soluble with $x, y \in k^{\rm rad}$, we have $\phi_d(k^{\rm rad}) = 1$ for every natural number d. Then as a corollary of Theorem 5.3 we have the following (see Wooley [84]).

Theorem 6.1 (Wooley). *Let k be a countable field of characteristic zero, and let d and r be natural numbers with $d \ge 2$. Then $v_{d,r}(k^{\rm rad}) \le (2r^2)^{2^{d-2}}$.*

Fixing attention temporarily on the most familiar case where $k = \mathbb{Q}$, one may ask whether $v_d(\mathbb{Q}^{\rm rad})$ can be arbitrarily large as d grows. In Wooley [84] we show that for infinitely many integers d one has $v_d(\mathbb{Q}^{\rm rad}) \ge d^{\frac{\log 2}{\log 5}}$, answering the latter question in the affirmative. But one may, in fact, provide a still larger lower bound for $v_d(\mathbb{Q}^{\rm rad})$ by use of an example motivated by §2(ii). For background on the necessary Galois theory, see either Garling [30] or Serre [70].

Theorem 6.2. *When $d = 2$, 3, or 4 one has $v_d(\mathbb{Q}^{\rm rad}) = 1$. But when d is a natural number with $d \ge 5$, one has $v_d(\mathbb{Q}^{\rm rad}) \ge d$.*

Proof. We have already discussed the first assertion of the theorem. Suppose next that d is an integer with $d \ge 5$, and consider the polynomial $f_d(x) = x^d - x - 1$. By Selmer [69], the polynomial $f_d(x)$ is irreducible over $\mathbb{Q}$. Let K be the splitting field of $f_d(x)$ over $\mathbb{Q}$. Then according to the remarks on p.42 of Serre [70], one can show that the field extension $K/\mathbb{Q}$ has Galois group Γ isomorphic to the full

symmetric group S_d. Since the group S_d is not solvable for $d \geq 5$, it follows that the polynomial $f_d(x)$ cannot be solved by radical extensions. We note also that $[K : \mathbb{Q}] = d!$.

Our next step is to show that $f_d(x)$ is irreducible over $\mathbb{Q}^{\mathrm{rad}}$. Suppose that $f_d(x)$ factors over $\mathbb{Q}^{\mathrm{rad}}$ in the form

$$f_d(x) = g_1(x)g_2(x)\dots g_t(x), \tag{6.2}$$

where the $g_i(x)$ are monic polynomials irreducible in $\mathbb{Q}^{\mathrm{rad}}[x]$ of degree d_i $(1 \leq i \leq t)$. Let L_0 denote the field extension of $\mathbb{Q}$ obtained by adjoining the coefficients of the g_i $(1 \leq i \leq t)$. Since each $g_i(x)$ splits over K, it follows that L_0 is contained in K. Consider the Galois group Γ_0 of the field extension $L_0/\mathbb{Q}$. Let σ be an automorphism in Γ_0, and consider its action on the polynomial $g_i(x)$. That is, consider the polynomial $g_i^\sigma(x)$ obtained by replacing the coefficients of $g_i(x)$ by their images under σ. Since $f_d(x)$ is invariant under the action of σ, it follows that $g_i^\sigma(x)$ divides $f_d(x)$. Consequently, one has that $g_i^\sigma(x)$ divides $f_d(x)$ for every $\sigma \in \Gamma_0$, and for each i with $1 \leq i \leq t$. But L_0 is the minimal field extension of $\mathbb{Q}$ containing the coefficients of the g_i, so for each $\sigma \in \Gamma_0$ other than the trivial automorphism, there is at least one g_i which is moved under the action of σ. It follows that Γ_0 is determined by its action on the g_i $(1 \leq i \leq t)$, whence it is isomorphic to some subgroup of the group of permutations on t elements. In particular, one has $|\Gamma_0| \leq t!$, whence also $[L_0 : \mathbb{Q}] \leq t!$.

Next observe that if some subset, say $\{g_{i_1}(x), \dots, g_{i_n}(x)\}$, is left fixed under the action of Γ_0, then the polynomial $\prod_{j=1}^n g_{i_j}(x)$ is also invariant under the action of Γ_0, and hence has rational coefficients. Then it follows from the irreducibility of $f_d(x)$ that $n = t$, and moreover there is no loss of generality in supposing that each $g_i(x)$ has the same degree. Thus t divides d, and the degree of each $g_i(x)$ is equal to d/t. Furthermore, one cannot have $t = d$, for then $f_d(x)$ splits over the radical field extension L_0 of $\mathbb{Q}$, and yet $f_d(x)$ has no radical roots. We now construct a tower of field extensions

$$\mathbb{Q} \subseteq L_0 \subseteq L_1 \subseteq \cdots \subseteq L_t = K,$$

as follows. For each i with $0 \leq i \leq t-1$ we take L_{i+1} to be the splitting field of $g_{i+1}(x)$ over L_i. That $K = L_t$ then follows from the factorisation (6.2) together with our earlier observations concerning the field L_0. But we have

$$[L_{i+1} : L_i] \leq (\deg(g_{i+1}))! = (d/t)! \quad (0 \leq i \leq t-1).$$

Consequently,

$$\begin{aligned}[K : \mathbb{Q}] &= [K : L_{t-1}][L_{t-1} : L_{t-2}] \dots [L_1 : L_0][L_0 : \mathbb{Q}] \\ &\leq t!((d/t)!)^t.\end{aligned}$$

By hypothesis, however, we have also $[K : \mathbb{Q}] = d!$, so that necessarily $d! \leq t!((d/t)!)^t$. Moreover, our earlier observation ensures that $t < d$. Since $d \geq 5$,

therefore, we are forced to conclude that $t = 1$ and hence that the polynomial $f_d(x)$ is irreducible over $\mathbb{Q}^{\rm rad}$.

Since $f_d(x)$ is irreducible over $\mathbb{Q}^{\rm rad}$, if θ is a zero of $f_d(x)$ in the splitting field of $f_d(x)$ over $\mathbb{Q}^{\rm rad}$, then one has $[\mathbb{Q}^{\rm rad}(\theta) : \mathbb{Q}^{\rm rad}] = d$. Write $M = \mathbb{Q}^{\rm rad}(\theta)$, and let $\omega_1, \dots, \omega_d$ be a basis for $M/\mathbb{Q}^{\rm rad}$. Consider the norm form $N(\mathbf{x}) = N_{M/\mathbb{Q}^{\rm rad}}(\omega_1 x_1 + \cdots + \omega_d x_d)$ defined to be the determinant of the linear transformation in M determined by multiplication by $\omega_1 x_1 + \cdots + \omega_d x_d$. Plainly $N(\mathbf{x})$ is a polynomial of degree d with $\mathbb{Q}^{\rm rad}$-rational coefficients. By the same multiplicative property discussed in §2(ii), moreoever, it follows that for $\mathbf{y} \in (\mathbb{Q}^{\rm rad})^d$, one has $N(\mathbf{y}) = 0$ only when $\mathbf{y} = \mathbf{0}$. Thus it follows that $v_d(\mathbb{Q}^{\rm rad}) \ge d$ whenever $d \ge 5$. This completes the proof of the theorem.

An inspection of the example constructed in the proof of Theorem 6.2 will reveal that the underlying polynomial splits over $\mathbb{C}$, and consequently the solution set of this polynomial is singular. Such is also the case for the example used in establishing the earlier bound $v_d(\mathbb{Q}^{\rm rad}) \ge d^{\frac{\log 2}{\log 5}}$ of Wooley [84]. It seems natural to ask for absolutely irreducible or even non-singular examples.

Problem. *Is there a curve defined by an absolutely irreducible homogeneous polynomial $p(\mathbf{x}) \in \mathbb{Q}^{\rm rad}[x_1, x_2, x_3]$ which has no radical points? Further, does such a curve exist which has no singular points?*

To be clear, any homogeneous polynomial $p(\mathbf{x}) \in \mathbb{Z}[x_1, x_2, x_3]$ possessing no radical zeros has the property that whenever $p(\mathbf{x}) = 0$, then either $\mathbf{x} = \mathbf{0}$, or else at least one of x_1, x_2, x_3 does not lie in $\mathbb{Q}^{\rm rad}$. The work of Rumely [56] may well be relevant to this problem.

One might conclude from the discussion thus far that solving in solvable extensions is a pursuit of wholly artificial nature. Maybe so, but there is at least one application worthy of mention, and indeed this application seems to be what prompted Brauer to investigate the solubility of forms in the first place. We recall the discussion of §3 of Brauer [14]. Let k be a countable field of characteristic zero, and consider the arbitrary algebraic equation of degree n in one variable given by (6.1), with $a_i \in k$ $(1 \le i \le n)$. Let the zeros of $f(x)$ be ω_i $(1 \le i \le n)$, and when $1 \le i \le n$, denote by $\theta_i = \theta_i(\mathbf{u})$ the polynomial

$$\theta_i(\mathbf{u}) = u_0 + u_1\omega_i + \cdots + u_{n-1}\omega_i^{n-1}.$$

It follows that the θ_i are roots of an equation

$$g(x) = x^n + b_1(\mathbf{u})x^{n-1} + \cdots + b_n(\mathbf{u}) = 0, \tag{6.3}$$

where the b_i are homogeneous polynomials in $u_0, \dots, u_{n-1}$ of degree i for $1 \le i \le n$ (this transformation is the classical Tschirnhaus transformation). Since $g(x)$ is invariant under conjugation, moreover, one finds that each $b_i(\mathbf{u})$ has k-rational coefficients for $1 \le i \le n$. Suppose that for some fixed d with $1 \le d \le n$, one is able to solve the system of equations

$$b_i(\mathbf{u}) = 0 \quad (1 \le i \le d) \tag{6.4}$$

non-trivially over k^{rad}. We will sketch below, in fact, an argument which employs the methods described in §5 which establishes the bound

$$V_d^{(0)}(1,1,\dots,1;k^{\mathrm{rad}}) \le 2^{2^{d-1}} - 1. \tag{6.5}$$

Moreover, as is evident from a cursory examination of the underlying arguments, the latter bound guarantees that when $n \ge 2^{2^{d-1}}$, the system (6.4) is soluble non-trivially over a solvable field extension of k whose degree depends at most on d, and such that any prime divisor of this degree is also bounded above by d. Thus it is possible to take $u_0,\dots,u_{n-1}$ in a field obtained from the field of rational functions of $a_1,\dots,a_n$ by adjoining a finite number of radicals. The equation (6.3) then takes the shape

$$x^n + b_{d+1}x^{n-d-1} + \cdots + b_n = 0. \tag{6.6}$$

By adjoining a further radical, moreover, there is no loss of generality in supposing that $b_n = 1$. Thus the roots of the equation (6.6) may be considered as algebraic functions of the $n-d-1$ quantities $b_{d+1}, b_{d+2},\dots,b_{n-1}$. Since each ω_i may be expressed in terms of θ_i $(1 \le i \le n)$, it follows that the solution of the general equation of nth degree may be expressed in terms of its coefficients, provided we use radicals and one algebraic function of $n-d-1$ variables.

For each natural number n, let l_n denote the smallest integer l with the property that the roots of the general equation of degree n may be expressed in terms of the coefficients by means of algebraic functions of at most l parameters. Then the discussion above shows that $l_n \le n-d-1$ whenever $n \ge 2^{2^{d-1}}$. Consequently, we have the following theorem.

Theorem 6.3. *Let n and d be natural numbers with $n \ge d \ge 2$. Then $l_n \le n-d$ whenever $n \ge 2^{2^{d-2}}$, and in particular*

$$l_n \le n - 2 - \left[\frac{\log((\log n)/(\log 2))}{\log 2}\right].$$

Proof. We start by establishing the promised bound (6.5). We note that $\phi_d(k^{\mathrm{rad}}) = 1$ for every natural number d, and in order to save effort, we observe that the bound (2.12) of Wooley [84] asserts in particular that

$$v_{d,1}^{(1)}(k^{\mathrm{rad}}) \le 1 + V_d^{(0)}(1,1,\dots,1;k^{\mathrm{rad}}).$$

Since the bound established for $v_{d,1}^{(1)}(k^{\mathrm{rad}})$ in the proof of Theorem 2.4 of Wooley [84] is derived directly from the latter inequality, we may conclude from the proof of Theorem 2.4 of Wooley [84] that

$$\begin{aligned} 1 + V_d^{(0)}&(1,1,\dots,1;k^{\mathrm{rad}}) \\ &\le 2(\phi_d(k^{\mathrm{rad}})+1)^{2^{d-2}} \prod_{i=2}^{d-1} \big(\phi_i(k^{\mathrm{rad}})+1\big)^{2^{i-2}} \\ &\le 2^{2^{d-1}}. \end{aligned}$$

The upper bound (6.5) is immediate, and the theorem then follows in the manner indicated above.

As far as we are aware, Theorem 6.3 provides the first explicit estimate for l_n as n grows. Brauer [14] had shown that $\lim_{n\to\infty}(n-l_n)=\infty$, and previously Hilbert had shown that $l_n \le n-4$ for $n \ge 5$, and $l_n \le n-5$ for $n \ge 9$, and Segre [68] established that $l_n \le n-6$ for $n \ge 157$. While Theorem 6.3 shows that $l_n \le n-d$ for $n \ge 2^{2^{d-2}}$, it would not be surprising if the lower bound on n in the latter could be replaced by a bound polynomial in d.

7. The truth in local fields

Having discussed upper bounds for $v_{d,r}(\mathbb{Q}_p)$ at some length, it seems appropriate next to discuss lower bounds for the latter quantity, and this permits us to recount one of those epic tales in number theory of Homeric dimensions. We take as our starting point a conjecture of Artin dating from 1936 (see Artin [4, p.x]), usually stated in a form equivalent to the following.

Conjecture (Artin). *For any prime p, whenever d and r_i $(1 \le i \le d)$ are integers with $d \ge 2$, one has*

$$V_d^{(0)}(r_d,\dots,r_1;\mathbb{Q}_p) = r_1 + 4r_2 + \cdots + d^2 r_d. \tag{7.1}$$

In particular, one has $v_d(\mathbb{Q}_p) = d^2$.

In order to establish Artin's Conjecture it suffices to show that $v_d(\mathbb{Q}_p) = d^2$ for each d and each prime p; see Lang [37] and Nagata [51] for details. That

$$V_d^{(0)}(r_d,\dots,r_1;\mathbb{Q}_p) \ge r_1 + 4r_2 + \cdots + d^2 r_d$$

follows on considering systems of forms of the shape (2.1) discussed in §2(ii), and so the content of Artin's Conjecture lies in the upper bound implicit in (7.1). The evidence in favour of Artin's Conjecture was always weak, but not inconsequential. The classical theory of quadratic forms shows that $v_2(\mathbb{Q}_p) = 4$ for every prime p (see Hasse [32]). In the middle of this century, Demyanov [26] (when $p \ne 3$) and Lewis [44] tackled cubic forms, showing that for every prime p one has $v_3(\mathbb{Q}_p) = 9$, and subsequently Demyanov [27] considered pairs of quadratic forms, establishing that $v_{2,2}(\mathbb{Q}_p) = 8$ for each prime p (see also the treatment of Birch, Lewis and Murphy [13]). Although Artin's Conjecture has never been established in any other instances, strong evidence in its favour has been derived from a number of partial results. Firstly, it was shown by Birch and Lewis [11] and Laxton and Lewis [40], that when $d = 5$, 7 or 11, there is a positive number $p_0(d)$ with the property that whenever $p > p_0(d)$, one has $v_d(\mathbb{Q}_p) = d^2$. The arguments used to derive these conclusions make essential use of the Lang-Weil theorem (see Lang and Weil [39]), and thus while no explicit estimate for permissible $p_0(d)$ is provided by these authors, there is in principle no barrier to providing such (see Leep and Yeomans [43], where it is shown that $p_0(5) = 43$ is permissible). Moreover, a crucial observation concerning certain factorisations of polynomials dictates that such methods are

successful only when d is a prime number not exceeding 11. Also, it follows from Birch and Lewis [12], together with a correction and refinement of Schuur [67], that $v_{2,3}(\mathbb{Q}_p) = 12$ for $p > 7$.

Given the limitations of the above direct approaches to Artin's Conjecture, it is impressive that Ax and Kochen [5], by employing methods from Mathematical Logic, were able to show that Artin's Conjecture is very nearly true in general.

Theorem 7.1 (Ax and Kochen). *For each natural number d, there is a positive number $p_0(d)$, depending at most on d, with the property that whenever $p > p_0(d)$ one has $v_d(\mathbb{Q}_p) = d^2$. More generally, when d and $r_1, \dots, r_d$ are integers with $d \geq 2$, there is a positive number $p_1 = p_1(r_d, \dots, r_1)$ with the property that whenever $p > p_1$, one has*

$$V_d(r_d, \dots, r_1; \mathbb{Q}_p) = r_1 + 4r_2 + \cdots + d^2 r_d.$$

Unfortunately, the methods of Ax and Kochen do not enable one to calculate explicit estimates for $p_0(d)$ and $p_1(\mathbf{r})$, and this remains a problem of great interest. The best that is known stems from an alternative treatment due to Cohen [19], which shows that $p_0(d)$ is bounded above by some primitive recursive function of the degree d, with a similar conclusion for $p_1(\mathbf{r})$.

The evidence that we have described thus far shows Artin's Conjecture to be "nearly" true. But in 1966, Terjanian [77] exhibited a homogeneous quartic polynomial with integral coefficients in 18 variables, which surprisingly failed to possess a non-trivial 2-adic solution. Since $18 > 4^2$, it follows that Artin's Conjecture fails when $d = 4$. Subsequently, Terjanian [78] showed that $v_4(\mathbb{Q}_2) \geq 20$ using another explicit example (see also Browkin [15]). While this example, and related ones, showed that Artin's Conjecture was not quite true, later work of Arkhipov and Karatsuba [2], motivated by investigations concerning a problem of Hilbert and Kamke, finally laid a torch to the conjecture. In a sharper form derived more or less simultaneously by Arkhipov and Karatsuba [3], Lewis and Montgomery [48] and Brownawell [16], we may reformulate this crushing of Artin's Conjecture as follows.

Theorem 7.2 (Arkhipov and Karatsuba; Lewis and Montgomery; Brownawell). *When d is a natural number and ε is a positive number, write*

$$\psi(d, \varepsilon) = \exp\left(\frac{d}{(\log d)(\log\log d)^{1+\varepsilon}}\right).$$

Then for each prime number p and positive number ε, there are infinitely many natural numbers d such that $v_d(\mathbb{Q}_p) > \psi(d, \varepsilon)$.

In other words, the number of variables required to guarantee p-adic solubility of a homogeneous equation of degree d may need to be exponentially large in terms of d. Thus, in a certain sense, Artin's Conjecture is spectacularly false! A similar conclusion holds in field extensions of $\mathbb{Q}_p$ (see Alemu [1]). An immediate corollary of Theorem 7.2, which we leave as an exercise to the reader, asserts that for each prime p and positive number ε, and for each natural number r, there are infinitely many d such that $v_{d,r}(\mathbb{Q}_p) > r\psi(d, \varepsilon)$. By only a modest elaboration of the techniques of Arkhipov and Karatsuba [3], Lewis and Montgomery [48] and Brownawell [16], one may sharpen the latter bound as follows (see Wooley [84]).

Theorem 7.3 (Wooley). *Let p be a prime number, and define $q = q(p)$ to be 6 when $p = 2$, and to be $p - 1$ when $p > 2$. Further, let $\alpha_p = (\log p)/(6q)$. There exist positive numbers $d_0(\varepsilon)$ and $r_0(d, \varepsilon)$ with the property that for each $\varepsilon > 0$, whenever d is an integer divisible by q with $d > d_0(\varepsilon)$, and $r > r_0(d, \varepsilon)$, then one has $v_{d,r}(\mathbb{Q}_p) > re^{(\alpha_p - \varepsilon)d}$.*

While the lower bound provided by Theorem 7.3 is larger than that following from the earlier methods, the significance of this conclusion lies in the extent to which Artin's Conjecture may now be said to fail. Thus, while the earlier arguments generated bad failures of Artin's Conjecture for a set of exponents d lying in an exponentially thin set, Theorem 7.3 does so for the prime p for all large exponents d divisible by $p - 1$. In particular, bad failures of Artin's Conjecture are essentially ubiquitous, and in particular occur for all large even degrees. A second consequence of the methods used in establishing Theorem 7.3 is a lower bound on the exceptional primes permitted by the Ax-Kochen theorem. For convenience, we abbreviate the notation of Theorem 7.1 by writing $p^*(r_d, d) = p_1(r_d, 0, \dots, 0)$.

Theorem 7.4. *One has $\lim_{D\to\infty} \sup_{1\le d\le D} \sup_{r\in\mathbb{N}} \frac{p^*(r,d)}{d} \ge \frac{1}{30}$.*

Despite the numerous counter-examples to Artin's Conjecture described above, we currently possess none of odd degree. This prompts a conjecture (see Lewis [47]).

Conjecture. *Let p be a prime number. Whenever d is odd and $r_1, r_3, \dots, r_d$ are non-negative integers with $r_d \ge 1$, one has*

$$V_d^{(0)}(r_d, 0, r_{d-2}, 0, \dots, 0, r_3, 0, r_1; \mathbb{Q}_p) = r_1 + 9r_3 + \cdots + d^2 r_d.$$

In particular, one has $v_d(\mathbb{Q}_p) = d^2$.

Some workers believe this conjecture to be more likely for prime exponents d.

8. Concluding remarks on solubility over the p-adic numbers

Despite discussing at length both upper and lower bounds for $v_{d,r}(\mathbb{Q}_p)$, we have neglected a number of topics worthy of investigation. Greater effort has been expended on bounds for $v_{d,r}(\mathbb{Q}_p)$ when d is small. Martin [50], improving on earlier work of Leep [41], has shown that $v_{2,r}(\mathbb{Q}_p) \le 2r^2$ when r is even, and $v_{2,r}(\mathbb{Q}_p) \le 2r^2 + 2$ when r is odd. Also, Schmidt [59], [60], [61] has applied analytic methods to establish that for each natural number r one has $v_{3,r}(\mathbb{Q}_p) \le 5300r(3r + 1)^2$. Notice that the bounds described thus far have all been non-linear in r, and in particular those from §5 take the shape $v_{d,r}(\mathbb{Q}_p) \ll_d r^{2^{d-1}}$ when r is large. This raises the problem of determining the true rate of growth of $v_{d,r}(\mathbb{Q}_p)$ in terms of r. For all we know, the following could be true.

Conjecture. *For each prime p, and each natural number d, one has $v_{d,r}(\mathbb{Q}_p) \ll_d r$.*

Finally, we observe that it would be desirable to know that a given system possesses non-singular p-adic solutions in order to successfully apply the Hardy-Littlewood method in some generality. For example, suppose that a system of

equations has a singular locus of very high dimension, but nonetheless possesses non-singular real and p-adic solutions for every prime p. Then one might hope that a suitable version of the circle method would establish an asymptotic formula for the number of rational points, up to a given height, in a neighbourhood away from the singular points. Unfortunately, the issue of existence of non-singular points is complicated by degeneracy. In any field k, for example, when s and d are natural numbers with $d > 1$, all solutions of the equation $(a_1x_1 + \cdots + a_sx_s)^d = 0$ are singular. Although we have no space to describe such matters herein, the author has made some progress on this problem by showing that given sufficiently many variables in terms of the degree, a form possesses non-singular solutions provided that it is not badly degenerate. We refer the reader to forthcoming work (Wooley [86]) for details.

9. Birch's method

Before discussions of Birch's method begin in earnest, it is useful to record some further notation relevant to systems of forms of odd degree. Let k be a field. When d is an odd number, we abbreviate

$$V_d^{(m)}(r_d, 0, r_{d-2}, 0, \dots, 0, r_3, 0, r_1; k)$$

to

$$w_d^{(m)}(r_d, r_{d-2}, \dots, r_3, r_1; k).$$

Next, when $m \ge 2$, we define $\mathcal{H}_d^{(m)}(r;k)$ to be the set of r-tuples, $(F_1, \dots, F_r)$, of homogeneous polynomials of degree d, with coefficients in k, for which no linearly independent k-rational vectors $\mathbf{e}_1, \dots, \mathbf{e}_m$ exist such that $F_i(t_1\mathbf{e}_1 + \cdots + t_m\mathbf{e}_m)$ is a diagonal form in $t_1, \dots, t_m$ for $1 \le i \le r$. We then define $\tilde{w}_d^{(m)}(r) = \tilde{w}_d^{(m)}(r;k)$ by

$$\tilde{w}_d^{(m)}(r;k) = \sup_{\mathbf{h} \in \mathcal{H}_d^{(m)}(r;k)} \nu(\mathbf{h}).$$

Further, we adopt the convention that $\tilde{w}_d^{(1)}(r;k) = 0$. Note that $\tilde{w}_d^{(m)}(r;k)$ is an increasing function of the arguments m and r. Moreover, when $s > \tilde{w}_d^{(m)}(r;k)$ and $F_1, \dots, F_r$ are homogeneous polynomials of degree d with coefficients in k possessing s variables, then there exist linearly independent k-rational vectors $\mathbf{e}_1, \dots, \mathbf{e}_m$ with the property that $F_i(t_1\mathbf{e}_1 + \cdots + t_m\mathbf{e}_m)$ is a diagonal form in $t_1, \dots, t_m$ for $1 \le i \le r$.

The historical sequence of events leading to the first bounds on $v_{d,r}(\mathbb{Q})$, for odd exponents d, illustrates the diverse nature of the ideas in this area. The interested reader will find a commentary on such matters provided by the editor of volume 4 of Mathematika. It seems that independently, Lewis, Birch and Davenport more or less simultaneously showed that a cubic form with rational coefficients in sufficiently many variables possesses a non-trivial rational solution (it seems that priority runs in the order indicated).

Lewis [46] observed that if $F(\mathbf{x}) \in \mathbb{Q}[x_1, \dots, x_s]$ is a cubic form, then it possesses non-trivial $\mathbb{Q}$-rational zeros provided only that it possesses non-trivial $\mathbb{Q}(\sqrt{-1})$-rational zeros. For suppose that the latter is the case, and that $\boldsymbol{\alpha}$ is a non-trivial

$\mathbb{Q}(\sqrt{-1})$-rational zero. If, under conjugation, this solution remains fixed (considered as a projective point on the hypersurface defined by $F = 0$), then this $\mathbb{Q}(\sqrt{-1})$-rational solution is equivalent to a non-trivial $\mathbb{Q}$-rational one. Otherwise, the two points $\boldsymbol{\alpha}$ and $\overline{\boldsymbol{\alpha}}$ are distinct, and by Bézout's theorem, the line passing through $\boldsymbol{\alpha}$ and $\overline{\boldsymbol{\alpha}}$ intersects the cubic hypersurface at some new point $\boldsymbol{\beta}$. But $\boldsymbol{\beta}$ is fixed under conjugation, so again we have a non-trivial $\mathbb{Q}$-rational zero. However, if s is sufficiently large, then it follows from Peck's theorem (see Peck [52], or Corollary 3 to Theorem 5.3 above) that F possesses a non-trivial $\mathbb{Q}(\sqrt{-1})$-rational zero, and we are done. What is astonishing about this idea of Lewis is that it generalises to show that for any number field K, and given any non-negative integers m and r with $r \geq 1$, one has $v_{3,r}^{(m)}(K) < \infty$. Unfortunately, however, the bounds stemming from such a method are weak, and indeed Lewis did not explicitly calculate a bound even for $v_3(\mathbb{Q})$.

Birch [8] cleverly adapted Brauer's elementary diagonalisation method, which we described in §5, in order to handle quite general systems.

Theorem 9.1 (Birch). *Let k be a field, and suppose that for each odd natural number i with $i \geq 3$ one has $\phi_i(k) < \infty$. Then for each odd natural number d, and for all non-negative integers $r_1, r_3, \dots, r_d$ and m, one has*

$$w_d^{(m)}(r_d, r_{d-2}, \dots, r_3, r_1; k) < \infty.$$

Since when j is odd the bound $\phi_j(k) < \infty$ holds in any algebraic number field k, as a consequence of Siegel's version (Siegel [71], [72]) of the Hardy-Littlewood method, it follows that $w_d^{(m)}(\mathbf{r}; k) < \infty$ for every number field k. Owing to the highly iterated nature of the induction leading to Birch's theorem, however, in general no explicit bounds were available for $w_d^{(m)}(\mathbf{r}; k)$ until very recently. We will discuss such matters further, and sketch a proof of Birch's theorem, later in this section.

Davenport's approach to bounding $v_3(\mathbb{Q})$ was through the use of the Hardy-Littlewood method (see, in particular, Davenport [20]). In a remarkable tour de force which has stimulated much subsequent work, Davenport initially succeeded in establishing that $v_3(\mathbb{Q}) \leq 31$ (see Davenport [20]), subsequently improving this bound first to $v_3(\mathbb{Q}) \leq 28$ (see Davenport [21]), and then $v_3(\mathbb{Q}) \leq 15$ (see Davenport [23]). The latter bound has never been improved, although in view of the local condition implicit in the conclusion $v_3(\mathbb{Q}_p) = 9$ for each prime p, one strongly suspects that $v_3(\mathbb{Q}) = 9$ (see Heath-Brown [33] and Hooley [34], [35], [36] for progress on non-singular cubic forms). In general the circle method is extremely difficult to apply to higher degree forms, although, as the strength of Davenport's bound suggests, a successful treatment should yield impressive consequences.

The solubility of a single cubic form over $\mathbb{Q}$ is the simplest problem along these lines to consider, and regrettably our knowledge extends hardly any further than this. Pleasants [54] has shown that in any number field K one has $v_3(K) \leq 15$ (see also Ramanujam [55] and Ryavec [57] for earlier results, and Skinner [73] for non-singular cubic forms). Schmidt [62] has studied systems of cubic forms via an impressive technical development of Davenport's methods. In particular, Schmidt

obtains the bound $v_{3,2}(\mathbb{Q}) \leq 5139$, and in general he shows that $v_{3,r}(\mathbb{Q}) \leq (10r)^5$. In an interesting twist of fate, the emergence of Birch's quite general methods (Birch [8]) seems to have obscured Lewis' work [46] of the same time. In any case, by employing the latter's ideas, the author (Wooley [82]) has shown that in any algebraic extension K of $\mathbb{Q}$ (possibly $\mathbb{Q}$ itself), one has $v_{3,2}(K) \leq 855$. Finally, Schmidt [65] has shown that as a consequence of the precise version of his Theorem 3.4 above, one may obtain a bound of the shape

$$v_{5,r}(\mathbb{Q}) < A \exp(\exp(Br)), \tag{9.1}$$

for suitable positive constants A and B.

Recently the author (Wooley [83], [85]) found that a rather efficient diagonalisation procedure could be engineered by exploiting ideas of Lewis and Schulze-Pillot [49]. So far as estimates for $v_{3,r}(\mathbb{Q})$ are concerned, this refinement of Birch's method yields weaker conclusions than those obtained by Schmidt [62]. However, the methods can be employed in any field k for which bounds are available for $\phi_{3,r}(k)$. Since a simple argument shows that for each natural number r one has $\phi_{3,r}(k) + 1 \leq (\phi_3(k) + 1)^r$ (see, for example, the argument of the proof of Lemma 10.4 below), it suffices simply to have an upper bound for $\phi_3(k)$.

Theorem 9.2 (Wooley). *Let k be a field, let m and r be non-negative integers with $r \geq 1$, and suppose that $\phi_{3,r}(k)$ is finite. Then*

$$v_{3,r}^{(m)}(k) \leq r^3(m+1)^5(\phi_{3,r}(k)+1)^5.$$

In particular, one has $v_{3,r}^{(m)}(k) \leq r^3(m+1)^5(\phi_3(k)+1)^{5r}$.

The methods described in Wooley [83] are already more effective than those available hitherto for systems of quintic forms. Thus the bound (9.1) due to Schmidt [65] may be improved as follows.

Theorem 9.3 (Wooley). *Let m and r be non-negative integers with $r \geq 1$. Then*

$$v_{5,r}^{(m)}(\mathbb{Q}) < \exp\left(10^{32}((m+1)r\log(3r))^{\kappa}\log(3r(m+1))\right),$$

where $\kappa = \frac{\log 3430}{\log 4} = 5.87199\ldots$. In particular, $v_{5,r}(\mathbb{Q}) = o(e^{r^6})$.

For systems of forms of degree higher than 5, the bounds provided by the methods of Wooley [83], [85] are embarrassingly weak, but currently such are the only explicit bounds available in Birch's theorem. In order to describe these bounds we will require some notation. Suppose that A is a subset of $\mathbb{R}$ and Ψ is a function mapping A into A. When α is a real number, write $[\alpha]$ for the largest integer not exceeding α. Then we adopt the notation that whenever x and y are real numbers with $x \geq 1$, then $\Psi_x(y)$ denotes the real number $a_{[x]}$, were $(a_n)_{n=1}^{\infty}$ is the sequence defined by taking $a_1 = \Psi(y)$, and $a_{i+1} = \Psi(a_i)$ $(i \geq 1)$. Finally, when n is a non-negative integer we define the functions $\psi^{(n)}(x)$ by taking $\psi^{(0)}(x) = \exp(x)$, and when $n > 0$ by putting

$$\psi^{(n)}(x) = \psi_{42\log x}^{(n-1)}(x). \tag{9.2}$$

Theorem 9.4 (Wooley). *Let d be an odd integer exceeding 5, and let r and m be non-negative integers with $r \ge 1$. Then*

$$v_{d,r}^{(m)}(\mathbb{Q}) < \psi^{((d-5)/2)}(dr(m+1)).$$

More generally, when $r_1, r_3, \dots, r_d$ are non-negative integers with $r_d \ge 1$, one has

$$w_d^{(m)}(r_d, \dots, r_1; \mathbb{Q}) \le \psi^{((d-5)/2)}(d(r_1 + r_3 + \cdots + r_d)(m+1)).$$

We note that the number 42 occurring in the definition (9.2) could certainly be reduced with greater effort, especially for large values of the parameters d, r and $m+1$. However, the level of iteration involved in the function $\psi^{(n)}$ seems difficult to improve, and in particular present methods seem unable to reduce the function $\log x$ in (9.2) with any function of significantly smaller rate of growth.

We now sketch the basic ideas underlying the proof of Birch's theorem (Theorem 9.1). Suppose that $w_D^{(M)}(\mathbf{r}; k) < \infty$ for each odd D with $D < d$, and for every $\mathbf{r}$ and m. In broad outline we follow the strategy for establishing Brauer's theorem as sketched in §5. In particular, it suffices to bound $v_d^{(m)}(k)$ for odd exponents d, and such is possible provided that $\tilde{w}_d^{(m)}(1; k) < \infty$ for each natural number m. We establish the latter bound by induction on m, noting trivially that $\tilde{w}_d^{(1)}(1; k) = 0$. Suppose then that $m \ge 1$ and that $\tilde{w}_d^{(m)}(1; k)$ is finite, and write $n = \tilde{w}_d^{(m)}(1; k)$. We take q to be a natural number sufficiently large in terms of d, n and k, and we take p to be a natural number sufficiently large in terms of d, n, q and k. Let $s = p + q$, and consider a linear subspace U of k^s of affine dimension p. We take V to be the complementary linear space of affine dimension q, so that $k^s = U \oplus V$. Let $\mathbf{v}_1, \dots, \mathbf{v}_q$ be a k-rational basis for V, and consider an arbitrary element $\mathbf{v} = c_1\mathbf{v}_1 + \cdots + c_q\mathbf{v}_q$ of V. Also, let $\mathbf{u}$ be an arbitrary element of U, and consider a form $F(\mathbf{x}) \in k[x_1, \dots, x_s]$ of odd degree d. Then for every $t, w \in k$,

$$F(t\mathbf{u} + w\mathbf{v}) = t^d F(\mathbf{u}) + w^d F(\mathbf{v}) + \sum_{\substack{i=1 \\ i \text{ odd}}}^{d-1} t^i w^{d-i} G_i(\mathbf{u}, \mathbf{v}) + \sum_{\substack{j=1 \\ j \text{ even}}}^{d-1} t^j w^{d-j} H_j(\mathbf{u}, \mathbf{v}), \tag{9.3}$$

where $G_i(\mathbf{u}, \mathbf{v}) \in k[\mathbf{u}, \mathbf{v}]$ is a homogeneous polynomial of odd degree i in $\mathbf{u}$ and even degree $d-i$ in $\mathbf{v}$ ($i = 1, 3, \dots, d-2$), and $H_j(\mathbf{u}, \mathbf{v}) \in k[\mathbf{u}, \mathbf{v}]$ is a homogeneous polynomial of odd degree $d-j$ in $\mathbf{v}$ and even degree j in $\mathbf{u}$ ($j = 2, 4, \dots, d-1$). On examining the coefficient of each term $c_1^{i_1} \dots c_q^{i_q}$ in (9.3), we find that the system of equations

$$G_i(\mathbf{u}, \mathbf{v}) = 0 \quad (i = 1, 3, \dots, d-2) \tag{9.4}$$

is satisfied for every $\mathbf{v} \in V$ provided only that a certain system of equations in $\mathbf{u}$ is satisfied. The latter system consists of homogeneous equations of odd degree at

most $d-2$, say r_j of degree j ($j = 1, 3, \dots, d-2$), with r_j bounded in terms of d and q for each j. Since we may suppose that $\dim(U) = p > w^{(0)}_{d-2}(\mathbf{r}; k)$, it follows that the system (9.4) is satisfied for every $\mathbf{v} \in V$ for some fixed non-trivial $\mathbf{u} \in U$. Consider next the system of equations

$$H_j(\mathbf{u}, \mathbf{v}) = 0 \quad (j = 2, 4, \dots, d-1). \tag{9.5}$$

Since $\mathbf{u}$ is now fixed, this is a system of equations of odd degree at most $d-2$ in $\mathbf{v}$, say with r'_j equations of degree j ($j = 1, 3, \dots, d-2$). Since we may suppose that $\dim(V) = q > w^{(n)}_{d-2}(\mathbf{r}'; k)$, it follows that the system (9.5) possesses a k-rational linear space of solutions of affine dimension $n+1 > \tilde{w}^{(m)}_d(1; k)$. But for each solution $\mathbf{v}$ lying in the latter linear space one has, for each $t, w \in k$, that $F(t\mathbf{u} + w\mathbf{v}) = t^d F(\mathbf{u}) + w^d F(\mathbf{v})$, and so it follows that the polynomial $F(\mathbf{x})$ may be reduced non-trivially to a diagonal form in at least $m+1$ variables, whence $\tilde{w}^{(m+1)}_d(1; k) < s < \infty$. Thus it follows that whenever both $\tilde{w}^{(m)}_d(1; k)$ and $w^{(M)}_{d-2}(\mathbf{r}; k)$ are finite, for each M and $\mathbf{r}$, then one has that $\tilde{w}^{(m+1)}_d(1; k)$ is finite. Our claim that $\tilde{w}^{(m)}_d(1; k) < \infty$ for each m therefore follows by induction.

We conclude by remarking that the above strategy may be improved, firstly by diagonalising a whole system of equations simultaneously, removing one of the unpleasant iterated steps suppressed above. Also, and this is an idea whose origins lie in work of Lewis and Schulze-Pillot [49], one may diagonalise in such a way that rather than iterating from $\tilde{w}^{(m)}_d(1; k)$ to $\tilde{w}^{(m+1)}_d(1; k)$, as sketched above, one may instead iterate from $\tilde{w}^{(m)}_d(1; k)$ to $\tilde{w}^{(2m)}_d(1; k)$. Such a procedure plainly has the potential to dramatically accelerate the diagonalisation process, and it is this idea which underlies the work of Wooley [83], [85] described above.

10. Birch's Theorem in algebraic number fields

The only major obstruction to establishing a strong analogue of Theorem 9.4 in algebraic number fields lies in our lack of knowledge concerning the solubility of simultaneous additive equations. Thus, while the bound

$$\phi_{d,r}(\mathbb{Q}) + 1 \leq 48rd^3 \log(3rd^2) \tag{10.1}$$

due to Brüdern and Cook [17], or earlier bounds due to Davenport and Lewis [25], provide a suitable foundation for Birch's method over $\mathbb{Q}$, we have no strong analogue of the bound (10.1) when the field $\mathbb{Q}$ is replaced by an algebraic number field. Thus, while there is no difficulty in principle to establishing such bounds, the significant quantity of work required to establish suitable estimates has thus far deterred detailed investigations. Such difficulties, moreover, are compounded when one is interested in bounds independent of the degree of the field extension. Since there appears to be some interest in this topic, we take the opportunity herein to conclude our discussion of diophantine problems in many variables by establishing an explicit version of Birch's theorem in algebraic number fields, albeit a weak one.

We begin by recalling some technical lemmata from Wooley [83], starting with a lemma which provides information concerning the number of variables required to diagonalise a system of forms. In what follows, we denote by k an arbitrary field.

Lemma 10.1. *Let d be an odd integer with $d \geq 3$, and let r, n and m be natural numbers. Then*

$$\tilde{w}_d^{(n+m)}(r;k) \leq s + w_{d-2}^{(M)}(\mathbf{R};k),$$

where

$$M = \tilde{w}_d^{(n)}(r;k), \quad s = 1 + w_{d-2}^{(N)}(\mathbf{S};k), \quad N = \tilde{w}_d^{(m)}(r;k),$$

and for $0 \leq u \leq (d-1)/2$,

$$R_{2u+1} = r\binom{s+d-2u-2}{d-2u-1} \quad \text{and} \quad S_{2u+1} = r\binom{n+d-2u-2}{d-2u-1}.$$

Proof. This is Lemma 2.1 of Wooley [83].

We next bound $v_{d,r}^{(m)}(k)$ in terms of $\tilde{w}_d^{(M)}(r;k)$.

Lemma 10.2. *Let d be an odd positive number, let r be a natural number, and let m be a non-negative integer. Then*

$$v_{d,r}^{(m)}(k) \leq \tilde{w}_d^{(M)}(r;k),$$

where $M = (m+1)(\phi_{d,r}(k)+1)$.

Proof. This is Lemma 2.2 of Wooley [83].

Finally, we provide a bound for $w_d^{(m)}(\mathbf{r};k)$ in terms of the quantities $w_{d-2}^{(M)}(\mathbf{r};k)$ and $v_{d,r}^{(m)}(k)$.

Lemma 10.3. *Let $d \geq 3$ be an odd positive number, and let $r_1, r_3, \dots, r_d$ be non-negative integers with $r_d > 0$. Then for each non-negative integer m one has*

$$w_d^{(m)}(r_d, r_{d-2}, \dots, r_1;k) \leq w_{d-2}^{(M)}(r_{d-2}, \dots, r_1;k),$$

where $M = v_{d,r_d}^{(m)}(k)$.

Proof. This is Lemma 2.3 of Wooley [83].

Henceforth we restrict attention to a fixed algebraic extension K of $\mathbb{Q}$, not necessarily of finite degree, and for the sake of concision, when it is convenient so to do, we drop explicit mention of this field from our various notations. In order to make use of Lemma 10.2 in our argument we require an estimate for $\phi_{d,r}(K)$, and here we are interested in simple estimates independent of K. The problem of bounding $\phi_{d,r}(K)$ is substantially more difficult, in general, than that of bounding $\phi_{d,r}(\mathbb{Q})$, in large part because the local solubility problem for systems of forms over K may be significantly more complicated than the corresponding problem over $\mathbb{Q}$. We circumvent such issues by employing only estimates of simple type depending on our knowledge of $\phi_d(K)$.

Lemma 10.4. *Let d be an odd positive number with $d \geq 3$, and let r be a natural number. Then one has $\phi_{d,r}(K) + 1 \leq e^{2dr}$.*

Proof. We consider the algebraic extension K of $\mathbb{Q}$. Let $s \geq 2^d + 1$, and suppose that $b_1, \dots, b_s \in K$. Note first that there is a finite extension L of $\mathbb{Q}$ with the property that $b_1, \dots, b_s \in L$, and moreover that whenever the equation

$$b_1 x_1^d + \cdots + b_s x_s^d = 0 \tag{10.2}$$

possesses a non-trivial solution in L, then it does so also in K. Next we recall that by using Siegel's version of the circle method (see Siegel [71], [72]), Birch [9, Theorem 3] was able to show that whenever $s > 2^d$, the equation (10.2) has a non-trivial solution in L provided that it has a non-trivial solution in every real and $\mathfrak{p}$-adic completion of L. The condition that the equation (10.2) be soluble in the real completion of L is, of course, trivially satisfied when that completion is $\mathbb{C}$. When that completion is $\mathbb{R}$, meanwhile, the equation (10.2) has a non-trivial solution in the real completion of L whenever d is odd. On the other hand, when M is a finite extension of $\mathbb{Q}_p$ and d is an integer with $d \geq 2$, it follows from Skinner [74] that

$$\phi_d(M) \leq d\left((d+1)^{\max\{2\log d/\log p, 1\}} - 1\right).$$

Consequently, when d is odd the equation (10.2) is soluble non-trivially over L, and hence also over K, provided only that

$$s > \max\{2^d, d((d+1)^{\max\{2\log d/\log p, 1\}} - 1)\}. \tag{10.3}$$

The simple bound $\phi_d(K) + 1 \leq e^{2d}$ follows from (10.3) with a modicum of computation.

Next suppose that $r > 1$, and write $m = \phi_{d,r-1}(K)$. Suppose that $s \geq (m+1)(\phi_d(K)+1)$, and consider elements $b_{ij} \in K$ $(1 \leq i \leq r,\ 1 \leq j \leq s)$, and the system of equations

$$\sum_{j=1}^{s} b_{ij} x_j^d = 0 \quad (1 \leq i \leq r). \tag{10.4}$$

Since $m + 1 > \phi_{d,r-1}(K)$, it follows that each of the systems

$$\sum_{j=t(m+1)+1}^{(t+1)(m+1)} b_{ij} x_j^d = 0 \quad (2 \leq i \leq r)$$

has a solution $\mathbf{x} = (a_{t(m+1)+1}, \dots, a_{(t+1)(m+1)}) \in K^{m+1} \setminus \{\mathbf{0}\}$ for $0 \leq t \leq \phi_d(K)$. On substituting

$$x_{t(m+1)+j} = a_{t(m+1)+j} y_t \quad (1 \leq j \leq m+1,\ 0 \leq t \leq \phi_d(K)),$$

we find that the system (10.4) is soluble provided that there is a non-trivial K-rational solution to the equation

$$c_0 y_0^d + \cdots + c_T y_T^d = 0, \tag{10.5}$$

where $T = \phi_d(K)$, and

$$c_t = \sum_{j=t(m+1)+1}^{(t+1)(m+1)} b_{1j} a_{t(m+1)+j}^d \quad (0 \le t \le \phi_d(K)).$$

But $T + 1 > \phi_d(K)$, and so the equation (10.5) does indeed possess a non-trivial K-rational solution. We therefore conclude that whenever $r > 1$, one has

$$\phi_{d,r}(K) + 1 \le (\phi_{d,r-1}(K) + 1)(\phi_d(K) + 1),$$

and hence by induction one obtains $\phi_{d,r}(K) + 1 \le (\phi_d(K) + 1)^r$. On recalling the conclusion of the previous paragraph, we therefore conclude that $\phi_{d,r}(K)+1 \le e^{2dr}$. This completes the proof of the lemma.

Having negotiated the preliminaries, we begin the main body of our investigation, and make no apology for following closely the argument of Wooley [85]. We start with bounds for $v_{3,r}(K)$ and $v_{5,r}(K)$, the former quantity being bounded easily by means of Theorem 9.2 above.

Theorem 10.5. *Let m and r be non-negative integers with $r \ge 1$. Then one has*

$$v_{3,r}^{(m)}(K) \le (m+1)^5 r^3 3^{10r}.$$

Proof. Since it is readily available from the literature, we make use of a sharper bound for $\phi_{3,r}(K)$ than is immediately available from Lemma 10.4. By Lewis [45], it follows that for any algebraic extension K_p of $\mathbb{Q}_p$, one has $\phi_3(K_p) \le 6$. Consequently, the argument of the proof of Lemma 10.4 shows that

$$\phi_3(K) + 1 \le \max\{7, 2^3 + 1\} = 9,$$

whence $\phi_{3,r}(K) + 1 \le 9^r$. On substituting the latter bound into the conclusion of Theorem 9.2, the desired conclusion is immediate.

We require a simplification of Theorem 10.5 of use in our main inductive process, and for this purpose the following lemma suffices.

Lemma 10.6. *Suppose that r_3, r_1 and m are non-negative integers with $r_1 < 3r_3^2$. Then*

$$w_3^{(m)}(r_3, r_1; K) < \exp(21 r_3 (m+1)).$$

Proof. Whenever $r_1 < 3r_3^2$, one finds by elimination of the implicit linear equations that

$$w_3^{(m)}(r_3, r_1) = r_1 + v_{3,r_3}^{(m)} < 3r_3^2 + (m+1)^5 r_3^3 3^{10r_3},$$

and a modest calculation therefore leads to the desired conclusion.

We must now dispose of systems of quintic forms, beginning with the diagonalisation process.

Lemma 10.7. *Suppose that m and r are natural numbers. Then*

$$\tilde{w}_5^{(m)}(r;K) < \exp_{5\log(5m)}(5rm).$$

Proof. When m and r are natural numbers, write

$$\overline{w}_5^{(m)}(r) = \exp_{5\log(5m)}(5rm). \tag{10.6}$$

We aim to show that for each R and M one has

$$\tilde{w}_5^{(M)}(R) < \overline{w}_5^{(M)}(R), \tag{10.7}$$

and from this the conclusion of the lemma is immediate. Note that by definition, for each natural number R one has $\tilde{w}_5^{(1)}(R) = 0$, so that (10.7) certainly holds when $M = 1$. Next suppose that $m > 1$, and that for each R the inequality (10.7) holds whenever $M < m$. We will establish that (10.7) holds for each R when $M = m$, whence (10.7) follows for all R and M by induction.

Let m and r be natual numbers with $m \geq 2$. Write $n = [(m+1)/2]$, and note that $n < m$. By Lemma 10.1 one has

$$\tilde{w}_5^{(m)}(r) \leq \tilde{w}_5^{(2n)}(r) \leq s + w_3^{(N)}(\mathbf{R}), \tag{10.8}$$

where

$$N = \tilde{w}_5^{(n)}(r), \quad s = 1 + w_3^{(N)}(\mathbf{S}), \tag{10.9}$$

and for $0 \leq u \leq 2$,

$$R_{2u+1} = r\binom{s+3-2u}{4-2u} \quad \text{and} \quad S_{2u+1} = r\binom{n+3-2u}{4-2u}.$$

We first bound s. Write $\overline{N} = [\overline{w}_5^{(n)}(r)]$, and note that since $n < m$, the inductive hypothesis shows that $N \leq \overline{N}$. Note also that for $0 \leq u \leq 2$ one has $S_{2u+1} \leq rn^{4-2u}$. Then the hypotheses required for the application of Lemma 10.6 to bound $w_3^{(\overline{N})}(\mathbf{S})$ are satisfied, and we may conclude from (10.9) that

$$s \leq 1 + w_3^{(\overline{N})}(rn^2, rn^4) \leq w_3^{(\overline{N})}(rn^2, 2rn^4),$$

whence

$$s < \exp(21rn^2(\overline{N}+1)). \tag{10.10}$$

But by (10.6) one has

$$\overline{N} \leq \overline{w}_5^{(n)}(r) = \exp_{5\log(5n)}(5rn) \tag{10.11}$$

and

$$\overline{N} = [\exp_{5\log(5n)}(5rn)] \geq 5rn. \tag{10.12}$$

Also, plainly, for each $m \geq 2$ it follows from (10.6) that $\overline{N} \geq \exp_5(5)$. Then by combining (10.10) and (10.12), we obtain

$$s \leq \exp((\overline{N}+1)^3) < \exp(\overline{N}^4). \tag{10.13}$$

Finally we bound $\tilde{w}_5^{(m)}(r)$ by substituting (10.13) into (10.8). Note that for $0 \leq u \leq 2$ one has $R_{2u+1} \leq rs^{4-2u}$. Then the hypotheses required for the application of Lemma 10.6 to bound $w_3^{(\overline{N})}(\mathbf{R})$ are satisfied, and we may conclude that

$$\tilde{w}_5^{(m)}(r) \leq s + w_3^{(\overline{N})}(rs^2, rs^4) \leq w_3^{(\overline{N})}(rs^2, 2rs^4),$$

whence

$$\tilde{w}_5^{(m)}(r) < \exp(21rs^2(\overline{N}+1)).$$

Write $\overline{s} = \exp(\overline{N}^4)$. Then by (10.12) and (10.13), one has

$$\tilde{w}_5^{(m)}(r) < \exp((s(\overline{N}+1))^3) \leq \exp(\overline{s}^6) = \exp_2(6\overline{N}^4) < \exp_2(\overline{N}^5).$$

We therefore deduce from (10.11) that

$$\tilde{w}_5^{(m)}(r) < \exp_3(5\log \overline{N}) < \exp_3(\exp_{5\log(5n)-1}(5rm)).$$

But on noting that whenever $m \geq 2$ one has

$$\left[5\log\left(5\left[\frac{m+1}{2}\right]\right)\right] \leq [5\log(5m) - 2],$$

we may conclude from (10.6) that

$$\tilde{w}_5^{(m)}(r) < \exp_{5\log(5m)}(5rm) = \overline{w}_5^{(m)}(r),$$

thereby establishing the inequality (10.7) with $M = m$ and $R = r$. Thus, on recalling the comments concluding the first paragraph of the proof, the proof of the lemma is complete.

A bound for $v_{5,r}^{(m)}(K)$ follows on substituting the conclusion of Lemma 10.7 into Lemma 10.2.

Theorem 10.8. *Suppose that m and r are non-negative integers with $r \geq 1$. Then*

$$v_{5,r}^{(m)}(K) < \exp_{67r(m+1)}(5r(m+1)).$$

Proof. By combining Lemmata 10.2 and 10.4 with Lemma 10.7, one obtains

$$v_{5,r}^{(m)}(K) < \exp_{5\log(5M)}(5rM), \tag{10.14}$$

where $M = (m+1)e^{10r}$. But a little calculation reveals that

$$\log(5M) < \log(5\exp(10r + (m+1))) < 13r(m+1),$$

and

$$\log(5rM) < 10r + \log(5r(m+1)) < \exp(5r(m+1)),$$

and hence (10.14) provides the estimate

$$v_{5,r}^{(m)} < \exp_{65r(m+1)+2}(5r(m+1)).$$

The conclusion of the lemma follows immediately.

We will require a slightly more general conclusion within our main induction.

Lemma 10.9. *Suppose that r_1, r_3, r_5 and m are non-negative integers with $r_1 \le 3r_3^2$ and $r_3 < 3r_5^2$. Then*

$$w_5^{(m)}(r_5, r_3, r_1) < \exp_{69r_5(m+1)}(5r_5(m+1)).$$

Proof. By Lemma 10.3 one has $w_5^{(m)}(\mathbf{r}) \le w_3^{(v)}(r_3, r_1)$, where $v = v_{5,r_5}^{(m)}$. But in view of the hypotheses concerning r_1 and r_3, we may apply Lemma 10.6 together with Theorem 10.8 to conclude that

$$\log w_5^{(m)}(\mathbf{r}) < 63r_5^2 \left(1 + \exp_{67r_5(m+1)}(5r_5(m+1))\right),$$

whence

$$\log_2 w_5^{(m)}(\mathbf{r}) < \exp_{67r_5(m+1)}(5r_5(m+1)).$$

The desired conclusion is essentially immediate from the latter inequality.

We have now established the basis for our induction. In order to establish the main inductive step, we require some further notation. We say that the function $\Psi : [1, \infty) \to [1, \infty)$ satisfies the exponential growth condition if it has derivatives of all orders on $[1, \infty)$, and moreover for each non-negative integer n, one has for each $x \in [1, \infty)$ that

$$\frac{d^n \Psi(x)}{dx^n} \ge e^x.$$

When D is an integer exceeding 3, we make use of the following hypothesis.

Hypothesis $\mathcal{H}_D(\Psi)$. *For all natural numbers M, and all $\frac{1}{2}(D+1)$-tuples $\mathbf{R} = (R_D, R_{D-2}, \dots, R_1)$ of non-negative integers satisfying $R_{D-2} < 3R_D^2$ and $R_i \le 3R_{i+2}^2$ $(i = 1, 3, \dots, D-4)$, one has*

$$w_D^{(M)}(\mathbf{R}) < \Psi(DR_D(M+1)). \tag{10.15}$$

Fortunately, the diagonalisation process is largely independent of the ambient field under consideration.

Lemma 10.10. *Let d be an odd integer exceeding 5. Suppose that Ψ is a function satisfying the exponential growth condition, and suppose further that the hypothesis $\mathcal{H}_{d-2}(\Psi)$ holds. Then whenever m and r are natural numbers, one has*

$$\tilde{w}_d^{(m)}(r) < \Psi_{5\log(dm)}(drm).$$

Proof. This is essentially Lemma 4.1 of Wooley [85].

On combining Lemma 10.10 with Lemma 10.2, we are able to bound $v_{d,r}^{(m)}(K)$ on the hypothesis $\mathcal{H}_{d-2}(\Psi)$.

Lemma 10.11. *Let d be an odd integer exceeding 5. Suppose that Ψ is a function satisfying the exponential growth condition, and suppose further that the hypothesis $\mathcal{H}_{d-2}(\Psi)$ holds. Then whenever m and r are non-negative integers with $r \geq 1$, one has*

$$v_{d,r}^{(m)}(K) < \Psi_{16dr(m+1)}(dr(m+1)).$$

Proof. On combining Lemmata 10.2 and 10.4 with Lemma 10.10, one obtains

$$v_{d,r}^{(m)}(K) < \Psi_{5\log(dM)}(drM), \tag{10.16}$$

where $M = (m+1)e^{2dr}$. But a modicum of computation reveals that

$$\log(dM) = 2dr + \log(d(m+1)) < 3dr(m+1),$$

and

$$\log(drM) = 2dr + \log(dr(m+1)) < 3dr(m+1) < \exp(dr(m+1)),$$

and hence (10.16) leads to the upper bound

$$v_{d,r}^{(m)}(K) < \Psi_{15dr(m+1)+2}(dr(m+1)).$$

The conclusion of the lemma follows immediately.

In order to complete the main inductive step we must combine the conclusion of Lemma 10.11 with the hypothesis $\mathcal{H}_{d-2}(\Psi)$ in order to bound $w_d^{(m)}(\mathbf{r}; K)$.

Lemma 10.12. *Let d be an odd integer exceeding 5. Suppose that Ψ is a function satisfying the exponential growth condition, and suppose further that the hypothesis $\mathcal{H}_{d-2}(\Psi)$ holds. Then whenever r_{2u+1} $(0 \leq u \leq \frac{1}{2}(d-1))$ and m are non-negative integers with $r_i \leq 3r_{i+2}^2$ $(i = 1, 3, \dots, d-4)$ and $r_{d-2} < 3r_d^2$, one has*

$$w_d^{(m)}(\mathbf{r}; K) < \Psi_{17dr_d(m+1)}(dr_d(m+1)).$$

Proof. By Lemma 10.3 one has

$$w_d^{(m)}(\mathbf{r}) \leq w_{d-2}^{(v)}(r_{d-2}, \dots, r_1),$$

where $v = v_{d,r_d}^{(m)}$. The hypotheses concerning r_i for $i = 1, 3, \dots, d-2$ permit us the use of the hypothesis $\mathcal{H}_{d-2}(\Psi)$ in order to bound the quantity $w_{d-2}^{(v)}(r_{d-2}, \dots, r_1)$, and thus on employing Lemma 10.11 to bound v, we deduce that

$$\begin{aligned} w_{d-2}^{(v)}(r_{d-2}, \dots, r_1) &< \Psi(3(d-2)r_d^2(v+1)) \\ &< \Psi_2(2\Psi_{16dr_d(m+1)-1}(dr_d(m+1))) \\ &\leq \Psi_{16dr_d(m+1)+2}(dr_d(m+1)). \end{aligned}$$

The conclusion of the lemma is now immediate.

We have now reached the crescendo of our argument, and this demands further notation. We define the functions $\phi^{(n)}(x)$ by taking $\phi^{(0)}(x) = \exp(x)$, and when $n > 0$ by putting

$$\phi^{(n)}(x) = \phi_{17x}^{(n-1)}(x). \tag{10.17}$$

Theorem 10.13. *Let K be an algebraic extension of $\mathbb{Q}$, let d be an odd integer exceeding 3, and let r and m be non-negative integers with $r \geq 1$. Then*

$$v_{d,r}^{(m)}(K) < \phi^{((d-3)/2)}(dr(m+1)).$$

Proof. The conclusion of the theorem is immediate when $d = 5$, in view of Theorem 10.8. Note next that by Lemma 10.9, the hypothesis $\mathcal{H}_5(\phi^{(1)})$ holds, where $\phi^{(1)}$ is defined by (10.17). Moreover $\phi^{(1)}$ plainly satisfies the exponential growth condition. Suppose now that d is an odd integer exceeding 5, and that the hypothesis $\mathcal{H}_{d-2}(\phi^{((d-5)/2)})$ holds. Since plainly $\phi^{((d-5)/2)}$ also satisfies the exponential growth condition, it follows from Lemma 10.12 that the hypothesis $\mathcal{H}_d(\phi^{((d-3)/2)})$ holds. We therefore deduce, by induction, that the hypothesis $\mathcal{H}_d(\phi^{((d-3)/2)})$ holds for every odd integer d exceeding 3. Consequently, on applying Lemma 10.11, we conclude that the inequality

$$v_{d,r}^{(m)}(K) < \phi_{16dr(m+1)}^{((d-5)/2)}(dr(m+1)) < \phi^{((d-3)/2)}(dr(m+1))$$

holds for every odd integer exceeding 3. This completes the proof of the theorem.

References

1. Y. Alemu, *On zeros of forms over local fields*, Acta Arith. **65** (1985), 163–171.
2. G. I. Arkhipov and A. A. Karatsuba, *Local representation of zero by a form*, Izv. Akad. Nauk SSSR Ser. Mat. **45** (1981), 948–961. (Russian)
3. G. I. Arkhipov and A. A. Karatsuba, *A problem of comparison theory*, Uspekhi Mat. Nauk **37** (1982), 161–162. (Russian)
4. E. Artin, *The collected papers of Emil Artin*, Addison-Wesley, 1965.
5. J. Ax and S. Kochen, *Diophantine problems over local fields, I*, Amer. J. Math. **87** (1965), 605–630.
6. R. C. Baker, *Diophantine inequalities*, Clarendon Press, Oxford, 1986.
7. V. Batyrev and Yu. Manin, *Sur le nombre des points rationnels de hauteur bornée des variétés algébriques*, Math. Ann. **286** (1990), 27–43.
8. B. J. Birch, *Homogeneous forms of odd degree in a large number of variables*, Mathematika **4** (1957), 102–105.
9. B. J. Birch, *Waring's problem in algebraic number fields*, Proc. Cambridge Philos. Soc. **57** (1961), 449–459.
10. B. J. Birch, *Forms in many variables*, Proc. Roy. Soc. Ser. A **265** (1961), 245–263.
11. B. J. Birch and D. J. Lewis, $\mathfrak{p}$*-adic forms*, J. Indian Math. Soc. **23** (1959), 11–31.
12. B. J. Birch and D. J. Lewis, *Systems of three quadratic forms*, Acta Arith. **10** (1965), 423–442.
13. B. J. Birch, D. J. Lewis and T. G. Murphy, *Simultaneous quadratic forms*, Amer. J. Math. **84** (1962), 110–115.
14. R. Brauer, *A note on systems of homogeneous algebraic equations*, Bull. Amer. Math. Soc. **51** (1945), 749–755.
15. J. Browkin, *On forms over p-adic fields*, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. **14** (1966), 489–492.
16. W. D. Brownawell, *On p-adic zeros of forms*, J. Number Theory **18** (1984), 342–349.
17. J. Brüdern and R. J. Cook, *On simultaneous diagonal equations and inequalities*, Acta Arith. **62** (1992), 125–149.
18. J. W. S. Cassels and M. J. T. Guy, *On the Hasse principle for cubic surfaces*, Mathematika **13** (1966), 111–120.

19. P. J. Cohen, *Decision procedures for real and p-adic fields*, Comm. Pure Appl. Math. **22** (1969), 131–151.
20. H. Davenport, *Cubic forms in thirty-two variables*, Philos. Trans. Roy. Soc. London Ser. A **251** (1959), 193–232.
21. H. Davenport, *Cubic forms in* 29 *variables*, Proc. Roy. Soc. Ser. A **266** (1962), 287–298.
22. H. Davenport, *Analytic methods for Diophantine equations and Diophantine inequalities*, Ann Arbor Publishers, Ann Arbor, 1962.
23. H. Davenport, *Cubic forms in* 16 *variables*, Proc. Roy. Soc. Ser. A **272** (1963), 285–303.
24. H. Davenport and D. J. Lewis, *Homogeneous additive equations*, Proc. Roy. Soc. Ser. A **274** (1963), 443–460.
25. H. Davenport and D. J. Lewis, *Simultaneous equations of additive type*, Philos. Trans. Roy. Soc. London Ser. A **264** (1969), 557–595.
26. V. B. Dem'yanov, *On cubic forms in discretely normed fields*, Dokl. Akad. Nauk SSSR **74** (1950), 889–891. (Russian)
27. V. B. Dem'yanov, *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. (Russian)
28. W. Duke, Z. Rudnick and P. Sarnak, *Density of integer points on affine homogeneous varieties*, Duke. Math. J. **71** (1993), 143–179.
29. G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpen*, Invent. Math. **73** (1983), 349–366.
30. D. J. H. Garling, *A course in Galois theory*, Cambridge University Press, Cambridge-New York, 1986.
31. M. J. Greenberg, *Lectures on forms in many variables*, W. A. Benjamin and Co., New York, 1969.
32. H. Hasse, *Über die Darstellbarkeit von Zahlen durch quadratische Formen in Körper der rationalen Zahlen*, J. Reine Angew. Math. **152** (1923), 129–148.
33. D. R. Heath-Brown, *Cubic forms in ten variables*, Proc. London Math. Soc. (3) **47** (1983), 225–257.
34. C. Hooley, *On nonary cubic forms*, J. Reine Angew. Math. **386** (1988), 32–98.
35. C. Hooley, *On nonary cubic forms. II*, J. Reine Angew. Math. **415** (1991), 95–165.
36. C. Hooley, *On nonary cubic forms. III*, J. Reine Angew. Math. **456** (1994), 53–63.
37. S. Lang, *On quasi algebraic closure*, Ann. of Math. **55** (1952), 373–390.
38. S. Lang, ed., *Number Theory III: Diophantine Geometry, Encyclopaedia Math. Sci.*, vol. 60, Springer-Verlag, Berlin, 1991.
39. S. Lang and A. Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819–827.
40. R. R. Laxton and D. J. Lewis, *Forms of degrees* 7 *and* 11 *over* $\mathfrak{p}$*-adic fields*, Proceedings of Symposia in Pure Mathematics, vol. 8, American Mathematical Society, 1965, pp. 16–21.
41. D. B. Leep, *Systems of quadratic forms*, J. Reine Angew. Math. **350** (1984), 109–116.
42. D. B. Leep and W. M. Schmidt, *Systems of homogeneous equations*, Invent. Math. **71** (1983), 539–549.
43. D. B. Leep and C. C. Yeomans, *Quintic forms over p-adic fields*, J. Number Theory **57** (1996), 231–241.
44. D. J. Lewis, *Cubic homogeneous polynomials over p-adic number fields*, Ann. of Math. (2) **56** (1952), 473–478.
45. D. J. Lewis, *Cubic congruences*, Michigan Math. J. **4** (1957), 85–95.
46. D. J. Lewis, *Cubic forms over algebraic number fields*, Mathematika **4** (1957), 97–101.
47. D. J. Lewis, *Diophantine problems: solved and unsolved*, Number Theory and Applications (Banff, AB, 1988), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci. (R. A. Mollin, ed.), vol. 265, Kluwer Academic Publishers, Dordrecht, 1989, pp. 103–121.
48. D. J. Lewis and H. L. Montgomery, *On zeros of p-adic forms*, Michigan Math. J. **30** (1983), 83–87.
49. D. J. Lewis and R. Schulze-Pillot, *Linear spaces on the intersection of cubic hypersurfaces*, Monatsh. Math. **97** (1984), 277–285.

50. G. Martin, *Solubility of systems of quadratic forms*, Bull. London Math. Soc. **29** (1997), 385–388.
51. M. Nagata, *Note on a paper of Lang concerning quasi algebraic closure*, Mem. Coll. Sci. Univ. Kyoto Ser. A. Math. **30** (1957), 237–241.
52. L. G. Peck, *Diophantine equations in algebraic number fields*, Amer. J. Math. **71** (1949), 387–402.
53. J. Pitman, *Cubic inequalities*, J. London Math. Soc. **43** (1968), 119–126.
54. P. A. B. Pleasants, *Cubic polynomials over algebraic number fields*, J. Number Theory **7** (1975), 310–344.
55. C. P. Ramanujam, *Cubic forms over algebraic number fields*, Proc. Cambridge Philos. Soc. **59** (1963), 683–705.
56. R. S. Rumely, *Arithmetic over the ring of all algebraic integers*, J. Reine Angew. Math. **368** (1986), 127–133.
57. C. Ryavec, *Cubic forms over algebraic number fields*, Proc. Cambridge Philos. Soc. **66** (1969), 323–333.
58. W. M. Schmidt, *Diophantine inequalities for forms of odd degree*, Adv. in Math. **38** (1980), 128–151.
59. W. M. Schmidt, *On cubic polynomials I. Hua's estimate of exponential sums*, Monatsh. Math. **93** (1982), 63–74.
60. W. M. Schmidt, *On cubic polynomials II. Multiple exponential sums*, Monatsh. Math. **93** (1982), 141–168.
61. W. M. Schmidt, *On cubic polynomials III. Systems of p-adic equations*, Monatsh. Math. **93** (1982), 211–223.
62. W. M. Schmidt, *On cubic polynomials IV. Systems of rational equations*, Monatsh. Math. **93** (1982), 329–348.
63. W. M. Schmidt, *Analytic methods for congruences, Diophantine equations and approximations*, Proceedings of the International Congress of Mathematicians, Vol. 1 (Warszaw, 1983), PWN, Warszaw, 1984, pp. 515–524.
64. W. M. Schmidt, *The solubility of certain p-adic equations*, J. Number Theory **19** (1984), 63–80.
65. W. M. Schmidt, *The density of integer points on homogeneous varieties*, Acta Math. **154** (1985), 243–296.
66. W. M. Schmidt, *Diophantine approximations and Diophantine equations, Lecture Notes in Mathematics*, vol. 1467, Springer-Verlag, Berlin, 1991.
67. S. E. Schuur, *On systems of three quadratic forms*, Acta Arith. **36** (1980), 315–322.
68. B. Segre, *The algebraic equations of degrees* $5, 9, 157, \ldots$, *and the arithmetic upon an algebraic variety*, Ann. of Math. (2) **46** (1945), 287–301.
69. E. S. Selmer, *On the irreducibility of certain trinomials*, Math. Scand. **4** (1956), 287–302.
70. J.-P. Serre, *Topics in Galois theory. Lecture notes prepared by Henri Darmon. With a foreword by Darmon and the author. Research Notes in Mathematics, 1*, Jones and Bartlett Publishers, Boston, MA, 1992.
71. C. L. Siegel, *Generalization of Waring's problem to algebraic number fields*, Amer. J. Math. **66** (1944), 122–136.
72. C. L. Siegel, *Sums of m-th powers of algebraic integers*, Ann. of Math. **46** (1945), 313–339.
73. C. M. Skinner, *Rational points on non-singular cubic hypersurfaces*, Duke Math. J. **75** (1994), 409–466.
74. C. M. Skinner, *Solvability of* $\mathfrak{p}$*-adic diagonal equations*, Acta Arith. **75** (1996), 251–258.
75. C. M. Skinner, *Forms over number fields and weak approximation*, Compositio Math. **106** (1997), 11–29.
76. W. Tartakovsky, *Über asymptotische Gesetze der allgemeinen Diophantischen Analyse mit vielen Unbekannten*, Bull. Acad. Sci. USSR (1935), 483–524.
77. G. Terjanian, *Un contre-example à une conjecture d'Artin*, C. R. Acad. Sci. Paris Ser. AB **262** (1966), A612.
78. G. Terjanian, *Formes p-adiques anisotropes*, J. Reine Angew. Math. **313** (1980), 217–220.

79. R. C. Vaughan, *The Hardy–Littlewood Method, second edition*, Cambridge University Press, 1997.
80. R. C. Vaughan and T. D. Wooley, *On a certain nonary cubic form and related equations*, Duke Math. J. **80** (1995), 669–735.
81. A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), 443–551.
82. T. D. Wooley, *Linear spaces on cubic hypersurfaces, and pairs of homogeneous cubic equations*, Bull. London Math. Soc. **29** (1997), 556–562.
83. T. D. Wooley, *Forms in many variables*, Analytic Number Theory: Proceedings of the 39th Taniguchi International Symposium, Kyoto, May 1996 (Y. Motohashi, ed.), London Mathematical Society Lecture Notes 247, Cambridge University Press, Cambridge, 1997, pp. 361–376.
84. T. D. Wooley, *On the local solubility of diophantine systems*, Compositio Math. **111** (1998), 149–165.
85. T. D. Wooley, *An explicit version of Birch's Theorem*, Acta Arith. **85** (1998), 79–96.
86. T. D. Wooley, *On the existence of non-singular local solutions to diophantine systems* (in preparation).

Department of Mathematics, University of Michigan, East Hall, 525 East University Avenue, Ann Arbor, MI 48109-1109, U.S.A.

E-mail address: wooley@math.lsa.umich.edu