Proc. Indian Acad. Sci. (Math. Sci.), Vol. 104, No. 1, February 1994, pp. 13–29.

The density of rational points on non-singular hypersurfaces

D R HEATH-BROWN
Magdalen College, Oxford OXI 4AU, England

Dedicated to the memory of Professor K G Ramanathan

Abstract. Let $F(\mathbf{x}) = F[x_1, \ldots, x_n] \in \mathbb{Z}[x_1, \ldots, x_n]$ be a non-singular form of degree $d \geqslant 2$, and let

$$N(F, X) = \#\{\mathbf{x} \in \mathbb{Z}^n; F(\mathbf{x}) = 0, |\mathbf{x}| \leqslant X\},$$

where

$$|\mathbf{x}| = \max_{1 \leqslant r \leqslant n} |x_r|.$$

It was shown by Fujiwara [4] [Upper bounds for the number of lattice points on hypersurfaces, *Number theory and combinatorics, Japan, 1984*, (World Scientific Publishing Co., Singapore, 1985)] that $N(F, X) \ll X^{n-2+2/n}$ for any fixed form F. It is shown here that the exponent may be reduced to $n - 2 + 2/(n+1)$, for $n \geqslant 4$, and to $n - 3 + 15/(n+5)$ for $n \geqslant 8$ and $d \geqslant 3$. It is conjectured that the exponent $n - 2 + \varepsilon$ is admissable as soon as $n \geqslant 3$. Thus the conjecture is established for $n \geqslant 10$. The proof uses Deligne's bounds for exponential sums and for the number of points on hypersurfaces over finite fields. However a composite modulus is used so that one can apply the 'q-analogue' of van der Corput's AB process.

Keywords. Rational points; hypersurface; counting function; multiple exponential sum; Deligne's bounds; singular locus.

1. Introduction

Let $F(\mathbf{x}) = F[x_1, \ldots, x_n] \in \mathbb{Z}[x_1, \ldots, x_n]$ be a non-zero form of degree d. We shall be concerned here with bounds for the number

$$N(F, X) = \#\{\mathbf{x} \in \mathbb{Z}^n; F(\mathbf{x}) = 0, |\mathbf{x}| \leqslant X\},$$

where

$$|\mathbf{x}| = \max_{1 \leqslant r \leqslant n} |x_r|.$$

It is trivial that

$$N(F, X) \ll_F X^{n-1}.$$

Moreover it is clear that $N(F, X) \gg_F X^{n-1}$ whenever F has a rational linear factor. However in all other cases one has

$$N(F, X) \ll_F X^{n-3/2} \log X. \tag{1}$$

This follows from Lemma 15 of Heath-Brown [7], where the result is deduced from estimates of Cohen [2]. It is reasonable to conjecture rather more:

CONJECTURE. *Let* $F(\mathbf{x}) = F[x_1, \dots, x_n] \in \mathbb{Z}[x_1, \dots, x_n]$ *be a non-zero form with no rational factor. Then*

$$N(F, X) \ll_{F,\varepsilon} X^{n-2+\varepsilon} \tag{2}$$

for any $\varepsilon > 0$.

When F is non-singular one has the bound $N(F, X) \ll_F X^{n-2+2/n}$ of Fujiwara [4], which approximates to (2) as n tends to infinity. Our first result gives a slight sharpening of Fujiwara's result and is of significance for small values of n.

Theorem 1. *Let* $F(\mathbf{x}) = F[x_1, \dots, x_n] \in \mathbb{Z}[x_1, \dots, x_n]$ *be a non-singular form of degree* $d \geqslant 2$, *and suppose that* $n \geqslant 4$. *Then*

$$N(F, X) \ll_F X^{n-2+2/(n+1)}.$$

In fact the proof shows that

$$N(F, X) \ll_F X^{3/2} \log X$$

for $n = 3$. However this estimate, without the factor $\log X$, can be obtained by a more elementary route. Indeed, using Falting's Theorem, one can show that (2) itself holds for $n = 3$.

Our main result establishes (2) for any non-singular form with $n \geqslant 10$, and, moreover, applies to appropriate inhomogeneous polynomials.

Theorem 2. *Let* $F(\mathbf{x}) = F(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$, *where* $n \geqslant 5$, *and write* $F_0(\mathbf{x})$ *for the homogeneous part of* F *of maximal degree. Suppose that* F_0 *is non-singular, with degree at least* 3. *Then*

$$N(F, X) \ll_F X^{n-3+15/(n+5)}.$$

This result improves on Theorem 1 as soon as $n > 7$. It is of course easy to see that (2) holds if F_0 is a non-singular quadratic form, provided that $n \geqslant 3$. However a non-singular quadratic form in 3 or more variables either vanishes only at $\mathbf{x} = 0$, or satisfies $N(F, X) \gg_F X^{n-2}$. Thus Theorem 2 itself cannot hold for quadratic polynomials in general.

It is reasonable to expect that Theorem 2 should hold with exponent $n - 3 + \varepsilon$, but some restriction on n will always be necessary, as the example $F = x_1^3 + x_2^3 + x_3^3 + x_4^3$ shows. This is non-singular, but has $N(F, X) \gg X^2$, in view of the trivial solutions $(a, -a, b, -b)$. Manin has formulated some very general conjectures covering such situations, see Franke *et al* [3], for example.

Our bounds for $N(F, X)$ come from estimating the number of solutions of a congruence:

$$N(F, X, m) = \#\{\mathbf{x} \in \mathbb{Z}^n : F(\mathbf{x}) \equiv 0 \pmod m, |\mathbf{x}| \leqslant X\}.$$

One trivially has $N(F, X) \leqslant N(F, X, m)$, and we use two different methods to bound

$N(F, X, m)$, to produce Theorems 1 and 2. It is a significant weakness of this approach that one considers essentially one value of m only. It would seem natural to try to use a sieve argument to take account of solvability to many moduli m simultaneously. The method of Cohen [2] does indeed do this, but the result already cited appears to be the best that one can achieve by this approach. One can also attempt to tackle the problem via the circle method. Thus, for example, the work of Birch [1] shows that $N(F, X) \ll_F X^{n-d}$ for non-singular F, as soon as $n > (d-1)2^d$. However in the present paper the emphasis is on results that are independent of the degree d of F, whereas Birch's result only takes affect when n is sufficiently large in comparison to d.

For the proof of Theorem 1 we take m to be prime, and apply Deligne's estimate to bound $N(F, X, m)$. For Theorem 2 we shall take m to be composite and use the 'q-analogue' of van der Corput's method. The interested reader is referred to the work of Heath-Brown [6], and of Graham and Ringrose [5] for other examples of this technique. We use the method in an n-dimensional setting, where 't-analogues' of van der Corput's method are extraordinarily cumbersome, to the extent that there has been no successful work for $n \geqslant 3$,. However for our q-analogue we are able to carry out the van der Corput AB process in full. It is possible therefore that this work could provide a model for future investigations into multi-dimensional exponential sums.

During the course of the proof of Theorem 2 we shall require an estimate for the number of solutions, suitably weighted, of a polynomial congruence in several variables. When the homogeneous part of the polynomial is non-singular, such an estimate follows naturally from the work of Deligne. However we shall be concerned with the general case. Here Hooley [8] has investigated the situation for unweighted solutions, and our situation may be viewed as a generalization of his. It seems to us that the result merits formal statement as a theorem.

Theorem 3. *Let $W(\mathbf{x})$ be an infinitely differentiable function, supported in a cube of side $2L$, and let $f(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}]$ be an arbitrary polynomial of degree $d \geqslant 2$ in n variables. Write f_0 for the homogeneous part of f of degree d, and define $s = s(f)$ to be the dimension of the projective algebraic set defined over the field of q elements by $\nabla f_0 = \mathbf{0}$. Here q is a prime greater than d. Then for any positive $N \ll q$ we have*

$$\sum_{\mathbf{x} \in \mathbb{Z}^n,\, q \mid f(\mathbf{x})} W\left(\frac{1}{N}\mathbf{x}\right) = q^{-1} \sum_{\mathbf{y} \in \mathbb{Z}^n} W\left(\frac{1}{N}\mathbf{y}\right) + O_{n,d,L}(D_{n+1} N^{s+1} q^{(n-s-1)/2}),$$

where D_k is the maximum of all k-th order partial derivatives of $W(\mathbf{x})$, taken over all $\mathbf{x} \in \mathbb{R}^n$.

Notice that s lies in the range $-1 \leqslant s \leqslant n-1$, and that $s = -1$ means that f_0 is non-singular. Taking $N = q$ we essentially recover Hooley's result.

2. Proof of Theorem 1

To prove Theorem 1 we shall consider $N(F, X, p)$ where $p \geqslant X$ is prime. It is convenient to introduce the weight function

$$w(\mathbf{z}) = \prod_{r=1}^{n} \left(\frac{\sin \pi z_r}{\pi z_r}\right)^2,$$

whose Fourier transform is

$$\hat{w}(\mathbf{y}) = \prod_{r=1}^{n} (\max\{1 - |y_r|, 0\}).$$

We then have

$$N(F,X) \leqslant N(F,X,p) \ll \sum_{\mathbf{x} \in \mathbb{Z}^n,\ p|F(\mathbf{x})} w\left(\frac{1}{2X}\mathbf{x}\right).$$

Using the Poisson summation formula we see that the sum on the right is

$$\begin{aligned}
&\sum_{\mathbf{y} (\mathrm{mod}\ p),\ p|F(\mathbf{y})} \sum_{\mathbf{z} \in \mathbb{Z}^n} w\left(\frac{1}{2X}(\mathbf{y} + p\mathbf{z})\right) \\
&= \sum_{\mathbf{y} (\mathrm{mod}\ p),\ p|F(\mathbf{y})} \sum_{\mathbf{u} \in \mathbb{Z}^n} \left(\frac{2X}{p}\right)^n e_p(\mathbf{u}.\mathbf{y}) \hat{w}\left(\frac{2X}{p}\mathbf{u}\right), \\
&= \left(\frac{2X}{p}\right)^n \sum_{\mathbf{u} \in \mathbb{Z}^n} \hat{w}\left(\frac{2X}{p}\mathbf{u}\right) S_p(\mathbf{u}),
\end{aligned}$$

where $e_p(x)$ is $\exp(2\pi i x/p)$ as usual and

$$S_p(\mathbf{u}) = \sum_{\mathbf{y} (\mathrm{mod}\ p),\ p|F(\mathbf{y})} e_p(\mathbf{u}.\mathbf{y}).$$

We therefore conclude that

$$N(F,X) \ll \left(\frac{X}{p}\right)^n \sum_{|\mathbf{u}| \ll p/X} |S_p(\mathbf{u})|. \tag{3}$$

When $p|\mathbf{u}$ we have

$$S_p(\mathbf{u}) = \#\{\mathbf{y} (\mathrm{mod}\ p) : p|F(\mathbf{y})\} \ll p^{n-1}.$$

We therefore proceed to examine the case $p \nmid \mathbf{u}$. Since F is homogeneous we have

$$\begin{aligned}
(p-1)S_p(\mathbf{u}) &= \sum_{a=1}^{p-1} \sum_{a\mathbf{y} (\mathrm{mod}\ p),\ p|F(a\mathbf{y})} e_p(a\mathbf{u}.\mathbf{y}) \\
&= \sum_{a=1}^{p-1} \sum_{\mathbf{y} (\mathrm{mod}\ p),\ p|F(\mathbf{y})} e_p(a\mathbf{u}.\mathbf{y}) \\
&= \sum_{\mathbf{y} (\mathrm{mod}\ p),\ p|F(\mathbf{y})} \sum_{a=1}^{p-1} e_p(a\mathbf{u}.\mathbf{y}) \\
&= p\#\{\mathbf{y} (\mathrm{mod}\ p) : p|F(\mathbf{y}), p|\mathbf{u}.\mathbf{y}\} - \#\{\mathbf{y} (\mathrm{mod}\ p) : p|F(\mathbf{y})\}.
\end{aligned}$$

Now, according to Deligne's estimate we have

$$\#\{\mathbf{y} (\mathrm{mod}\ p) : p|F(\mathbf{y}), p|\mathbf{u}.\mathbf{y}\} = p^{n-2} + O_{n,d}(p^{(n-1)/2}), \tag{4}$$

providing that $F(\mathbf{y}) = \mathbf{u}.\mathbf{y} = 0$ defines a non-singular absolutely irreducible variety of dimension $n-3$ over the field of p elements. Since F is non-singular there is a form $G(\mathbf{u})$ with integer coefficients, depending only on F, such that (4) holds whenever $p \nmid G(\mathbf{u})$. The form G will be absolutely irreducible and will have degree 2 or more. The existence of such a form follows from the argument of Heath-Brown [7; Lemma 6], where forms F of degree 3 were considered. Since F is non-singular Deligne's estimate also gives

$$\#\{\mathbf{y} (\mathrm{mod}\, p) : p | F(\mathbf{y})\} = p^{n-1} + O_{n,d}(p^{n/2})$$

for all sufficiently large primes p. It therefore follows that

$$\begin{aligned} S_p(\mathbf{u}) &\ll_F \frac{1}{p-1}\{p(p^{n-2} + O_{n,d}(p^{(n-1)/2})) - (p^{n-1} + O_{n,d}(p^{n/2}))\} \\ &\ll_F p^{(n-1)/2} \end{aligned}$$

whenever $p \nmid G(\mathbf{u})$. For the remaining values of $\mathbf{u}$ we have

$$S_p(\mathbf{u}) = p^{-1} \sum_{a (\mathrm{mod}\, p)} \sum_{\mathbf{y} (\mathrm{mod}\, p)} e_p(aF(\mathbf{y}) + \mathbf{u}.\mathbf{y}).$$

For $p \nmid a$ the sum over $\mathbf{y}$ is $O_{n,d}(p^{n/2})$ by Deligne's bound for exponential sums, since F has degree at least 2. In the remaining case $p | a$ the sum is zero, since we are assuming that $p \nmid \mathbf{u}$. Thus

$$S_p(\mathbf{u}) \ll_{n,d} p^{n/2}$$

whenever $p \nmid \mathbf{u}$.

We now insert our bounds for $S_p(\mathbf{u})$ into the estimate (3) to obtain

$$N(F, X) \ll_F X^n p^{-1} + p^{(n-1)/2} + X^n p^{-n/2} \#\{|\mathbf{u}| \ll p/X : p | G(\mathbf{u})\}.$$

providing that $p \geqslant X$. Finally we average this result over all primes p in the interval $[P, 2P]$, so that

$$N(F, X) \ll_F X^n P^{-1} + P^{(n-1)/2} + X^n P^{-n/2} M, \tag{5}$$

where

$$\begin{aligned} M &= \frac{\log P}{P} \sum_p \#\{|\mathbf{u}| \ll P/X : p | G(\mathbf{u})\} \\ &\ll \frac{\log P}{P} \sum_{|\mathbf{u}| \ll P/X} \#\{p | G(\mathbf{u}) : P \leqslant p \leqslant 2P\}. \end{aligned}$$

However

$$G(\mathbf{u}) \ll |\mathbf{u}|^D \ll P^D,$$

where D is the degree of G, and hence a non-zero value of $G(\mathbf{u})$ can have at most $D \ll 1$ prime factors $p \geqslant P$. It follows that

$$M \ll \left(\frac{P}{X}\right)^n \frac{\log P}{P} + \#\{\mathbf{u} \ll P/X : G(\mathbf{u}) = 0\}$$

$$\ll \left(\frac{P}{X}\right)^n \frac{\log P}{P} + \left(\frac{P}{X}\right)^{n-3/2} \log P$$

on applying the bound (1) to the form G. In view of (5) we now have

$$N(F,X) \ll_F X^n P^{-1} + P^{(n-1)/2} + X^n P^{-n/2}\left(\left(\frac{P}{X}\right)^n \frac{\log P}{P} + \left(\frac{P}{X}\right)^{n-3/2} \log P\right).$$

We choose $P = X^{2n/(n+1)} \geqslant X$, which makes the first two terms above equal, and Theorem 1 follows.

3. Proof of Theorem 2: Preliminary manipulations

Deligne's estimate for 'complete' exponential sums, as used in the proof of Theorem 1, is essentially best possible, and the problem of improving on the corresponding estimate for 'incomplete' sums is notoriously difficult, even for sums in one variable. Thus one has

$$\sum_{1 \leqslant n \leqslant N} e_p(f(n)) \ll_f N p^{-1/2} + p^{1/2} \log p$$

for any non-constant integer polynomial f, and one suspects that better bounds should be possible when N is a suitable power of p. However in general nothing can be proved. To circumvent this difficulty we shall use composite moduli, where the 'q-analogue' of van der Corput's method is available. We begin by taking two primes p and q, with

$$p < X < q, \tag{6}$$

and considering $N(F,X,pq)$. It is convenient to use an infinitely differentiable weight with compact support, and we shall therefore define

$$\omega_0(t) = \begin{cases} \exp((1-t^2)^{-1}), & |t| < 1, \\ 0, & |t| \geqslant 1, \end{cases}$$

and

$$\omega(\mathbf{t}) = \prod_{r=1}^{n} \omega_0(t_r).$$

Then ω is infinitely differentiable, and its Fourier transform satisfies

$$\hat{\omega}(\mathbf{t}) \ll_A |\mathbf{t}|^{-A}, \quad |\mathbf{t}| \geqslant 1, \tag{7}$$

for any $A > 0$. We now begin our analysis with the inequalities

$$N(F,X) \leqslant N(F,X,pq)$$

$$\ll \sum_{\mathbf{x}\in\mathbb{Z}^n,\ pq|F(\mathbf{x})} \omega\left(\frac{1}{2X}\mathbf{x}\right)$$
$$= S + K\#\{\mathbf{y} (\mathrm{mod}\, p) : p|F(\mathbf{y})\}$$
$$\ll S + Kp^{n-1}, \tag{8}$$

where K is a parameter to be chosen and

$$S = \sum_{\mathbf{y} (\mathrm{mod}\, p),\ p|F(\mathbf{y})} \left\{ \sum_{\mathbf{x}\equiv \mathbf{y} (\mathrm{mod}\, p),\ q|F(\mathbf{x})} \omega\left(\frac{1}{2X}\mathbf{x}\right) - K \right\}$$
$$\ll p^{(n-1)/2} \left\{ \sum_{\mathbf{y} (\mathrm{mod}\, p),\ p|F(\mathbf{y})} \left| \sum_{\mathbf{x}\equiv \mathbf{y} (\mathrm{mod}\, p),\ q|F(\mathbf{x})} \omega\left(\frac{1}{2X}\mathbf{x}\right) - K \right|^2 \right\}^{1/2}$$
$$= p^{(n-1)/2} \Sigma^{1/2}, \tag{9}$$

say. Here we have used Cauchy's inequality, together with the observation that there are $O(p^{n-1})$ solutions of $p|F(\mathbf{y})$ modulo p.

At this point, somewhat surprisingly, we include a number of extra terms in Σ. This, however, has the desirable effect of producing a sum in which there are only congruences modulo q. We have

$$\Sigma \leqslant \sum_{\mathbf{y} (\mathrm{mod}\, p)} \sum_{a (\mathrm{mod}\, q)} \left| \sum_{\substack{\mathbf{x}\equiv \mathbf{y} (\mathrm{mod}\, p) \\ F(\mathbf{x})\equiv a (\mathrm{mod}\, q)}} \omega\left(\frac{1}{2X}\mathbf{x}\right) - K \right|^2. \tag{10}$$

When the sum on the right is expanded there are cross terms

$$K \sum_{\mathbf{y} (\mathrm{mod}\, p)} \sum_{a (\mathrm{mod}\, q)} \sum_{\substack{\mathbf{x}\equiv \mathbf{y} (\mathrm{mod}\, p) \\ F(\mathbf{x})\equiv a (\mathrm{mod}\, q)}} \omega\left(\frac{1}{2X}\mathbf{x}\right) = K \sum_{\mathbf{x}\in\mathbb{Z}^n} \omega\left(\frac{1}{2X}\mathbf{x}\right).$$

Hence if we choose

$$K = p^{-n} q^{-1} \sum_{\mathbf{x}\in\mathbb{Z}^n} \omega\left(\frac{1}{2X}\mathbf{x}\right) \tag{11}$$

then (10) yields

$$\Sigma \leqslant \sum_{\mathbf{x}\in\mathbb{Z}^n} \omega\left(\frac{1}{2X}\mathbf{x}\right) \sum_{\substack{\mathbf{x}'\equiv \mathbf{x} (\mathrm{mod}\, p), \\ F(\mathbf{x}')\equiv F(\mathbf{x}) (\mathrm{mod}\, q)}} \omega\left(\frac{1}{2X}\mathbf{x}'\right) - p^n q K^2.$$

On writing $\mathbf{x}' = \mathbf{x} + p\mathbf{y}$ and

$$F(\mathbf{x};\mathbf{y}) = F(\mathbf{x}+p\mathbf{y}) - F(\mathbf{x}),\quad W(\mathbf{x};\mathbf{y}) = \omega\left(\frac{1}{2X}\mathbf{x}\right)\omega\left(\frac{1}{2X}(\mathbf{x}+p\mathbf{y})\right), \tag{12}$$

we find that

$$\Sigma \leqslant \sum_{\mathbf{y}} \sum_{q|F(\mathbf{x};\mathbf{y})} W(\mathbf{x};\mathbf{y}) - p^n q K^2. \tag{13}$$

The expected value of the sum over $\mathbf{x}$ is

$$q^{-1}\sum_{\mathbf{x}} W(\mathbf{x};\mathbf{y}) = K(\mathbf{y}), \tag{14}$$

say. By the Poisson summation formula we have

$$\begin{aligned}\sum_{\mathbf{y}} K(\mathbf{y}) &= q^{-1}\sum_{\mathbf{x}} \omega\left(\frac{1}{2X}\mathbf{x}\right)\sum_{\mathbf{y}} \omega\left(\frac{1}{2X}(\mathbf{x}+p\mathbf{y})\right)\\ &= q^{-1}\sum_{\mathbf{x}} \omega\left(\frac{1}{2X}\mathbf{x}\right)\left(\frac{2X}{p}\right)^n \sum_{\mathbf{z}} e_p(\mathbf{z}.\mathbf{x})\hat{\omega}\left(\frac{2X}{p}\mathbf{z}\right).\end{aligned}$$

However, in view of (6) and (7), the terms with $\mathbf{z} \neq 0$ contribute

$$O_A(q^{-1}X^n(X/p)^{n-A}).$$

Hence

$$\begin{aligned}\sum_{\mathbf{y}} K(\mathbf{y}) &= q^{-1}\sum_{\mathbf{x}} \omega\left(\frac{1}{2X}\mathbf{x}\right)\left(\frac{2X}{p}\right)^n \hat{\omega}(0) + O_A(q^{-1}X^n(X/p)^{n-A})\\ &= (2X)^n K\hat{\omega}(0) + O_A(q^{-1}X^n(X/p)^{n-A}),\end{aligned}$$

by the definition (11). However, a second application of the Poisson summation formula yields

$$\begin{aligned}K &= p^{-n}q^{-1}\sum_{\mathbf{x}} \omega\left(\frac{1}{2X}\mathbf{x}\right)\\ &= p^{-n}q^{-1}(2X)^n\sum_{\mathbf{z}} \hat{\omega}(2X\mathbf{z})\\ &= p^{-n}q^{-1}(2X)^n\hat{\omega}(0) + O_A(p^{-n}q^{-1}X^{n-A}).\end{aligned}$$

We therefore see that

$$\begin{aligned}\sum_{\mathbf{y}} K(\mathbf{y}) &= p^n qK^2 + O_A\left(\frac{X^n}{q}\left(\frac{X}{p}\right)^{n-A}\right) + O_A\left(\frac{X^n}{p^n q}X^{n-A}\right) + O_A\left(\frac{X^{2(n-A)}}{p^n q}\right)\\ &= p^n qK^2 + O_A\left(\frac{X^n}{q}\left(\frac{X}{p}\right)^{n-A}\right),\end{aligned}$$

so that (13) can be rewritten in the form

$$\Sigma \leqslant \sum_{\mathbf{y}}\left\{\sum_{q|F(\mathbf{x};\mathbf{y})} W(\mathbf{x};\mathbf{y}) - K(\mathbf{y})\right\} + O_A\left(\frac{X^n}{q}\left(\frac{X}{p}\right)^{n-A}\right). \tag{15}$$

We now combine the estimates (8), (9), (11) and (15) in the following lemma.

Lemma 1. *If* $p < X < q$ *we have*

$$N(F,X) \ll \frac{X^n}{pq} + p^{(n-1)/2}\left\{\sum_{\mathbf{y}\in\mathbb{Z}^n} |\Delta(\mathbf{y})|\right\}^{1/2} + \left\{\frac{(pX)^n}{pq}\left(\frac{X}{p}\right)^{n-A}\right\}^{1/2},$$

for any $A > 0$, where

$$\Delta(\mathbf{y}) = \sum_{\mathbf{x} \in \mathbb{Z}^n,\ q \mid F(\mathbf{x};\mathbf{y})} W(\mathbf{x};\mathbf{y}) - K(\mathbf{y}).$$

4. Proof of Theorem 2

We can now use Theorem 3, which we shall prove later, to estimate $\Delta(\mathbf{y})$. We take $N = X$ and

$$W\left(\frac{1}{N}\mathbf{x}\right) = W(\mathbf{x};\mathbf{y}) = \omega\left(\frac{1}{2X}\mathbf{x}\right)\omega\left(\frac{1}{2X}(\mathbf{x}+p\mathbf{y})\right),$$

so that $W(\mathbf{x})$ is supported on a cube of side $L = 4$. With this choice of $W(\mathbf{x})$ we have $D_k \ll_k 1$. According to the definition (14) we see that the main term in Theorem 3 is just $K(\mathbf{y})$, while the error term becomes $O(X^{s+1}q^{(n-s-1)/2})$, where $s = s(F(\mathbf{x};\mathbf{y})) = s(\mathbf{y})$, say. With this notation it follows that

$$\Delta(\mathbf{y}) \ll q^{n/2}(Xq^{-1/2})^{1+s(\mathbf{y})}.$$

We now insert the above bound into Lemma 1. In doing so we observe that, according to the definition (12), $W(\mathbf{x};\mathbf{y})$ vanishes whenever $|\mathbf{y}| \gg X/p$. We therefore obtain

$$N(F,X) \ll \frac{X^n}{pq} + p^{(n-1)/2}q^{n/4}\left\{\sum_{|\mathbf{y}| \ll X/p}(Xq^{-1/2})^{1+s(\mathbf{y})}\right\}^{1/2} + \left\{\frac{(pX)^n}{pq}\left(\frac{X}{p}\right)^{n-A}\right\}^{1/2}. \tag{16}$$

It remains to consider how often each value of $s(\mathbf{y})$ can arise. The homogeneous part of maximal degree in

$$f(\mathbf{x}) = F(\mathbf{x};\mathbf{y}) = F(\mathbf{x}+p\mathbf{y}) - F(\mathbf{x})$$

will be $p\mathbf{y}.\nabla F_0(\mathbf{x})$, unless this happens to vanish identically in $\mathbf{x}$. We now use the following lemmas, which we will prove at the end of this section.

Lemma 2. Let $f(\mathbf{x})$ be a non-singular form of degree d in n variables, defined over the field of q elements, where $q > d$ is a prime. Let $S_{\mathbf{y}} = S_{\mathbf{y}}(f)$ be the affine algebraic set

$$S_{\mathbf{y}} = \{\mathbf{x} : \mathbf{y}\cdot\nabla^2 f(\mathbf{x}) = 0\},$$

and let

$$T_s = \{\mathbf{y} : \dim(S_{\mathbf{y}}) \geqslant s\}.$$

Then T_s is a projective affine set of dimension at most $n-s$, defined by $O_{n,d}(1)$ equations, each of degree $O_{n,d}(1)$.

Lemma 3. Let q be a prime, and let $G_1, \ldots, G_s$ be polynomials in n variables, defined

over the field of q elements, and producing an affine algebraic set all of whose components have dimension at most $r \geqslant 0$. Suppose further that the degrees of the polynomials G_i are all at most D. Then for any B with $1 \leqslant B \ll q$ the number of integer solutions of the simultaneous congruences

$$G_i(\mathbf{x}) \equiv 0 (\mathrm{mod}\, q), \quad (1 \leqslant i \leqslant s)$$

in the region $|\mathbf{x}| \leqslant B$ is $O_{s,n,D}(B^r)$.

Taking $f = F_0$ we see that if $\mathbf{y}.\nabla F_0(\mathbf{x})$ vanishes identically in $\mathbf{x}$, then $\mathbf{y} \in T_n$, which has dimension zero, by Lemma 2. Hence there are only $O_{n,d}(1)$ possible values of $\mathbf{y}$ in the range $|\mathbf{y}| \ll X/p$. Here we use the observation that $X/p < q$. In the remaining cases Lemmas 2 and 3 show that there are $O_{n,d}((X/p)^{n-s-1})$ values of $\mathbf{y}$ with $s(\mathbf{y}) = s$. It therefore follows that

$$\sum_{|\mathbf{y}| \ll X/p} (Xq^{-1/2})^{1+s(\mathbf{y})} \ll \sum_{s=-1}^{n-1} (Xq^{-1/2})^{1+s}(Xp^{-1})^{n-s-1}$$
$$\ll (Xp^{-1})^n + (Xq^{-1/2})^n.$$

The estimate (16) now yields

$$N(F,X) \ll \frac{X^n}{pq} + p^{(n-1)/2} q^{n/4} \{(Xp^{-1})^n + (Xq^{-1/2})^n\}^{1/2}$$
$$+ \left\{ \frac{(pX)^n}{pq} \left(\frac{X}{p} \right)^{n-A} \right\}^{1/2},$$

for any $A > 0$, subject to the conditions $p < X < q$. We therefore choose primes p and q for which

$$X^{n/(n+5)} \ll p \ll X^{n/(n+5)}, X^{2n/(n+5)} \ll q \ll X^{n/(n+5)}.$$

This is an admissable choice providing that $n \geqslant 5$, and yields

$$N(F,X) \ll X^{n-3+15/(n+5)},$$

providing that A is chosen large enough. This completes the proof of Theorem 2.

It remains to establish Lemmas 2 and 3. The result of Lemma 2 may be viewed as an extension of Lemma 2 of the author's work [7]. However the proof given there is not strictly correct. (The set $\pi^{-1}(\mathbf{x})$ is $\{(\mathbf{x},\mathbf{y}) \in V : \mathbf{B}(\mathbf{x},\mathbf{y}) = \mathbf{0}\}$ rather than $\{(\mathbf{x},\mathbf{y}) : \mathbf{B}(\mathbf{x},\mathbf{y}) = \mathbf{0}\}$.) We therefore use a slightly different approach.

We begin by showing that T_s is an algebraic set. To do this we take a generic linear space L of dimension $n-s$. Then T_s consists of those points $\mathbf{y}$ for which $S_{\mathbf{y}} \cap L$ is non-empty. However $S_{\mathbf{y}} \cap L$ is given by $n+s$ equations in $\mathbf{x}$, the first n of which are $\mathbf{y}.\nabla^2 f(\mathbf{x}) = \mathbf{0}$, and the remaining s of which are the linear equations which specify that $\mathbf{x} \in L$. It follows from elimination theory that the condition for $S_{\mathbf{y}} \cap L$ to be non-empty is the simultaneous vanishing of $O_{n,d}(1)$ homogeneous polynomials of degrees $O_{n,d}(1)$ in $\mathbf{y}$.

We have now to consider the dimension of T_s. We shall write S for the set

$$S = \{(\mathbf{x},\mathbf{y}) : \mathbf{y}.\nabla^2 f(\mathbf{x}) = 0\},$$

which we shall regard as a subset of $2n$-dimensional affine space. We begin by observing that $\dim(S) \leqslant n$, for otherwise S would have non-trivial points in common with the diagonal $\{(\mathbf{x}, \mathbf{x})\}$, which itself has dimension n. Any such common point would produce a non-zero solution $\mathbf{x}$ of

$$(d-1)\nabla f(\mathbf{x}) = \mathbf{x}.\nabla^2 f(\mathbf{x}) = 0,$$

contradicting the non-singularity assumption.

We now prove that $\dim(T_s) \leqslant n - s$. Let U be an irreducible component of T_s, and take $\mathbf{P}$ to be a generic point of U. We write

$$W = \{(\mathbf{x}, \mathbf{y}) : \mathbf{y}.\nabla^2 f(\mathbf{x}) = 0, \mathbf{y} \in U\},$$

and decompose W into irreducible components $W_1 \cup \cdots \cup W_r$. With this notation it follows that

$$S_{\mathbf{P}} = \{\mathbf{x} : (\mathbf{x}, \mathbf{P}) \in W\} = \cup_{i=1}^{r} \{\mathbf{x} : (\mathbf{x}, \mathbf{P}) \in W_i\}.$$

Since $\mathbf{P} \in T_s$, at least one of the components of $S_{\mathbf{P}}$ has dimension s or more. Consequently there is at least one index i for which

$$\dim(\{\mathbf{x} : (\mathbf{x}, \mathbf{P}) \in W_i\}) \geqslant s.$$

For ease of notation we take $i = 1$. We now consider the mapping

$$\pi : W_1 \to U$$

given by $\pi(\mathbf{x}, \mathbf{y}) = \mathbf{y}$. This is a regular mapping between irreducible varieties. Moreover there is at least one point of the form $(\mathbf{x}, \mathbf{P})$ in W_1, so that the image of π contains the point $\mathbf{P}$. However the image of π will be a closed subset of U, and $\mathbf{P}$ is generic on U, so that π must in fact be onto. It now follows by the theorem on the dimension of fibres (Shafarevich [9; page 60] for example) that

$$\dim(\pi^{-1}(\mathbf{P})) = \dim(W_1) - \dim(U).$$

We therefore deduce that

$$\begin{aligned} \dim(U) &= \dim(W_1) - \dim(\pi^{-1}(\mathbf{P})) \\ &\leqslant \dim(S) - \dim(\{\mathbf{x} : (\mathbf{x}, \mathbf{P}) \in W_i\}) \\ &\leqslant n - s. \end{aligned}$$

as required.

Lemma 3 is related to Lemma 2 of Hooley [8], and to the principle described by the author [7; page 229]. Indeed Hooley's result is essentially the case $B = q$. For the proof we first remark that the algebraic set

$$G : G_1 = \ldots = G_s = 0$$

has $O_{s,n,D}(1)$ components of dimension r. To show this we intersect G with a generic linear space L of dimension $n - r$. This will produce a set of isolated points only, at least one for each component of G of dimension r. Moreover distinct components

will produce distinct points of intersection with L. The number of components is thus at most the number of points in $G \cap L$. Since L is given by r linear equations, $G \cap L$ is given by $O_{s,n,D}(1)$ equations of degrees $O_{s,n,D}(1)$. A straightforward application of elimination theory now shows that $G \cap L$ has $O_{s,n,D}(1)$ points, and the result follows.

We can now give the proof of the lemma. We shall use induction on n, the result being trivial for $n = 0$. For the general case we write $\mathbf{x} = (x, \mathbf{y})$, where $\mathbf{y}$ is an $n-1$ dimensional vector. Since the algebraic set defined by $G_1 = \ldots = G_s = 0$ has $O_{n,D,s}(1)$ components of dimension r, there are $O_{n,D,s}(1)$ values of x for which the hyperplane $x_1 = x$ can contain such a component. For the remaining values of x every component of the set

$$x_1 = x,\ G_1 = \ldots = G_s = 0$$

has dimension at most $r-1$. Applying the case $n-1$ of the lemma to each hyperplane section there will be $O_{n,D,s}(1)$ contributions $O_{n,D,s}(B^r)$ from values of x of the first type, and $O(B)$ contributions $O_{n,D,s}(B^{r-1})$ from values of x of the second type. The case n of the lemma then follows.

5. Proof of Theorem 3

Before beginning the proof we record the remark that

$$D_k \ll_{n,L} D_{k+1},$$

which follows from the fact W is supported on a cube of side $2L$. The theorem will be proved by induction on s, and our first task is to establish the base step $s = -1$. We commence by using the manipulations with which we began the proof of Theorem 1. We have

$$\begin{aligned}\sum_{\mathbf{x}\in\mathbf{Z}^n,\, q\mid f(\mathbf{x})} W\left(\frac{1}{N}\mathbf{x}\right) &= \sum_{\mathbf{z} (\mathrm{mod}\, q),\, q\mid f(\mathbf{z})} \sum_{\mathbf{u}\in\mathbf{Z}^n} W\left(\frac{1}{N}(\mathbf{z}+q\mathbf{u})\right) \\ &= \sum_{\mathbf{z} (\mathrm{mod}\, q),\, q\mid f(\mathbf{z})} \left(\frac{N}{q}\right)^n \sum_{\mathbf{v}\in\mathbf{Z}^n} e_q(\mathbf{v}.\mathbf{z})\, \hat{W}\left(\frac{N}{q}\mathbf{v}\right) \\ &= \left(\frac{N}{q}\right)^n \sum_{\mathbf{v}\in\mathbf{Z}^n} \hat{W}\left(\frac{N}{q}\mathbf{v}\right) \Sigma_q(\mathbf{v}),\end{aligned}$$

where

$$\begin{aligned}\Sigma_q(\mathbf{v}) &= \sum_{\mathbf{z} (\mathrm{mod}\, q),\, q\mid f(\mathbf{z})} e_q(\mathbf{v}.\mathbf{z}) \\ &= q^{-1} \sum_{a (\mathrm{mod}\, q)} \sum_{\mathbf{z} (\mathrm{mod}\, q)} e_q(af(\mathbf{z}) + \mathbf{v}.\mathbf{z}).\end{aligned}$$

When $q \nmid a$ the homogeneous part of $af(\mathbf{z}) + \mathbf{v}.\mathbf{z}$ of maximal degree is just $af_0(\mathbf{z})$, since $d \geqslant 2$. However we are assuming that f_0 is non-singular, whence Deligne's estimate shows that the $\mathbf{z}$ sum is $O_{n,d}(q^{n/2})$. When $q \mid a$ the sum is q^n for $q \mid \mathbf{v}$, and vanishes in

the remaining cases. It therefore follows that

$$\sum_{\mathbf{x}\in\mathbb{Z}^n,\, q\mid f(\mathbf{x})} W\left(\frac{1}{N}\mathbf{x}\right) = \frac{N^n}{q}\sum_{\mathbf{w}\in\mathbb{Z}^n}\hat{W}(N\mathbf{w}) + O_{n,d}\left(\frac{N^n}{q^{n/2}}\sum_{\mathbf{v}\in\mathbb{Z}^n}\left|\hat{W}\left(\frac{N}{q}\mathbf{v}\right)\right|\right)$$

$$= q^{-1}\sum_{\mathbf{y}\in\mathbb{Z}^n} W\left(\frac{1}{N}\mathbf{y}\right) + O_{n,d}\left(\frac{N^n}{q^{n/2}}\sum_{\mathbf{v}\in\mathbb{Z}^n}\left|\hat{W}\left(\frac{N}{q}\mathbf{v}\right)\right|\right),$$

on using the Poisson summation formula again.

On integrating by parts $n+1$ times one finds that

$$\hat{W}(\mathbf{t}) \ll_{n,L} D_{n+1}|\mathbf{t}|^{-n-1}$$

for $|\mathbf{t}| \geqslant 1$. For smaller $\mathbf{t}$ one may use the trivial bound

$$\hat{W}(\mathbf{t}) \ll_{n,L} D_0 \ll_{n,L} D_{n+1}.$$

These estimates show that

$$\sum_{\mathbf{v}\in\mathbb{Z}^n}\left|\hat{W}\left(\frac{N}{q}\mathbf{v}\right)\right| \ll_{n,L} D_{n+1}\left(\frac{q}{N}\right)^n,$$

and hence

$$\sum_{\mathbf{x}\in\mathbb{Z}^n,\, q\mid f(\mathbf{x})} W\left(\frac{1}{N}\mathbf{x}\right) = q^{-1}\sum_{\mathbf{y}\in\mathbb{Z}^n} W\left(\frac{1}{N}\mathbf{y}\right) + O_{n,d,L}(D_{n+1}q^{n/2}),$$

as required.

For the induction step we shall count points of affine hyperplanes $\mathbf{m}.\mathbf{x} = c$. For any non-zero vector $\mathbf{m}$ we therefore define a form $f_0^{(\mathbf{m})}$ corresponding to the intersection of $f_0 = 0$ with $\mathbf{m}.\mathbf{x} = 0$. For an explicit representation of $f_0^{(\mathbf{m})}$ one can label the coordinates so that $m_1 \neq 0$, and set

$$f_0^{(\mathbf{m})}(x_2,\ldots,x_n) = f_0\left(-\frac{m_2x_2+\ldots+m_nx_n}{m_1}, x_2,\ldots,x_n\right).$$

In the next section we shall prove the following lemma.

Lemma 4. *Suppose that* $s(f_0) \geqslant 0$. *Then there is a non-zero integer vector* $\mathbf{m}$, *with*

$$\mathbf{m} \ll_{d,n} 1,$$

for which $s(f_0^{(\mathbf{m})}) = s(f_0) - 1$.

In particular $f_0^{(\mathbf{m})}$ is not identically zero. Clearly we can assume that $\mathbf{m}$ is primitive, so that there is a unimodular $n \times n$ matrix M all of whose entries are $O_{n,d}(1)$ and such that the first column of $(M^T)^{-1}$ is the vector $\mathbf{m}$. We now define a new polynomial and a new weight function by

$$f_M(\mathbf{x}) = f(M\mathbf{x}), \quad W_M(\mathbf{x}) = W(M\mathbf{x}).$$

Since the entries of M^{-1} are all $O_{n,d}(1)$ it follows that W_M is supported on a cube of

side $2L'$, depending only on n, d and L. We now have

$$\sum_{\mathbf{x}\in\mathbb{Z}^n,\, q\mid f(\mathbf{x})} W\left(\frac{1}{N}\mathbf{x}\right) = \sum_{\mathbf{x}\in\mathbb{Z}^n,\, q\mid f_M(\mathbf{x})} W_M\left(\frac{1}{N}\mathbf{x}\right)$$

$$= \sum_{-NL'\leqslant x\leqslant NL'} \sum_{\mathbf{y}\in\mathbb{Z}^{n-1},\, q\mid f_M(x,\mathbf{y})} W_M\left(\frac{1}{N}(x,\mathbf{y})\right). \tag{17}$$

Here we have used the fact that $W_M(\frac{1}{N}(x,\mathbf{y}))=0$ unless $-NL'\leqslant x\leqslant NL'$, since W_M is supported in a cube of side $2L'$. Now if $g(\mathbf{y})=f_M(x,\mathbf{y})$ then $g_0(\mathbf{y})=f_0(M(0,\mathbf{y}))$. Since $M^T\mathbf{m}=(1,0,\ldots,0)$ we have $\mathbf{m}.M\mathbf{x}=(M^T\mathbf{m}).\mathbf{x}=x_1$. However $f_0^{(\mathbf{m})}$, which corresponds to substituting $\mathbf{m}.\mathbf{x}=0$ in f_0, is equivalent, under linear substitution, to the form obtained by substituting $\mathbf{m}.M\mathbf{x}=x_1=0$ in $f_0(M\mathbf{x})$. It follows that $f_0^{(\mathbf{m})}$ is equivalent to $g_0(\mathbf{y})$, so that $s(g)=s-1$.

We are now ready to apply to induction assumption to the inner sum in (17). We have

$$\sum_{\mathbf{y}\in\mathbb{Z}^{n-1},\, q\mid f_M(x,\mathbf{y})} W_M\left(\frac{1}{N}(x,\mathbf{y})\right)$$

$$= q^{-1}\sum_{\mathbf{y}\in\mathbb{Z}^{n-1}} W_M\left(\frac{1}{N}(x,\mathbf{y})\right) + O_{n-1,d,L}(D_n(M)N^s q^{(n-s-1)/2}),$$

where $D_n(M)$ is the maximum of all n-th order partial derivatives of $W_M(x,\mathbf{y})$. In view of the definition of W_M we have

$$D_n(M)\ll_{n,d,L} D_n,$$

whence, on summing over x, we see from (17) that

$$\sum_{\mathbf{x}\in\mathbb{Z}^n,\, q\mid f(\mathbf{x})} W\left(\frac{1}{N}\mathbf{x}\right) = \sum_{-NL'\leqslant x\leqslant NL'} \sum_{\mathbf{y}\in\mathbb{Z}^{n-1},\, q\mid f_M(x,\mathbf{y})} W_M\left(\frac{1}{N}(x,\mathbf{y})\right)$$

$$= \sum_{-NL'\leqslant x\leqslant NL'} q^{-1}\sum_{\mathbf{y}\in\mathbb{Z}^{n-1}} W_M\left(\frac{1}{N}(x,\mathbf{y})\right)$$

$$+ O_{n,d,L}(D_n N^{s+1} q^{(n-s-1)/2}).$$

Since $D_n\ll D_{n+1}$, the error term is of the form required for Theorem 3. Moreover, since, W_M is supported on a cube of side $2L'$, the main term is just

$$q^{-1}\sum_{x\in\mathbb{Z}}\sum_{\mathbf{y}\in\mathbb{Z}^{n-1}} W_M\left(\frac{1}{N}(x,\mathbf{y})\right) = q^{-1}\sum_{\mathbf{x}\in\mathbb{Z}^n} W_M\left(\frac{1}{N}\mathbf{x}\right)$$

$$= q^{-1}\sum_{\mathbf{x}\in\mathbb{Z}^n} W\left(\frac{1}{N}\mathbf{x}\right),$$

since M is a unimodular integer matrix. The main term is therefore also of the form required for Theorem 3.

6. Proof of Lemma 4

Lemma 4 will be deduced from Lemma 3, together with the following result.

Lemma 5. *Let q be a prime, and let g be a homogeneous form of degree d in n variables, defined over the field K of q elements. Suppose further that $2 \leqslant d < q$. For any non-zero vector $\mathbf{m} \in K^n$ let $g^{(\mathbf{m})}$ be the form in $n-1$ variables obtained by substituting $\mathbf{m}.\mathbf{x} = \mathbf{0}$ in $g(\mathbf{x})$, and let $s(g)$ and $s(g^{(\mathbf{m})})$ be defined as in Theorem* 3. *Then $s(g^{(\mathbf{m})}) \geqslant s(g) - 1$ for all non-zero $\mathbf{m}$. Moreover if $s(g) \neq -1$, there is a non-zero form G depending on g, such that the degree of G is bounded in terms of n and d alone, and such that $s(g^{(\mathbf{m})}) = s(g) - 1$ whenever $q \nmid G(\mathbf{m})$.*

Lemma 4 clearly follows from Lemmas 3 and 5, since Lemma 3, with $s = 1, r = n-1$ and $D = O_{n,d}(1)$ will produce a non-zero $\mathbf{m}$ with $q \nmid G(\mathbf{m})$ and $|\mathbf{m}| \leqslant B$, as soon as $B \gg_{n,d} 1$.

Lemma 5 is essentially contained in § 2 of Hooley [8]. However, since the result we require is not explicitly stated by Hooley, we shall give an appropriate modification of Hooley's treatment here.

We begin our proof by making a linear change of variables so that the hyperplane $\mathbf{m}.\mathbf{x} = 0$ becomes $x_1 = 0$. The singular loci $\mathscr{S}$ and $\mathscr{S}^{(\mathbf{m})}$ of g and $g^{(\mathbf{m})}$ are then given by the systems

$$\frac{\partial g}{\partial x_1} = \ldots = \frac{\partial g}{\partial x_n} = 0$$

and

$$x_1 = \frac{\partial g}{\partial x_2} = \ldots = \frac{\partial g}{\partial x_n} = 0$$

respectively. We shall write $\mathscr{L}$ for the hyperplane $x_1 = 0$ and $\mathscr{S}_0$ for the set

$$\frac{\partial g}{\partial x_2} = \ldots = \frac{\partial g}{\partial x_n} = 0.$$

Thus

$$\mathscr{S}^{(\mathbf{m})} \cap \left\{ \frac{\partial g}{\partial x_1} = 0 \right\} = \mathscr{S} \cap \mathscr{L},$$

whence

$$\begin{aligned} s(g^{(\mathbf{m})}) &= \dim(\mathscr{S}^{(\mathbf{m})}) \\ &\geqslant \dim\left(\mathscr{S}^{(\mathbf{m})} \cap \left\{ \frac{\partial g}{\partial x_1} = 0 \right\} \right) \\ &= \dim(\mathscr{S} \cap \mathscr{L}) \\ &\geqslant \dim(\mathscr{S}) - 1 \\ &= s(g) - 1. \end{aligned}$$

It follows that $s(g^{(\mathbf{m})}) \geqslant s(g) - 1$, as required. Moreover if $s(g^{(\mathbf{m})}) \neq s(g) - 1$, then either

$\dim(\mathscr{S} \cap \mathscr{L}) = \dim(\mathscr{S})$ or

$$\dim(\mathscr{S}^{(\mathbf{m})}) > \dim\left(\mathscr{S}^{(\mathbf{m})} \cap \left\{ \frac{\partial g}{\partial x_1} = 0 \right\} \right). \tag{18}$$

In the former case one sees that $\mathscr{L}$ must contain an irreducible component of $\mathscr{S}$ of maximal dimension. Reverting to our original coordinate system we therefore let $\mathscr{M}_1$ be the set of non-zero vectors $\mathbf{m}$ for which the hyperplane $\mathbf{m}.\mathbf{x} = 0$ contains an irreducible component of the singular locus $\nabla g = \mathbf{0}$ of maximal dimension. The number D', say of such components satisfies $D' = O_{n,d}(1)$ (as in the proof of Lemma 3) and picking a point $\mathbf{p}_i$ from each we deduce that

$$G_0(\mathbf{m}) = \prod_i \mathbf{p}_i.\mathbf{m} = 0$$

whenever $\mathbf{m} \in \mathscr{M}_1$. It may happen that the form G_0 is defined over a finite extension K' of K, in which case a suitable constant multiple of the form G_0 will have a trace G_1 which does not vanish identically. Then G_1 is defined over K, has degree D', and has the property that $G_1(\mathbf{m}) = 0$ whenever $\mathbf{m} \in \mathscr{M}_1$.

We write $\mathscr{M}_2$ for the set of non-zero vectors $\mathbf{m}$ for which (18) holds. For such an $\mathbf{m}$ there is a point $\mathbf{p}$, say, in $\mathscr{S}^{(\mathbf{m})}$, for which $\partial g/\partial x_1 \neq 0$. It follows that $p_1 = 0$, since $\mathbf{p}$ is on $\mathscr{L}$, and that

$$\frac{\partial g}{\partial x_2} = \ldots = \frac{\partial g}{\partial x_n} = 0$$

at $\mathbf{p}$. We therefore see that $\mathbf{p}.\nabla g(\mathbf{p}) = 0$, whence $g(\mathbf{p}) = 0$. Moreover $\nabla g(\mathbf{p})$ is proportional to the vector $(1, 0, 0, \ldots, 0)$. On returning to our original coordinate system we see that every $\mathbf{m} \in \mathscr{M}_2$ can be represented as $\nabla g(\mathbf{p})$ for some $\mathbf{p}$ on the hypersurface $g = 0$. Here $\mathbf{p}$ may be defined over some finite extension of K.

We now show that there is a non-zero form G_2 of degree $D'' = O_{n,d}(1)$ such that $G_2(\nabla g(\mathbf{x}))$ is identically divisible by $g(\mathbf{x})$. To do this we observe, via elimination theory, that for any $\mathbf{y}$, the equation $\nabla g(\mathbf{x}) = \mathbf{y}$ is solvable with $g(\mathbf{x}) = 0$, if and only if $\mathbf{y}$ satisfies one of a set of conditions

$$C_i: E_{1,i}(\mathbf{y}) = 0 \quad \text{and} \quad E_{2,i}(\mathbf{y}) \neq 0, \ (1 \leqslant i \leqslant I).$$

Here $E_{1,i}$ and $E_{2,i}$ are forms of degrees $O_{n,d}(1)$ and $I = O_{n,d}(1)$. If $E_{1,i}$ were to vanish identically for every i then the image of $g = 0$ under ∇ would be a non-empty Zariski open subset a affine n-space, and would therefore have dimension n. Since $g = 0$ only has dimension $n - 1$, we conclude that at least one of the forms $E_{1,i}$ does not vanish. Taking G_2 to be any such form we have $G_2(\nabla g(\mathbf{x})) = 0$ whenever $g(\mathbf{x}) = 0$, whence $g(\mathbf{x})$ divides $G_2(\nabla g(\mathbf{x}))$ as required.

Finally we observe that $G_2(\mathbf{m}) = 0$ whenever $\mathbf{m} \in \mathscr{M}_2$. Lemma 5 now follows on taking $G = G_1 G_2$ and $D = D' + D''$.

7. Acknowledgement

It is a pleasure to record the support of the Isaac Newton Institute, Cambridge, where this work was carried out.

References

[1] Birch B J, Forms in many variables, *Proc. R. Soc.* **A265** (1961/62) 245–263
[2] Cohen S D, The distribution of Galois groups and Hilbert's irreducibility theorem, *Proc. Lond. Math. Soc.* (*3*), **43** (1981) 227–250
[3] Franke J, Manin Y I and Tschinkel Y, Rational points of bounded height on Fano varieties, *Invent. Math.* **95** (1989) 421–435
[4] Fujiwara M, Upper bounds for the number of lattice points on hypersurfaces, *Number theory and combinatorics, Japan, 1984* (Singapore: World Scientific Publishing Co.) (1985)
[5] Graham S W and Ringrose C J, Lower bounds for least quadratic non-residues, Analytic number theory, Allerton Park, II 1989 *Prog. Math.*, **85** (Boston: Birkhauser) (1990) 245–263
[6] Heath-Brown D R, Hybrid bounds for L-functions: a q-analogue of van der Corput's method and a t-analogue of Burgess' method, *Recent progress in analytic number theory, Vol. I*, (London: Academic Press) (1981) 121–126
[7] Heath-Brown D R, Cubic forms in ten variables, *Proc. Lond. Math. Soc.* (*3*), **47** (1983), 225–257
[8] Hooley C, On the number of points on a complete intersection over a finite field, *J. Number Theory*, **38** (1991) 338–358
[9] Shararevich I R, *Basic algebraic geometry*, (New York: Springer) (1977)