ACTA ARITHMETICA
XLIV (1984)

Bounds for exponential sums*

by

Wolfgang M. Schmidt (Boulder, Colo.)

1. Introduction. Let F_q be the finite field of $q = p^l$ elements where p is a prime. Suppose $\mathfrak{P}(X) = \mathfrak{P}(X_1, \ldots, X_s)$ is a polynomial with coefficients in F_q. Consider the sum

$$S = \sum_{x} e\big(p^{-1}\,\mathfrak{T}(\mathfrak{P}(x))\big),$$

where $e(z) = e^{2\pi iz}$, where $\mathfrak{T}$ denotes the trace from F_q to the prime field F_p, and where the sum is over the points x of F_q^s.

Suppose that $d \geqslant 2$ and that

$$\mathfrak{P} = \mathfrak{F}^{(d)} + \ldots + \mathfrak{F}^{(1)} + \mathfrak{F}^{(0)}, \tag{1.1}$$

where $\mathfrak{F}^{(j)}$ is a form of degree j. We write

$$h = h(\mathfrak{P}) = h(\mathfrak{F}^{(d)})$$

for the smallest number h such that $\mathfrak{F}^{(d)}$ may be written as

$$\mathfrak{F}^{(d)} = \mathfrak{A}_1 \mathfrak{B}_1 + \ldots + \mathfrak{A}_h \mathfrak{B}_h \tag{1.2}$$

with forms $\mathfrak{A}_i$, $\mathfrak{B}_i$, each of positive degree and with coefficients in F_q. The quantity h is invariant under linear substitutions of the variables with coefficients in F_q.

Theorem 1. *For $p > d$ we have*

$$|S| \ll q^{s-\varkappa} \tag{1.3}$$

with

$$\varkappa = 2^{1-d} \lceil h/\Phi(d) \rceil, \tag{1.4}$$

where $\lceil \alpha \rceil$ denotes the smallest integer $\geqslant \alpha$, and where $\Phi(d)$ depends only on d. We may take e.g. $\Phi(2) = \Phi(3) = 1$, $\Phi(4) = 3$, $\Phi(5) = 13$, and $\Phi(d) < (\log 2)^{-d} d!$ in general. The constant in $\ll$ depends only on s and d.

* Written with partial support from NSF-MCS-8211461.

The common zeros of $\mathfrak{A}_1, \mathfrak{B}_1, \ldots, \mathfrak{A}_h, \mathfrak{B}_h$ in (1.2) are singular points of $\mathfrak{I}^{(d)}$, and hence $s-2h \leqslant \dim V^*$, where V^* is the locus of singular points of $\mathfrak{I}^{(d)}$ (in some "universal domain"). So our bound is useful in particular when $\dim V^*$ is rather smaller than s. In the case when $\mathfrak{I}^{(d)}$ is nonsingular, $h \geqslant s/2$, but in this case Deligne [6] has given the much sharper estimate $|S| \ll q^{s/2}$. It is reasonable to expect that eventually Theorem 1 (in a sharper form) will be a consequence of Deligne's work and of algebraic geometry. But at present, our conclusion has not been derived in this way. This is because our present knowledge of Betti numbers is poor.

Conversely, our theorem yields information about Betti numbers. Let $\bar{h} = \bar{h}(\mathfrak{P})$ be the least number h such that $\mathfrak{I}^{(d)}$ may be written in the form (1.2), with forms $\mathfrak{A}_i$, $\mathfrak{B}_i$ of positive degree having coefficients in the algebraic closure $\bar{\boldsymbol{F}}_q$ of $\boldsymbol{F}_q$. According to our theorem, the sums

$$S_l = \sum_{\boldsymbol{x} \in \boldsymbol{F}_{q^l}^s} e\big(p^{-1}\,\mathfrak{T}_l(\mathfrak{P}(\boldsymbol{x}))\big),$$

where $\mathfrak{T}_l$ is the trace from $\boldsymbol{F}_{q^l}$ to $\boldsymbol{F}_p$, have

$$|S_l| \ll q^{l(s-\bar{\varkappa})},$$

where $\bar{\varkappa}$ is defined just like $\varkappa$ by (1.4), but with $\bar{h}$ in place of h. It follows ([7], Chapter 2) that the Betti numbers B_r with $r > 2s-2\bar{\varkappa}$ vanish.

The case $d = 3$ of Theorem 1 is due to Davenport and Lewis [5], who point out that the case $d = 2$ is fairly obvious. Their work is based on a method developed by Davenport [4] in his investigation of cubic equations. The present work is based on the author's extension [13] of Davenport's approach to forms of degree higher than 3. Our method is "elementary", but perhaps not simple.

The sums of Theorem 1 are "complete" sums. We next will consider "incomplete" sums, of the type

$$S_{\mathfrak{B}} = \sum_{\boldsymbol{x} \in \mathfrak{B}} e\big(p^{-1}\,\mathfrak{T}(\mathfrak{P}(\boldsymbol{x}))\big),$$

where $\mathfrak{B}$ is a "box" contained in $\boldsymbol{F}_q^s$. That is,

$$\mathfrak{B} = \mathfrak{J}_1 \times \ldots \times \mathfrak{J}_s, \tag{1.5}$$

with $\mathfrak{J}_i$ a set of elements $\alpha_i + c_{i1}\alpha_{i1} + \ldots + c_{il}\alpha_{il}$ in $\boldsymbol{F}_q$, where α_i is a fixed element of $\boldsymbol{F}_q$, where $\alpha_{i1}, \ldots, \alpha_{il}$ is a fixed basis of $\boldsymbol{F}_q$ over $\boldsymbol{F}_p$, and where the c_{ij} $(1 \leqslant i \leqslant s,\ 1 \leqslant j \leqslant l)$ run through the integers in $1 \leqslant c_{ij} \leqslant P_{ij}$, where the P_{ij} are fixed integers in $1 \leqslant P_{ij} \leqslant p$. In the case when $P_{ij} = p$ $(1 \leqslant i \leqslant s,\ 1 \leqslant j \leqslant l)$, the box $\mathfrak{B} = \boldsymbol{F}_q^s$, and $S_{\mathfrak{B}}$ is the complete sum S. In general, when $1 \leqslant P_{ij} \leqslant P \leqslant p$ $(1 \leqslant i \leqslant s,\ 1 \leqslant j \leqslant l)$, we will say that $\mathfrak{B}$ is *of size* $\leqslant P$. On the other hand we will say that $\mathfrak{B}$ is *of size* $\geqslant P$ when $1 \leqslant P \leqslant P_{ij} < p$.

THEOREM 2. *Let* $P = p^\delta$ *where* $d^{-1} < \delta \leqslant 1$, *and put*

$$\varkappa = \varkappa(\delta) = (d-\delta^{-1})(d-1)^{-1}\,2^{1-d}\lceil h/\Phi(d)\rceil. \tag{1.6}$$

Then if $\mathfrak{B}$ *is a box of size* $\leqslant P$, *we have for every* $\varepsilon > 0$

$$|S_{\mathfrak{B}}| \ll P^{sl-\varkappa l+\varepsilon}, \tag{1.7}$$

with the constant in $\ll$ *depending only on* s, d, l, δ, ε.

Except for the ε in the exponent, and the dependency of the constant on ε and l (which renders the assertion useless for small p), Theorem 2 contains Theorem 1 as the special case $\delta = 1$.

Serre ([15], théorème A.5) has pointed out how a method of Hua leads from information on complete sums to information on incomplete sums. But this approach leads to nontrivial bounds only when $\delta > 1/2$. Hence it appears that the present methods of algebraic geometry are by and large unsuitable for incomplete sums. It should be noted that our restriction $\delta > d^{-1}$ is a natural one: when $\delta < d^{-1}$ and when the coefficients of $\mathfrak{P}$ are small, then clearly one cannot expect much more than the trivial bound.

Now let $\boldsymbol{\mathfrak{P}} = (\mathfrak{P}_1, \ldots, \mathfrak{P}_r)$ be an r-tuple of polynomials. We are not so much interested in these r polynomials themselves, as we are in the *pencil* generated by them, i.e. the set of polynomials

$$\mathfrak{P} = \boldsymbol{a}\boldsymbol{\mathfrak{P}} = a_1\mathfrak{P}_1 + \ldots + a_r\mathfrak{P}_r$$

with $\boldsymbol{a} = (a_1, \ldots, a_r) \in \boldsymbol{F}_q^r$, but $\boldsymbol{a} \neq \boldsymbol{0}$. We will suppose that each polynomial of the pencil is of degree $\geqslant 2$. Then we define

$$h(\boldsymbol{\mathfrak{P}}) := \min h(\mathfrak{P}), \tag{1.8}$$

with the minimum to be taken over polynomials $\mathfrak{P}$ of the pencil. In the special case when each polynomial of the pencil is of degree d, and using the notation (1.1) for each $\mathfrak{P}_i$, we have $h(\boldsymbol{\mathfrak{P}}) = h(\boldsymbol{\mathfrak{I}}^{(d)})$ with $\boldsymbol{\mathfrak{I}}^{(d)} = (\mathfrak{I}_1^{(d)}, \ldots, \mathfrak{I}_r^{(d)})$. More generally, when each polynomial is of degree $\leqslant d$, one has $s - 2h \leqslant \dim V^*$, where V^* is the manifold of singular points of $\boldsymbol{\mathfrak{I}}^{(d)}$, i.e. points where the matrix $(\partial\mathfrak{I}_i^{(d)}/\partial x_j)$ $(1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant s)$ has rank $< r$. Thus $h \geqslant s/2$ when $\boldsymbol{\mathfrak{I}}^{(d)}$ is nonsingular.

Given a box $\mathfrak{B} \subseteq \boldsymbol{F}_q^s$, denote its cardinality by $|\mathfrak{B}|$, and write $N_{\mathfrak{B}} = N_{\mathfrak{B}}(\boldsymbol{\mathfrak{P}})$ for the number of common zeros of $\boldsymbol{\mathfrak{P}}$ in $\mathfrak{B}$.

THEOREM 3. *Let* $\boldsymbol{\mathfrak{P}}$ *be an* r*-tuple of polynomials such that every polynomial in its pencil has a degree between* d_0 *and* d, *where* $2 \leqslant d_0 \leqslant d$ *are given. Suppose that* $p > d$, *that* $P = p^\delta$ *with* $d_0^{-1} < \delta \leqslant 1$. *Write* $h = h(\boldsymbol{\mathfrak{P}})$, *and let* $\varkappa = \varkappa(\delta)$ *be defined by* (1.6). *Then given* $\varepsilon > 0$ *and given a box* $\mathfrak{B}$ *of* $\boldsymbol{F}_q^s$ *of size* $\leqslant P$, *we have*

$$N_{\mathfrak{B}} = q^{-r}|\mathfrak{B}| + O(P^{sl-\varkappa l+\varepsilon}), \tag{1.9}$$

with a constant in O *depending only on* s, d, l, δ, ε.

In particular, $N_{\mathfrak{B}} > 0$ when $\mathfrak{B}$ is a box of size $\geqslant p^{\delta}$, provided that

$$h > r(d-1)(d\delta-1)^{-1}2^{d-1}\Phi(d), \tag{1.10}$$

and that $p > p_1(s, d, r, l, \delta)$.

Estimates for $N_{\mathfrak{B}}$ had been given by several authors, e.g. Chalk and Williams [3], and Smith [16]. It follows immediately (at least in the case when $q = p$, i.e. $l = 1$) from work of Deligne and the Appendix of Serre [15] that

$$N_{\mathfrak{B}} = q^{-r}|\mathfrak{B}| + O\left(q^{s/2}(\log p)^{ls}\right) \tag{1.11}$$

when the form of highest degree of each polynomial of the pencil is nonsingular, so in particular when the r-tuple $\mathfrak{F}^{(d)}$ is nonsingular. The constant in O here depends on s, d, l. Hence $N_{\mathfrak{B}} > 0$ when

$$|\mathfrak{B}| > c_1(s, d, l)\, q^{(s/2)+r}(\log p)^{ls}. \tag{1.12}$$

Myerson [9] in the case $q = p$ used Deligne's results more carefully to see that (under some extra conditions on $\mathfrak{P}$) $N_{\mathfrak{B}} > 0$ when $p > p_2(s, d, \varepsilon)$ and

$$|\mathfrak{B}| > (1+\varepsilon)^s(2d-2)^s p^{(s/2)+r}. \tag{1.13}$$

In particular, $N_{\mathfrak{B}} > 0$ when $\mathfrak{B}$ is a box of size

$$> (1+\varepsilon)(2d-2)\, p^{(1/2)+(r/s)}.$$

In these results which follow from Deligne's work, it was assumed that the form of highest degree of each polynomial of the pencil was nonsingular. We do not have this requirement in Theorem 3. But the biggest difference is that (1.11), (1.12), (1.13) give significant results only for boxes of size $\geqslant p^{\delta}$ with $\delta > 1/2$, whereas we allow δ to lie in $d_0^{-1} < \delta \leqslant 1$.

THEOREM 4. *Given d, r, and $\delta > 1/2$, there is an $s_1 = s_1(d, r, \delta)$ as follows. Let $\mathfrak{F}$ be a system of r forms of degree $\leqslant d$ with integer coefficients in $s > s_1$ variables. Then for every prime p, the system of congruences*

$$\mathfrak{F}(\boldsymbol{x}) \equiv \boldsymbol{0} \pmod{p} \tag{1.14}$$

has a solution $\boldsymbol{x} \neq \boldsymbol{0}$ whose size $|\boldsymbol{x}| = \max(|x_1|, \ldots, |x_s|)$ has

$$|\boldsymbol{x}| \ll p^{\delta}, \tag{1.15}$$

with a constant in $\ll$ which depends only on d, r, δ.

The theorem probably remains true with the prime p replaced by an arbitrary modulus m. I hope to come back to this question in subsequent work.

When k is even and $\mathfrak{F} = (X_1^2 + \ldots + X_s^2)^{k/2}$, then every solution $\boldsymbol{x} \neq \boldsymbol{0}$ of (1.14) has $|\boldsymbol{x}| \geqslant p^{1/2}$, which shows that the theorem would become false for $\delta < 1/2$. The case $\delta = 1/2$ is open. But in the case when all the forms of $\mathfrak{F}$ are of odd degree, the theorem is true for any $\delta > 0$. In this case the author [11] has shown that the system of diophantine equations $\mathfrak{F}(\boldsymbol{x}) = \boldsymbol{0}$ has a solution with $0 < |\boldsymbol{x}| \ll p^{\delta}$ if the coefficients of $\mathfrak{F}$ have modulus $\leqslant p$. The interesting case of Theorem 4 is thus when the forms of $\mathfrak{F}$ are even degree. The following cases had been obtained with an arbitrary modulus m. Schinzel, Schlickewei and Schmidt [10] dealt with a single quadratic form, and R. C. Baker [1] with a system of quadratic forms. He also dealt with a single quartic form, but only with $\delta > 3/4$.

2. Composite moduli. Given a form $\mathfrak{F}$ of degree $d \geqslant 2$ with coefficients in a commutative ring A, we can again define $h = h(\mathfrak{F})$: It is the smallest integer such that $\mathfrak{F}$ may be written as (1.2), with $\mathfrak{A}_i$, $\mathfrak{B}_i$ being forms of positive degree with coefficients in A. In particular, when $A = A_m = \boldsymbol{Z}/m\boldsymbol{Z}$ and when $\mathfrak{F}$ is a form in $A_m[X]$, the invariant $h(\mathfrak{F})$ is well defined. More generally, let a be a divisor of m. There is a natural map $A_m \to A_a$, and a natural map of polynomial rings $A_m[X] \to A_a[X]$, mapping $\mathfrak{F}(X) \mapsto \mathfrak{F}_a(X)$, say. We write $h_a(\mathfrak{F}) = h(\mathfrak{F}_a)$, and we define $h_a(\mathfrak{P})$ for polynomials $\mathfrak{P}$ in $A_m[X]$ of degree $\leqslant d$ by using their homogeneous part $\mathfrak{F}^{(d)}$.

Again when $\mathfrak{P} \in A_m[X]$, we consider sums

$$S_{\mathfrak{B}} = \sum_{x \in \mathfrak{B}} e\left(m^{-1}\mathfrak{P}(x)\right),$$

where $\mathfrak{B}$ is a box in A_m^s, i.e. it is a product set (1.5) where $\mathfrak{F}_i$ is a set of elements $\alpha_i + c_i\beta_i$ in A_m, where α_i is a fixed element of A_m, β_i is a fixed unit of A_m, and c_i $(i = 1, \ldots, s)$ runs through $1, 2, \ldots, P_i$, with the P_i being fixed integers in $1 \leqslant P_i \leqslant m$. The box is said to be of size $\leqslant P$ if $1 \leqslant P_i \leqslant P \leqslant m$.

THEOREM 5. *Let $\mathfrak{P}$ be a polynomial of degree $\leqslant d$ with coefficients in A_m where m is square free. Let $\mathfrak{B}$ be a box of size $\leqslant P = m^{\delta}$ with $d^{-1} < \delta \leqslant 1$. Suppose that*

$$|S_{\mathfrak{B}}| \geqslant P^{s-K}$$

where $K \geqslant 1$. When $\Gamma > 1$ is an integer and when $m \geqslant m_1(s, d, \delta, \Gamma)$, there is a factorization $m = ab$ such that $b \leqslant P^{1/\Gamma}$ and

$$h_a(\mathfrak{F}^{(d)}) \leqslant (d-\delta^{-1})^{-1}d^2 2^{d-1}\Phi(d)K\Gamma. \tag{2.1}$$

3. A basic inequality. Let G, H be additive groups, and $\mathfrak{G}$ a map $G \to H$. As in [11], define

$$\mathfrak{G}_k(g_1, \ldots, g_k) = \sum_{\varepsilon_1=0}^{1} \ldots \sum_{\varepsilon_k=0}^{1} (-1)^{\varepsilon_1+\ldots+\varepsilon_k}\mathfrak{G}(\varepsilon_1 g_1 + \ldots + \varepsilon_k g_k),$$

so that $\mathfrak{G}_k$ is a symmetric function from $G \times \ldots \times G$ into H. Given a subset $\mathfrak{A} \subseteq G$, we write $\mathfrak{A}^D$ for the difference set, i.e. the set of differences $a - a'$ with $a, a' \in \mathfrak{A}$. Let $\mathfrak{A} - g$ be the translated set of elements $a - g$ with $a \in \mathfrak{A}$, and let

$$\mathfrak{A}(g_1, \ldots, g_t) = \bigcap_{\varepsilon_1=0}^{1} \ldots \bigcap_{\varepsilon_t=0}^{1} (\mathfrak{A} - \varepsilon_1 g_1 - \ldots - \varepsilon_t g_t).$$

When $\mathfrak{A}$ is finite, its cardinality is denoted by $|\mathfrak{A}|$.

The exponential function $e(z) = e^{2\pi i z}$ is defined for $z \in \boldsymbol{R}/\boldsymbol{Z}$.

LEMMA 3.1. *Let $\mathfrak{G}$ be a map $G \to H$ where H is a subgroup of $\boldsymbol{R}/\boldsymbol{Z}$. Let $\mathfrak{A}$ be a finite subset of G, and put*

$$S = S_{\mathfrak{A}} = \sum_{g \in \mathfrak{A}} e(\mathfrak{G}(g)). \tag{3.1}$$

Then for each $d \geqslant 2$,

$$|S|^{2^{d-1}} \leqslant |\mathfrak{A}^D|^{2^{d-1}-d} \sum_{g_1 \in \mathfrak{A}^D} \ldots \sum_{g_{d-1} \in \mathfrak{A}^D} \Big| \sum_{g_d \in \mathfrak{A}(g_1, \ldots, g_{d-1})} e(\mathfrak{G}_d(g_1, \ldots, g_d))\Big|.$$

Proof. This is a version of Weyl's inequality. It was shown in the case $G = \boldsymbol{Z}^s$ in [13], Lemma 11.1, and in the case $\mathfrak{A} = G$ in [12], Lemma 5. The general case is an obvious generalization.

4. A subset $\mathfrak{M}$ of G^{d-1}, and complete sums. Again let $\mathfrak{G}$: $G \to H$ be a map of additive groups. In [12], Lemma 1, we showed that $\mathfrak{G}_d(g_1, \ldots, g_d)$ where $d \geqslant 1$ is "multilinear", i.e. it is a homomorphism in each argument g_i, if and only if $\mathfrak{G}_{d+1}(g_1, \ldots, g_{d+1})$ is identically zero. Such a map will be called a *polynomial of degree* $\leqslant d$.

So now let $\mathfrak{G}$: $G \to H$ be a polynomial of degree $\leqslant d$ where $d \geqslant 2$. With $\mathfrak{G}$ we associate the subset $\mathfrak{M}$ of $G^{d-1} = G \times \ldots \times G$, consisting of $(g_1, \ldots, g_{d-1})$ for which $\mathfrak{G}_d(g_1, \ldots, g_{d-1}, g) = 0$, identically in g. If, say, $e_1, \ldots, e_T$ is a set of generators of G, then $(g_1, \ldots, g_{d-1})$ lies in $\mathfrak{M}$ precisely when $\mathfrak{G}_d(g_1, \ldots, g_{d-1}, e_i) = 0$ $(1 \leqslant i \leqslant T)$.

LEMMA 4.1. *Suppose G is finite, $\mathfrak{G}$ is a polynomial from G into $H \subseteq \boldsymbol{R}/\boldsymbol{Z}$ of degree $\leqslant d$ where $d \geqslant 2$, and S is given by* (3.1) *with $\mathfrak{A} = G$, so that S is a complete sum. Then*

$$|S|^{2^{d-1}} \leqslant |G|^{2^{d-1}-d+1} |\mathfrak{M}|.$$

Proof. This follows from [12], Lemma 6, and is an easy consequence of Lemma 3.1: consider the inner sum in the conclusion of that lemma. We have $\mathfrak{A}(g_1, \ldots, g_{d-1}) = G$, and $e(\mathfrak{G}_d(g_1, \ldots, g_{d-1}, g)) = \chi(g)$, say, is a character on G. Thus the inner sum is a character sum, and it is equal to $|G|$ when $(g_1, \ldots, g_{d-1}) \in \mathfrak{M}$, and equal to 0 otherwise.

LEMMA 4.2. *Make the assumptions of Lemma* 4.1, *in the special case when $G = \boldsymbol{F}_q^s$. Then for each K we have either*

$$|S| \leqslant q^{s-K},$$

or

$$|\mathfrak{M}| \geqslant q^{s(d-1)-2^{d-1}K}.$$

Proof. This is an immediate consequence of the preceding lemma.

LEMMA 4.3. *Let $G = \boldsymbol{F}_q^s$ and $H = (p^{-1}\boldsymbol{Z}/\boldsymbol{Z})$, i.e. the rationals $p^{-1}a$ with $a \in \boldsymbol{Z}$, taken modulo 1. Let $\mathfrak{P}(X) = \mathfrak{P}(X_1, \ldots, X_s)$ be a polynomial in the traditional sense of the type* (1.1) *and with coefficients in $\boldsymbol{F}_q$. Then*

$$\mathfrak{G}(x) = p^{-1}\mathfrak{T}(\mathfrak{P}(x))$$

is a polynomial of degree $\leqslant d$ from G to H in the sense of this section. Moreover, $\mathfrak{M}(\mathfrak{G}) = \mathfrak{M}(\mathfrak{F}^{(d)})$, i.e. $\mathfrak{M} = \mathfrak{M}(\mathfrak{G})$ consists of $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{d-1})$ with $\boldsymbol{x}_i \in \boldsymbol{F}_q^s$ having $\mathfrak{F}_d^{(d)}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{d-1}, X) = 0$, identically in X.

Proof. First of all, the map $\boldsymbol{x} \mapsto \mathfrak{P}(x)$ is a polynomial of degree $\leqslant d$ in the sense of this section from G into $H_1 = \boldsymbol{F}_q$. We have $\mathfrak{P}_d(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_d) = \mathfrak{F}_d^{(d)}(x_1, \ldots, x_d)$. Next, the map $x \mapsto p^{-1}\mathfrak{T}(x)$ is a homomorphism from H_1 into H. Thus

$$\mathfrak{G}_d(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_d) = p^{-1}\mathfrak{T}(\mathfrak{F}_d^{(d)}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_d)),$$

and this is multilinear. So $\mathfrak{G}$ is a polynomial of degree $\leqslant d$.

Now if $x \in \boldsymbol{F}_q$ is such that $p^{-1}\mathfrak{T}(\alpha x) = 0$ (the zero element of H) for each $\alpha \in \boldsymbol{F}_q$, then necessarily $x = 0$. Further $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{d-1})$ lies in $\mathfrak{M} = \mathfrak{M}(\mathfrak{G})$ precisely when $p^{-1}\mathfrak{T}(\mathfrak{F}_d^{(d)}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{d-1}, \boldsymbol{x})) = 0$ for each $\boldsymbol{x} \in \boldsymbol{F}_q^s$. Replacing $\boldsymbol{x}$ by $\alpha\boldsymbol{x}$ and noting that $\mathfrak{F}_d^{(d)}$ is linear in each argument, we may conclude that $\mathfrak{F}_d^{(d)}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{d-1}, \boldsymbol{x}) = 0$ for every $\boldsymbol{x} \in \boldsymbol{F}_q^s$, and hence $\mathfrak{F}_d^{(d)}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{d-1}, X) = 0$, identically in X.

5. $\mathfrak{M}$ and incomplete sums. Our goal here is to carry over Lemma 4.2 to incomplete sums as far as possible.

Denote by $\|z\|$ the distance from an element $z \in \boldsymbol{R}/\boldsymbol{Z}$ to the zero element. Then $\|z\| = \min|x|$, over $x \in \boldsymbol{R}$ whose image in $\boldsymbol{R}/\boldsymbol{Z}$ is z.

A finite subset $\mathfrak{B}$ of G will be called a *box* of dimension B if it consists of elements $e_0 + c_1 e_1 + \ldots + c_B e_B$ where $e_0, e_1, \ldots, e_B$ are fixed elements of G, where each c_i runs through some sequence $1, 2, \ldots, Q_i$, and where the $Q_1 Q_2 \ldots Q_B$ elements so obtained are distinct. We will call $e_1, \ldots, e_B$ a *basis* of the box (although the box depends on e_0 as well), and we will say that it is of size $\leqslant P$ if each $Q_i \leqslant P$. Note that the "dimension" B and $e_0, e_1, \ldots, e_B$ are not necessarily determined by $\mathfrak{B}$.

LEMMA 5.1. *Let $\mathfrak{G}$ be a polynomial of degree $\leqslant d$ (where $d \geqslant 2$) from G into $H \subseteq \boldsymbol{R}/\boldsymbol{Z}$. Let $\mathfrak{B} \subseteq G$ be a box of size $\leqslant P$ with basis $e_1, \ldots, e_B$. Define the sum $S_{\mathfrak{B}}$ as in* (3.1). *Then*

$$|S_{\mathfrak{B}}|^{2^{d-1}} \ll P^{(2^{d-1}-d)B} \sum \Big(\prod_{i=1}^{B} \min(P, \|\mathfrak{G}_d(g_1, \ldots, g_{d-1}, e_i)\|^{-1})\Big),$$

where the sum is over $(d-1)$-tuples of elements $g_1, \ldots, g_{d-1}$ of $\mathfrak{B}^D$. The constant in $\ll$ depends only on B, d.

Proof. This is essentially Lemma 13.1 of [13]. When $\mathfrak{L}\colon G \to H$ is "linear", i.e. when it is a homomorphism, then

$$\Big|\sum_{g\in\mathfrak{B}} e(\mathfrak{L}(g))\Big| = \prod_{i=1}^{B} \Big|\sum_{c_i=1}^{Q_i} e(c_i\,\mathfrak{L}(e_i))\Big| \leqslant \prod_{i=1}^{B} \min\Big(Q_i, \frac{2}{|e(\mathfrak{L}(e_i))-1|}\Big)$$
$$\ll \prod_{i=1}^{B} \min(P, \|\mathfrak{L}(e_i)\|^{-1}).$$

We simply have to apply this remark to the inner sum of Lemma 3.1, and we have to observe that $|\mathfrak{B}^D| \ll P^B$, and that each set $\mathfrak{B}(g_1, \ldots, g_{d-1})$ is the union of a bounded number of boxes with basis $e_1, \ldots, e_B$ and of size $\leqslant P$.

Lemma 5.2. *Make the same assumptions as in the preceding lemma. Suppose further that*

$$|S_{\mathfrak{B}}| \geqslant P^{B-K}$$

where $K > 0$. Then the number N of $(d-1)$-tuples of elements $g_1, \ldots, g_{d-1}$ in $\mathfrak{B}^D$ with

$$\|\mathfrak{G}_d(g_1, \ldots, g_{d-1}, e_i)\| < P^{-1} \quad (i = 1, \ldots, B)$$

satisfies

$$N \gg P^{B(d-1)-2^{d-1}K-\varepsilon},$$

where $\varepsilon > 0$ is arbitrary and where the constant in $\gg$ depends only on B, d, ε.

Proof. Just as for Lemma 13.2 of [13].

Let P be natural and let $e_1, \ldots, e_B$ be elements of G. We now make the assumption that

(5.1) *the P^B elements $c_1 e_1 + \ldots + c_B e_B$ with*
$1 \leqslant c_1, \ldots, c_B \leqslant P$ are distinct.

Given a box $\mathfrak{B}$ with basis $e_1, \ldots, e_B$ and of size $\leqslant P$, the difference set $\mathfrak{B}^D$ is contained in the set $\mathfrak{E}(P)$ of elements $c_1 e_1 + \ldots + c_B e_B$ with $|c_i| \leqslant P$ $(i = 1, \ldots, B)$. More generally, when $1 \leqslant R \leqslant P$, write $\mathfrak{E}(R)$ for the set of elements $c_1 e_1 + \ldots + c_B e_B$ with $|c_i| \leqslant R$ $(i = 1, \ldots, B)$. These elements are not necessarily distinct, but by (5.1) at most 3^B of them can be equal.

Lemma 5.3. *Make the same assumptions as in the preceding lemma, and further suppose that (5.1) holds. Let $0 < \eta \leqslant 1$. Then the number $N(\eta)$ of $(d-1)$-tuples $g_1, \ldots, g_{d-1}$ in $\mathfrak{E}(P^\eta)$ with*

$$\|\mathfrak{G}_d(g_1, \ldots, g_{d-1}, e_i)\| < P^{-d+(d-1)\eta} \quad (i = 1, \ldots, B) \tag{5.2}$$

satisfies

$$N(\eta) \gg P^{B(d-1)\eta-2^{d-1}K-\varepsilon}.$$

The constant in $\gg$ depends only on B, d, η, ε.

Proof. This is essentially the case $d = k$ of Lemma 14. 2 of [13]. By our condition (5.1) we lose at most a factor 3^B at each step of the proof.

Given a box $\mathfrak{B}$ and a polynomial $\mathfrak{G}$ as above, write $\mathfrak{M}(R)$ for the subset of $\mathfrak{M}$ consisting of $(g_1, \ldots, g_{d-1})$ in $\mathfrak{M}$ with each $g_i \in \mathfrak{E}(R)$.

Lemma 5.4. *Suppose $d \geqslant 2$ and $\mathfrak{G}$ is a polynomial of degree $\leqslant d$ from G into $H = (m^{-1}\mathbf{Z}/\mathbf{Z})$, i.e. the rationals with denominator m, taken modulo 1. Suppose that $d^{-1} < \delta \leqslant 1$, $\varepsilon > 0$,*

$$0 < \eta < (d-\delta^{-1})/(d-1). \tag{5.3}$$

Suppose $\mathfrak{B} \subseteq G$ is a box of size $\leqslant P = m^\delta$, and with a basis $e_1, \ldots, e_B$ which generates G. Suppose that (5.1) holds. Then given $K > 0$, we have either

$$|S_{\mathfrak{B}}| \leqslant P^{B-K}, \tag{5.4}$$

or $R = P^\eta$ has

$$|\mathfrak{M}(R)| \gg R^{B(d-1)-2^{d-1}(K/\eta)-\varepsilon}. \tag{5.5}$$

The constant in $\gg$ here depends only on B, d, η, ε.

Proof. By (5.3), and since $P = m^\delta$, the right hand side of (5.2) is less than m^{-1}. (At least when $m > 1$; but the case $m = 1$ is trivial.) Since the values of $\mathfrak{G}_d$ lie in $(m^{-1}\mathbf{Z}/\mathbf{Z})$, the relation (5.2) then leads to $\mathfrak{G}_d(g_1, \ldots, g_{d-1}, e_i) = 0$ $(i = 1, \ldots, B)$.

6. Invariants h, $\bar{h}$, $\bar{g}$. Now let F be an arbitrary field, and $\mathfrak{J}$ a form in s variables of degree $d \geqslant 2$ with coefficients in F. One may again define $h = h(\mathfrak{J})$ as the least number k such that $\mathfrak{J}$ may be written as

$$\mathfrak{J} = \mathfrak{A}_1\mathfrak{B}_1 + \ldots + \mathfrak{A}_k\mathfrak{B}_k, \tag{6.1}$$

with forms $\mathfrak{A}_i$, $\mathfrak{B}_i$ of positive degree and with coefficients in F. We further define $\bar{h} = \bar{h}(\mathfrak{J})$ as the least integer k such that $\mathfrak{J}$ may be as (6.1), with forms $\mathfrak{A}_i$, $\mathfrak{B}_i$ having coefficients in any extension field of F. Then clearly $\bar{h}$ is the least number k such that $\mathfrak{J}$ is writeable as (6.1) with coefficients in the algebraic closure $\bar{F}$ of F. We have $\bar{h} \leqslant h$.

We define $\mathfrak{M}$ as the subset of $F^{s(d-1)}$ consisting of $(d-1)$-tuples $\mathbf{x}_1, \ldots, \mathbf{x}_{d-1}$ with $\mathfrak{J}_d(\mathbf{x}_1, \ldots, \mathbf{x}_{d-1}, \mathbf{X}) = 0$, identically in $\mathbf{X}$. Now let Ω be some "universal domain" over F, i.e. a field containing F which is algebraically closed and of infinite transcendence degree over F. We define $\overline{\mathfrak{M}}$ as the set of $(d-1)$-tuples $\mathbf{x}_1, \ldots, \mathbf{x}_{d-1}$ with components in Ω for which $\mathfrak{J}_d(\mathbf{x}_1, \ldots, \mathbf{x}_{d-1}, \mathbf{X}) = 0$. Then $\overline{\mathfrak{M}}$ is an algebraic manifold in $\Omega^{s(d-1)}$; we denote its codimension by $\bar{g} = \bar{g}(\mathfrak{J})$. One proves as in [13], Lemma 16.1, that

$$\bar{g} \leqslant 2^{d-1}\bar{h}. \tag{6.2}$$

Proposition Ī. *When F is of characteristic $> d$, then*

$$\bar{h} < \Phi(d)\bar{g}.$$

The case $\boldsymbol{F} = \boldsymbol{C}$ is Proposition III_C of [13]. Practically no changes are necessary in the general case. (One can avoid formula (20.1) of [11], with $n!$ in the denominator.) Writing $\mathfrak{G}(X) = \mathfrak{J}_d(X, \ldots, X)$, one finds (corresponding to [13], § 23) that $\bar{h}(\mathfrak{G}) \leqslant \Phi(d)\bar{g}(\mathfrak{J})$. When the characteristic exceeds d, then the relation $\mathfrak{G}(X) = (-1)^d d!\,\mathfrak{J}(X)$ shows that also $\bar{h}(\mathfrak{J}) \leqslant \Phi(d)\bar{g}(\mathfrak{J})$.

Now let $\mathfrak{D}(Z)$ be a subset of $\boldsymbol{F}^s$ such that the projection on any coordinate axis contains at most Z elements. Thus $\mathfrak{D}(Z) \subseteq \mathfrak{D}_1 \times \ldots \times \mathfrak{D}_s$ where $\mathfrak{D}_i \subseteq \boldsymbol{F}$ has cardinality $|\mathfrak{D}_i| \leqslant Z$. Let $\mathfrak{M}(\mathfrak{D}(Z))$ consist of $(d-1)$-tuples $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{d-1}) \in \mathfrak{M}$ with each $\boldsymbol{x}_j \in \mathfrak{D}(Z)$ $(j = 1, \ldots, d-1)$.

Proposition I. *Suppose that $\mathfrak{J}$ is a form of degree $d > 1$ with coefficients in a perfect field $\boldsymbol{F}$ of characteristic $> d$. Suppose that for some set $\mathfrak{D}(Z)$, where $Z > 1$, we have*

$$|\mathfrak{M}(\mathfrak{D}(Z))| > CZ^{s(d-1)-\gamma-1}, \tag{6.3}$$

where $C = C(s, d)$ is a constant independent of $\boldsymbol{F}$, $\mathfrak{J}$, and where γ is an integer. Then

$$h(\mathfrak{J}) \leqslant \Phi(d)\gamma. \tag{6.4}$$

This corresponds to Proposition III of [13], which contains essentially the case $\boldsymbol{F} = \boldsymbol{Q}$. We are really interested in Proposition I rather than Proposition Ī, which was stated for background, and since it is a little easier.

The definition of $\bar{g}$ implies (see the Appendix) that

$$|\mathfrak{M}(\mathfrak{D}(Z))| \leqslant BZ^{s(d-1)-\bar{g}}$$

with $B = B(s, d)$. Hence when C is sufficiently large, (6.3) implies that $\gamma \geqslant \bar{g}$, and Proposition Ī gives $\bar{h}(\mathfrak{J}) \leqslant \Phi(d)\gamma$. But this is weaker than (6.4).

The proof of Proposition III in [13] carries over to the present situation. We just have to replace $\boldsymbol{Q}$ by $\boldsymbol{F}$, and $\boldsymbol{C}$ by a universal domain Ω over $\boldsymbol{F}$. The following extra remarks might be helpful.

When V is an algebraic subset of Ω^S, one could define "V is defined over $\boldsymbol{F}$" by either

(i) the ideal $\mathfrak{J}(V)$ of polynomials $f \in \Omega[X]$ which vanish on V has a basis in $\boldsymbol{F}[X]$, or by

(ii) V is the set of zeros of an ideal $\mathfrak{K}$ which has a basis in $\boldsymbol{F}$.

Both of these concepts occur in the proof. E.g. (i) is the required definition for Lemma 19.1 of [13], more precisely for the last assertion of that lemma. On the other hand it is seen that e.g. in Lemma 24.2 of [13] "defined over $\boldsymbol{F}$" refers to property (ii).

However, for a perfect field $\boldsymbol{F}$, every algebraic extension is separable, and hence (i), (ii) are the same by the equivalence of C6, C7 in Lang [8], § III.5.

The second remark is that when $\mathfrak{D}(Z) \subseteq \Omega^S$, then an algebraic set $V \subseteq \Omega^S$ (such as the set V' in [13], § 24) of dimension e has

$$|V \cap \mathfrak{D}(Z)| \leqslant c(S, l)Z^e, \tag{6.5}$$

provided V lies in a certain class $\mathfrak{C}(l)$. This will be proved in the Appendix. As a consequence, [13], (24.3), can again be established, and Proposition I follows as in [13].

7. Proof of Theorems 1 and 2.

Let $\varkappa$ be given by (1.4), and set

$$\gamma = \lceil h(\mathfrak{J})/\Phi(d) \rceil - 1 = 2^{d-1}\varkappa - 1.$$

Put

$$K = \varkappa - (\log C/2^{d-1}\log q),$$

where $C = C(s, d)$ is the constant in Proposition I. Now if S is a complete sum of the type considered in Theorem 1, then by Lemma 4.2 we have either

$$|S| \leqslant q^{s-K} = C^{2^{1-d}} q^{s-\varkappa}, \tag{7.1}$$

or

$$|\mathfrak{M}| \geqslant q^{s(d-1)-2^{d-1}K} = Cq^{s(d-1)-2^{d-1}\varkappa} = Cq^{s(d-1)-\gamma-1}. \tag{7.2}$$

When $p > d$, we may apply Proposition I with $Z = q$ and $\mathfrak{D} = \boldsymbol{F}_q^s$. We see that (7.2), which now is the same as (6.3), leads to $h(\mathfrak{J}) \leqslant \Phi(d)\gamma$, contradicting our choice of γ. Thus (7.1) must hold.

We now turn to Theorem 2. Again set $\gamma = \lceil h(\mathfrak{J})/\Phi(d) \rceil - 1$, but this time let $\varkappa$ be given by (1.6), so that

$$2^{d-1}\varkappa(d-1)(d-\delta^{-1})^{-1} = \gamma + 1.$$

Let $\varepsilon > 0$ be given. Pick η with (5.3), i.e. with $0 < \eta < (d-\delta^{-1})/(d-1)$, and so close to the right end point of this interval that

$$2^{d-1}((\varkappa/\eta) - (\varepsilon/l)) + (\varepsilon/l) < \gamma + 1. \tag{7.3}$$

We can choose $\eta = \eta(s, d, l, \delta, \varepsilon)$. Finally set

$$K = \varkappa l - \varepsilon.$$

The map $\boldsymbol{x} \mapsto \mathfrak{G}(\boldsymbol{x}) = p^{-1}\mathfrak{T}(\mathfrak{P}(\boldsymbol{x}))$ occurring in the sum $S_{\mathfrak{P}}$ is a polynomial of degree $\leqslant d$ from $G = \boldsymbol{F}_q^s$ into $H = (p^{-1}\boldsymbol{Z})/\boldsymbol{Z}$. We now apply Lemma 5.4 with $m = p$, $P = p^\delta$, $B = sl$. The sum $S_{\mathfrak{P}}$ of Theorem 2 then either has (5.4), i.e.

$$|S_{\mathfrak{P}}| \leqslant P^{B-K} = P^{sl-\varkappa l+\varepsilon}, \tag{7.4}$$

or $R = P^\eta$ satisfies (5.5). The constant in $\gg$ in (5.5) depends on $B = sl$, d, η, ε, hence only on s, d, l, δ, ε.

The projection of $\mathfrak{M}(R)$ on each of the s coordinates axes contains at most $Z = (2R+1)^l$ elements. Hence $\mathfrak{M}(R) = \mathfrak{M}(\mathfrak{D}(Z))$, and (5.5) becomes

$$|\mathfrak{M}(\mathfrak{D}(Z))| \gg Z^{s(d-1)-2^{d-1}((\varkappa/\eta)-(\varepsilon/l))-(\varepsilon/l)}.$$

Thus in view of (7.3) we have

$$|\mathfrak{M}(\mathfrak{D}(Z))| \geqslant CZ^{s(d-1)-\gamma-1},$$

provided p, and hence P, R and Z is large. Here $C = C(s, d)$ is the constant of Proposition I. When $p > d$, this proposition yields $h(\mathfrak{I}) \leqslant \Phi(d)\gamma$, which contradicts our choice of γ. Thus (7.4) must hold, and Theorem 2 is correct.

8. Proof of Theorem 3. The relation

$$\sum_{\mathbf{a}\in F_q^r} e(p^{-1}\mathfrak{T}(\mathbf{a}\mathbf{y})) = \begin{cases} q^r & \text{when } \mathbf{y} = \mathbf{0}, \\ 0 & \text{when } \mathbf{y} \in F_q^r \setminus \mathbf{0}, \end{cases}$$

is well known. Thus

$$N_{\mathfrak{B}} = q^{-r}|\mathfrak{B}| + q^{-r} \sum_{\substack{\mathbf{a}\in F_q^r \\ \mathbf{a}\neq \mathbf{0}}} \sum_{\mathbf{x}\in\mathfrak{B}} e\big(p^{-1}\mathfrak{T}(\mathbf{a}\mathfrak{P}(\mathbf{x}))\big). \tag{8.1}$$

Each polynomial $\mathbf{a}\mathfrak{P}$ occurring here is of degree $\geqslant d_0$. Since $d_0^{-1} \cdot \delta \leqslant 1$, given a box $\mathfrak{B}$ of size $\leqslant P = p^\delta$ we may apply Theorem 2, to see that the inner sum on the right hand side of (8.1) is $\ll P^{sl-\varkappa l+\varepsilon}$. Thus (1.9) follows.

Since h is an integer, (1.10) implies that h divided by the right hand side of (1.10) is $\geqslant 1+2\xi$ with $\xi = \xi(d, r, \delta)$. As a consequence, $\delta\varkappa \geqslant r(1+2\xi)$. We choose $\varepsilon = \varepsilon(d, r, \delta) > 0$ with

$$r(1+2\xi)(1-\varepsilon)-\varepsilon \geqslant r+\xi.$$

Now suppose that $\mathfrak{B}$ is a box with $P_{ij} = P = [p^\delta]$, i.e. the integer part of p^δ $(1 \leqslant i \leqslant s,\ 1 \leqslant j \leqslant l)$. Then $|\mathfrak{B}| = P^{sl}$, and (1.9) yields

$$N_{\mathfrak{B}}/|\mathfrak{B}| = q^{-r}+O(P^{-\varkappa l+\varepsilon}).$$

When $p > p^*(d, r, \delta)$, then $P \geqslant p^{\delta(1-\varepsilon)} = q^{(\delta/l)(1-\varepsilon)}$, and since

$$(\varkappa l-\varepsilon)(\delta/l)(1-\varepsilon) > \delta\varkappa(1-\varepsilon)-\varepsilon \geqslant r(1+2\xi)(1-\varepsilon)-\varepsilon \geqslant r+\xi,$$

we have

$$N_{\mathfrak{B}}/|\mathfrak{B}| = q^{-r}(1+O(q^{-\xi})).$$

The constant in O here depends on s, d, r, l, δ, and hence we certainly have $N_{\mathfrak{B}} > 0$ when $p > p_1(s, d, r, l, \delta)$.

9. Proof of Theorem 4. Let $\mathfrak{I} = (\mathfrak{I}^{(k)}, \ldots, \mathfrak{I}^{(2)}, \mathfrak{I}^{(1)})$ be a system of forms, with the subsystem $\mathfrak{I}^{(d)}$ consisting of $r_d \geqslant 0$ forms of degree d. Such a system will be called of type $\mathbf{r} = (r_k, \ldots, r_2, r_1)$. We have to prove that given $\mathbf{r}$ and $\delta > 1/2$, there is an $s_2 = s_2(\mathbf{r}, \delta)$ such that for a system of forms of type $\mathbf{r}$ in $s > s_2$ variables, the congruences (1.14) have a nontrivial solution $\mathbf{x}$ with (1.15).

Given $\mathbf{r} = (r_k, \ldots, r_1)$ and $\mathbf{r}' = (r'_l, \ldots, r'_1)$ with nonnegative integer components and with $r_k \neq 0$, we write $\mathbf{r} \succ \mathbf{r}'$ if either $k > l$ or if $k = l$ and there is a t in $1 \leqslant t \leqslant k$ having $r_t > r'_t$ and $r_i = r'_i$ for $t < i \leqslant k$. Then $\succ$ establishes a well ordering among tuples $\mathbf{r}$, and we may prove Theorem 4 by induction.

Our first observation is that the theorem is true for $\mathbf{r} = (r_1)$, and that the truth of the theorem for $\mathbf{r} = (r_k, \ldots, r_2, 0)$ implies its truth for $(r_k, \ldots, r_2, r_1)$: for when we are given linear forms $\mathfrak{L}_i$ $(i = 1, \ldots, r_1)$ in s variables and with coefficients of absolute value $< p$, they have a common integer zero $\mathbf{y}$ with $0 < |\mathbf{y}| < (sp)^{r_1/(s-r_1)}$ (Cassels [2], § VI.3, Lemma 3; this is sometimes called "Siegel's Lemma"). Thus when $s > \varepsilon^{-1}(1+\varepsilon)r_1$, there is a nontrivial zero with $|\mathbf{y}| \leqslant (sp)^\varepsilon$, and when $s > l(\varepsilon^{-1}(1+\varepsilon)r_1+1)$, there are l linearly independent such zeros $\mathbf{y}_1, \ldots, \mathbf{y}_l$. We now set $\mathbf{x} = z_1\mathbf{y}_1+\ldots+z_l\mathbf{y}_l$. With each form $\mathfrak{I}_i$ of $\mathfrak{I}$ we associate a new form $\mathfrak{I}_i^*(\mathbf{Z}) = \mathfrak{I}_i(Z_1\mathbf{y}_1+\ldots+Z_l\mathbf{y}_l)$. Since the r_1 linear forms $\mathfrak{L}_i^*(\mathbf{Z})$ vanish identically, it remains to solve $\mathfrak{I}_i^*(\mathbf{z}) \equiv \mathbf{0} \pmod{p}$ for a system $\mathfrak{I}^*$ of type $\mathbf{r}$. When $l > s_2(\mathbf{r}, (\delta/2)+(1/4))$, there is such a $\mathbf{z}$ with $|\mathbf{z}| \ll p^{(\delta/2)+(1/4)}$. Thus with $\varepsilon = (\delta/2)-(1/4)$, the vector $\mathbf{x} = z_1\mathbf{y}_1+ +\ldots+z_l\mathbf{y}_l$ will have both (1.14) and (1.15).

It will thus suffice to prove the theorem for $\mathbf{r} = (r_k, \ldots, r_2, 0)$, assuming its truth for each $\mathbf{r}' \prec \mathbf{r}$. Write $r = r_k+\ldots+r_2$, and let N be the number of solutions of (1.14) with (1.15). Thus $N = N_{\mathfrak{B}}$ where $\mathfrak{B}$ is the box $|\mathbf{x}| \leqslant p^\delta$. According to (8.1),

$$N = p^{-r}\Big(|\mathfrak{B}| + \sum_{\substack{\mathbf{a} \pmod{p} \\ \mathbf{a}\neq\mathbf{0}}} \sum_{\mathbf{x}\in\mathfrak{B}} e(p^{-1}\mathbf{a}\mathfrak{I}(\mathbf{x}))\Big).$$

Suppose for the moment that for each $\mathbf{a} \neq \mathbf{0}$, the inner sum over $\mathbf{x}\in\mathfrak{B}$ has absolute value $\leqslant |\mathfrak{B}|\,p^{-r-1}$. Then since the number of possibilities for $\mathbf{a}$ is less than p^r, we obtain

$$N \geqslant p^{-r}|\mathfrak{B}|(1-p^{-1}).$$

In particular, when s is large, we may infer that $N > 1$, and there is a nontrivial solution in the box $\mathfrak{B}$.

We may therefore suppose that at least one of the inner sums is $> |\mathfrak{B}|\,p^{-r-1}$ in absolute value. The box $\mathfrak{B}$ is of size $\leqslant P$ with $P = 2[p^\delta]+1$, and there is an $\mathbf{a}$ with a sum

$$|S_{\mathfrak{B}}| > |\mathfrak{B}|\,p^{-r-1} \geqslant P^{s-(r+1)/\delta}. \tag{9.1}$$

Here

$$S_{\mathfrak{B}} = \sum_{\mathbf{x}\in\mathfrak{B}} e(p^{-1}\mathfrak{P}(\mathbf{x}))$$

with

$$\mathfrak{P}(\mathbf{x}) = \mathbf{a}\mathfrak{I}(\mathbf{x}) = \sum_{d=2}^{r}\sum_{i=1}^{r_d} \mathfrak{I}_i^{(d)}(\mathbf{x}),$$

in an obvious notation. There is a unique d in $2 \leqslant d \leqslant k$ such that some coefficient $a_{di} \neq 0$, while all the coefficients a_{ti} with $d < t \leqslant k$ vanish. Thus the polynomial $\mathfrak{P} \in F_p[X]$ is of degree d. By Theorem 2, the inequality (9.1) with p large is possible only when $h(\mathfrak{P})$ is small, say when $h(\mathfrak{P}) \leqslant c_2(d, r, \delta)$. In other words, $h(\mathfrak{J}) \leqslant c_2(d, r, \delta)$, where

$$\mathfrak{J} = a_{d1}\mathfrak{J}_1^{(d)} + \ldots + a_{dr_d}\mathfrak{J}_{r_d}^{(d)}.$$

Say $a_{d1} \in F_p$ is not zero. Then in our given system $\mathfrak{J}$, we may replace $\mathfrak{J}_1^{(d)}$ by the form $\mathfrak{J}$. This does not change the type r of the system. Moreover, we may replace $\mathfrak{J}$ by a system of at most $c_2(d, r, \delta)$ forms of degree less than d, i.e. less than the degree of $\mathfrak{J}$. Hence we may replace $\mathfrak{J}$ by a system $\mathfrak{J}'$ of type $r' \prec r$. Since each component of r' is bounded in terms of r and δ, this completes our inductive proof of Theorem 4.

10. The invariants h_a.

Let $\mathfrak{J}$ be a form of degree $d > 1$ with coefficients in $A_m = Z/mZ$ where m is square free. The map $x \mapsto m^{-1}\mathfrak{J}(x)$ is a polynomial map of degree $\leqslant d$ from $G = A_m^s$ into $H = (m^{-1}Z)/Z$. Thus $\mathfrak{M}$ and $\mathfrak{M}(R)$ may be defined as in Section 5.

Proposition II. *Suppose that $\Gamma > 1$ is an integer, and that*

$$|\mathfrak{M}(R)| \geqslant R^{s(d-1)-\gamma} \tag{10.1}$$

where $R \geqslant R_1(s, d, \Gamma)$ and where $\gamma > 0$ is an integer. Then there is a fa torization $m = ab$ with

$$h_a(\mathfrak{J}) \leqslant d\Phi(d)\gamma\Gamma \tag{10.2}$$

and $b \leqslant R^{1/\Gamma}$.

Proof. For each divisor n of m, we write $\mathfrak{M}_n$ for the set of $(d-1)$-tuples $x_1, \ldots, x_{d-1}$ with $x_i \in A_n^s$ such that $(\mathfrak{J}_n)_d(x_1, \ldots, x_{d-1}, X) = 0$, i.e. $\mathfrak{J}_d(x_1, \ldots, x_{d-1}, X) \equiv 0 \pmod{n}$. Since m is square free, and by the Chinese Remainder Theorem,

$$|\mathfrak{M}_{nl}| = |\mathfrak{M}_n|\,|\mathfrak{M}_l| \tag{10.3}$$

when nl divides m.

We may suppose that $R \geqslant 3^{sd}C(s,d)$, with the constant C of Proposition I. We now divide the prime divisors p of m into four classes. The first class consists of primes $\geqslant 3R$. The second class contains primes p in $C(s, d) \leqslant p < 3R$ with

$$|\mathfrak{M}_p| \geqslant p^{s(d-1)-2\gamma\Gamma}.$$

The third class consists of prime divisors in $C(s, d) \leqslant p < 3R$ with

$$|\mathfrak{M}_p| < p^{s(d-1)-2\gamma\Gamma}, \tag{10.4}$$

and the fourth class of primes $\leqslant C(s, d)$.

We write $m = ab$, where a is the product of primes of the first and second class, and b is the product of primes of the third and fourth class.

The set $\mathfrak{M}(R)$ is a set $\mathfrak{M}(\mathfrak{D}(Z))$ as an Proposition I with $Z = 2R+ +1 \leqslant 3R$. For primes of the first class, $p \geqslant Z$ and $p \geqslant 3R > 3^{sd}C(s, d)$, so that (10.1) implies

$$|\mathfrak{M}_p(R)| \geqslant R^{s(d-1)-\gamma} \geqslant (Z/3)^{s(d-1)-\gamma} \geqslant C(s, d)Z^{s(d-1)-\gamma-1}.$$

Proposition I yields $h_p(\mathfrak{J}) \leqslant \Phi(d)\gamma$. For primes of the second class, Proposition I yields $h_p(\mathfrak{J}) \leqslant 2\gamma\Gamma\Phi(d)$. Thus when p is a prime factor of a, we may write

$$\mathfrak{J} \equiv \sum_{i=1}^{[d/2]} (\mathfrak{A}_1^{(i)}\mathfrak{B}_1^{(i)} + \ldots + \mathfrak{A}_k^{(i)}\mathfrak{B}_k^{(i)}) \pmod{p},$$

where $k = 2\gamma\Gamma\Phi(d)$ and where $\deg\mathfrak{A}_j^{(i)} = i$, $\deg\mathfrak{B}_j^{(i)} = d-i$. An application of the Chinese Remainder Theorem yields

$$h_a(\mathfrak{J}) \leqslant [d/2]k \leqslant d\Phi(d)\gamma\Gamma.$$

Suppose now that l is a divisor of m in $1 < l < 3R$ with

$$|\mathfrak{M}_l| < l^{s(d-1)-2\gamma\Gamma}. \tag{10.5}$$

Then

$$|\mathfrak{M}(R)| \leqslant \lceil 3R/l \rceil^{s(d-1)}|\mathfrak{M}_l| \leqslant (6R)^{s(d-1)}l^{-2\gamma\Gamma},$$

which in conjunction with (10.1) gives

$$l \leqslant 6^{s(d-1)}R^{1/2\Gamma} \leqslant R^{2/3\Gamma} < R^{1/2} \tag{10.6}$$

when $R \geqslant R_1(s, d, \Gamma)$. Hence in particular the primes of the third class are $\leqslant R^{2/3\Gamma}$. We claim that the product of primes of the third class is $\leqslant R^{2/3\Gamma}$. For suppose we know that a product of some of these primes is $\leqslant R^{2/3\Gamma}$, say that $p_1 \ldots p_t \leqslant R^{2/3\Gamma}$, and let p_{t+1} be a further prime of the third class. Then $p_1 \ldots p_t p_{t+1} = l$, say, has $l < R^{1/2} \cdot R^{1/2} < 3R$. Moreover, repeated application of (10.3), (10.4) yields (10.5). Thus indeed (10.6) holds. Finally the primes of the fourth class have a product $\leqslant c_3(s, d) \leqslant R^{1/3\Gamma}$, so that altogether $b \leqslant R^{1/\Gamma}$.

11. Proof of Theorem 5.

Set $\eta = (4/5)(d-\delta^{-1})/(d-1)$. We are going to apply Lemma 5.4 with $G = A_m^s$ and with $B = s$. Then either $|S_{\mathfrak{B}}| \leqslant P^{s-K}$, or $R = P^\eta$ has

$$|\mathfrak{M}(R)| \geqslant R^{s(d-1)-2^{d-1}(K/\eta)-\varepsilon}.$$

Thus if we set $\gamma = [2^{d-1}(K/\eta)+(3/2)]$, then

$$|\mathfrak{M}(R)| \geqslant R^{s(d-1)-\gamma},$$

provided only that R is large, i.e. provided only that $m \geqslant m_2(s, d, \delta)$.

Now again, if R is large, i.e. if $m \geqslant m_1(s, d, \delta, \Gamma)$, Proposition II gives us a factorization $m = ab$ with $b \leqslant R^{1/\Gamma} < m^{\delta\eta/\Gamma} \leqslant m^{\delta/\Gamma}$, and with

$$h_a(\mathfrak{J}^{(d)}) \leqslant d\Phi(d)\gamma\Gamma.$$

In view of

$$\gamma \leqslant 2^{d-1}(5/4)(d-1)(d-\delta^{-1})^{-1}K+(3/2) \leqslant 2^d(d-1)(d-\delta^{-1})^{-1}K,$$

this gives (2.1), as desired.

Appendix

Given a universal domain Ω and a number S, let $\mathfrak{C}(l)$ be the class of algebraic manifolds in Ω^S which can be defined by a set of equations $f_1 = \ldots \ldots = f_l = 0$, where each f_i is a polynomial of total degree $\leqslant l$.

LEMMA. *Let $\mathfrak{D}(Z)$ be a subset of Ω^S whose projection $\mathfrak{D}_i$ on the i-th coordinate axis contains at most Z elements ($i = 1, \ldots, S$). Now if V is a manifold of dimension e belonging to $\mathfrak{C}(l)$, then* (6.5) *holds.*

Proof. V is a union $V_1 \cup \ldots \cup V_m$, where $m \leqslant l^*$ and where each V_j is an irreducible algebraic variety in $\mathfrak{C}(l^*)$, with $l^* = l^*(S, l)$ (Seidenberg [14], § 65). We may therefore suppose that V is irreducible.

Let $\boldsymbol{F}$ be a field of definition of V, and without loss of generality let $(\boldsymbol{\xi}, \boldsymbol{\eta}) = (\xi_1, \ldots, \xi_e, \eta_1, \ldots, \eta_t)$ with $t = S-e$ be a generic point of V over $\boldsymbol{F}$, such that ξ has transcendence degree e over $\boldsymbol{F}$. Each η_j is algebraic over $\boldsymbol{F}(\xi)$, and since V lies in $\mathfrak{C}(l)$, there are nonzero polynomials $g_j(X, Y_j)$ ($j = 1, \ldots, t$) with coefficients in $\boldsymbol{F}$, with $g_j(\xi, \eta_j) = 0$ and of degree $\leqslant l_1$, where $l_1 = l_1(S, l)$. The number of $\boldsymbol{x} = (x_1, \ldots, x_e) \in \mathfrak{D}_1 \times \ldots \times \mathfrak{D}_e$ is $\leqslant Z^e$, and given such $\boldsymbol{x}$ with $g_j(\boldsymbol{x}, Y_j) \neq 0$ ($j = 1, \ldots, t$), the number of $\boldsymbol{y}$ with $(\boldsymbol{x}, \boldsymbol{y}) \in V$ is $\leqslant l_1^t$. So there are at most $l_1^t Z^e$ such points.

When $e = 0$, then $l_1^t Z^e = l_1^S$ is a bound for the number of points of V. When $e > 0$, then we also have to consider points $(\boldsymbol{x}, \boldsymbol{y})$ on V with $g_1(\boldsymbol{x}, Y_1) \ldots g_t(\boldsymbol{x}, Y_t) = 0$. These form a submanifold W of V, and since V was irreducible, $\dim W < \dim V = e$. Moreover, W lies in $\mathfrak{C}(l_2)$ with $l_2 = l_2(S, l)$. So if we assume inductively that the lemma is true for dimension less than e, we may infer that $|W \cap \mathfrak{D}(Z)| \leqslant c(S, l_2)Z^{e-1}$, and therefore

$$|V \cap \mathfrak{D}(Z)| \leqslant l_1^t Z^e + c(S, l_2)Z^{e-1} \leqslant c(S, l)Z^e.$$

Added in proof. Theorem 4 is generalized to general moduli in *Small solutions of congruences in a large number of variables*, Canad. Math. Bull. (to appear). See also R. C. Baker, *Small solutions of congruences*, Mathematika 30 (1983), pp. 164–188 and forthcoming work of D. R. Heath-Brown on quadratic forms.

References

[1] R. C. Baker, *Small solutions of quadratic and quartic congruences*, Mathematika 27 (1980), pp. 30–45.

[2] J. W. S. Cassels, *An introduction to diophantine approximation*, Cambridge Tracts in Math. and Math. Physics 45, 1957.

[3] H. H. Chalk and K. S. Williams, *The distribution of solutions of congruences*, Mathematika 12 (1965), pp. 176–192.

[4] H. Davenport, *Cubic forms in 16 variables*, Proc. Royal Soc. A, 272 (1963), pp. 285–303.

[5] H. Davenport and D. J. Lewis, *Exponential sums in many variables*, Amer. J. Math. 84 (1962), pp. 649–665.

[6] P. Deligne, *La conjecture de Weil I*, Publ. Math. IHES 43 (1974), pp. 273–307.

[7] N. Katz, *Sommes exponentielles*, Astérisque 79.

[8] S. Lang, *Introduction to algebraic geometry*, Interscience Tracts in Pure and Applied Math., 1958.

[9] G. Myerson, *The distribution of rational points on varieties defined over a finite field*, Mathematika 28 (1981), pp. 153–159.

[10] A. Schinzel, H. P. Schlickewei and W. M. Schmidt, *Small solutions of quadratic congruences and small fractional parts of quadratic forms*, Acta Arith. 37 (1980), pp. 241–248.

[11] W. M. Schmidt, *Diophantine inequalities for forms of odd degree*, Advances in Math. 38 (1980), pp. 128–151.

[12] — *On cubic polynomials II. Multiple exponential sums*, Mh. Math. 93 (1982), pp. 141–168.

[13] — *The density of integer points on homogeneous varieties*, Acta Math. (To appear.)

[14] A. Seidenberg, *Constructions in algebra*, Trans. Amer. Math. Soc. 197 (1974), pp. 273–313.

[15] J. P. Serre, *Majorations de sommes exponentielles*, Astérisque 41-42 (1977), pp. 111–126.

[16] R. A. Smith, *The distribution of rational points on hypersurfaces defined over a finite field*, Mathematika 17 (1970), pp. 328–332.

UNIVERSITY OF COLORADO
Boulder, Colorado, USA

Received on 13. 9. 1983 (1374)