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 $\Psi(X) = \Psi(X_1, \ldots, X_r)$ is a polynomial with coefficients in $F_q$. Consider the sum

$$S = \sum_x e\left(p^{-1} \mathcal{T}(\Psi(x))\right),$$

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

Suppose that $d \geq 2$ and that

$$\Psi = \mathcal{T}^{(d)} + \ldots + \mathcal{T}^{(1)} + \mathcal{T}^{(0)},$$

where $\mathcal{T}^{(0)}$ is a form of degree $1$. We write

$$h = h(\Psi) = h(\mathcal{T}^{(0)})$$

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

$$\mathcal{T}^{(d)} = \mathcal{U}_1 \mathcal{B}_1 + \ldots + \mathcal{U}_h \mathcal{B}_h$$

with forms $\mathcal{U}_i, \mathcal{B}_i$, 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

$$|S| \ll q^{d-x}$$

with

$$x = 2^{1-d} \left\lceil \frac{\log h}{\Phi(d)} \right\rceil,$$

where $\lceil x \rceil$ denotes the smallest integer $\geq x$, 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 \( \mathfrak{A}_1, \mathfrak{A}_1, \ldots, \mathfrak{A}_n, \mathfrak{A}_n \) in (1.2) are singular points of \( \mathfrak{J}^{(d)} \), and hence \( s-2h \leq \dim V^* \), where \( V^* \) is the locus of singular points of \( \mathfrak{J}^{(d)} \) (in some "universal domain"). So our bound is useful in particular when \( \dim V^* \) is rather smaller than \( s \). In the case when \( \mathfrak{J}^{(d)} \) is nonsingular, \( h \geq s/2 \), but in this case Deligne [6] has given the much sharper estimate \( |S| \leq q^{n/2} \). 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 \( \overline{h} = \overline{h}(\mathfrak{J}) \) be the least number \( h \) such that \( \mathfrak{J}^{(d)} \) may be written in the form (1.2), with forms \( \mathfrak{A}_1, \mathfrak{A}_2 \) of positive degree having coefficients in the algebraic closure \( F_q \) of \( F_p \). According to our theorem, the sums

\[
S_{\mathfrak{J}} = \sum_{x \in \mathfrak{J}_{\mathfrak{J}}} e\left(p^{-1} \mathfrak{I}(\mathfrak{J}(x))\right),
\]

where \( \mathfrak{I}_{\mathfrak{J}} \) is the trace from \( F_{q^d} \) to \( F_q \), have

\[
|S| \leq q^{\overline{h}(\mathfrak{J})},
\]

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

\[
S_{\mathfrak{J}} = \sum_{x \in \mathfrak{J}_{\mathfrak{J}}} e\left(p^{-1} \mathfrak{I}(\mathfrak{J}(x))\right),
\]

where \( \mathfrak{J} \) is a "box" contained in \( F_q \). That is,

\[
\mathfrak{J} = \mathfrak{J}_1 \times \cdots \times \mathfrak{J}_n,
\]

with \( \mathfrak{J}_i \) a set of elements \( a_i + c_{i1}x_{i1} + \cdots + c_{ij}x_{ij} \) in \( F_q \), where \( a_i \) is a fixed element of \( F_q \), where \( a_{ij} \) is a fixed basis of \( F_q \), where \( 1 \leq i \leq l \) run through the integers in \( 1 \leq c_{ij} \leq P_{ij} \), where the \( P_{ij} \) are fixed integers in \( 1 \leq P_{ij} \leq p \). In the case when \( P_{ij} = p \) (1 \( \leq i \leq s \), \( 1 \leq j \leq l \)), the box \( \mathfrak{J} = \mathfrak{J}_{\mathfrak{J}} \), and \( S_{\mathfrak{J}} \) is the complete sum \( S \). In general, when \( 1 \leq P_{ij} \leq p \) (1 \( \leq i \leq s \), \( 1 \leq j \leq l \)), we will say that \( \mathfrak{J} \) is of size \( \leq P \). On the other hand we will say that \( \mathfrak{J} \) is of size \( \geq P \) when 1 \( \leq P \leq P_{ij} \leq P \).

**Theorem 2.** Let \( P = p^d \) where \( d-1 < \delta \leq 1 \), and put

\[
\alpha = \alpha(\delta) = (d-\delta^{-1})(d-1)^{-1} 2^{-d} \log(\delta). \tag{1.6}
\]

Then if \( \mathfrak{J} \) is a box of size \( \leq P \), we have for every \( \varepsilon > 0 \)

\[
|S_{\mathfrak{J}}| \leq q^{\alpha - \varepsilon}, \tag{1.7}
\]

with the constant in \( \alpha \) depending only on \( s, d, l, \delta, \varepsilon \).

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

Serre ([15], thèorème 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 \( \mathfrak{J} \) are small, then clearly one cannot expect much more than the trivial bound.

Now let \( \mathfrak{J} = (\mathfrak{J}_1, \ldots, \mathfrak{J}_n) \) 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

\[
\mathfrak{J} = \mathfrak{J}_1 = a_1 \mathfrak{J}_1 + \cdots + a_r \mathfrak{J}_r,
\]

with \( a = (a_1, \ldots, a_r) \in F_q^r \), but \( a \neq 0 \). We will suppose that each polynomial of the pencil is of degree \( \geq 2 \). Then we define

\[
h(\mathfrak{J}) := \min h(\mathfrak{J}),
\]

with the minimum to be taken over polynomials \( \mathfrak{J} \) 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 \( \mathfrak{J}_i \), we have \( h(\mathfrak{J}) = h(\mathfrak{J}^{(d)}) \) with \( \mathfrak{J}^{(d)} = (\mathfrak{J}_1^{(d)}, \ldots, \mathfrak{J}_n^{(d)}) \).

More generally, when each polynomial is of degree \( \leq d \), one has \( s-2h \leq \dim V^* \), where \( V^* \) is the manifold of singular points of \( \mathfrak{J}^{(d)} \), i.e., points where the matrix \( (\partial \mathfrak{J}^{(d)}/\partial x) \) (1 \( \leq i \leq s \), \( 1 \leq j \leq d \)) has rank \( \leq r \). Thus \( h \geq s/2 \) when \( \mathfrak{J}^{(d)} \) is nonsingular.

Given a box \( \mathfrak{J} \subseteq F_q \), denote its cardinality by \( |\mathfrak{J}| \), and write \( N_{\mathfrak{J}} = N_{\mathfrak{J}}(\mathfrak{J}) \) for the number of common zeros of \( \mathfrak{J} \) in \( \mathfrak{J} \).

**Theorem 3.** Let \( \mathfrak{J} \) be an \( r \)-tuple of polynomials such that every polynomial in its pencil has a degree between \( d_0 \) and \( d_1 \), where \( 2 \leq d_0 \leq d_1 \) are given. Suppose that \( p > d_1 \), that \( P = p^d \) with \( d_0^* \leq d_0 \leq d_1 \). Write \( h = h(\mathfrak{J}) \), and let \( \alpha = \alpha(\delta) \) be defined by (1.6). Then given \( \varepsilon > 0 \) and given a box \( \mathfrak{J} \) of size \( \leq P \), we have

\[
N_{\mathfrak{J}} = q^{\alpha - \varepsilon} |\mathfrak{J}| + O(q^{\alpha - \varepsilon + \varepsilon}), \tag{1.9}
\]

with a constant in \( O \) depending only on \( s, d, l, \delta, \varepsilon \).
In particular, \( N_s > 0 \) when \( \mathcal{B} \) is a box of size \( \geq p^s \), provided that
\[
with \( p = p(\delta, d, r, l, \delta) \).
\]
Estimates for \( N_s \) have 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
\[
N_s = q^{-r} |\mathcal{B}| + O(q^{1/2} \log q)^{2r}
\]
when the form of highest degree of each polynomial of the pencil is nonsingular, so in particular when the \( r \)-tuple \( \mathcal{B}^{(r)} \) is nonsingular. The constant in \( O \) here depends on \( s, d, l \). Hence \( N_s > 0 \) when
\[
|\mathcal{B}| > c_1(d, l)q^{(s/2)+r} \log q^{3r}.
\]
Myerson [9] in the case \( q = p \) used Deligne's results more carefully to see that (under some extra conditions on \( \mathcal{B} \)) \( N_s > 0 \) when \( p = p_2(s, d, r) \) and
\[
|\mathcal{B}| > (1+c_2)(2d-2)^r p^{(23+1)/2}.
\]
In particular, \( N_s > 0 \) when \( \mathcal{B} \) is a box of size
\[
(1+c_2)(2d-2)^r p^{(23+1)/2}.
\]
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 \( \geq p^s \) with \( \delta > 1/2 \), whereas we allow \( \delta \) to lie in \( \delta_0^{-1} < \delta \leq 1 \).

**Theorem 4.** Given \( d, r, \) and \( \delta > 1/2 \), there is an \( s_1 = s_1(d, r, \delta) \) as follows.

Let \( \mathcal{S} \) be a system of \( r \) forms of degree \( \leq d \) with integer coefficients in \( s > s_1 \) variables. Then for every prime \( p \), the system of congruences
\[
\mathcal{S}(x) = 0 \pmod{p}
\]
has a solution \( x \neq 0 \) whose size \( |x| = \max(|x_1|, \ldots, |x_d|) \) has
\[
|\mathcal{S}(x) = 0 | \leq p^s,
\]
with a constant in \( \mathcal{S}_0 \) which depends only on \( d, r, \delta \).

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 \( \mathcal{S} = (X_1^2 + \ldots + X_k^2)^{k/2} \), then every solution \( x \neq 0 \) of (1.14) has \( |x| \geq p^{1/k} \), 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 \( \mathcal{S} \) 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 \( \mathcal{S}(x) = 0 \) has a solution with \( 0 < |x| < p^k \) if the coefficients of \( \mathcal{S} \) have modulus \( \leq p \). The interesting case of Theorem 4 is thus when the forms of \( \mathcal{S} \) are even degree. The cases had been obtained with an arbitrary modulus \( m \). Schinzel, Schlickewie 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 \( \mathcal{S} \) of degree \( d \geq 2 \) with coefficients in a commutative ring \( A \), we can again define \( h = h(3) \): it is the smallest integer such that \( \mathcal{S} \) may be written as (1.2), with \( \mathcal{A}_i \), \( \mathcal{B}_i \) being forms of positive degree with coefficients in \( A \). In particular, when \( A = \mathbb{Z}[X] \) and when \( \mathcal{S} \) is a form in \( A_m[X] \), the invariant \( h(3) \) is well defined. More generally, let \( a \) be a divisor of \( m \). There is a natural map \( A_n \to A_m \), and a natural map of polynomial rings \( A_n[X] \to A_m[X] \), mapping \( \mathcal{S}(X) \mapsto \mathcal{S}(X) \). Let \( n \) be the divisor of \( (3) \), and we define \( h_n(\mathcal{S}) \) for polynomials \( \mathcal{S} \) in \( A_m[X] \) of degree \( \leq d \) by using their homogeneous part \( \mathcal{S}^{(d)} \).

Again when \( \mathcal{B} \in A_m[X] \), we consider sums
\[
S_s = \sum_{x \in \mathcal{B}} e(m^{-1} \mathcal{S}(x)),
\]
where \( \mathcal{B} \) is a box in \( A_m \), i.e., it is a product set (1.5) where \( \mathcal{S} \) is a set of elements \( \alpha \in \mathcal{B} \), where \( \alpha \) is a fixed element of \( A_m \), \( \beta \) 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 \( 1 \leq P_i \leq m \). The box is said to be of size \( \leq P \) if \( 1 \leq P_i \leq P \leq m \).

**Theorem 5.** Let \( \mathcal{S} \) be a polynomial of degree \( \leq d \) with coefficients in \( A_m \) \( m \) where \( s \) is square free. Let \( \mathcal{B} \) be a box of size \( \leq P = m^s \) with \( \delta > 1/2 \).

Suppose that
\[
|S_s| \geq P^{-k}
\]
where \( K \geq 1 \). When \( K > 1 \) is an integer and when \( m \geq m_1(s, d, \delta, \Gamma) \), there is a factorization \( m = ab \) such that \( b \leq P^{1/K} \) and
\[
h_a(\mathcal{S}^{(d)}) \leq (d - \delta^{-1})^{d} d^{2\delta - 1} \Phi(d) K \Gamma.
\]

**3. A basic inequality.** Let \( G, H \) be additive groups, and \( \Phi \) a map \( G \to H \). As in [11], define
\[
\delta_\Phi(g_1, \ldots, g_r) = \sum_{s_1=0}^1 \cdots \sum_{s_k=0}^1 (-1)^{s_1 + \ldots + s_k} \delta_{g_1, \ldots, g_r}(s_1, g_1 + \ldots + s_k g_k),
\]
so that \( \delta_\Phi \) is a symmetric function from \( G \times \cdots \times G \) into \( H \). Given a subset \( \mathcal{U} \subseteq G \), we write \( \mathcal{U}^{\Phi} \) for the difference set, i.e., the set of differences \( a - a' \) with \( a, a' \in \mathcal{U} \). Let \( \mathcal{W} - g \) be the translated set of elements \( a - g \) with \( a \in \mathcal{W} \), and let
\[
\mathcal{U}(g_1, \ldots, g_r) = \mathcal{W} - g_1 \cdots \mathcal{W} - g_r = \bigcap_{s_1=0}^1 \cdots \bigcap_{s_k=0}^1 (\mathcal{W} - s_1 g_1 - \ldots - s_k g_k).
\]
When \( \mathfrak{U} \) is finite, its cardinality is denoted by \(|\mathfrak{U}|\).

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

**Lemma 3.1.** Let \( \mathfrak{U} \) be a map \( G \to H \) where \( H \) is a subgroup of \( \mathbb{R}/\mathbb{Z} \). Let \( \mathfrak{V} \) be a finite subset of \( G \), and put

\[
S = S_{\mathfrak{V}} = \sum_{\theta \in \mathfrak{V}} e(\theta(a)),
\]

Then for each \( d \geq 2 \),

\[
|S|^{d^2 - 1} \leq |\mathfrak{U}| \prod_{d-1} \sum_{\theta \in \mathfrak{V}} \sum_{|\mathfrak{U}(\theta, \ldots, \theta, \ldots, \theta)| = \sum_{\theta \in \mathfrak{V}} e(\theta(a_1, \ldots, a_d))|.
\]

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

**4. A subset \( \mathfrak{V} \) of \( G^{d+1} \), and complete sums.** Again let \( \mathfrak{U} : G \to H \) be a map of additive groups. In [12], Lemma 1, we showed that \( \mathfrak{U}(g_1, \ldots, g_d) \) where \( d \geq 1 \) is "multilinear", i.e. it is a homomorphism in each argument \( g_i \), if and only if \( \mathfrak{U}(g_1, \ldots, g_{d-1}) = 0 \). Such a map will be called a polynomial of degree \( \leq d \).

So now let \( \mathfrak{U} : G \to H \) be a polynomial of degree \( \leq d \) where \( d \geq 2 \). With \( d \) we associate the subset \( \mathfrak{V} \) of \( G^{d+1} = G \times \cdots \times G \), consisting of \( (g_1, \ldots, g_{d-1}, g) \) for which \( \mathfrak{U}(g_1, \ldots, g_{d-1}, g) = 0 \), identically in \( g \). If, say, \( e_1, \ldots, e_r \) is a set of generators of \( G \), then \( (g_1, \ldots, g_{d-1}) \) lies in \( \mathfrak{V} \) precisely when \( \mathfrak{U}(g_1, \ldots, g_{d-1}, e) = 0 \) (\( 1 \leq i \leq r \)).

**Lemma 4.1.** Suppose \( G \) is finite, \( \mathfrak{U} \) is a polynomial from \( G \) into \( H \subseteq \mathbb{R}/\mathbb{Z} \) of degree \( \leq d \) where \( d \geq 2 \), and \( S \) is given by (3.1) with \( \mathfrak{V} = \mathfrak{G} \), so that \( S \) is a complete sum. Then

\[
|S|^{d^2 - 1} \leq |\mathfrak{U}|^{d^2 - 1 - d} |\mathfrak{U}|.
\]

**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 \( \mathfrak{U}(g_1, \ldots, g_{d-1}) = G \), and \( \mathfrak{U}(g_1, \ldots, g_{d-1}, g) = \mathfrak{U}(g) \), say, is a character on \( G \). Thus the inner sum is a character sum, and it is equal to \( |\mathfrak{U}| \) when \( (g_1, \ldots, g_{d-1}) \in \mathfrak{U} \), and equal to 0 otherwise.

**Lemma 4.2.** Make the assumptions of Lemma 4.1, in the special case when \( G = F_q^k \). Then for each \( K \) we have either

\[
|S| \leq q^{d^2 - K},
\]

or

\[
|\mathfrak{U}| \geq q^{(d^2 - 1) - 2^{d-1} K}.
\]

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

**5. \( \mathfrak{V} \) and incomplete sums.** Our goal here is to carry over Lemma 4.2 to incomplete sums as far as possible.

Denote by \( |x| \) the distance from an element \( x \in \mathbb{R}/\mathbb{Z} \) to the zero element. Then \( |x| = \min|x| \) over \( x \in T \) whose image in \( \mathbb{R}/\mathbb{Z} \) is \( x \).

A finite subset \( \mathfrak{V} \) of \( \mathbb{G} \) 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 \( \mathbb{G} \), 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 \( \leq P \) if each \( Q_i \leq P \). Note that the "dimension" \( B \) and \( e_0, e_1, \ldots, e_B \) are not necessarily determined by \( \mathfrak{V} \).

**Lemma 5.1.** Let \( \mathfrak{U} \) be a polynomial of degree \( \leq d \) (where \( d \geq 2 \)) from \( G \) into \( H \subseteq \mathbb{R}/\mathbb{Z} \). Let \( \mathfrak{V} \subseteq \mathbb{G} \) be a box of size \( \leq P \) with basis \( e_1, \ldots, e_B \). Define the sum \( S_{\mathfrak{V}} \) as in (3.1). Then

\[
|S_{\mathfrak{V}}|^{d^2 - 1} \leq P^{d^2 - 1 - dB} \sum \left( \prod_{i=1}^B \min(P, |\mathfrak{U}(g_i, \ldots, g_{d-1}, e)|^{-1}) \right),
\]

where the sum is over \( (d-1) \)-tuples of elements \( g_1, \ldots, g_{d-1} \) of \( \mathfrak{V} \). The constant in \( \leq \) depends only on \( B, d \).
Proof. This is essentially Lemma 13.1 of [13]. When \( \mathcal{B}: G \to H \) is "linear", i.e. when it is a homomorphism, then
\[
\sum_{g \in \mathcal{B}} e(\mathcal{B}(g)) = \sum_{i=1}^{n} \prod_{c_i \in \mathcal{B}} e(c_i \mathcal{B}(e_i)) \leq \prod_{i=1}^{n} \min \left( Q_i, \frac{2}{e(c_i \mathcal{B}(e_i)) - 1} \right) 
\leq \prod_{i=1}^{n} \min \left( P, \frac{2}{e(c_i \mathcal{B}(e_i)) - 1} \right).
\]
We simply have to apply this remark to the inner sum of Lemma 3.1, and we have to observe that \( |\mathcal{B}| \leq P^n \), and that each set \( \mathcal{B}(g_1, \ldots, g_{d-1}) \) is the union of a bounded number of boxes with basis \( e_1, \ldots, e_d \) and of size \( \leq P \).

**Lemma 5.2.** Make the same assumptions as in the preceding lemma. Suppose further that
\[
\|g_1 \| \geq P^{-K}
\]
where \( K > 0 \). Then the number \( N \) of \( (d-1) \)-tuples of \( g_1, \ldots, g_{d-1} \) in \( \mathcal{B} \) with
\[
\|g_i(g_1, \ldots, g_{d-1}, e_i)\| < P^{-1} \quad (i = 1, \ldots, B)
\]
satisfies
\[
N \geq P^{n(d-1) - 2d^{-1}K - 1}
\]
where \( e > 0 \) is arbitrary and where the constant in \( \geq \) depends only on \( B \), \( d \), \( e \).

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

Let \( P \) be natural and let \( e_1, \ldots, e_d \) be elements of \( G \). We now make the assumption that
\[
\tag{5.1} \text{the } P \text{-tuple } e_1 e_1 \ldots e_d \text{ with}
\]
\[
1 \leq c_1, \ldots, c_d \leq P \text{ are distinct.}
\]
Given a box \( \mathcal{B} \) with basis \( e_1, \ldots, e_d \) and of size \( \leq P \), the difference set \( \mathcal{B}^d \) is contained in the set \( \mathcal{B}(P) \) of \( d \)-tuples \( c_1 e_1 \ldots e_d e_1 \) with \( |c_i| \leq P \) \( (i = 1, \ldots, B) \). More generally, when \( 1 \leq m \leq P \), write \( \mathcal{B}(R) \) for the set of \( d \)-tuples \( c_1 e_1 \ldots c_d e_d \) with \( |c_i| \leq R \) \( (i = 1, \ldots, B) \). These \( d \)-tuples are not necessarily distinct, but by (5.1) at most \( \lambda^m \) 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 \( 0 < \eta \leq 1 \). Then the number \( N(\eta) \) of \( (d-1) \)-tuples \( g_1, \ldots, g_{d-1} \) in \( \mathcal{B}(P) \) with
\[
\|g_i(g_1, \ldots, g_{d-1}, e_i)\| < P^{-1} + (d-1)^{-1} \eta \quad (i = 1, \ldots, B)
\]
satisfies
\[
N(\eta) \geq P^{n(d-1) - 2d^{-1}K - 1} \eta.
\]
The constant in \( \geq \) depends only on \( B \), \( d \), \( \eta \), \( e \).

**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 \( 3^k \) at each step of the proof.

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

**Lemma 5.4.** Suppose \( d \geq 2 \) and \( \mathcal{B} \) is a polynomial of degree \( \leq d \) from \( G \) into \( H = (m^{-1} \mathbb{Z}/\mathbb{Z}) \), i.e. the rationals with denominator \( m \), taken modulo \( 1 \). Suppose that \( d^{-1} < \delta \leq 1 \), \( c > 0 \),
\[
0 < \eta < (d - \delta^{-1})(d - 1) - 1.
\]
Suppose \( \mathcal{B} \subseteq G \) is a box of size \( \leq P = m^e \), and with a basis \( e_1, \ldots, e_d \) which generates \( G \). Suppose that (5.1) holds. Then given \( K > 0 \), we have either
\[
\|g_1 \| \geq P^{-K}
\]
or \( R = P \) has
\[
|\mathcal{M}(R)| \geq R^{n(d-1) - 2d^{-1}K - 1} - 1.
\]
The constant in \( \geq \) here depends only on \( B \), \( d \), \( \eta \), \( c \).

**Proof.** By (5.3), and since \( P = m^e \), 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 \( \mathcal{B}(g_i) \) lie in \( (m^{-1} \mathbb{Z}/\mathbb{Z}) \), the relation (5.2) then leads to \( \mathcal{B}(g_i, \ldots, g_{d-1}, e_i) = 0 \) \( (i = 1, \ldots, B) \).

**6. Invariants** \( h, \bar{h}, \bar{g} \). Now let \( F \) be an arbitrary field, and \( \mathfrak{I} \) a form in \( \mathfrak{s} \) variables of degree \( d \geq 2 \) with coefficients in \( F \). One may again define \( h = h(\mathfrak{I}) \) as the least integer \( k \) such that \( \mathfrak{I} \) may be written as
\[
\mathfrak{I} = \mathfrak{I}_1 \mathfrak{I}_1 + \ldots + \mathfrak{I}_k \mathfrak{I}_k,
\]
with forms \( \mathfrak{I}_1, \mathfrak{I}_2 \) of positive degree and with coefficients in \( F \). We further define \( \bar{h} = h(\mathfrak{I}) \) as the least integer \( k \) such that \( \mathfrak{I} \) may be as in (6.1), with forms \( \mathfrak{I}_1, \mathfrak{I}_2 \) having coefficients in any extension field of \( F \). Then clearly \( \mathfrak{I} \) is the least number \( k \) such that \( \mathfrak{I} \) is writable as (6.1) with coefficients in the algebraic closure \( \overline{F} \) of \( F \). We have \( \bar{h} \leq h \).

We define \( \mathfrak{M} \) as the subset of \( F^{d-1} \) consisting of \( (d-1) \)-tuples \( x_1, \ldots, x_{d-1} \) with \( \mathcal{I}_k(x_1, \ldots, x_{d-1}, X) = 0 \), identically in \( X \). Now let \( \Omega \) 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 \( \mathfrak{M} \) as the set of \( (d-1) \)-tuples \( x_1, \ldots, x_{d-1} \) with \( \mathcal{I}_k(x_1, \ldots, x_{d-1}, X) = 0 \). Then \( \mathfrak{M} \) is an algebraic manifold in \( \Omega^{d-1} \); we denote its codimension by \( \bar{g} = g(\mathfrak{I}) \). One proves as in [13], Lemma 16.1, that
\[
\bar{g} \leq 2d^{-1} \bar{h}.
\]

**Proposition I.** When \( F \) is of characteristic \( > d \), then
\[
\bar{h} < \Phi(d) \bar{g}.
\]
The case $F = C$ 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 $B_0(X) = B_0(X, \ldots, X)$, one finds (corresponding to [13], § 23) that \( h(\mathfrak{m}) \leq \Phi(d) \tilde{g}(\mathfrak{m}) \). When the characteristic exceeds $d$, then the relation $B_0(X) = (-1)^d d! B_0(X)$ shows that also $h(\mathfrak{m}) \leq \Phi(d) \tilde{g}(\mathfrak{m})$.

Now let $\mathfrak{D}(Z)$ be a subset of $F^n$ such that the projection on any coordinate axis contains at most $Z$ elements. Thus $\mathfrak{D}(Z) \subseteq \mathfrak{D}_1 \times \ldots \times \mathfrak{D}_n$ where $\mathfrak{D}_i \subseteq F$ has cardinality $|\mathfrak{D}_i| \leq Z$. Let $\mathfrak{W}(\mathfrak{D}(Z))$ consist of $(d-1)$-tuples $(x_1, \ldots, x_{d-1}) \in \mathfrak{W}$ with each $x_i \in \mathfrak{D}(Z)$ $(i = 1, \ldots, d-1)$.

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

$$(6.3) \quad |\mathfrak{W}(\mathfrak{D}(Z))| > CZ^{(d-1)\gamma-1},$$

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

$$(6.4) \quad h(\mathfrak{D}) \leq \Phi(d) \gamma.$$ 

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

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

$$(6.5) \quad |\mathfrak{W}(\mathfrak{D}(Z))| \leq BZ^{(d-1)-\gamma}$$

with $B = B(s, d)$. Hence when $C$ is sufficiently large, (6.3) implies that $\gamma \geq \tilde{g}$, and Proposition I gives $h(\mathfrak{D}) \leq \Phi(d) \gamma$. 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 $\mathfrak{D}$ by $F$, and $C$ by a universal domain $\mathfrak{O}$ over $F$. The following extra remarks might be helpful.

When $V$ is an algebraic subset of $\mathfrak{O}^n$, one could define "$V$ is defined over $F$" by either

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

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

Both of these concepts occur in the proof. E.g. (i) is the required definition for Lemma 19.1.2 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 $F$" refers to property (ii).

However, for a perfect field $F$, 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 $\mathfrak{D}(Z) \subseteq \Omega^3$, then an algebraic set $V \subseteq \Omega^n$ (such as the set $V'$ in [13], § 24) of dimension $\epsilon$ has

$$(6.6) \quad |V \cap \mathfrak{D}(Z)| \leq c(s, \delta) Z^{\epsilon},$$

provided $V$ lies in a certain class $\mathfrak{C}(\mathfrak{D})$. 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 $x$ be given by (1.4), and set

$$\gamma = \left\lfloor \frac{h(\mathfrak{D})}{\Phi(d)} \right\rfloor - 1 = 2^{d-1} \chi - 1.$$ 

Put

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

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

$$|S| \leq q^{2^{-K}} = C^{2^{-d}} q^{2^{-\chi}},$$

or

$$|S| \geq q^{(d-1)2^{-d-1}} K = C q^{(d-1)2^{-d-1}} - C q^{(d-1)2^{-d-1}} = C q^{(d-1)2^{-d-1}} - 1.$$

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

We now turn to Theorem 2. Again set $\gamma = \left\lfloor \frac{h(\mathfrak{D})}{\Phi(d)} \right\rfloor - 1$, but this time let $x$ be given by (1.6), so that

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

Let $\epsilon > 0$ be given. Pick $\eta$ 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

$$2^{d-1} ((\eta/\eta') - (\eta/\eta')) + (\eta/\eta') < \gamma + 1.$$ 

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

$$K = x + \epsilon.$$ 

The map $x \mapsto B_0(x) = p^{-1} B(\mathfrak{D}(x))$ occurring in the sum $S_0$ is a polynomial of degree $< d$ from $G = F_p$ into $H = (p^{-1} Z)/Z$. We now apply Lemma 5.4 with $m = p$, $P = p^d$, $B = s l$. The sum $S_0$ of Theorem 2 then either has (5.4), i.e.

$$|S_0| \leq p^{m-K} = p^{2^{d-1} - 1},$$

or $R = P^s$ satisfies (5.5). The constant in $\varepsilon$ in (5.5) depends on $B = s l$, $d$, $\eta$, $\epsilon$, hence only on $s$, $d$, $\delta$, $\epsilon$.

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

$$|\mathfrak{W}(\mathfrak{D}(Z))| \geq Z^{(d-1)2^{-d-1}} (\eta/\eta')^{-1/\eta'},$$
Thus in view of (7.3) we have
\[ |\mathcal{B}(\mathfrak{T}(Z))| \geq CZ^{(d-1)\gamma-1}, \]
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 \(h(\mathcal{B}) \leq \Phi(d)\gamma\), which contradicts our choice of \(\gamma\). Thus (7.4) must hold, and Theorem 2 is correct.

8. Proof of Theorem 3. The relation
\[ \sum_{a \in \mathfrak{P}^+} e(p^{-1} \bar{\zeta}(ay)) = \begin{cases} q^r & \text{when } y = 0, \\ 0 & \text{when } y \neq P \mod \mathfrak{P}, \end{cases} \]
is well known. Thus
\[ N_0 = q^{-r}|\mathfrak{B}| + q^{-r} \sum_{a \in \mathfrak{P}^+} \sum_{x \in \mathfrak{B}} e(p^{-1} \bar{\zeta}(ax)). \]

Each polynomial \(a \mathfrak{B}\) occurring here is of degree \(\geq d_0\). Since \(d_0^{-1} \delta \leq \delta \leq 1\), given a box \(\mathfrak{B}\) of size \(\leq P = p^e\), we may apply Theorem 2, to see that the inner sum on the right hand side of (8.1) is \(\leq q^{rd+xi} \delta^e\). Thus (1.8) follows.

Since \(h\) is an integer, (1.10) implies that \(h_I\) divided by the right hand side of (1.10) is \(\geq 1 + 2\delta\sqrt{e} + \tilde{\zeta}(d, r, \delta)\). As a consequence, \(\delta \sqrt{e} \geq r(1 + 2\sqrt{e})\). We choose \(\varepsilon = \varepsilon(d, r, \delta) > 0\) with
\[ r(1 + 2\sqrt{e})(1 - \varepsilon) - \varepsilon \geq r + \tilde{\zeta}. \]

Now suppose that \(\mathfrak{B}\) is a box with \(P_0 = P = [p^e]\), i.e. the integer part of \(p^e\) \((1 \leq i \leq s, 1 \leq j \leq l)\). Then \(|\mathfrak{B}| = P_0^d\), and (1.9) yields
\[ N_0/|\mathfrak{B}| = q^{-r} + O(P^{-\tilde{\zeta}} + e). \]

When \(p > p^e(d, r, \delta)\), then \(P \geq p^{e/2}(1 - \varepsilon)\), and since
\[ (x(1 - \varepsilon))^{(d/2) - 1} \geq (1 - \varepsilon)^{d} \geq r + 1 + \sqrt{e} \geq r + 2\sqrt{e}, \]
we have
\[ N_0/|\mathfrak{B}| = q^{-r} + O(q^{-\tilde{\zeta}}). \]
The constant in \(O\) here depends on \(s, d, r, l, \delta\), and hence we certainly have \(N_0 > 0\) when \(p > p_1(s, d, r, l, \delta)\).

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

Given \(r = (r_1, \ldots, r_N)\) and \(r' = (r'_1, \ldots, r'_l)\) with nonnegative integer components and with \(r_k \neq 0\), we write \(r > r'\) if either \(k > l\) or if \(k = l\) and

there is a \(t \in 1 \leq t \leq k\) having \(r_t > r'_t\), and \(r_t = r'_t\), for \(t \leq i \leq k\). Then \(r > r'\) establishes a well ordering among tuples \(r\), and we may prove Theorem 4 by induction.

Our first observation is that the theorem is true for \(r = (r_1)\), and that the truth of the theorem for \(r = (r_1, r_2, 0)\) implies its truth for \((r_1, r_2, r_2, r_1)\); for when we are given linear forms \(\mathfrak{a} = (a, \ldots, a)\) in \(s\) variables and with coefficients of absolute value \(\leq p\), they have a common integer zero \(y\) with \(0 < |y| < (sp)^{(1/2) + \varepsilon}\) (Cassels [2], § VI.3, Lemma 3; this is sometimes called "Siegel's Lemma"). Thus when \(s > e^{-1}(1 + \varepsilon)k\), there is a nontrivial zero with \(|y| \leq (sp)^{e}\), and when \(s > (e^{-1}(1 + \varepsilon)k + 1)\), there is a linearly independent such zeros \(y_1, \ldots, y_l\). We now set \(x = z_1y_1 + \ldots + z_ly_l\). With each form \(\mathfrak{S}\) of \(\mathfrak{S}\) we associate a new form \(\mathfrak{S}^{(1)}(Z) = \mathfrak{S}(z_1y_1 + \ldots + z_ly_l)\). Since the \(r_1\) linear forms \(\mathfrak{a}^{(1)}(Z)\) vanish identically, it remains to solve \(\mathfrak{S}^{(1)}(Z) \equiv 0 (mod p)\) for a system \(\mathfrak{S}^{(1)}\) of type \(r\). When \(l > s_2(r, (e^{-1}(1 + \varepsilon)k + 1), (e^{-1}(1 + \varepsilon)k + 1))\), there is such a \(z\) with \(|z| \leq (e^{-1}(1 + \varepsilon)k + 1)\). Thus with \(\varepsilon = (e^{-1}(1 + \varepsilon)k + 1)\), the vector \(x = z_1y_1 + \ldots + z_ly_l\) will have both (1.14) and (1.15).

It will thus suffice to prove the theorem for \(r = (r_1, \ldots, r_2, 0)\), assuming its truth for each \(r' < r\). Write \(r = r_1 + \ldots + r_2, r_2\), and let \(N\) be the number of solutions of (1.14) with (1.15). Thus \(N = N_0\), where \(\mathfrak{S}\) is the box \(|x| \leq p^e\).

According to (8.1),
\[ N = p^{-r}(|\mathfrak{B}| + \sum_{e \text{mod } p} e(p^{-1} \mathfrak{a}(x))). \]

Suppose for the moment that for each \(a \neq 0\), the inner sum on \(e \text{mod } p\) has absolute value \(\leq |\mathfrak{B}|p^{-r-1}\). Then since the number of possibilities for \(a\) is less than \(p^e\), we obtain
\[ N \geq p^{-r}(|\mathfrak{B}|(1 - p^{-1})). \]

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

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

Here
\[ S_a = \sum_{x \in \mathfrak{B}} e(p^{-1} \mathfrak{a}(x)) \]
with
\[ \mathfrak{a}(x) = a \mathfrak{a}(x) = \sum_{d=1}^{r} \sum_{l=1}^{d} \mathfrak{a}(x). \]
in an obvious notation. There is a unique $d$ in $2 \leq d \leq k$ such that some coefficient $a_{d,i} \neq 0$, while all the coefficients $a_d$ with $d < i \leq k$ vanish. Thus the polynomial $\mathcal{P} \in F_p[X]$ is of degree $d$. By Theorem 2, the inequality (9.1) with $p$ large is possible only when $h(\mathcal{P})$ is small, say when $h(\mathcal{P}) \leq c_2(d, r, \delta)$. In other words, $h(\mathcal{P}) \leq c_2(d, r, \delta)$, where

$$I = a_{d,1} \mathcal{P}^0 + \ldots + a_{d, \delta} \mathcal{P}_d^0.$$ 

Say $a_{d,1} \in F_p$ is not zero. Then in our given system $\mathcal{P}$, we may replace $\mathcal{P}_d^0$ by the form $\mathcal{P}$. This does not change the type $r$ of the system. Moreover, we may replace $\mathcal{P}$ by a system of at most $c_2(d, r, \delta)$ forms of degree less than $d$, i.e., less than the degree of $\mathcal{P}$. Hence we may replace $\mathcal{P}$ by a system $\mathcal{P}'$ of type $r' < r$. Since each component of $r'$ is bounded in terms of $r$ and $\delta$, this completes our inductive proof of Theorem 4.

10. The invariants $h_\gamma$. Let $\mathcal{P}$ be a form of degree $d > 1$ with coefficients in $A_n = \mathbb{Z}/m\mathbb{Z}$ where $m$ is square free. The map $x \mapsto m^{-1} \mathcal{P}(x)$ is a polynomial map of degree $d$, into $H = (m^{-1} \mathbb{Z}/\mathbb{Z})$. Thus $\mathcal{P}$ and $\mathfrak{m}(R)$ may be defined as in Section 5.

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

$$|\mathfrak{m}(R)| \geq R^{d-1-\gamma}$$

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

$$h_\gamma(\mathcal{P}) \leq d\Phi(d) \gamma^\Gamma$$

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

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 $x_i \in A_n$ such that $(\mathcal{P}_n)(x_1, \ldots, x_{d-1}, X) \equiv 0 \pmod{n}$, i.e., $\mathcal{P}_n(x_1, \ldots, x_{d-1}, X) \equiv 0 \pmod{n}$. Since $m$ is square free, and by the Chinese Remainder Theorem,

$$|\mathfrak{m}_m| = |\mathfrak{m}_d||\mathfrak{m}_l|$$

when $nl$ divides $m$.

We may suppose that $R \geq 3dC(s,d)$, 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 $p \leq 3R$. The second class contains primes $p$ in $C(s, d) \leq p < 3R$ with

$$|\mathfrak{m}_p| \geq p^{d-1-2\gamma^\Gamma}.$$ 

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

$$|\mathfrak{m}_p| \leq p^{d-1-2\gamma^\Gamma}$$

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

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 $\mathfrak{m}(\Sigma(Z))$ as an Proposition I with $Z = 2R + 1 \leq 3R$. For primes of the first class, $p \geq Z$ and $p \geq 3R > 3dC(s, d)$, so that (10.1) implies

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

Proposition I yields $h_\gamma(\mathcal{P}) \leq \Phi(d)$; for primes of the second class, Proposition I yields $h_\gamma(\mathcal{P}) \leq 2\gamma^\Gamma\Phi(d)$. Thus when $p$ is a prime factor of $a$, we may write

$$\mathcal{P} = \sum_{i=1}^{d-1} (\mathcal{P}_0 \mathcal{P}_i^0 + \ldots + \mathcal{P}_k \mathcal{P}_k^0) \pmod{p},$$

where $k = 2\gamma^\Gamma\Phi(d)$ and where $\deg(\mathcal{P}_0^0) = i, \deg(\mathcal{P}_k^0) = d-i$. An application of the Chinese Remainder Theorem yields

$$h_\gamma(\mathcal{P}) \leq \gamma^\Gamma.$$ 

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

$$|\mathfrak{m}_l| < R^{d-1-2\gamma^\Gamma}.$$

Then

$$|\mathfrak{m}(R)| \geq |3R/l|^{d-1-\gamma} |\mathfrak{m}_l| \leq (6R)^{d-1-1} l^{2\gamma^\Gamma},$$

which in conjunction with (10.1) gives

$$|\mathfrak{m}(R)| \leq (6R)^{d-1-1} l^{2\gamma^\Gamma} < R^{3\gamma^\Gamma} < R^{1/2}$$

when $R \geq R_1(s, d, \Gamma)$. Hence in particular the primes of the third class are $\leq R^{2\gamma^\Gamma}$. We claim that the product of primes of the third class is $\leq R^{2\gamma^\Gamma}$. For suppose we know that a product of some of these primes is $\leq R^{2\gamma^\Gamma}$, say that $p_1 \ldots p_t \leq R^{2\gamma^\Gamma}$, 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 $l < R^{1/2} < R^{1/2} < R^{3\gamma^\Gamma}$. 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 $\leq c_3(s, d) \leq R^{3\gamma^\Gamma}$, so that altogether $b \leq R^{1/\Gamma}$.

11. Proof of Theorem 5. Set $\eta = (4/5)(d-\delta-1)/(d-1)$. We are going to apply Lemma 5.4 with $G = A_n$ and with $B = s$. Then either $|S_\delta| \leq p^{r_e}\epsilon$, or $R = p^m$ has

$$|\mathfrak{m}(R)| \geq R^{d-1-2\epsilon^{1+(K/m)^{\epsilon}}}.$$ 

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

$$|\mathfrak{m}(R)| \geq R^{d-1-\gamma},$$

provided only that $R$ is large, i.e., provided only that $m \geq m_2(s, d, \delta).$
Now again, if $R$ is large, i.e., if $m \geq m_0$, Proposition II gives
us a factorization $m = ab$ with $b \leq R^{1/4} \leq m^{1/2} \leq m^{1/4}$, and with
$$h_a(Z^b) \leq d \Phi(d) \gamma^f.$$ 
In view of
$$y \leq 2^{f-1} (5/4)(d-1)(d-\delta^{-1})^{-1} K + (3/2) \leq 2^f (d-1)(d-\delta^{-1})^{-1} K,$$
this gives (2.1), as desired.

Appendix

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

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

**Proof.** $\mathfrak{D}$ is a union $\mathfrak{D}_1 \cup \cdots \cup \mathfrak{D}_S$, where $\mathfrak{D}_i$ is irreducible algebraic variety in $C(l^i)$, with $l^i = l^i(S, l)$ (Seidenberg [14], sec. 65). We may therefore suppose that $\mathfrak{D}$ is irreducible.

Let $F$ be a field of definition of $\mathfrak{D}$, and without loss of generality let $(x, \eta) = (x_1, \ldots, x_S, \eta_1, \ldots, \eta_S)$ with $t = S - e$ be a generic point of $\mathfrak{D}$ over $F$, such that $\eta$ has transcendence degree $d$ over $F$. Each $\eta_i$ is algebraic over $F(x, \eta)$, and since $\mathfrak{D}$ lies in $C(l)$, there are nonzero polynomials $y_i(x, \eta)$ with coefficients in $F$, with $y_i(\xi, \eta) = 0$ and of degree $\leq l_i$, where $l_i = l_i(S, l)$. The number of $x = (x_1, \ldots, x_S) \in \mathfrak{D}_1 \times \cdots \times \mathfrak{D}_S$ is $\leq Z^e$, and given such $x$ with $y_i(x, \eta) \neq 0$ $(i = 1, \ldots, e)$, the number of $y$ with $(x, y) \in \mathfrak{D}$ is $\leq l_i^e$. So there are at most $l_i^e Z^e$ such points.

When $e = 0$, then $l_i^e Z^e = l_i^e$ is a bound for the number of points of $\mathfrak{D}$. When $e > 0$, then we also have to consider points $(x, y)$ on $\mathfrak{D}$ with $y_i(x, \eta) \neq 0$. These form a submanifold $W$ of $\mathfrak{D}$, and since $\mathfrak{D}$ was irreducible, $\dim W < \dim \mathfrak{D} = e$. Moreover, $W$ lies in $C(l_2)$ 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 $|W \cap \mathfrak{D}(Z)| \leq c(S, l_2) Z^{e-1}$, and therefore
$$|\mathfrak{D}(Z)| \leq l_1^e Z^e + c(S, l_2) Z^{e-1} \leq c(S, l) Z^e.$$ 


**References**


UNIVERSITY OF COLORADO
Boulder, Colorado, USA

Received on 13. 9. 1983 (1374)