J. Austral. Math. Soc. (*Series A*) **33** (1982), 125–134

ESTIMATES FOR MULTIPLE EXPONENTIAL SUMS

JOHN H. LOXTON and ROBERT A. SMITH

(Received 23 April 1981)

Communicated by A. J. van der Poorten

Abstract

We give estimates for exponential sums of the shape $\Sigma \exp(2\pi i F(x_1,\ldots,x_n)/q)$, where F is a polynomial with integer coefficients and each component of $(x_1,\ldots,x_n)$ in the sum runs through a complete set of residues modulo q.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 10 G 10.

1. Introduction

For each positive integer q and for each non-linear polynomial $F \in \mathbf{Z}[\mathbf{X}]$ in n variables $\mathbf{X} = (X_1,\ldots,X_n)$ over the ring of integers $\mathbf{Z}$ of degree $m+1$, we define the multiple exponential sum

$$S_F(q) = S(F;q) = \sum_{\mathbf{x} \bmod q} e_q(F(\mathbf{x})),$$

where the summation condition "$\mathbf{x} \bmod q$" means that each component of $\mathbf{x} = (x_1,\ldots,x_n) \in \mathbf{Z}^n$ runs through a complete set of residues modulo q and $e_q(t) = \exp(2\pi i t/q)$ for any $t \in \mathbf{Z}$. The importance of such exponential sums in analytic number theory is well-known (see, for example, Davenport [1] or Igusa [3]). In 1974, Deligne [2, Theorem 8.4] deduced from his work on the Weil Conjectures that if p is a prime, then

$$|S_F(p)| \leqslant m^n p^{n/2} \tag{2}$$

whenever the homogeneous part of F (viewed modulo p) of maximal degree is non-singular modulo p. For $n = 1$, Smith [8] has proved that if the discriminant $D(F')$ of the derivative F' of F does *not* vanish, then

$$|S_F(q)| \leqslant q^{1/2}(D(F'), q)d_m(q) \tag{3}$$

holds for all $q \geqslant 1$, where $d_m(q)$ denotes the number of representations of q as a product of m positive integers and (a, b) denotes the greatest common divisor of the integers a and b. In this paper, we will use Deligne's estimate to develop an analogue of (3) for multiple exponential sums. More precisely, we will prove that if F is a polynomial in $\mathbf{Z}[\mathbf{X}]$ such that the associated projective variety defined by the gradient ∇F of F is non-singular and of dimension 0 over $\mathbf{C}$, say, then there exists a certain positive integer $D(\nabla F)$, the discriminant of ∇F, such that

$$|S_F(q)| \leqslant q^{n/2}\big(D(\nabla F)^5, q\big)^{n/2} d_m^n(q)$$

holds for all $q \geqslant 1$, *provided* that Deligne's estimate (2) holds for all primes p. The proof of this result is based upon the ideas developed in [8] for $n = 1$.

2. Preliminaries

As is customary in studying exponential sums, it will be useful to select a special set of representatives in $\mathbf{Z}^n$ for the residue classes modulo q. The most convenient way in which to make this selection is to introduce n-dimensional boxes defined by

$$B_n(q) = \{\mathbf{x} \in \mathbf{Z}^n : 0 \leqslant x_i < q \text{ for all } = 1, \ldots, n\}.$$

The basic property of these boxes is described by the following decomposition theorem. For each pair of positive integers M and N,

$$B_n(MN) = MB_n(N) \oplus B_n(M), \tag{4}$$

the scalar multiplication and addition in (4) being inherited from the $\mathbf{Z}$-module structure of $\mathbf{Z}^n$. In other words, (4) asserts that for each $\mathbf{x} \in B_n(MN)$, there exist unique n-tuples $\mathbf{u} \in B_n(N)$ and $\mathbf{v} \in B_n(M)$ such that $\mathbf{x} = M\mathbf{u} + \mathbf{v}$.

If q is a positive integer, there exist unique positive integers k and r such that $q = k^2 r$, where r is square free and k is positive. For each polynomial F in $\mathbf{Z}[\mathbf{X}]$ and $\mathbf{x}, \mathbf{y}$ in $\mathbf{Z}^n$, Taylor's theorem implies that

$$F(\mathbf{x} + k\mathbf{y}) \equiv F(\mathbf{x}) + k\nabla F(\mathbf{x}) \cdot \mathbf{y} \bmod k^2, \tag{5}$$

where $\mathbf{x} \cdot \mathbf{y}$ denotes the ordinary dot product of $\mathbf{x}$ and $\mathbf{y}$. Consequently, if the congruences $\nabla F(\mathbf{x}) \equiv \mathbf{0} \bmod k$ hold, $F(\mathbf{x} + k\mathbf{y}) \equiv F(\mathbf{x}) \bmod k^2$ from which it

https://doi.org/10.1017/S1446788700017687 Published online by Cambridge University Press

follows that the exponential sum

$$S_F(q;\mathbf{x}) = \sum_{\mathbf{y} \bmod r} e_q(F(\mathbf{x}+k\mathbf{y}) - F(\mathbf{x})) \tag{6}$$

is well-defined modulo r. We now have

THEOREM 1. *Let q be a positive integer and F be a polynomial in $\mathbf{Z}[\mathbf{X}]$. Then*

$$S_F(q) = k^n \sum_{\substack{\mathbf{x} \in B_n(k) \\ \nabla F(\mathbf{x}) \equiv \mathbf{0} \bmod k}} e_q(F(\mathbf{x}))S_F(q;\mathbf{x}),$$

where k and r are the positive integers uniquely determined by $q = k^2 r$ with r square free.

PROOF. If we take $M = kr$ and $N = k$ in (4), then (5) implies that

$$\begin{aligned} S_F(q) &= \sum_{\mathbf{v} \in B_n(k)} e_q(F(\mathbf{v})) \sum_{\mathbf{u} \in B_n(k)} e_k(\nabla F(\mathbf{v}) \cdot \mathbf{u}) \\ &= k^n \sum_{\substack{\mathbf{v} \in B_n(kr) \\ \nabla F(\mathbf{v}) \equiv \mathbf{0} \bmod k}} e_q(F(\mathbf{v})), \end{aligned}$$

from which the theorem follows by a second application of (4) with $M = k$ and $N = r$.

By a trivial modification of the proof of Theorem 1 in [8], it follows that $S_F(q) = S(F; q)$ is multiplicative in q. More precisely, we have

THEOREM 2. *Let q_1 and q_2 be relatively prime positive integers, and choose integers m_1 and m_2 satisfying $m_1 q_1 + m_2 q_2 = 1$. If F is a polynomial in $\mathbf{Z}[\mathbf{X}]$, then $S(F; q_1 q_2) = S(m_2 F; q_1)S(m_1 F; q_2)$.*

Consequently, it suffices to examine the exponential sum $S_F(q)$ with q a prime power p^α. If α is even, $S_F(q;\mathbf{x}) = 1$ so that by Theorem 1, $|S_F(q)|$ is bounded above by $q^{n/2}$ times the number of solutions of the system of congruences $F(\mathbf{X}) \equiv \mathbf{0} \bmod q^{1/2}$, the latter being essentially bounded as $q \to \infty$ if the discriminant of ∇F is non-zero. If $\alpha > 1$ is odd, the exponential sum $S_F(q;\mathbf{x})$ is a Gaussian sum associated with the quadratic form defined by the Jacobian matrix of F at $\mathbf{x}$. In view of these remarks, the next two sections will be devoted to (i) counting the number of solutions of certain systems of polynomial congruences modulo q, and (ii) an examination of Gaussian sums associated with quadratic forms modulo p.

3. A generalization of a theorem of Nagell and Ore

Let $\mathbf{f} = (f_1,\ldots,f_n)$ be an n-tuple of polynomials in $\mathbf{Z}[\mathbf{X}]$, where $\mathbf{X} = (X_1,\ldots,X_n)$. For any positive integer q, let $V_{\mathbf{f}}(q)$ denote the zero set of $\mathbf{f}$ modulo q, that is, $V_{\mathbf{f}}(q) = \{\mathbf{x} \bmod q : \mathbf{f}(\mathbf{x}) \equiv \mathbf{0} \bmod q\}$. In this section, we shall examine upper bounds for the cardinality of $V_{\mathbf{f}}(q)$, which we denote by $N_{\mathbf{f}}(q)$. Since $N_{\mathbf{f}}(q)$ is multiplicative in q, it suffices to assume that q is a prime power p^α. Since $V_{\mathbf{f}}(p^\alpha) \subseteq V_{\mathbf{f}}(p) \oplus pB_n(p^{\alpha-1})$, it follows that

$$N_{\mathbf{f}}(p^\alpha) \leqslant p^{n(\alpha-1)} N_{\mathbf{f}}(p) \tag{7}$$

for all $\alpha \geqslant 1$. For $n = 1$, (7) implies that

$$N_{\mathbf{f}}(p^\alpha) \leqslant (\deg f) p^{\alpha-1}. \tag{8}$$

In 1921, Nagell and Ore proved independently [5, page 90] that if the discriminant $D(f)$ of f does not vanish identically, then (8) can be sharpened to

$$N_f(p^\alpha) \leqslant (\deg f) p^{2 \operatorname{ord}_p D(f)} \tag{9}$$

for all $\alpha \geqslant 1$, where ord_p denotes the p-adic order valuation. In particular, (9) implies that $N_f(p^\alpha)$ is bounded as $\alpha \to \infty$ for fixed p.

In order to obtain an n-dimensional analogue of (9), we first need a suitable analogue of the discriminant of $\mathbf{f}$. If $\mathcal{J}_{\mathbf{f}}$ denotes the $n \times n$ Jacobian matrix of $\mathbf{f}$, let $J_{\mathbf{f}} = \det \mathcal{J}_{\mathbf{f}} \in \mathbf{Z}[\mathbf{X}]$ denote the Jacobian of $\mathbf{f}$. By van der Waerden [9, Section 82], there exists a non-negative integer R, called the resultant of $\mathbf{f}$ and $J_{\mathbf{f}}$, which belongs to the ideal of $\mathbf{Z}[\mathbf{X}]$ generated by $J_{\mathbf{f}}$ and the components of $\mathbf{f}$. Furthermore, if $R \neq 0$ then the associated projective variety defined by $\mathbf{f}$ is non-singular and of dimension 0 over some algebraically closed field K containing $\mathbf{Q}$. We therefore define the *discriminant* $D(\mathbf{f})$ of $\mathbf{f}$ as follows. If $R = 0$, set $D(\mathbf{f}) = 0$; otherwise, let $D(\mathbf{f})$ denote the smallest positive integer in this ideal.

For any prime p, let $\mathbf{Q}_p$ denote the p-adic completion of $\mathbf{Q}$. The p-adic order valuation ord_p on $\mathbf{Q}$ extends uniquely to $\mathbf{Q}_p$; we denote the extension by ord_p. For any $\mathbf{z} = (z_1,\ldots,z_n) \in \mathbf{Q}_p^n$, we write $\operatorname{ord}_p \mathbf{z} = \min_{1 \leqslant i \leqslant n} \operatorname{ord}_p z_i$. The estimate for $N_{\mathbf{f}}(p^\alpha)$ follows from the following version of Hensel's lemma.

LEMMA. *Let p be a prime and let $\mathbf{f}$ be an n-tuple of polynomials in $\mathbf{Z}[\mathbf{X}]$. Suppose $\mathbf{x}_0 \in \mathbf{Z}^n$ satisfies*

$$\operatorname{ord}_p \mathbf{f}(\mathbf{x}_0) > 2 \operatorname{ord}_p J_{\mathbf{f}}(\mathbf{x}_0).$$

Then there exists a unique $\mathbf{x}$ in $\mathbf{Q}_p^n$ such that $f(\mathbf{x}) = \mathbf{0}$ and

$$\operatorname{ord}_p(\mathbf{x} - \mathbf{x}_0) \geqslant \operatorname{ord}_p \mathbf{f}(\mathbf{x}_0) - \operatorname{ord}_p J_{\mathbf{f}}(\mathbf{x}_0).$$

PROOF. By Taylor's theorem, we can write

$$\mathbf{f}(\mathbf{x}+\mathbf{y}) = \mathbf{f}(\mathbf{x}) + \mathbf{y}\mathcal{J}_{\mathbf{f}}(\mathbf{x}) + \mathbf{g}(\mathbf{x},\mathbf{y}),$$

where $\mathbf{g}(\mathbf{X},\mathbf{Y})$ is an n-tuple of polynomials in $\mathbf{Y}$ with coefficients in $\mathbf{Z}[\mathbf{X}]$, all of whose terms have degree at least 2 in $\mathbf{Y}$. Similarly,

$$\mathcal{J}_{\mathbf{f}}(\mathbf{x}+\mathbf{y}) = \mathcal{J}_{\mathbf{f}}(\mathbf{x}) + \mathcal{H}(\mathbf{x},\mathbf{y}),$$

where all the terms of $\mathcal{H}(\mathbf{X},\mathbf{Y})$, as polynomials in $\mathbf{Y}$, have degree at least 1. Starting with $\mathbf{x}_0$, we define sequences $\{\mathbf{x}_n\}$ and $\{\mathbf{y}_n\}$ in $\mathbf{Q}_p^n$ by the equations

$$\mathbf{x}_n = \mathbf{x}_{n-1} + \mathbf{y}_n,$$
$$\mathbf{y}_n\mathcal{J}_{\mathbf{f}}(\mathbf{x}_{n-1}) = -\mathbf{f}(\mathbf{x}_{n-1}).$$

It now follows by an induction argument, based upon the above Taylor expansions of $\mathbf{f}$ and $\mathcal{J}_{\mathbf{f}}$, that

$$\operatorname{ord}_p \mathbf{y}_n \geqslant \operatorname{ord}_p f(\mathbf{x}_{n-1}) - \operatorname{ord}_p J_{\mathbf{f}}(\mathbf{x}_{n-1}),$$
$$\operatorname{ord}_p J_{\mathbf{f}}(\mathbf{x}_n) = \operatorname{ord}_p J_{\mathbf{f}}(\mathbf{x}_{n-1}), \quad \text{and}$$
$$\operatorname{ord}_p \mathbf{f}(\mathbf{x}_n) \geqslant 2\operatorname{ord}_p \mathbf{y}_n.$$

Hence,

$$\operatorname{ord}_p J_{\mathbf{f}}(\mathbf{x}_n) = \operatorname{ord}_p J_{\mathbf{f}}(\mathbf{x}_0),$$
$$\operatorname{ord}_p \mathbf{y}_n \geqslant \operatorname{ord}_p J_{\mathbf{f}}(\mathbf{x}_0) + 2^{n-1}, \quad \text{and}$$
$$\operatorname{ord}_p \mathbf{f}(\mathbf{x}_n) \geqslant 2\operatorname{ord}_p J_{\mathbf{f}}(\mathbf{x}_0) + 2^n$$

for each n, and so $\mathbf{x} = \lim_{n\to\infty} \mathbf{x}_n$ has the properties required in the lemma. Finally, if $\mathbf{x}$ and $\mathbf{x}+\mathbf{y}$ are both zeros of $\mathbf{f}$ in $\mathbf{Q}_p^n$, the Taylor expansion of $\mathbf{f}(\mathbf{x}+\mathbf{y})$ yields $\mathbf{y}\mathcal{J}_{\mathbf{f}}(\mathbf{x}) = -\mathbf{g}(\mathbf{x},\mathbf{y})$, whence $\operatorname{ord}_p \mathbf{y} \geqslant 2\operatorname{ord}_p \mathbf{y} - \operatorname{ord}_p J_{\mathbf{f}}(\mathbf{x})$, that is, $\operatorname{ord}_p \mathbf{y} \leqslant \operatorname{ord}_p J_{\mathbf{f}}(\mathbf{x})$. So, there is at most one zero of $\mathbf{f}$ satisfying $\operatorname{ord}_p(\mathbf{x}-\mathbf{x}_0) > \operatorname{ord}_p J_{\mathbf{f}}(\mathbf{x}_0)$.

THEOREM 3. *Let p be a prime and let $\mathbf{f}$ be an n-tuple of polynomials in $\mathbf{Z}[\mathbf{X}]$ with $D(\mathbf{f}) \neq 0$. If $\delta = \operatorname{ord}_p D(\mathbf{f})$, then*

$$N_{\mathbf{f}}(p^\alpha) \leqslant \begin{cases} p^{n\alpha} & \text{for } \alpha \leqslant 2\delta, \\ (\operatorname{Deg}\mathbf{f})p^{n\delta} & \text{for } \alpha > 2\delta, \end{cases}$$

where $\operatorname{Deg}\mathbf{f}$ *denotes the product of the degrees of all the components of* $\mathbf{f}$.

PROOF. The assertion is trivial for $\alpha \leqslant 2\delta$. So, we may assume that $\alpha > 2\delta$ and let $\mathbf{x}_0$ be a point in $V_{\mathbf{f}}(p^\alpha)$. Since $D(\mathbf{f})$ is in the ideal of $\mathbf{Z}[\mathbf{X}]$ generated by the components of $\mathbf{f}$ and $J_{\mathbf{f}}$, then $\operatorname{d}_p J_{\mathbf{f}}(\mathbf{x}_0) \leqslant \delta$. By the lemma, there is a unique $\mathbf{x}$ in $\mathbf{Q}_p^n$ such that $\mathbf{f}(\mathbf{x}) = \mathbf{0}$ and $\operatorname{ord}_p(\mathbf{x}-\mathbf{x}_0) \geqslant \alpha - \delta$. Thus, each $\mathbf{x}_0$ in $V_{\mathbf{f}}(p)$ is associated with a p-adic solution of the equations $\mathbf{f}(\mathbf{X}) = \mathbf{0}$ and each p-adic

https://doi.org/10.1017/S1446788700017687 Published online by Cambridge University Press

solution corresponds in this way to at most $p^{n\delta}$ points in $V_{\mathbf{f}}(p^{\alpha})$. Our estimate for $N_{\mathbf{f}}(p^{\alpha})$ therefore follows from Bezout's theorem which implies that the number of p-adic solutions of the equation $f(\mathbf{X}) = \mathbf{0}$ is at most $\operatorname{Deg}\mathbf{f}$ under our assumption that $D(\mathbf{f}) \neq 0$. To see this, let K denote an algebraic closure of $\mathbf{Q}_p$ and let V be an irreducible component of the affine variety $V(\mathbf{f})$ in K^n defined by $\mathbf{f}$. The assumption $D(\mathbf{f}) \neq 0$ implies that each point $\mathbf{x}$ of the variety V is a simple point, and furthermore, the rank of $\mathfrak{J}_{\mathbf{f}}(\mathbf{x})$ is maximal. Consequently, the dimension of the tangent space of V at $\mathbf{x}$ must be zero and so the dimension of the variety V must also be zero, and V is therefore finite [7, page 78]. Since $V(\mathbf{f})$ is the finite union of irreducible varieties, then $V(\mathbf{f})$ is finite, whence by Bezout's theorem [7, page 198], $\operatorname{card} V(\mathbf{f}) \leqslant \operatorname{Deg}\mathbf{f}$.

The following less precise form of our estimate for $N_{\mathbf{f}}(p^{\alpha})$ is more manageable for applications to exponential sums.

COROLLARY. *Let p be a prime and let $\mathbf{f}$ be an n-tuple of polynomials in $\mathbf{Z}[\mathbf{X}]$ with $D(\mathbf{f}) \neq 0$. Then*

$$N_{\mathbf{f}}(p^{\alpha}) \leqslant (\operatorname{Deg}\mathbf{f})\big(D(\mathbf{f})^2, p^{\alpha}\big)^n.$$

4. Gaussian sums of a quadratic form

If $Q(\mathbf{X})$ is an integral quadratic form in n variables $\mathbf{X} = (X_1, \ldots, X_n)$, there exists a unique symmetric matrix $A \in M_{n\times n}(\mathbf{Z})$ such that

$$Q(\mathbf{X}) = \tfrac{1}{2}\mathbf{X}A\mathbf{X}^t, \tag{10}$$

where $\mathbf{X}^t$ denotes the transpose of $\mathbf{X}$; in case Q is defined by A as in (10), it will be convenient to write Q_A instead of Q. For each positive integer q and $\mathbf{a} \in \mathbf{Z}^n$, we define the Gaussian sum associated with the quadratic form Q by

$$G_Q(q; \mathbf{a}) = \sum_{\mathbf{x} \bmod q} e_q(Q(\mathbf{x}) + \mathbf{a}\cdot\mathbf{x}).$$

Although for the purposes of this paper, it would suffice to obtain an upper bound for $G_Q(q; \mathbf{a})$ for q a prime, we will obtain a more general result.

For any subset S of $\mathbf{Z}^n$, we say that $\mathbf{x} \in \mathbf{Z}^n$ is *q-orthogonal* to S if

$$\mathbf{x}\cdot\boldsymbol{\gamma} = \begin{cases} 0 \bmod q & \text{for all } \boldsymbol{\gamma} \in S \text{ if } q \text{ is odd,} \\ 0 \text{ or } \tfrac{1}{2}q \bmod q & \text{for all } \boldsymbol{\gamma} \in S \text{ if } q \text{ is even.} \end{cases}$$

For any matrix $A \in M_{n\times n}(\mathbf{Z})$, let $\operatorname{Ker}_q A$ be the $\mathbf{Z}/q\mathbf{Z}$-module defined by

$$\operatorname{Ker}_q A = \{\mathbf{x} \bmod q; \mathbf{x}A \equiv 0 \bmod q\}.$$

https://doi.org/10.1017/S1446788700017687 Published online by Cambridge University Press

THEOREM 4. *Let q be a positive integer and $\mathbf{a} \in \mathbf{Z}^n$. Then a necessary and sufficient condition for the Gaussian sum $G_Q(q; \mathbf{a})$ to be non-zero is that $\mathbf{a}$ be q-orthogonal to $\mathrm{Ker}_q A$, in which case $|G_Q(q; \mathbf{a})|^2 = q^n |\mathrm{Ker}_q A|$, where A is the matrix of Q.*

PROOF. From the definition of the Gaussian sum, we have

$$|G_Q(q; \mathbf{a})|^2 = \sum_{\mathbf{y} \bmod q} \sum_{\mathbf{x} \bmod q} e_q(Q(\mathbf{x}) - Q(\mathbf{y}) + \mathbf{a} \cdot (\mathbf{x} - y)). \tag{11}$$

Since $Q(\mathbf{x} + \mathbf{y}) = Q(\mathbf{x}) + \mathbf{x}A\mathbf{y}^t + Q(\mathbf{y})$, the automorphism $\mathbf{x} \mapsto \mathbf{x} + \mathbf{y}$ of the residue classes modulo q in $\mathbf{Z}^n$ transforms (11) into

$$|G_Q(q; \mathbf{a})|^2 = q^n \sum_{\mathbf{x} \in \mathrm{Ker}_q A} e_q(Q(\mathbf{x}) + \mathbf{a} \cdot \mathbf{x}). \tag{12}$$

Therefore, if the congruence

$$Q(\boldsymbol{\gamma}) + \mathbf{a} \cdot \boldsymbol{\gamma} \equiv 0 \bmod q \tag{13}$$

holds for all $\boldsymbol{\gamma} \in \mathrm{Ker}_q A$, (12) then implies that

$$|G_Q(q; \mathbf{a})|^2 = q^n |\mathrm{Ker}_q A|;$$

on the other hand, if there eixsts a $\boldsymbol{\gamma} \in \mathrm{Ker}_q A$ such that the congruence (13) does not hold, then the automorphism $\mathbf{x} \mapsto \mathbf{x} + \boldsymbol{\gamma}$ of $\mathrm{Ker}_q A$ transforms (12) into $|G_Q(q; \mathbf{a})|^2 = e_q(Q(\boldsymbol{\gamma}) + \mathbf{a} \cdot \boldsymbol{\gamma}) |G_Q(q; \mathbf{a})|^2$, whence $G_Q(q; \mathbf{a}) = 0$. Consequently, we have proved that $G_Q(q; \mathbf{a}) \neq 0$ if and only if the congruence (13) holds for all $\boldsymbol{\gamma} \in \mathrm{Ker}_q A$.

To complete the proof, it remains to linearize the congruence condition in (13). First, we assume that q is odd. Then for any $\boldsymbol{\gamma} \in \mathrm{Ker}_q A$, the congruence $\boldsymbol{\gamma}A \equiv \mathbf{0} \bmod q$ clearly implies that $Q(\boldsymbol{\gamma}) \equiv 0 \bmod q$ so that the congruence (13) is then clearly equivalent to $\mathbf{a} \cdot \boldsymbol{\gamma} \equiv 0 \bmod q$. On the other hand, if q is even, then for any $\boldsymbol{\gamma} \in \mathrm{Ker}_q A$, the congruence $\boldsymbol{\gamma}A \equiv \mathbf{0} \bmod q$ implies that $Q(\boldsymbol{\gamma}) \equiv 0 \bmod \frac{1}{2}q$, in which case (13) implies that $\mathbf{a} \cdot \boldsymbol{\gamma} \equiv 0$ or $\frac{1}{2}q \bmod q$. Hence, the congruence (13) is equivalent to the linear congruence $\mathbf{a} \cdot \boldsymbol{\gamma} \equiv 0$ or $\frac{1}{2}q \bmod q$, as required.

5. The basic estimate for $S_F(p^\alpha)$

In view of the above preparation, we can now establish an estimate for $S_F(p^\alpha)$ for any polynomial F in $\mathbf{Z}[\mathbf{X}]$ whose gradient has a non-zero discriminant, provided of course that $\alpha > 1$.

https://doi.org/10.1017/S1446788700017687 Published online by Cambridge University Press

THEOREM 5. *Let p be a prime and let F be a non-linear polynomial in $\mathbf{Z}[\mathbf{X}]$ of degree $m+1$ such that $D(\nabla F) \neq 0$. Then for any $\alpha > 1$,*

$$|S_F(p^\alpha)| \leqslant m^n p^{n\alpha/2}\big(D(\nabla F)^5, p^\alpha\big)^{n/2}.$$

PROOF. In view of the discussion at the end of Section 2 together with the Corollary to Theorem 3, Theorem 5 certainly holds for α even, and so we may assume that $\alpha = 2\beta + 1$ with $\beta \geqslant 1$. In order to determine explicitly the auxiliary exponential sum $S_F(p^\alpha; \mathbf{x})$ defined by (6) with $\nabla F(\mathbf{x}) \equiv \mathbf{0} \bmod p^\beta$, we must first refine the congruence in (5). Indeed, for any $\mathbf{x}, \mathbf{y} \in \mathbf{Z}^n$, Taylor's theorem implies that

$$F(\mathbf{x} + p^\beta \mathbf{y}) \equiv F(\mathbf{x}) + p^\beta \nabla F(\mathbf{x}) \cdot \mathbf{y} + p^{2\beta} Q_{H(\mathbf{x})}(\mathbf{y}) \bmod p^\alpha,$$

where $Q_{H(\mathbf{x})}$ is the quadratic form associated with the Hessian matrix of F at $\mathbf{x}$, that is, $H(\mathbf{x}) = \mathcal{H}_F(\mathbf{x}) \in M_{n\times n}(\mathbf{Z})$. Consequently, Theorem 1 implies that

$$S_F(p^\alpha) = p^{n\beta} \sum_{\mathbf{x} \in V_{\nabla F}(p^\beta)} e_{p^\alpha}(F(\mathbf{x})) G_{Q_{H(\mathbf{x})}}(p; p^{-\beta}\nabla F(\mathbf{x})),$$

which by Theorem 4 implies

$$|S_F(p^\alpha)| \leqslant p^{n\alpha/2} \sum_{\mathbf{x} \in V_{\nabla F}(p^\beta)} |\operatorname{Ker}_p H(\mathbf{x})|^{1/2}.$$

Let $\delta = \operatorname{ord}_p D(\nabla F)$. If $\delta = 0$, then $\operatorname{Ker}_p H(\mathbf{x})$ is trivial so that the estimate follows from the Corollary to Theorem 3. On the other hand, if $\delta > 0$, then $|\operatorname{Ker}_p H(\mathbf{x})| \leqslant p^n$ and so we get

$$\begin{aligned} |S_F(p^\alpha)| &\leqslant m^n p^{n\alpha/2} p^{n/2 + n\min\{2\delta, (\alpha-1)/2\}} \\ &\leqslant m^n p^{n\alpha/2} p^{n\min\{5\delta/2, \alpha/2\}}, \end{aligned}$$

as required.

6. The main theorem

Although Deligne has established the existence of a large class of polynomials in n variables over $\mathbf{Z}$ which satisfy the inequality (2), it is nevertheless not clear at present how large the class of polynomials satisfying (2) actually is. In order to avoid unnecessarily restricting the polynomials considered in our main result, Theorem 6, we define a special set of polynomials $\mathfrak{N}_n \subset \mathbf{Z}[\mathbf{X}]$ as follows. For each non-linear polynomial F in $\mathbf{Z}[\mathbf{X}]$ and for each prime p, we know there exists a unique integer $t_p \geqslant 0$ and a unique polynomial $F_p \in \mathbf{Z}[\mathbf{X}] - p\mathbf{Z}[\mathbf{X}]$ such that

https://doi.org/10.1017/S1446788700017687 Published online by Cambridge University Press

$F = p'^{p}F_p$, and $F_p = F$ for all but a finite number of p. We say that $F \in \mathfrak{D}_n$ if and only if for all primes p,

$$|S_{F_p}(p)| \leqslant (\deg F - 1)^n p^{n/2}.$$

THEOREM 6. *Let q be a positive integer and F be a polynomial in $\mathfrak{D}_n$ with $D(\nabla F) \neq 0$. Then*

$$|S_F(q)| \leqslant q^{n/2}\big(D(\nabla F)^5, q\big)^{n/2} d_m^n(q),$$

where $m = \deg F - 1$.

PROOF. This result follows directly from Theorems 2 and 5, if we observe that for any positive integer q, $qD(\mathbf{f})$ divides $D(q\mathbf{f})$ for any n-tuple $\mathbf{f}$ of polynomials in $\mathbf{Z}[\mathbf{X}]$. We omit the details as they are virtually identical with the proof given in [8] for the special case $n = 1$.

7. General remarks

One special class of polynomials for which estimates of the quality of Theorem 6 would have significant implications for number theory would be for $F_{\mathbf{a}}(\mathbf{X}) = F(\mathbf{X}) + \mathbf{a} \cdot \mathbf{X}$, where $F \in \mathfrak{D}_n$ is a form of degree $m + 1 \geqslant 3$ and $\mathbf{a} \in \mathbf{Z}^n$ is arbitrary (see [1] and [3].) In the particular case $a = 0$, we will always have $D(\nabla F) = 0$, by Euler's theorem, so that Theorem 6 is inapplicable. This raises the question: what is the analogue of Theorem 6 in this situation? On the other hand, if $F \in \mathfrak{D}_n$ satisfies $D(\nabla F_{\mathbf{a}}) = D(\nabla F + \mathbf{a}) \neq 0$ for all $\mathbf{a} \neq \mathbf{0}$ in $\mathbf{Z}^n$, then Theorem 6 implies that

$$|S(F_{\mathbf{a}}; q)| \leqslant c_F(\mathbf{a}) q^{n/2} d_m^n(q),$$

where $c_F(\mathbf{a}) = D(\nabla F + \mathbf{a})^{5n/2}$. This poses a second problem of determining explicitly the dependence of $c_F(\mathbf{a})$ on $\mathbf{a}$.

As for possible improvements of Theorem 6, we first note that for $n = 1$, (3) is stronger than Theorem 6, the reason being that in [8], a stronger form of the theorem of Nagell and Ore is used that is due to Sándor [6]. Indeed, Sándor's result asserts that $N_f(p^\alpha)$ is stationary for $\alpha > \delta$, $\delta = \operatorname{ord}_p D(f')$, while Nagell and Ore assert $N_f(p^\alpha)$ is stationary only for $\alpha > 2\delta$. This suggests a possible improvement in Theorem 3, which in turn would produce a corresponding improvement in Theorem 6. On the other hand, Loxton and Smith [4] have recently shown, by different methods, that in (3), the factor $(D(F'), q)$ can be

replaced by $(D(F'), q)^{1/2}$. Similarly, it may be possible to replace the factor $(D(\nabla F)^5, q)$ in Theorem 6 by $(D(\nabla F), q)$. And finally, what is the analogue of Theorem 6 when $f \in \mathfrak{D}_n$ and $D(\nabla F) = 0$? In this direction, see [4].

Note added in proof. A more precise and explicit description required here has been given by W. Krull, 'Funktionaldeterminanten und Diskriminanten bei Polynomen in mehrerer Unbestimmten', *Monatshefte Math. u. Phys.* **48** (1939), 353–368, and **50** (1942), 234–256.

References

1. H. Davenport, 'Cubic forms in 32 variables,' *Philos. Trans. Roy. Soc. London Ser. A*, **251** (1959), 193–232.
2. P. Deligne, 'La conjecture de Weil, I,' *Inst. Hautes Études Sci. Publ. Math.* **43** (1974), 273–307.
3. J.-I. Igusa, *Lectures on forms of higher degree* (Tata Institute of Fundamental Research, Bombay, 1978).
4. J. H. Loxton and R. A. Smith, 'On Hua's estimate for exponential sums,' to appear.
5. T. Nagell, *Introduction to number theory* (Wiley, New York, 1951).
6. G. Sándor, 'Über die Anzahl der Lösungen einer Kongruenz,' *Acta Math.* **87** (1952), 13–17.
7. I. R. Shafarevich, *Basic algebraic geometry* (Springer-Verlag, Berlin/New York, 1977).
8. R. A. Smith, 'Estimates for exponential sums,' *Proc. Amer. Math. Soc.* **79** (1980), 365–368.
9. B. L. van der Waerden, *Modern Algebra*, vol. II, (Ungar, New York, 1950).

Department of Mathematics
University of New South Wales
Kensington, N.S.W. 2033
Australia

Department of Mathematics
University of Toronto
Toronto, Ontario M5S 1A1
Canada