Mathematical Proceedings of the Cambridge Philosophical Society

VOL. 99 MARCH 1986 PART 2

Math. Proc. Camb. Phil. Soc. (1986), **99**, 189
Printed in Great Britain

A note on trigonometric sums in several variables

By R. W. K. ODONI
Department of Mathematics, University of Exeter

(*Received* 24 *July* 1985)

0. *Introduction*

In [3, 4] we showed how the use of a random-walk analogue can be made to yield non-trivial information about the behaviour of certain trigonometric sums in one variable. Our aim here is to show how our method can be adapted to yield similar results for a broad class of trigonometric sums in several variables. Let

$$f(\mathbf{x}) = f(x_1, \ldots, x_\nu) \in \mathbb{Z}[x_1, \ldots, x_\nu]$$

be a polynomial in ν independent variables with integral coefficients. We choose integers $n \geqslant 0$, $d \geqslant 1$ and $p \geqslant 2$, with p prime, and assume that $f(\mathbf{x})$ has total degree $\leqslant d+1$. We shall consider the problem of obtaining non-trivial upper bounds for the absolute value of sums of the type

$$S(f) = \sum_{\mathbf{x} \in P^\nu} \exp(2\pi i f(x_1^{p^n}, \ldots, x_\nu^{p^n})/p^{n+1}), \tag{0·1}$$

where $P = \{1, 2, \ldots, p\}$ and f is non-constant.

For $n = 0$ the methods of modern algebraic geometry were introduced by Weil [5], who, having proved the Riemann hypothesis for zeta functions of curves over finite fields, was able to obtain the estimate $|S(f)| \leqslant dp^{\frac{1}{2}}$ when $\nu = 1$, $d > 0$ and $p > p_0$. For $n = 0$, $\nu \geqslant 1$, Deligne [1] obtained the estimate $|S(f)| \leqslant d^\nu p^{\nu/2}$, provided that $F(\mathbf{x})$, the homogeneous part of f of highest degree, is such that the variety $F(\mathbf{x}) = 0$, in projective $(\nu-1)$-dimensional space over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, is non-singular. Deligne's proof uses some of the deepest known results and techniques of modern algebraic geometry, including his own proofs of Weil's conjectures on non-singular projective varieties over finite fields. If $F(\mathbf{x}) = 0$ is not non-singular there is no very sharp estimate available (indeed, any bound likely to emerge out of Deligne's approach would necessarily involve various subtle geometrical invariants); there is, however, a relatively weak, older result $|S(f)| = O(p^{\nu-\frac{1}{2}})$ (d fixed), due to Lang and Weil [2], applicable to all non-constant f. This result is best-possible at this level of generality, as is shown by the example $f(\mathbf{x}) = x_1^2$, $|S(f)| = p^{\nu-\frac{1}{2}}$, for $p > 2$, $\nu \geqslant 1$.

https://doi.org/10.1017/S0305004100064100 Published online by Cambridge University Press

If $n \geqslant 1$ there is apparently no published non-trivial estimate for $|S(f)|$; even for $\nu = 1$ it is not known whether $|S(f)| = o(p)$ when f is fixed and $p \to \infty$, although, in a certain sense, the results in [4] show that $|S(f)| = O(p^{\frac{1}{2}})$ for 'most' f.

We shall adapt and improve our random-walk method of [3, 4] to obtain interesting results about the 'typical' $S(f)$ of (0·1), for arbitrary fixed $n \geqslant 0$, $\nu \geqslant 1$. We shall regard d as a function $d(p)$ of p, tending to ∞ with p, as slowly as desired, and always subject to the condition $1 \leqslant d < p$. We choose, for given prime p, any non-constant polynomial $g_p(\mathbf{x}) \in \mathbb{Z}/p^{n+1}\mathbb{Z}[\mathbf{x}]$, and consider the set

$$\mathscr{F} = \mathscr{F}(p, n, \nu, d, g_p) = \{g_p(\mathbf{x}) + \sum_{\mathbf{b} \in B} a(\mathbf{b}) x_1^{b_1} \dots x_\nu^{b_\nu};\ a(\mathbf{b}) \in \mathbb{Z}/p^{n+1}\mathbb{Z}, \forall \mathbf{b} \in B\}, \quad (0{\cdot}2)$$

where $B = \{\mathbf{b} = (b_1, \dots, b_\nu); b_i \geqslant 0, 1 \leqslant \sum_{1 \leqslant i \leqslant \nu} b_i \leqslant d\}$. If $\# B = \beta$ we have $\# \mathscr{F} = p^{\beta(n+1)}$. To each subset A of $\mathscr{F}$ we assign the probability measure $\# A / \# \mathscr{F}$. We then choose $f(\mathbf{x})$ 'at random in $\mathscr{F}$', in the sense that $\text{Prob}\,(f(\mathbf{x}) \in A) = \# A / \# \mathscr{F}$. In this way $S = S(f)$ of (0·1) becomes a $\mathbb{C}$-valued random variable on $\mathscr{F}$, and our aim is to determine asymptotic forms for its distribution as $p \to \infty$. We adopt a very naive random-walk analogue for the behaviour of S on $\mathscr{F}$, comparing it with $Z = \sum_{1 \leqslant j \leqslant p^\nu} e^{2\pi i \Theta_j}$, where the Θ_j are independent random variables, each uniformly distributed on the interval $[0, 1]$. There is no strong *a priori* reason to suppose that S and Z are close in distribution, except that, in [3, 4], we showed that the agreement is quite strong in the case $\nu = 1$. We shall see that the same situation holds when $\nu > 1$. In the following we shall denote the expectation of a $\mathbb{C}$-valued random variable X by $\mathscr{E}(X)$. Our results are as follows.

THEOREM 1. *For any integral $k \geqslant 0$, $\nu \geqslant 1$ and prime p we have*

$$\mathscr{E}(|Z|^{2k}) = \sum_{\mathbf{r} \in \mathscr{R}} \binom{k}{\mathbf{r}}^2,$$

where

$$\binom{k}{\mathbf{r}} = \frac{k!}{r_1!, \dots, r_{p^\nu}!},$$

and $\mathscr{R}$ is the set of all ordered p^ν-tuples $\mathbf{r} = (r_1, \dots, r_{p^\nu})$ such that $0 \leqslant r_i \in \mathbb{Z}$ and

$$\sum_{1 \leqslant i \leqslant p^\nu} r_i = k.$$

THEOREM 2. *For fixed $\nu \geqslant 1$ we have*

$$\lim_{p \to \infty} \text{Prob}\,(|Z|^2 \geqslant p^\nu \xi) = e^{-\xi}$$

for any fixed real $\xi \geqslant 0$.

THEOREM 3. *Let $I_0(t) = \sum_{k \geqslant 0} (k!)^{-2} (t/2)^{2k}$ $(t \in \mathbb{C})$. Then $\mathscr{E}(I_0(t|Z|)) = I_0(t)^{p^\nu}$, for any fixed $t \in \mathbb{C}$, $\nu \geqslant 1$ and prime $p \geqslant 2$.*

THEOREM 4. *For any integral k, $0 \leqslant k \leqslant d = d(p) < p$, we have $\mathscr{E}(|S|^{2k}) = \mathscr{E}(|Z|^{2k})$, for any fixed p, n, ν.*

THEOREM 5. *If $d = d(p) \to \infty$ with p, with $1 \leqslant d < p$, we have*

$$\lim_{p \to \infty} \text{Prob}\,(|S|^2 \geqslant p^\nu \xi) = e^{-\xi},$$

for any fixed real $\xi \geqslant 0$, and any fixed integral $n \geqslant 0$, $\nu \geqslant 1$.

https://doi.org/10.1017/S0305004100064100 Published online by Cambridge University Press

THEOREM 6

(I) *Let $c > 0$ be fixed. Then*

$$\text{Prob}\,(|S| \geqslant 2dp^{\nu/2}c^{-1}) \leqslant 4e^{c^2/4}.\sqrt{(\pi d)}\,e^{-2d}\{1+O(d^{-1})\}.$$

(II) *If $y \to \infty$ with p, we have*

$$\text{Prob}\,(|S| > ydp^{\nu/2}) \leqslant e^{\frac{1}{4}}.2\pi d \exp\left(-2d\log\frac{ye}{2}\right)\{1+O(y^{-2})\}\{1+O(d^{-1})\}.$$

Of these, Theorems 1–3 are trivial modifications of the corresponding results in [4], and the proofs can be omitted. Once we have proved Theorem 4 the proofs of Theorems 5 and 6 follow closely those of the corresponding results in [4], on replacing p there by p^ν, and we shall again omit the proofs. Thus we shall confine our efforts to the proof of Theorem 4.

We take the opportunity here to correct some misprints in [4]. The left-hand side of (4·2) should read $\mathscr{E}(I_0(t|Z_p|))$. The substitution at the beginning of Section 6 should read $tw = x = 2d$; the stated estimate (6·2) remains valid, but is not as sharp as it should be; the sharper version corresponds to the case $\nu = 1$ of the present Theorem 6 (I).

We remark that the parameter n does not appear in these estimates, a rather curious situation, since the corresponding problem of obtaining a non-trivial upper bound for all $|S(f)|$ appears to be very sensitive to changes in n (and, indeed, is unsolved when $n > 0$).

1. *Proof of Theorem* 4

1A. To begin with we write $\eta(t) = \exp(2\pi it/p^{n+1})$ for $t \in \mathbb{Z}$. Then, by (0·2),

$$|S(f)|^{2k} = \overline{S(f)^k}\,S(f)^k$$
$$= \sum_X \sum_Y \eta\left(\sum_{j=1}^{k}\{g_p(\mathbf{x}(j)^{p^n}) - g_p(\mathbf{y}(j)^{p^n})\}\right)\eta\left(\sum_{\mathbf{b}\in B} a(\mathbf{b})\left\{\sum_{j=1}^{k}(\mathbf{x}(j)^{p^n\mathbf{b}} - \mathbf{y}(j)^{p^n\mathbf{b}})\right\}\right). \tag{1·1}$$

The notation here is as follows. X and Y run over all $k \times \nu$ matrices with entries in $P = \{1, 2, \ldots, p\}$, the (j, s) entry of X being $x(j, s)$, while the jth row of X is written $\mathbf{x}(j)$. By $\mathbf{x}(j)^{\mathbf{m}}$ we mean $x(j,1)^{m_1}\ldots x(j,\nu)^{m_\nu}$ ($\mathbf{m} = (m_1, \ldots, m_\nu)$ being a vector of non-negative integers), while $\mathbf{x}(j)^{p^n}$ is $(x(j,1)^{p^n}, \ldots, x(j,\nu)^{p^n})$ and B is as in (0·2).

If we now sum (1·1) over all $a(\mathbf{b})$ ($\mathbf{b} \in B$), and use the orthogonality relations for additive characters of $\mathbb{Z}/p^{n+1}\mathbb{Z}$, we obtain

$$\mathscr{E}(|S|^{2k}) = \sum_{X \leftrightarrow Y}\sum \eta\left(\sum_{j=1}^{k}\{g_p(\mathbf{x}(j)^{p^n}) - g_p(\mathbf{y}(j)^{p^n})\}\right), \tag{1·2}$$

where $X \leftrightarrow Y$ means that

$$\sum_{j=1}^{k}\mathbf{x}(j)^{p^n\mathbf{b}} \equiv \sum_{j=1}^{k}\mathbf{y}(j)^{p^n\mathbf{b}} \pmod{p^{n+1}}, \quad \forall \mathbf{b} \in B, \tag{1·3}$$

and the summation in (1·2) is over all ordered pairs (X, Y) of matrices satisfying $X \leftrightarrow Y$.

1B. Suppose that $X \leftrightarrow Y$ (notation as in Section 1A). Then certainly

$$\sum_{j=1}^{k}\mathbf{x}(j)^{\mathbf{b}} \equiv \sum_{j=1}^{k}\mathbf{y}(j)^{\mathbf{b}} \pmod{p}, \quad \forall b \in B. \tag{1·4}$$

We denote by $x_*(j, s)$ and $y_*(j, s)$ respectively the (mod p)-reductions of $x(j, s)$ and $y(j, s)$ ($1 \leqslant j \leqslant k$, $1 \leqslant s \leqslant \nu$). Thus, in $\mathbb{F}_p$, (1·4) implies that

$$\sum_{j=1}^{k}\mathbf{x}_*(j)^{\mathbf{b}} = \sum_{j=1}^{k}\mathbf{y}_*(j)^{\mathbf{b}}. \tag{1·5}$$

https://doi.org/10.1017/S0305004100064100 Published online by Cambridge University Press

Let $t_1, \ldots, t_\nu$ be ν algebraically independent quantities over $\mathbb{F}_p$. Since B consists of all vectors $\mathbf{b}$ with $b_i \geqslant 0$, $1 \leqslant \sum_{1 \leqslant i \leqslant \nu} b_i \leqslant d$, we see from (1·5) that

$$\sum_{j=1}^{k} \xi_j^r = \sum_{j=1}^{k} \eta_j^r \quad (1 \leqslant r \leqslant d), \tag{1·6}$$

in $\mathbb{F}_p(\mathbf{t}) = \mathbb{F}_p(t_1, \ldots, t_\nu)$, where

$$\xi_j = \sum_{s=1}^{\nu} t_s x_*(j,s) \quad \text{and} \quad \eta_j = \sum_{s=1}^{\nu} t_s y_*(j,s). \tag{1·7}$$

By hypothesis, $0 \leqslant k \leqslant d < p$, while $\mathbb{F}_p(\mathbf{t})$ is of characteristic p. We may therefore apply the Newton–Waring identities connecting elementary symmetric functions and symmetric power sums to the relations (1·6). We see easily that the elementary symmetric functions of $\xi_1, \ldots, \xi_k$ and of $\eta_1, \ldots, \eta_k$ coincide, degree by degree. Consequently there is a permutation $\sigma \in S_k$ such that $\eta_j = \xi_{\sigma(j)}$ for $1 \leqslant j \leqslant k$, i.e.

$$\sum_{s=1}^{\nu} t_s y_*(j,s) = \sum_{s=1}^{\nu} t_s x_*(\sigma(j),s) \quad (1 \leqslant j \leqslant k).$$

Since $t_1, \ldots, t_\nu$ are algebraically independent over $\mathbb{F}_p$, we deduce that

$$y_*(j,s) = x_*(\sigma(j),s)$$

for all $1 \leqslant j \leqslant k$, $1 \leqslant s \leqslant \nu$. But $x(j,s), y(j,s) \in P$, so we must have $y(j,s) = x(\sigma(j),s)$ for all j, s.

It follows that $X \leftrightarrow Y$ implies that Y is a row permutation of X. In particular we must then have

$$\sum_{j=1}^{k} g_p(\mathbf{x}(j)^{p^n}) \equiv \sum_{j=1}^{k} g_p(\mathbf{y}(j)^{p^n}) \pmod{p^{n+1}}. \tag{1·8}$$

Conversely, if Y is a row permutation of X then certainly (1·8) holds and, moreover, $X \leftrightarrow Y$. We deduce from this and (1·2) that

$$\mathscr{E}(|S|^{2k}) = \sum_{X} \sum_{Y \sim X} 1, \tag{1·9}$$

where the summation is over all ordered pairs (X, Y) of $k \times \nu$ matrices over P, the notation $X \sim Y$ meaning that Y is a row permutation of X.

1C. It now only remains to evaluate the right-hand side of (1·9), and compare it with $\mathscr{E}(|Z|^{2k})$. In all there are exactly p^ν distinct possible rows for $k \times \nu$ matrices over P; let these row vectors be denoted by $\mathbf{R}_1, \ldots, \mathbf{R}_{p^\nu}$ in some order. A $k \times \nu$ matrix will be said to be of type $\mathbf{r} = (r_1, \ldots, r_{p^\nu})$ if exactly r_i of its rows coincide with $\mathbf{R}_i$ $(1 \leqslant i \leqslant p^\nu)$. The number of matrices of type $\mathbf{r}$ is then precisely

$$\binom{k}{\mathbf{r}} = \frac{k!}{r_1! \ldots r_{p^\nu}!} \quad \text{(multinomial coefficient)},$$

while two matrices X, Y satisfy $X \sim Y$ if and only if X and Y are of the same type. It follows that the right-hand side of (1·9) equals

$$\sum_{\mathbf{r} \in \mathscr{R}} \binom{k}{\mathbf{r}}^2,$$

with $\mathscr{R}$ as in Theorem 1, and this completes the proof of Theorem 4.

https://doi.org/10.1017/S0305004100064100 Published online by Cambridge University Press

2. *Concluding remarks*

(*a*) There is no difficulty in principle in varying the probability space $\mathscr{F}$ of (0·2), by omitting certain monomials $\mathbf{x}^{\mathbf{b}}$. The limit theorems and asymptotic formulae will be unchanged, but the extra power obtained from such modifications hardly justifies the complication of detail involved in formulating precise statements of the results.

(*b*) For $n = 0$ we may replace $\mathbb{F}_p$ by any finite field $\mathbb{F}_q$ of characteristic p, provided that $\exp(2\pi ix/p)$ is replaced by some non-trivial additive character of $\mathbb{F}_q$. The same limit theorems are obtained with q in place of p, provided $p \to \infty$ with q.

REFERENCES

[1] P. Deligne. La conjecture de Weil – I. *I.H.E.S. Publ. Math.* **43** (1974), 273–307.
[2] S. Lang and A. Weil. Number of points of varieties in finite fields. *Amer. J. Math.* **76** (1954), 819–827.
[3] R. W. K. Odoni. The statistics of Weil's trigonometric sums. *Math. Proc. Cambridge Philos. Soc.* **74** (1973), 467–471.
[4] R. W. K. Odoni. Trigonometric sums of Heilbronn's type, *Math. Proc. Cambridge Philos. Soc.* **98** (1985), 389–396.
[5] A. Weil. On some exponential sums. *Proc. Nat. Acad. Sci. U.S.A.* **34** (1948), 204–207.

https://doi.org/10.1017/S0305004100064100 Published online by Cambridge University Press