Uniform Distribution Theory **2** (2007), no.2, 67–72

uniform distribution theory

EXPONENTIAL SUMS WITH POLYNOMIAL VALUES OF THE DISCRETE LOGARITHM

William D. Banks — Igor E. Shparlinski

ABSTRACT. We estimate exponential sums of the form

$$\sum_{M+1\leqslant n\leqslant M+N} \exp\left(2\pi i\,\frac{f(\operatorname{ind} n)}{p-1}\right),$$

where f is a polynomial with integer coefficients, and $\operatorname{ind} n$ is the discrete logarithm of n modulo an odd prime p and a primitive root g. We apply this estimate to show that the values $\operatorname{ind} n, \ldots, (\operatorname{ind} n)^m$, $M+1 \leqslant n \leqslant M+N$, are uniformly and independently distributed modulo $p-1$.

Communicated by Sergei Konyagin

1. Introduction

For any positive integer k, we use the notation

$$\mathbf{e}_k(z) = \exp(2\pi i z/k) \qquad (z \in \mathbb{R}).$$

Let $p \geqslant 3$ be a fixed prime and g a *primitive root* modulo p. For every integer n coprime to p we denote by $\operatorname{ind} n$ its *discrete logarithm* or *index relative to* g; by definition this is the least non-negative integer u such that $g^u \equiv n \pmod p$.

Let χ be the multiplicative character modulo p given by

$$\chi(n) = \begin{cases} \mathbf{e}_{p-1}(\operatorname{ind} n) & p \nmid n; \\ 0 & p \mid n. \end{cases}$$

The study of multiplicative character sums of the form

$$\sum_{n=M+1}^{M+N} \chi(f(n)) = \sum_{\substack{n=M+1 \\ p\nmid f(n)}}^{M+N} \mathbf{e}_{p-1}(\operatorname{ind} f(n))$$

2000 Mathematics Subject Classification: 11K31, 11K38, 11L07.
Keywords: Discrete logarithm, primitive root, index, uniform distribution.

with a polynomial $f \in \mathbb{Z}[X]$ has had a long and glorious history and has produced many spectacular applications; see, for example, [3, 4]. In the present note, we consider typographically similar sums in which the functions f and ind are composed in the opposite order; that is, we study sums of the form

$$S(M,N,f) = \sum_{\substack{n=M+1 \\ p \nmid n}}^{M+N} \mathbf{e}_{p-1}(f(\operatorname{ind} n)).$$

These sums appear to be new, and their treatment requires a different set of techniques from those used to bound sums with multiplicative characters. We use our bounds on the sums $S(M,N,f)$ (see Theorem 1) to estimate the uniformity of distribution within the m-dimensional unit cube of vectors of fractional parts

$$\left(\left\{ \frac{\operatorname{ind} n}{p-1} \right\}, \ldots, \left\{ \frac{(\operatorname{ind} n)^m}{p-1} \right\} \right) \qquad (M+1 \leqslant n \leqslant M+N), \tag{1}$$

where $0 \leqslant M < N+M < p$ (see Theorem 2).

Throughout the paper, any constants implied by the symbols O or $\ll$ may depend (where obvious) on the degree m of the polynomial $f \in \mathbb{Z}[X]$ but are absolute otherwise. We recall that for functions F and $G \geqslant 0$ the notations $F \ll G$ and $F = O(G)$ mean that the inequality $|F| \leqslant cG$ holds with some constant $c > 0$.

2. Exponential sums

Following a standard approach we begin by estimating complete sums of the form

$$T(a,f) = \sum_{n=1}^{p-1} \mathbf{e}_{p-1}(f(\operatorname{ind} n))\, \mathbf{e}_p(an) \qquad (a \in \mathbb{Z}),$$

where f is a nonzero polynomial in $\mathbb{Z}[X]$ with constant term zero. Using the change of variables $u = \operatorname{ind} n$ we see that

$$T(a,f) = \sum_{u=0}^{p-2} \mathbf{e}_{p-1}(f(u))\, \mathbf{e}_p(ag^u).$$

In the case that $p \mid a$ we have the following bound of Hua (see [5]):

$$T(a,f) = T(0,f) = \sum_{u=0}^{p-2} \mathbf{e}_{p-1}(f(u)) \ll p^{1-1/m} d^{1/m}, \tag{2}$$

where m is the degree of f, and d is the largest integer that divides $p-1$ and all of the coefficients of f.

We now use an adaptation of the *Weyl method* (see [3, Section 8.2]) to estimate the sums $T(a,f)$ in the case that $p \nmid a$. We remark that a similar method has been used in [6] to bound related (but different) exponential sums.

Lemma 1. Uniformly for all integers a not divisible by p we have

$$T(a,f) \ll p^{1-2^{-m}}.$$

P r o o f. Write

$$f(X) = A_m X^m + \cdots + A_1 X$$

with $A_m \neq 0$. We prove the result by induction on the degree m.

If $m=1$ and $f(X) = AX$, then using classical results on Gauss sums it is easy to see that

$$\left|T(a,f)\right| = \left|\sum_{n=1}^{p-1} \mathbf{e}_{p-1}(A \operatorname{ind} n)\, \mathbf{e}_p(an)\right| = \begin{cases} p^{1/2} & \text{if } A \not\equiv 0 \pmod{p-1}; \\ 1 & \text{if } A \equiv 0 \pmod{p-1}. \end{cases}$$

For example, one can apply [1, Chapter 9, equations (2) and (5)] and the fact that $\chi(n) = \mathbf{e}_{p-1}(A \operatorname{ind} n)$ is a primitive character modulo p when $(p-1) \nmid A$ and $p \nmid a$.

For a polynomial $f \in \mathbb{Z}[X]$ of degree $m \geqslant 2$ we have

$$\begin{aligned} \left|T(a,f)\right|^2 &= \left|\sum_{u=0}^{p-2} \mathbf{e}_{p-1}(f(u))\, \mathbf{e}_p\left(ag^u\right)\right|^2 \\ &= \sum_{u,v=0}^{p-2} \mathbf{e}_{p-1}(f(u)-f(v))\, \mathbf{e}_p\left(ag^u - ag^v\right). \end{aligned}$$

Writing $v = u + w$ we obtain that

$$\begin{aligned} \left|T(a,f)\right|^2 &= \sum_{u,w=0}^{p-2} \mathbf{e}_{p-1}(f(u)-f(u+w))\, \mathbf{e}_p(ag^u(1-g^w)) \\ &\leqslant \sum_{w=0}^{p-2} \left|\sum_{u=0}^{p-2} \mathbf{e}_{p-1}(f(u)-f(u+w))\, \mathbf{e}_p(ag^u(1-g^w))\right|. \end{aligned}$$

For $w=0$ we estimate the inner sum trivially as p. For $w \neq 0$ we note that $g_w(X) = f(X) - f(X+w)$ is a polynomial of degree at most $m-1$, and since $a(1-g^w) \not\equiv 0 \pmod{p}$ the induction hypothesis applies; thus, we have

$$|T(a,f)|^2 \ll p + p \cdot p^{1-2^{-(m-1)}} \ll \left(p^{1-2^{-m}}\right)^2,$$

which yields the desired result. □

Our main result is the following:

THEOREM 1. Let M, N be integers with $0 \leqslant M < N + M < p$, and let

$$f(X) = A_m X^m + \cdots + A_1 X \in \mathbb{Z}[X]$$

with

$$\gcd(A_1, \ldots, A_m, p-1) = d.$$

Then the following uniform bound holds:

$$S(M,N,f) \ll N p^{-1/m} d^{1/m} + p^{1-2^{-m}} \log p.$$

Proof. Using the identity

$$\frac{1}{p} \sum_{|a| \leqslant (p-1)/2} \mathbf{e}_p(av) = \begin{cases} 1 & \text{if } v \equiv 0 \pmod p; \\ 0 & \text{if } v \not\equiv 0 \pmod p, \end{cases}$$

we have

$$\begin{aligned} S(M,N,f) &= \sum_{n=M+1}^{M+N} \mathbf{e}_{p-1}(f(\operatorname{ind} n)) \\ &= \sum_{n=1}^{p-1} \mathbf{e}_{p-1}(f(\operatorname{ind} n)) \sum_{k=M+1}^{M+N} \frac{1}{p} \sum_{|a| \leqslant (p-1)/2} \mathbf{e}_p(a(n-k)) \\ &= \frac{1}{p} \sum_{|a| \leqslant (p-1)/2} T(a,f) \sum_{k=M+1}^{M+N} \mathbf{e}_p(-ak) \\ &= \frac{N}{p} T(0,f) + \frac{1}{p} \sum_{\substack{|a| \leqslant (p-1)/2 \\ a \neq 0}} T(a,f) \sum_{k=M+1}^{M+N} \mathbf{e}_p(-ak). \end{aligned}$$

Using (2), Lemma 1, and the bound

$$\left| \sum_{k=M+1}^{M+N} \mathbf{e}_p(-ak) \right| \ll \min\{N, p/|a|\},$$

which holds for any integer a with $1 \leqslant |a| \leqslant (p-1)/2$ (see [3, Bound (8.6)]), the result follows after a straightforward calculation. □

3. Discrepancy

For any sequence Γ of N points in the m-dimensional unit cube $[0,1)^m$, the *discrepancy* of Γ is the quantity

$$\Delta_\Gamma = \sup_{B \subseteq [0,1)^m} \bigl| V_\Gamma(B) - N|B| \bigr|,$$

where $V_\Gamma(B)$ is the number of points of Γ in the polyhedron

$$B = [\alpha_1, \beta_1) \times \cdots \times [\alpha_m, \beta_m) \subseteq [0,1)^m,$$

$|B|$ is the Lebesgue measure of B, and the supremum is taken over all such polyhedra.

The link between the discrepancy and exponential sums is given by the celebrated *Koksma–Szüsz inequality*; see [2, Theorem 1.21]. We state the inequality here in the following form:

Lemma 2. There exists an absolute constant $C > 0$ such that, for any integer $L > 1$ and any sequence

$$\Gamma = \bigl((\gamma_{1,k}, \dots, \gamma_{m,k})\bigr)_{k=1}^N$$

of N points in the m-dimensional unit cube, the following bound holds:

$$\Delta_\Gamma \ll \frac{N}{L} + \sum_{0 < |A_1| + \cdots + |A_m| \leqslant L} \bigl|\widehat{S}_{A_1,\dots,A_m}(\Gamma)\bigr| \prod_{j=1}^m \frac{1}{\max\{1, |A_j|\}},$$

where

$$\widehat{S}_{A_1,\dots,A_m}(\Gamma) = \sum_{k=1}^N \exp(2\pi i (A_1\gamma_{1,k} + \cdots + A_m\gamma_{m,k})).$$

Theorem 2. Let M, N be integers with $0 \leqslant M < N + M < p$, and let $D(M,N)$ be the discrepancy of the sequence Γ defined by (1). Then,

$$D(M,N) \ll p^{1-2^{-m}} (\log p)^{m+1}.$$

Proof. Put $L = \lfloor p^{1/2} \rfloor$. Clearly, if

$$0 < |A_1| + \cdots + |A_m| \leqslant L,$$

then $\gcd(A_1, \dots, A_m, p-1) \leqslant p^{1/2}$. Also, $\widehat{S}_{A_1,\dots,A_m}(\Gamma) = S(M,N,f)$, where $f(X) = A_m X^m + \cdots + A_1 X$. Hence, by Theorem 1 we have the bound

$$\widehat{S}_{A_1,\dots,A_m}(\Gamma) \ll N p^{-1/(2m)} + p^{1-2^{-m}} \log p.$$

Taking into account the bound

$$\sum_{0<|A_1|+\cdots+|A_m|\leqslant L} \prod_{j=1}^{m} \frac{1}{\max\{1,|A_j|\}} \leqslant \left(\sum_{|A|\leqslant L} \frac{1}{\max\{1,|A|\}} \right)^m \ll (\log p)^m,$$

Lemma 2 immediately implies that

$$D(M,N) \ll Np^{-1/2} + \Big(Np^{-1/(2m)} + p^{1-2^{-m}} \log p \Big) (\log p)^m.$$

Since $2m \leqslant 2^m$ for all $m \geqslant 1$, we obtain the desired result. □

REFERENCES

[1] DAVENPORT, H.: *Multiplicative Number Theory*, Second edition, Graduate Texts in Mathematics, **74**, Springer-Verlag, New York-Berlin, 1980.
[2] DRMOTA, M. – TICHY, R.F.: *Sequences, Discrepancies and Applications*, Lecture Notes in Mathematics **1651**, Springer-Verlag, Berlin, Heidelberg, 1997.
[3] IWANIEC, H. – KOWALSKI, E.: *Analytic Number Theory*, Amer. Math. Soc., Providence, RI, 2004.
[4] LIDL, R. – NIEDERREITER, H.: *Finite Fields*, Cambridge University Press, Cambridge, 1997.
[5] STEČKIN, S.B.: *An estimate of a complete rational exponential sum*, Proc. Math. Inst. Acad. Sci. USSR, Moscow, **143** (1977), 188–207 (in Russian).
[6] YU, H.B.: *On two problems of Mordell about exponential sums*, Acta Arith. **86** (1998), 149–154.

Received August 7, 2007
Accepted October 29, 2007

William D. Banks
Department of Mathematics
University of Missouri
Columbia, MO 65211
USA
E-mail: bbanks@math.missouri.edu

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109
AUSTRALIA
E-mail: igor@ics.mq.edu.au