I. E. SHPARLINSKI
KODAI MATH. J.
32 (2009), 172–177

ON THE DISTRIBUTION OF ARGUMENTS OF GAUSS SUMS

Igor E. Shparlinski

Abstract

Let $\mathbf{F}_q$ be a finite field of q elements of characteristic p. N. M. Katz and Z. Zheng have shown the uniformity of distribution of the arguments $\arg G(a,\chi)$ of all $(q-1)(q-2)$ nontrivial Gauss sums

$$G(a,\chi) = \sum_{x \in \mathbf{F}_q} \chi(x) \exp(2\pi i \operatorname{Tr}(ax)/p),$$

where χ is a non-principal multiplicative character of the multiplicative group $\mathbf{F}_q^*$ and $\operatorname{Tr}(z)$ is the trace of $z \in \mathbf{F}_q$ into $\mathbf{F}_p$.

Here we obtain a similar result for the set of arguments $\arg G(a,\chi)$ when a and χ run through arbitrary (but sufficiently large) subsets $\mathscr{A}$ and $\mathscr{X}$ of $\mathbf{F}_q^*$ and the set of all multiplicative characters of $\mathbf{F}_q^*$, respectively.

1. Introduction

Let $\mathbf{F}_q$ be a finite field of q elements and let $\mathbf{F}_q^*$ be the multiplicative group $\mathbf{F}_q$.

For $a \in \mathbf{F}_q^*$ and a non-principal multiplicative character χ of the multiplicative group $\mathbf{F}_q^*$, we consider the Gauss sums

$$G(a,\chi) = \sum_{x \in \mathbf{F}_q} \chi(x) \exp(2\pi i \operatorname{Tr}(ax)/p),$$

where $\operatorname{Tr}(z)$ is the trace of $z \in \mathbf{F}_q$ into $\mathbf{F}_p$, we refer to [3, Chapter 3] for a background on characters and Gauss sums.

Since $|G(a,\chi)| = q^{1/2}$, we can define its argument $\arg G(a,\chi)$ by the relation

$$G(a,\chi) = e^{i \arg G(a,\chi)} q^{1/2}.$$

N. M. Katz and Z. Zheng [4] have shown that if χ runs through all multiplicative characters of $\mathbf{F}_q^*$ and a runs through all elements of $\mathbf{F}_q^*$, then the ratio $\arg G(a,\chi)/2\pi$ is asymptotically uniformly distributed in $[0,1]$, see also [3, Theorem 21.6].

2000 Mathematics Subject Classification: 11K38, 11L07, 11T24.
Received October 24, 2007; revised September 11, 2008.

Here we obtain a similar result for the set of arguments $\arg G(a,\chi)$ when a and χ run through arbitrary (but sufficiently large) subsets $\mathscr{A}$ and $\mathscr{X}$ of $\mathbf{F}_q^*$ and of the set of all multiplicative characters of $\mathbf{F}_q^*$, respectively. Namely, our result is nontrivial if

$$\#\mathscr{A}\#\mathscr{X} \ge q^{1+\varepsilon} \tag{1}$$

for some fixed $\varepsilon > 0$ provided that q is large enough. We also show that this condition is tight and for any field $\mathbf{F}_q$ with and odd q there are corresponding sets $\mathscr{A}$ and $\mathscr{X}$ with

$$\#\mathscr{A}\#\mathscr{X} = (q-1)/2$$

for which $\arg G(a,\chi)$ for all $a \in \mathscr{A}$ and $\chi \in \mathscr{X}$ is constant and thus is not uniformly distributed.

Throughout the paper, the implied constants in the symbols 'O', and '$\ll$' are absolute. We recall that the notations $U = O(V)$ and $V \ll U$ are both equivalent to the assertion that the inequality $|U| \le cV$ holds for some constant $c > 0$.

2. Discrepancy

To formulate and prove our main result we need to use some notions and facts from the theory of uniform distribution.

For a sequence of N real numbers $\gamma_1, \dots, \gamma_N \in [0,1)$ the *discrepancy* is defined by

$$\Delta = \max_{0 \le \gamma \le 1} |T(\gamma, N) - \gamma N|,$$

where $T(\gamma, N)$ is the number of $n \le N$ such that $\gamma_n \le \gamma$, see [1, 5].

We recall that a sequence $\gamma_1, \dots, \gamma_N \in [0,1)$ is called *uniformly distributed* if for its the discrepancy satisfies $\Delta = o(N)$.

The most common way of estimating the discrepancy is via the following *Erdős–Turán inequality* (see [1, 5]), which links the discrepancy with exponential sums.

Lemma 1. *For any integer $H \ge 1$, the discrepancy Δ of a sequence of N real numbers $\gamma_1, \dots, \gamma_N \in [0,1)$ satisfies the inequality*

$$\Delta \ll \frac{N}{H} + \sum_{h=1}^{H} \frac{1}{h} \left| \sum_{n=1}^{N} \exp(2\pi i h \gamma_n) \right|.$$

3. Incomplete power moments of Gauss sums

Lemma 2. *Let $\mathscr{A} \subseteq \mathbf{F}_q^*$ and let $\mathscr{X}$ be a set of nonprincipal multiplicative characters of $\mathbf{F}_q^*$. For any integer $h \ge 1$, we have*

$$\sum_{a\in\mathscr{A}}\sum_{\chi\in\mathscr{X}} G(a,\chi)^h \le q^{(h+1)/2}\sqrt{d\#\mathscr{A}\#\mathscr{X}},$$

where $d = \gcd(h, q-1)$.

Proof. As in [4], we recall that

$$G(a,\chi) = \bar{\chi}(a)G(1,\chi), \tag{2}$$

where $\bar{\chi}(a)$ is the complex conjugate character, see [3, Lemma 3.2]. Therefore,

$$\sum_{a\in\mathscr{A}}\sum_{\chi\in\mathscr{X}} G(a,\chi)^h \ll \sum_{\chi\in\mathscr{X}} |G(\chi,1)|^h \left|\sum_{a\in\mathscr{A}} \bar{\chi}(a)^h\right| = q^{h/2}W_h, \tag{3}$$

where

$$W_h = \sum_{\chi\in\mathscr{X}}\left|\sum_{a\in\mathscr{A}} \bar{\chi}(a)^h\right|.$$

By the Cauchy inequality we obtain

$$W_h^2 \le \#\mathscr{X}\sum_{\chi\in\mathscr{X}}\left|\sum_{a\in\mathscr{A}} \bar{\chi}(a)^h\right|^2. \tag{4}$$

Let ϑ be a primitive root of $\mathbf{F}_q$. For $a \in \mathbf{F}_q^*$ we define $\operatorname{ind} a$ by the relations

$$a = \vartheta^{\operatorname{ind} a} \quad \text{and} \quad 0 \le \operatorname{ind} a \le q-2.$$

Then for every integer $s = 0, \ldots, q-2$, the function

$$\chi_s(a) = \exp(2\pi i s \operatorname{ind} a/(q-1))$$

is a multiplicative character of $\mathbf{F}_q^*$, and every character can be represented in such a way (where $s = 0$ corresponds to the principal character χ_0). Thus, extending the summation in (4) over all multiplicative characters (including the principal character), we derive

$$\begin{aligned} W_h^2 &\le \#\mathscr{X}\sum_{s=0}^{q-2}\left|\sum_{a\in\mathscr{A}} \exp(2\pi i h s \operatorname{ind} a/(q-1))\right|^2 \\ &= \#\mathscr{X}\sum_{s=0}^{q-2}\sum_{a,b\in\mathscr{A}} \exp(2\pi i h s(\operatorname{ind} a - \operatorname{ind} b)/(q-1)) \\ &= \#\mathscr{X}\sum_{a,b\in\mathscr{A}}\sum_{s=0}^{q-2} \exp(2\pi i h s(\operatorname{ind} a - \operatorname{ind} b)/(q-1)). \end{aligned}$$

Clearly the inner sum vanishes unless

$$h(\operatorname{ind} a - \operatorname{ind} b) \equiv 0 \pmod{q-1}, \tag{5}$$

in which case it is equal to $q-1$. Clearly, the congruence (5) is equivalent to $\operatorname{ind} a \equiv \operatorname{ind} b \pmod{(q-1)/d}$. For every $b \in \mathscr{A}$ we see that $\operatorname{ind} a$ is uniquely defined modulo $(q-1)/d$ and thus belongs to at most d residue classes modulo $q-1$, after which a is uniquely defined. Thus (5) has at most $d\#\mathscr{A}$ solutions in $a, b \in \mathscr{A}$. Therefore $W_h^2 \le d(q-1)\#\mathscr{A}\#\mathscr{X}$. Recalling (3), we conclude the proof. □

4. Main result

THEOREM 3. *Let $\mathscr{A} \subseteq \mathbf{F}_q^*$ and let $\mathscr{X}$ be a set of nonprincipal multiplicative characters of $\mathbf{F}_q^*$. For the discrepancy $\Delta(\mathscr{A}, \mathscr{X})$ of the set*

$$\left\{\frac{\arg G(a,\chi)}{2\pi} : a \in \mathscr{A}, \chi \in \mathscr{X}\right\}$$

we have the following bound:

$$\Delta(\mathscr{A}, \mathscr{X}) \le \sqrt{\#\mathscr{A}\#\mathscr{X}}\, q^{1/2+o(1)}.$$

Proof. Using Lemma 1 we see that for every integer $H \ge 1$

$$\begin{aligned}\Delta(\mathscr{A}, \mathscr{X}) &\ll \frac{\#\mathscr{A}\#\mathscr{X}}{H} + \sum_{h=1}^{H} \frac{1}{h} \left| \sum_{a \in \mathscr{A}} \sum_{\chi \in \mathscr{X}} \exp(ih \arg G(a,\chi)) \right| \\ &= \frac{\#\mathscr{A}\#\mathscr{X}}{H} + \sum_{h=1}^{H} \frac{1}{hq^{h/2}} \left| \sum_{a \in \mathscr{A}} \sum_{\chi \in \mathscr{X}} G(a,\chi)^h \right|.\end{aligned}$$

Applying the bound of Lemma 2 we obtain

$$\begin{aligned}\Delta(\mathscr{A}, \mathscr{X}) &\ll \frac{\#\mathscr{A}\#\mathscr{X}}{H} + \sqrt{q\#\mathscr{A}\#\mathscr{X}} \sum_{h=1}^{H} \frac{\sqrt{\gcd(h, q-1)}}{h} \\ &\le \frac{\#\mathscr{A}\#\mathscr{X}}{H} + \sqrt{q\#\mathscr{A}\#\mathscr{X}} \sum_{d \mid q-1} d^{1/2} \sum_{\substack{h=1 \\ h \equiv 0 \pmod d}}^{H} \frac{1}{h} \\ &\le \frac{\#\mathscr{A}\#\mathscr{X}}{H} + \sqrt{q\#\mathscr{A}\#\mathscr{X}} \sum_{d \mid q-1} d^{1/2} \sum_{1 \le k \le H/d} \frac{1}{kd} \\ &\ll \frac{\#\mathscr{A}\#\mathscr{X}}{H} + \sqrt{q\#\mathscr{A}\#\mathscr{X}} \log H \sum_{d \mid q-1} d^{-1/2}.\end{aligned}$$

Taking $H = q$ and recalling that

$$\sum_{d \mid q-1} d^{-1/2} \le \sum_{d \mid q-1} 1 = q^{o(1)}$$

as $q \to \infty$, see [3, Bound (12.82)], we obtain

$$\Delta(\mathscr{A}, \mathscr{X}) \ll \#\mathscr{A}\#\mathscr{X}q^{-1} + \sqrt{\#\mathscr{A}\#\mathscr{X}}q^{1/2+o(1)}.$$

Clearly, $\#\mathscr{A}\#\mathscr{X}q^{-1} \le \sqrt{q\#\mathscr{A}\#\mathscr{X}}$, thus the first term can be discarded, which concludes the proof. □

5. Comments

Clearly the bound of Theorem 3 is nontrivial, that is, of the form $o(\#\mathscr{A}\#\mathscr{X})$, under the condition (1). Now, for an odd q, we take $\mathscr{A}$ to be the set of all quadratic residues of $\mathbf{F}_q$ and $\mathscr{X}$ to be the set consisting of just one quadratic character χ_2. Since $\overline{\chi_2}(a) = \chi_2(a) = 1$, we now see from (2) that $G(a, \chi_2)$ takes just one value. for all $a \in \mathscr{A}$. Hence in general (1) cannot be substantially relaxed. Certainly this is a somewhat pathological example as the set $\mathscr{X}$ consists of just one element. So one may ask whether it is possible to replace (1) with a weaker condition provided that both sets $\mathscr{A}$ and $\mathscr{X}$ are not too small, for example, under the additional assumption that

$$\#\mathscr{A} \ge q^{\varepsilon} \quad \text{and} \quad \#\mathscr{X} \ge q^{\varepsilon}$$

for some fixed $\varepsilon > 0$. We show that this is still impossible, and in fact for any $\varepsilon > 0$ there are infinitely many primes p for which there are sets $\mathscr{A}$ and $\mathscr{X}$ over $\mathbf{F}_p$ with

$$\#\mathscr{A} \ge p^{1/2-\varepsilon}, \quad \#\mathscr{X} \ge p^{1/2+\varepsilon/2} \quad \text{and} \quad \#\mathscr{A}\#\mathscr{X} \ge (p-1)/2$$

and such that either

$$\arg G(a, \chi) \in [0, 1/2], \quad a \in \mathscr{A}, \chi \in \mathscr{X},$$

or

$$\arg G(a, \chi) \in [1/2, 1], \quad a \in \mathscr{A}, \chi \in \mathscr{X}.$$

By a result of K. Ford [2, Theorem 7] there are infinitely many primes p such that $p-1$ has a divisor d with

$$p^{1/2-\varepsilon} \le d \le p^{1/2-2\varepsilon/3}$$

(in fact this holds for a set of primes of positive relative density). We take $\mathscr{A}$ to the set of all d elements $a \in \mathbf{F}_p$ of order d, that is, $a^d = 1$ for $a \in \mathscr{A}$. Since for any $a \in \mathscr{A}$ there is $b \in \mathbf{F}_p$ with $a = b^{(p-1)/d}$, the relation (2) implies that for any character χ of order $(p-1)/d$, that is, for any character with $\chi^{(p-1)/d} = \chi_0$, we have

$$G(a, \chi) = \bar{\chi}(a)G(1, \chi) = \bar{\chi}(b^{(p-1)/d})G(1, \chi) = \bar{\chi}(b)^{(p-1)/d}G(1, \chi) = G(1, \chi).$$

Let us separate the $(p-1)/d$ characters of order $(p-1)/d$ into two sets $\mathscr{X}_0$ and $\mathscr{X}_1$ depending whether $\arg G(1, \chi) \in [0, 1/2]$ or $\arg G(1, \chi) \in [1/2, 1]$. Taking $\mathscr{X}$ as the largest set out of $\mathscr{X}_0$ and $\mathscr{X}_1$ we have $\#\mathscr{X} \ge (p-1)/(2d)$ and the desired assertion follows (provided that p is large enough).

N. M. Katz and Z. Zheng [4] have also considered a similar question for the set of all Jacobi sums

$$J(\chi, \psi) = \sum_{x \in \mathbf{F}_q} \chi(x)\psi(1 - x),$$

where χ and ψ are nonprincipal multiplicative characters of $\mathbf{F}_q^*$ with $\psi \neq \bar{\chi}$ and shown that their arguments are uniformly distributed. It would be interesting to obtain an analogue of this result in the case where χ and ψ run through arbitrary sufficiently large sets of characters.

References

[1] M. Drmota and R. Tichy, Sequences, discrepancies and applications, Springer-Verlag, Berlin, 1997.

[2] K. Ford, The distribution of integers with a divisor in a given interval, Annals Math. **168** (2008), 367–433.

[3] H. Iwaniec and E. Kowalski, Analytic number theory, American Mathematical Society, Providence, RI, 2004.

[4] N. M. Katz and Z. Zheng, On the uniform distribution of Gauss sums and Jacobi sums, Analytic number theory, Allerton Park, 1995, Progress in mathematics **139**, Birkhäuser, Basel, 1996, 537–558.

[5] L. Kuipers and H. Niederreiter, Uniform distribution of sequences, Wiley-Interscience, New York-London-Sydney, 1974.

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