Journal de Théorie des Nombres
de Bordeaux **13** (2001), 53–63

Incomplete character sums and a special class of permutations

par S. D. COHEN, H. NIEDERREITER, I. E. SHPARLINSKI
et M. ZIEVE

Résumé. Nous donnons une méthode pour majorer des sommes incomplètes des valeurs d'un caractère d'un groupe abélien fini, en des éléments générés par une récurrence d'ordre 1. Cette méthode est particulièrement explicite lorsque la récurrence implique un type special de permutations, appelées $\mathcal{R}$-orthomorphismes. Nous donnons quelques exemples de ces $\mathcal{R}$-orthomorphismes.

Abstract. We present a method of bounding incomplete character sums for finite abelian groups with arguments produced by a first-order recursion. This method is particularly effective if the recursion involves a special type of permutation called an $\mathcal{R}$-orthomorphism. Examples of $\mathcal{R}$-orthomorphisms are given.

1. Introduction

Let G be a finite abelian group of order $m \geq 2$ and $\mathrm{Sym}(G)$ the group of permutations of G. For a fixed permutation $\psi \in \mathrm{Sym}(G)$ the sequence $u_0, u_1, \dots$ of elements of G is generated by the recursion

$$u_{n+1} = \psi(u_n) \quad \text{for } n = 0, 1, \dots , \tag{1}$$

where u_0 is a given initial value. This sequence is purely periodic with least period $t \leq m$. For $1 \leq N \leq t$ and a nontrivial character χ of G we consider the problem of finding nontrivial upper bounds for the absolute value of the character sum

$$\sum_{n=0}^{N-1} \chi(u_n). \tag{2}$$

This problem arises in applications such as pseudorandom number generation for simulation methods and for cryptography. In these applications the typical groups G are $\mathbf{Z}/M\mathbf{Z}$ – the additive group of residue classes mod M, $(\mathbf{Z}/M\mathbf{Z})^*$ – the multiplicative group of reduced residue classes mod M, $\mathbf{F}_q$

Manuscrit reçu le 1er novembre 1999.

– the additive group of the finite field of order q, and $\mathbb{F}_q^*$ – the multiplicative group of nonzero elements of $\mathbb{F}_q$, as well as their subgroups.

Until recently, nontrivial bounds for the character sum (2) have been known only in some very special cases. If we write the operation in G additively, then an easy case arises when $\psi(g) = g + a$ for all $g \in G$, where $a \in G$ is fixed. A less trivial case that has been treated before is $G = \mathbf{Z}/M\mathbf{Z}$ and $\psi(g) = ag$ for all $g \in G$, where $a \in (\mathbf{Z}/M\mathbf{Z})^*$ is fixed (see [4], [6, Section 8], [12, Section 9.2]). In 1998 Niederreiter and Shparlinski [7] invented a new method for the case where $G = \mathbb{F}_p$, p prime, and $\psi(g) = a\overline{g} + b$ for all $g \in G$, where $a \in \mathbb{F}_p^*$ and $b \in \mathbb{F}_p$ are fixed, $\overline{g}$ denotes the multiplicative inverse of g for $g \in \mathbb{F}_p^*$, and $\overline{0} = 0$ for the zero element $0 \in \mathbb{F}_p$. This method was later applied to related cases (see [3], [8], [9], [10]).

In the present paper we develop the method of [7] for bounding the character sum (2) in a general framework. The method is particularly effective if the permutation ψ in the recursion (1) is a so-called $\mathcal{R}$-orthomorphism. This special type of permutation is also of interest for other applications, such as to combinatorial design theory. We devote some attention to this special case, in particular to the construction of $\mathcal{R}$-orthomorphisms.

2. Bounds for incomplete character sums

The notation in the previous section remains in force and we introduce some further notation. Without loss of generality we write G additively. For a positive integer r we define the complete character sum

$$S_r(\chi, \psi) = \sum_{g \in G} \chi(\psi^r(g) - g). \tag{3}$$

If $\mathcal{K}$ is a finite nonempty set of integers, then $A_r(\mathcal{K})$ denotes the number of ordered pairs $(i, j) \in \mathcal{K}^2$ with $i - j = r$. Note that $A_r(\mathcal{K}) = 0$ for all sufficiently large r. Now we are ready to prove a bound for the incomplete character sum (2) in terms of the complete character sums (3).

Theorem 1. *Let G be a finite abelian group of order $m \geq 2$ and let $u_0, u_1, \ldots$ be the sequence generated by* (1) *with least period t. Then for any nontrivial character χ of G and for any finite nonempty set $\mathcal{K}$ of integers we have*

$$\left| \sum_{n=0}^{N-1} \chi(u_n) \right| \leq K^{-1/2} N^{1/2} m^{1/2} + \frac{\sqrt{2} N^{1/2}}{K} \left(\sum_{r=1}^{\infty} A_r(\mathcal{K}) |S_r(\chi, \psi)| \right)^{1/2} + \frac{2}{K} \sum_{k \in \mathcal{K}} |k| \quad \text{for } 1 \leq N \leq t,$$

where K is the cardinality of $\mathcal{K}$.

Proof. We use the abbreviation

$$S = \sum_{n=0}^{N-1} \chi(u_n).$$

From (1) we get $u_n = \psi^n(u_0)$ for all integers $n \geq 0$, and we use this identity to define u_n for all negative integers n. It is easy to see that for any integer k we have

$$\left| S - \sum_{n=0}^{N-1} \chi(u_{n+k}) \right| \leq 2|k|.$$

If we use this for all $k \in \mathcal{K}$, then we get

$$K|S| \leq W + 2 \sum_{k \in \mathcal{K}} |k|, \tag{4}$$

where

$$W = \sum_{n=0}^{N-1} \left| \sum_{k \in \mathcal{K}} \chi(u_{n+k}) \right| = \sum_{n=0}^{N-1} \left| \sum_{k \in \mathcal{K}} \chi(\psi^k(u_n)) \right|.$$

By the Cauchy–Schwarz inequality we obtain

$$\begin{aligned}
W^2 &\leq N \sum_{n=0}^{N-1} \left| \sum_{k \in \mathcal{K}} \chi\left(\psi^k(u_n)\right) \right|^2 \\
&\leq N \sum_{g \in G} \left| \sum_{k \in \mathcal{K}} \chi\left(\psi^k(g)\right) \right|^2 \\
&= N \sum_{g \in G} \sum_{i,j \in \mathcal{K}} \chi\left(\psi^i(g) - \psi^j(g)\right) \\
&\leq N \sum_{i,j \in \mathcal{K}} \left| \sum_{g \in G} \chi\left(\psi^i(g) - \psi^j(g)\right) \right| \\
&= KNm + 2N \sum_{\substack{i,j \in \mathcal{K} \\ i > j}} \left| \sum_{g \in G} \chi\left(\psi^i(g) - \psi^j(g)\right) \right|.
\end{aligned}$$

Since ψ^j is a permutation of G, the inner sum in the last expression is equal to the sum $S_{i-j}(\chi, \psi)$ in (3). Thus we get

$$W^2 \leq KNm + 2N \sum_{r=1}^{\infty} A_r(\mathcal{K}) |S_r(\chi, \psi)|,$$

and by appealing to (4) we arrive at the desired result. □

Corollary 1. *Let G be a finite abelian group of order $m \geq 2$ and let $u_0, u_1, \dots$ be the sequence generated by* (1) *with least period t. Then for any nontrivial character χ of G and any positive integer K we have*

$$\left|\sum_{n=0}^{N-1} \chi(u_n)\right| \leq K^{-1/2} N^{1/2} m^{1/2} + \frac{\sqrt{2} N^{1/2}}{K} \left(\sum_{r=1}^{K-1} (K-r)|S_r(\chi,\psi)|\right)^{1/2} + \frac{K}{2} \quad \text{for } 1 \leq N \leq t.$$

Proof. Apply Theorem 1 with

$$\mathcal{K} = \left\{k \in \mathbf{Z} : -\frac{K}{2} + 1 \leq k \leq \frac{K}{2}\right\}$$

if K is even and

$$\mathcal{K} = \left\{k \in \mathbf{Z} : -\frac{K-1}{2} \leq k \leq \frac{K-1}{2}\right\}$$

if K is odd. □

In various applications the complete character sums $S_r(\chi, \psi)$ can be bounded by known results, *e.g.* the Weil bound or the Bombieri-Weil bound. In such cases one obtains good bounds for the character sum (2) by optimizing the choice of $\mathcal{K}$ in Theorem 1 or the choice of K in Corollary 1 (see *e.g.* [7], [10]). A similar procedure, applied to subgroups G of the group of $\mathbb{F}_q$-rational points of an elliptic curve over $\mathbb{F}_q$, may yield results of interest for cryptology.

3. $\mathcal{R}$-orthomorphisms

A particularly favorable case arises in the bounds in Section 2 if the complete character sums $S_r(\chi, \psi)$ vanish. This happens, for instance, if the corresponding maps $\psi^r - \iota$ are permutations of G, where ι is the identity map on G. This observation suggests the following definition.

Definition 1. Let G be a finite abelian group and $\mathcal{R}$ a nonempty set of nonzero integers. Then a permutation ψ of G is called an *$\mathcal{R}$-orthomorphism* of G if $\psi^r - \iota \in \mathrm{Sym}(G)$ for all $r \in \mathcal{R}$.

In the case $\mathcal{R} = \{1\}$ we get the classical concept of an orthomorphism of G which is useful for the construction of orthogonal Latin squares (see [13, Chapter 22]). An application of orthomorphisms to cryptology appears in the work of Schnorr and Vaudenay [11]. Special types of $\mathcal{R}$-orthomorphisms with applications to combinatorial design theory arise in the recent paper of Dénes and Owens [2].

Since it is obvious that $\psi^r - \iota \in \mathrm{Sym}(G)$ if and only if $\psi^{-r} - \iota \in \mathrm{Sym}(G)$, it suffices to take $\mathcal{R}$ to be a nonempty set of positive integers. In fact, we can take

$$\mathcal{R} \subseteq \{1, 2, \ldots, \operatorname{ord}(\psi) - 1\} \subseteq \{1, 2, \ldots, e(G) - 1\},$$

where $\operatorname{ord}(\psi)$ is the order of ψ in $\operatorname{Sym}(G)$ and $e(G)$ is the exponent of $\operatorname{Sym}(G)$. It is also trivial that if $\mathcal{S}$ is a nonempty subset of $\mathcal{R}$ and ψ is an $\mathcal{R}$-orthomorphism of G, then ψ is an $\mathcal{S}$-orthomorphism of G.

The following result is an immediate consequence of Corollary 1 if ψ is a suitable $\mathcal{R}$-orthomorphism of G.

Corollary 2. *Let G be a finite abelian group of order $m \geq 2$ and for some integer $K \geq 2$ let ψ be an $\mathcal{R}$-orthomorphism of G with $\mathcal{R} = \{1, 2, \ldots, K-1\}$. Then for the sequence $u_0, u_1, \ldots$ generated by* (1) *with least period t and for any nontrivial character χ of G we have*

$$\left| \sum_{n=0}^{N-1} \chi(u_n) \right| \leq K^{-1/2} N^{1/2} m^{1/2} + \frac{K}{2} \quad \textit{for } 1 \leq N \leq t.$$

Corollary 3. *Let G be a finite abelian group of order $m \geq 2$ and let $u_0, u_1, \ldots$ be the sequence generated by* (1) *with least period t. Let the integer N with $1 \leq N \leq t$ be given and assume that the permutation ψ in* (1) *is an $\mathcal{R}$-orthomorphism of G with $\mathcal{R} = \{1, 2, \ldots, L-1\}$ for some integer $L \geq N^{1/3} m^{1/3}$. Then for any nontrivial character χ of G we have*

$$\left| \sum_{n=0}^{N-1} \chi(u_n) \right| \leq \frac{3}{2} N^{1/3} m^{1/3} + \frac{1}{2}.$$

Proof. Apply Corollary 2 with $K = \lceil N^{1/3} m^{1/3} \rceil$. □

We now show that some variation of our method produces a bound that is sometimes better than the result of Corollary 2.

Theorem 2. *Let G be a finite abelian group of order $m \geq 2$ and let $u_0, u_1, \ldots$ be the sequence generated by* (1) *with least period t. Let the integer N with $1 \leq N \leq t$ be given and assume that the permutation ψ in* (1) *is an $\mathcal{R}$-orthomorphism of G with $\mathcal{R} = \{1, 2, \ldots, K-1\}$ for some integer $K \geq 2$. Then for any nontrivial character χ of G we have*

$$\left| \sum_{n=0}^{N-1} \chi(u_n) \right| < K^{-1/2} t^{1/2} m^{1/2} \left(\frac{4}{\pi^2} \log t + 2 \right).$$

Proof. Let us consider the sums

$$\sigma_a = \sum_{n=0}^{t-1} \chi(u_n) \exp(2\pi i a n / t), \qquad a = 0, 1, \ldots, t-1.$$

We first show that

$$|\sigma_a| \le K^{-1/2} t^{1/2} m^{1/2}. \tag{5}$$

Fix a and note that for any integer $k \ge 0$ we have

$$\sigma_a = \sum_{n=0}^{t-1} \chi(u_{n+k}) \exp(2\pi i a(n+k)/t)$$

since the terms of the sum σ_a have period t. It follows that

$$\begin{aligned}
|\sigma_a| &= \frac{1}{K} \left| \sum_{n=0}^{t-1} \sum_{k=0}^{K-1} \chi(u_{n+k}) \exp(2\pi i a(n+k)/t) \right| \\
&\le \frac{1}{K} \sum_{n=0}^{t-1} \left| \sum_{k=0}^{K-1} \chi\left(\psi^k(u_n)\right) \exp(2\pi i a(n+k)/t) \right| \\
&= \frac{1}{K} \sum_{n=0}^{t-1} \left| \sum_{k=0}^{K-1} \chi\left(\psi^k(u_n)\right) \exp(2\pi i a k/t) \right|.
\end{aligned}$$

By the Cauchy–Schwarz inequality we obtain

$$\begin{aligned}
|\sigma_a|^2 &\le \frac{t}{K^2} \sum_{n=0}^{t-1} \left| \sum_{k=0}^{K-1} \chi\left(\psi^k(u_n)\right) \exp(2\pi i a k/t) \right|^2 \\
&\le \frac{t}{K^2} \sum_{g \in G} \left| \sum_{k=0}^{K-1} \chi\left(\psi^k(g)\right) \exp(2\pi i a k/t) \right|^2 \\
&= \frac{t}{K^2} \sum_{g \in G} \sum_{h,j=0}^{K-1} \chi\left(\psi^h(g) - \psi^j(g)\right) \exp(2\pi i a(h-j)/t) \\
&= \frac{t}{K^2} \sum_{h,j=0}^{K-1} \exp(2\pi i a(h-j)/t) \sum_{g \in G} \chi\left(\psi^h(g) - \psi^j(g)\right).
\end{aligned}$$

The inner sum is equal to m if $h = j$ and equal to 0 otherwise, and so (5) follows.

To bound the sum in the theorem, we use a standard method by starting from the identity

$$\sum_{n=0}^{N-1} \chi(u_n) = \sum_{n=0}^{t-1} \chi(u_n) \sum_{b=0}^{N-1} \frac{1}{t} \sum_{a=0}^{t-1} \exp(2\pi i a(n-b)/t),$$

which is valid since the sum over b is 1 for $0 \le n \le N-1$ and 0 for $N \le n \le t-1$. Rearranging terms, we get

$$\sum_{n=0}^{N-1} \chi(u_n) = \frac{1}{t} \sum_{a=0}^{t-1} \sigma_a \sum_{b=0}^{N-1} \exp(-2\pi i ab/t).$$

In view of (5) this yields

$$\begin{aligned} \left| \sum_{n=0}^{N-1} \chi(u_n) \right| &\le K^{-1/2} t^{-1/2} m^{1/2} \sum_{a=0}^{t-1} \left| \sum_{b=0}^{N-1} \exp(2\pi i ab/t) \right| \\ &= K^{-1/2} t^{-1/2} m^{1/2} \left(N + \sum_{a=1}^{t-1} \left| \frac{\sin(\pi a N/t)}{\sin(\pi a/t)} \right| \right). \end{aligned}$$

By an inequality of Cochrane [1] we have

$$\sum_{a=1}^{t-1} \left| \frac{\sin(\pi a N/t)}{\sin(\pi a/t)} \right| < \frac{4}{\pi^2} t \log t + \frac{t}{2} + 1,$$

and so the result of the theorem follows. □

Remark 1. There is also an alternative method of improving the result of Corollary 3 if larger values of L are available, but not so large that Theorem 2 becomes efficient. The method is based on induction on the sum length N. Indeed, using the representation

$$\sum_{n=0}^{N-1} \chi(u_n) = \sum_{n=0}^{N-1} \chi(u_{n+k}) + \sum_{n=0}^{k-1} \chi(u_n) - \sum_{n=N}^{N+k-1} \chi(u_n)$$

for integers $k > 0$ (and analogously for $k < 0$), one can bound the last two sums inductively rather than trivially (as we have done in Theorem 1 and thus in Corollary 3).

4. Examples of $\mathcal{R}$-orthomorphisms

We present two classes of examples of $\mathcal{R}$-orthomorphisms for $G = \mathbb{F}_q$. The first class of examples is obtained from linear algebra.

Proposition 1. *Let ψ be a linear operator on the vector space $\mathbb{F}_q$ over its prime subfield $\mathbb{F}_p$ and let $\mathcal{R}$ be a nonempty set of positive integers. Then ψ is an $\mathcal{R}$-orthomorphism of $\mathbb{F}_q$ if and only if neither 0 nor an rth root of unity for some $r \in \mathcal{R}$ is an eigenvalue of ψ.*

Proof. This follows from the definition of an $\mathcal{R}$-orthomorphism and elementary linear algebra. □

Remark 2. To get a concrete example from Proposition 1, let ψ be such that its characteristic polynomial f is irreducible over $\mathbb{F}_p$, with $f(0) \ne 0$ if $q = p$. Let h be the order of f in the sense of [5, Definition 3.2], then all roots of f have order h in $\mathbb{F}_q^*$. It follows therefore from Proposition 1 that ψ is an $\mathcal{R}$-orthomorphism of $\mathbb{F}_q$ whenever $\mathcal{R}$ contains no multiple of h. For instance, if $q \geq 3$ and the characteristic polynomial of ψ is primitive over $\mathbb{F}_p$, so that $h = q-1$, then ψ is an $\mathcal{R}$-orthomorphism of $\mathbb{F}_q$ with $\mathcal{R} = \{1, 2, \dots, q-2\}$.

Remark 3. The last example in Remark 2 is best possible in the sense that if G is an arbitrary finite abelian group of order $m \geq 2$, then there are no $\mathcal{R}$-orthomorphisms of G with $\mathcal{R} = \{1, 2, \dots, m-1\}$. To see this, observe that an orthomorphism ψ of G has a (unique) fixed point, hence the length c of any other cycle of ψ satisfies $c \leq m-1$, and so ψ is not a $\{c\}$-orthomorphism of G. Similarly, if the sequence in (1) has least period $t \geq 2$, then the permutation ψ in (1) is not an $\mathcal{R}$-orthomorphism of G with $\mathcal{R} = \{1, 2, \dots, t\}$.

In the second class of examples we consider maps of the following form. Let $q \geq 5$ be odd and choose $a \in \mathbb{F}_q$ with $a \neq 0, \pm 1$. Then the self-map ψ_a of $\mathbb{F}_q$ is defined by

$$\psi_a(c) = c\left(c^{(q-1)/2} - a\right)^2 \quad \text{for } c \in \mathbb{F}_q. \tag{6}$$

By [5, Theorem 7.10] or by a simple direct argument (compare with the proof of Proposition 2 below), ψ_a is a permutation of $\mathbb{F}_q$.

Proposition 2. *Let the permutation ψ_a of $\mathbb{F}_q$ be as in* (6) *and let $\mathcal{R}$ be a nonempty set of positive integers. Then ψ_a is an $\mathcal{R}$-orthomorphism of $\mathbb{F}_q$ if and only if*

$$\eta\left(((a-1)^{2r} - 1)((a+1)^{2r} - 1)\right) = 1 \quad \textit{for all } r \in \mathcal{R},$$

where η is the quadratic character of $\mathbb{F}_q$.

Proof. Note that the map ψ_a in (6) can be described also by $\psi_a(c) = c(a-1)^2$ if c is a square in $\mathbb{F}_q$ and $\psi_a(c) = c(a+1)^2$ if c is a nonsquare in $\mathbb{F}_q$. We remark in passing that this shows that ψ_a is a permutation of $\mathbb{F}_q$. By straightforward induction it is seen that for any positive integer r we have $\psi_a^r(c) = c(a-1)^{2r}$ if c is a square in $\mathbb{F}_q$ and $\psi_a^r(c) = c(a+1)^{2r}$ if c is a nonsquare in $\mathbb{F}_q$. From this it follows immediately that $\psi_a^r - \iota \in \mathrm{Sym}(\mathbb{F}_q)$ if and only if

$$\eta\left(((a-1)^{2r} - 1)((a+1)^{2r} - 1)\right) = 1,$$

and this yields the result of the proposition. □

We now show a sufficient condition for the existence of $\mathcal{R}$-orthomorphisms of the form (6) for suitable sets $\mathcal{R}$.

Theorem 3. *Let q be odd and let $\mathcal{R}$ be a finite nonempty set of positive integers. Suppose that*

$$\frac{q-1}{2^R} - (q^{1/2}+1)\sum_{r\in\mathcal{R}}(2r-1) \geq 2,$$

where R is the cardinality of $\mathcal{R}$. Then there exists an $a \in \mathbb{F}_q$ such that the map ψ_a in (6) is an $\mathcal{R}$-orthomorphism of $\mathbb{F}_q$.

Proof. Let $L(\mathcal{R})$ denote the number of $a \in \mathbb{F}_q^*$ for which

$$\eta\left(((a-1)^{2r}-1)((a+1)^{2r}-1)\right) = 1 \quad \text{for all } r \in \mathcal{R}.$$

Furthermore, we put

$$d_r(x) = \frac{((x-1)^{2r}-1)((x+1)^{2r}-1)}{x^2} \in \mathbb{F}_q[x] \quad \text{for } r \in \mathcal{R}.$$

Then

$$L(\mathcal{R}) \geq \sum_{a\in\mathbb{F}_q^*}\prod_{r\in\mathcal{R}}\frac{1}{2}\left(1+\eta(d_r(a))\right) - \frac{A}{2}$$

with

$$A = \#\{a \in \mathbb{F}_q^* : \prod_{r\in\mathcal{R}} d_r(a) = 0\} \leq \sum_{r\in\mathcal{R}}(4r-2).$$

Therefore

$$L(\mathcal{R}) \geq \frac{1}{2^R}\sum_{a\in\mathbb{F}_q^*}\prod_{r\in\mathcal{R}}\left(1+\eta(d_r(a))\right) - \sum_{r\in\mathcal{R}}(2r-1). \tag{7}$$

Moreover,

$$\sum_{a\in\mathbb{F}_q^*}\prod_{r\in\mathcal{R}}(1+\eta(d_r(a))) = q-1+\sum_{k=1}^{R}\sum_{\substack{r_1<r_2<\ldots<r_k\\ r_i\in\mathcal{R}}}\sum_{a\in\mathbb{F}_q^*}\eta(d_{r_1}(a)\cdots d_{r_k}(a)). \tag{8}$$

Consider the innermost sum on the right-hand side of (8). If the polynomial $d_{r_1}\cdots d_{r_k}$ is the square of a polynomial, then the corresponding sum is clearly nonnegative. If $d_{r_1}\cdots d_{r_k}$ is not the square of a polynomial, then by the Weil bound (see [5, Theorem 5.41]) we obtain

$$\left|\sum_{a\in\mathbb{F}_q^*}\eta\left(d_{r_1}(a)\cdots d_{r_k}(a)\right)\right| < q^{1/2}\sum_{i=1}^{k}(4r_i-2).$$

Together with (8) this yields

$$\begin{aligned}\sum_{a\in\mathbb{F}_q^*}\prod_{r\in\mathcal{R}}(1+\eta(d_r(a))) &> q-1-q^{1/2}\sum_{k=1}^{R}\sum_{\substack{r_1<r_2<\ldots<r_k\\ r_i\in\mathcal{R}}}\sum_{i=1}^{k}(4r_i-2)\\ &= q-1-4q^{1/2}\sum_{k=1}^{R}\sum_{\substack{r_1<r_2<\ldots<r_k\\ r_i\in\mathcal{R}}}(r_1+\cdots+r_k)+2q^{1/2}\sum_{k=1}^{R}k\binom{R}{k}\\ &= q-1-2^{R+1}q^{1/2}\sum_{r\in\mathcal{R}}r+2^R Rq^{1/2}.\end{aligned}$$

Going back to (7), we get

$$L(\mathcal{R})>\frac{q-1}{2^R}-(q^{1/2}+1)\sum_{r\in\mathcal{R}}(2r-1).$$

By assumption, the last expression is at least 2, and so $L(\mathcal{R})\geq 3$. Hence there exists an $a\in\mathbb{F}_q^*$ with $a\neq\pm1$ that is counted by $L(\mathcal{R})$, which means by Proposition 2 that ψ_a is an $\mathcal{R}$-orthomorphism of $\mathbb{F}_q$. $\square$

Remark 4. For sets $\mathcal{R}$ of the form $\mathcal{R}=\{1,2,\ldots,K-1\}$ the condition on $\mathcal{R}$ in Theorem 3 is satisfied with some $K\sim 0.5\log_2 q$.

It would be desirable to find further examples, besides those in Remark 2, of $\mathcal{R}$-orthomorphisms of groups G with $\mathcal{R}=\{1,2,\ldots,K-1\}$ and K large relative to the order m of G. According to Remark 3 we must have $K\leq m-1$, so one may ask for K at least of the order of magnitude m^θ for some $0<\theta\leq 1$. Such examples are of interest not only in their own right, but also in view of the bounds for character sums in Section 3 and for applications to combinatorial design theory (see [2] for such applications).

References

[1] T. COCHRANE, *On a trigonometric inequality of Vinogradov.* J. Number Theory **27** (1987), 9–16.

[2] J. DÉNES, P.J. OWENS, *Some new Latin power sets not based on groups.* J. Combinatorial Theory Ser. A **85** (1999), 69–82.

[3] J. GUTIERREZ, H. NIEDERREITER, I.E. SHPARLINSKI, *On the multidimensional distribution of inversive congruential pseudorandom numbers in parts of the period.* Monatsh. Math. **129** (2000), 31–36.

[4] N.M. KOROBOV, *On the distribution of digits in periodic fractions.* Math. USSR Sbornik **18** (1972), 659–676.

[5] R. LIDL, H. NIEDERREITER, *Finite Fields.* Cambridge Univ. Press, Cambridge, 1997.

[6] H. NIEDERREITER, *Quasi-Monte Carlo methods and pseudo-random numbers.* Bull. Amer. Math. Soc. **84** (1978), 957–1041.

[7] H. NIEDERREITER, I.E. SHPARLINSKI, *On the distribution of inversive congruential pseudorandom numbers in parts of the period.* Math. Comp., to appear.

[8] H. NIEDERREITER, I.E. SHPARLINSKI, *On the distribution and lattice structure of nonlinear congruential pseudorandom numbers.* Finite Fields Appl. **5** (1999), 246–253.

[9] H. Niederreiter, I.E. Shparlinski, *Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus.* Acta Arith. **92** (2000), 89–98.

[10] H. Niederreiter, I.E. Shparlinski, *On the distribution of pseudorandom numbers and vectors generated by inversive methods.* Applicable Algebra Engrg. Comm. Comput. **10** (2000), 189–202.

[11] C.P. Schnorr, S. Vaudenay, *Black box cryptanalysis of hash networks based on multipermutations.* Advances in Cryptology – EUROCRYPT '94 (A. De Santis, ed.), Lecture Notes in Computer Science, Vol. **950**, pp. 47–57, Springer, Berlin, 1995.

[12] I.E. Shparlinski, *Finite Fields: Theory and Computation.* Kluwer Academic Publ., Dordrecht, 1999.

[13] J.H. van Lint, R.M. Wilson, *A Course in Combinatorics.* Cambridge Univ. Press, Cambridge, 1992.

S. D. Cohen
Department of Mathematics
University of Glasgow
University Gardens
Glasgow G12 8QW
Scotland
E-mail : sdc@maths.gla.ac.uk

H. Niederreiter
Department of Mathematics
National University of Singapore
2 Science Drive 2
Singapore 117543
Republic of Singapore
E-mail : nied@math.nus.edu.sg

I. E. Shparlinski
Department of Computing
Macquarie University
NSW 2109
Australia
E-mail : igor@comp.mq.edu.au

M. Zieve
Center for Communications Research
29 Thanet Road
Princeton, NJ 08540
USA
E-mail : zieve@idaccr.org