Cyclotomic $\mathscr{R}$-orthomorphisms and character sums

Jordan Bell

Ontario Combinatorics Workshop, Fields Institute, April 21–22, 2006

We define a recurrence sequence in a finite abelian group G by successively applying a permutation ψ of G to an initial element. We will give nontrivial upper bounds on the incomplete character sums of this sequence, for all nontrivial characters of G.

If ψ is an $\mathscr{R}$-orthomorphism of the additive group $\mathbb{F}_q$ (i.e. an elementary abelian group), we significantly improve these bounds. We finally give a construction of $\mathscr{R}$-orthomorphisms using cyclotomic mappings.

Bounds on incomplete character sums have applications in pseudorandom number generation and cryptography. Orthomorphisms have applications in the theory of finite projective planes, block ciphers in cryptography, and the construction of atomic Latin squares and Room squares. In particular, $\mathscr{R}$-orthomorphisms have applications in the construction of atomic Latin squares.

Let G be a finite abelian group of order $m \geq 2$. Let ψ be a permutation of G. For $u_0 \in G$, define a recurrence sequence $\{u_n\}$ by

$$u_{n+1} = \psi(u_n),$$

i.e.

$$u_n = \psi^n(u_0).$$

Clearly this sequence has least period $t \leq m$. Indeed, t is equal to the length of the cycle of ψ that contains u_0 in the decomposition of ψ into disjoint cycles.

For a nontrivial character χ of G, for all $1 \leq N \leq t$ we would like to give nontrivial upper bounds on the absolute value of the incomplete character sum $\sum_{n=0}^{N-1} \chi(u_n)$.

Let r be a positive integer. Define the complete character sum

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

For $\mathcal{K}$ a finite nonempty set of integers, define

$$A_r(\mathcal{K}) = \#\{(i, j) \in \mathcal{K}^2 : i - j = r\}.$$

Clearly $A_r(\mathcal{K}) = 0$ for all sufficiently large r. Set $K = |\mathcal{K}|$.

The following theorem is from Cohen, Niederreiter, Shparlinski and Zieve (2001):

Theorem 1 *Let G be a finite abelian group of order $m \geq 2$ and $\{u_n\}$ defined as above with least period t. Then for any nontrivial character χ of G and for any finite nonempty set $\mathcal{K}$ of integers, we have:*

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

$$\frac{\sqrt{2} N^{1/2}}{K} \left(\sum_{r=1}^{\infty} A_r(\mathcal{K}) |S_r(\chi, \psi)| \right)^{1/2} + \frac{2}{K} \sum_{k \in \mathcal{K}} |k|.$$

This is proved using the Cauchy-Schwarz inequality (and a lot of manipulation!).

Clearly if we add a fixed integer to the elements in $\mathcal{K}$, we only affect the last term above. Thus we can minimize the above sum by choosing $\mathcal{K} = \{k : -K/2 + 1 \leq k \leq K/2\}$ if K is even, and $\mathcal{K} = \{k : -(K-1)/2 \leq k \leq (K-1)/2$ if K is odd, to minimize the absolute values of the elements in $\mathcal{K}$. This makes the last term $K/2$.

Let χ be a nontrivial character of an abelian group G. Since χ is nontrivial, there exists a $\beta \in G$ such that $\chi(\beta) \neq 1$. Thus:

$$\begin{aligned} \chi(\beta) \sum_{g \in G} \chi(g) &= \sum_{g \in G} \chi(\beta)\chi(g) \\ &= \sum_{g \in G} \chi(\beta g) \\ &= \sum_{h \in G} \chi(h). \end{aligned}$$

Since $\chi(\beta) \neq 1$, thus $\sum_{g \in G} \chi(g) = 0$.

Thus if for each $r \leq K$ in the above theorem, $\psi^r(x) - x$ is a permutation, then the complete character sum $S_r(\chi, \psi) = 0$.

A permutation f of a group G is called an *orthomorphism* if $f(x) - x$ is also a permutation. For $\mathscr{R}$ a finite nonempty set of positive integers, if f^r is an orthomorphism for all $r \in \mathscr{R}$, then f is called an *$\mathscr{R}$-orthomorphism*.

Hence if for $\mathscr{R} = \{1, 2, \ldots, K-1\}$, ψ is an $\mathscr{R}$-orthomorphism, then the complete character sum $S_r(\chi, \psi) = 0$. Thus we have the following theorem from Cohen, Niederreiter, Shparlinski and Zieve (2001):

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 $\mathscr{R}$-orthomorphism of G for $\mathscr{R} = \{1, 2, \ldots, K-1\}$. Then for any sequence $\{u_n\}$ defined as before with least period t, and for any nontrivial character χ of G, for all $1 \leq N \leq t$ we have:*

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

The following is another upper bound of Cohen, Niederreiter, Shparlinski and Zieve (2001) that is sometimes better than the above corollary. It is proved using the Cauchy-Schwarz inequality and the result of Cochrane (1987) that

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

Theorem 3 *With the above definitions,*

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

We now give a construction for $\mathscr{R}$-orthomorphisms of (the additive group of) $\mathbb{F}_q$ by cyclotomic mappings of Niederreiter and Winterhof (2005).

Let $\gamma \in \mathbb{F}_q$ be primitive. For n a positive divisor of $q-1$, put

$$C_0 = \left\{ \gamma^{jn} : j = 0, 1, \ldots, \frac{q-1}{n} - 1 \right\},$$

and

$$C_i = \gamma^i C_0,$$

for $1 \leq i \leq n-1$. These are called the *cyclotomic cosets*, and partition $\mathbb{F}_q^*$.

Define $f_{a_0,a_1,\ldots,a_{n-1}}$ by

$$f_{a_0,a_1,\ldots,a_{n-1}}(x) = \begin{cases} a_i x, & x \in C_i, \\ 0, & x = 0. \end{cases}$$

This is called a *cyclotomic mapping*.

Let q be a prime power, $n > 1$ a divisor of $q-1$, $t \in \mathbb{F}_q^*$ and $\mathscr{R}$ a set of positive integers of cardinality $R \geq 1$. If

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

then there exists a $b \in \mathbb{F}_q \setminus \{0,-t\}$ such that $f_{(b+t)^n,b^n,\ldots,b^n}$ is an $\mathscr{R}$-orthomorphism of $\mathbb{F}_q$.

Finally, Cohen, Niederreiter, Shparlinski and Zieve (2001) also prove that if $q \geq 3$ is a power of a prime p and ψ is an $\mathbb{F}_p$-linear mapping of $\mathbb{F}_q$, if the characteristic polynomial of ψ is primitive over $\mathbb{F}_p$, then ψ is an $\mathscr{R}$-orthomorphism of $\mathbb{F}_q$ for $\mathscr{R} = \{1, 2, \ldots, q-2\}$.

Workshops, Ottawa, May 12-16

http://www.fields.utoronto.ca/programs/scientific/05-06/discrete_math/
http://www.fields.utoronto.ca/programs/scientific/05-06/covering_arrays/

- Ottawa-Carleton DISCRETE MATH DAY
- May 12-13 (Friday-Saturday)
- Plenary Speakers:
  Bill Cook, Anthony Evans, Jonathan Jedwab, Pierre Leroux, Kieka Mynhardt

- Workshop on COVERING ARRAYS
- May 14-16 (Sunday-Tuesday)
- Plenary Speakers:
  Rick Brewster, Charlie Colbourn, Peter Gibbons, Alan Hartman, Brett Stevens, Doug Stinson.

DEADLINE APRIL 26

- Student financial support to travel to Ottawa
- Submission of abstracts for contributed talks