Sequence families with low correlation derived from multiplicative and additive characters

Kai-Uwe Schmidt

17 September 2009 (revised 01 September 2010)

Abstract

For integer $r$ satisfying $0 \leq r \leq p - 2$, a sequence family $\Omega_r$ of polyphase sequences of prime period $p$, size $(p - 2)p^r$, and maximum correlation at most $2 + (r + 1)\sqrt{p}$ is presented. The sequence families are nested, that is, $\Omega_r$ is contained in $\Omega_{r+1}$, which provides design flexibility with respect to family size and maximum correlation. The sequences in $\Omega_r$ are derived from a combination of multiplicative and additive characters of a prime field. Estimates on hybrid character sums are then used to bound the maximum correlation. This construction generalizes $\Omega_0$, which was previously proposed by Scholtz and Welch. Sequence family $\Omega_2$ is closely related to a recent design by Wang and Gong, who bounded its maximum correlation using methods from representation theory and asked for a more direct proof of this bound. Such a proof is given here and an improvement of the bound is provided.

Keywords
Character sum, correlation, finite field, polyphase, sequence set

1 Introduction

We consider a sequence $s$ of period $n$ to be a mapping $s : \mathbb{Z} \to \mathbb{C}$ satisfying $s(k) = s(n + k)$ for each $k \in \mathbb{Z}$. We say that a sequence $s$ is a polyphase sequence with alphabet size $q$ if $s(k)$ is a $q$th root of unity for each $k \in \mathbb{Z}$. The periodic crosscorrelation at displacement $u \in \mathbb{Z}$ between sequences $s$ and $t$ of period $n$ is given by

$$C_{s,t}(u) := \sum_{k=0}^{n-1} s(k)\overline{t(k+u)},$$

and the periodic autocorrelation at displacement $u$ of the sequence $s$ is $C_s(u) := C_{s,s}(u)$.

Consider a collection of $M$ sequences

$$\mathcal{F} = \{s_i : 1 \leq i \leq M\},$$

Kai-Uwe Schmidt is with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC V5A 1S6, Canada. He is supported by Deutsche Forschungsgemeinschaft (German Research Foundation) under Research Fellowship SCHM 2609/1-1. Email: kuschmidt@sfu.ca.
where each \( s_i \) is a sequence of period \( n \). We say that \( \mathcal{F} \) is a sequence family of period \( n \). The size \( M \), the maximum autocorrelation

\[
\theta_A(\mathcal{F}) := \max \{|C_s(u)|: s \in \mathcal{F}, u \not\equiv 0 \pmod{n}\},
\]

and the maximum crosscorrelation

\[
\theta_C(\mathcal{F}) := \max \{|C_{s,t}(u)|: s, t \in \mathcal{F}, s \neq t, u \in \mathbb{Z}\}
\]

are key parameters of \( \mathcal{F} \) when \( \mathcal{F} \) is employed in a code-division multiple access (CDMA) system (for background see [HK98], for example). Large family size is required to support a large number of simultaneous users. Small autocorrelation \( \theta_A(\mathcal{F}) \) is required to ensure message synchronization, and small crosscorrelation \( \theta_C(\mathcal{F}) \) is required to minimize interference among different users.

Many authors do not distinguish between autocorrelations and crosscorrelations and define \( \theta(\mathcal{F}) := \max\{\theta_A(\mathcal{F}), \theta_C(\mathcal{F})\} \) as the maximum correlation of \( \mathcal{F} \). A useful benchmark for \( \mathcal{F} \) is given by the famous Welch bound [Wel74], which asserts

\[
\theta(\mathcal{F}) \geq n \sqrt{\frac{M - 1}{Mn - 1}}, \tag{1}
\]

provided that \( \sum_{k=0}^{n-1}|s_i(k)|^2 = n \) for each \( i = 1, 2, \ldots, M \) (which is satisfied for polyphase sequences). When \( M \) and \( n \) both tend to infinity, the bound (1) asserts that \( \theta(\mathcal{F}) \) must grow at least like \( \sqrt{n} \).

There exist many designs of sequence families that meet this asymptotic bound with equality; a good overview is given in [HK98]. It appears however that the size of such sequence families is limited by approximately the period of the sequence family. This motivates the construction of sequence families that allow a tradeoff between size and maximum correlation.

A reference design that provides such a tradeoff was proposed by Kumar, Helleseth, and Calderbank [KHC95]. Given a prime \( p \) and positive integers \( e \) and \( m \), [KHC95] constructs a family of polyphase sequences with alphabet size \( p^e \) having period \( p^m - 1 \), size at least \( p^m (r+1) \), and maximum correlation at most \( 1 + (r+1)\sqrt{p^m} \), where \( r \) is an integer satisfying \( 0 \leq r < p^e - 2 \). When \( e = 1 \), this sequence family was discovered much earlier by Sidelnikov [Sid71, Thm. 3]. The construction is based on evaluating additive characters of polynomials over a Galois ring (or over a Galois field if \( e = 1 \)). A bound on character sums involving polynomial arguments is then used to estimate the maximum correlation.

The contribution of this paper is a construction of a sequence family \( \Omega^*_r \) of prime period \( p \), size \( (p-2)p^r \), and maximum correlation at most \( (r+1)\sqrt{p} \), where \( r \) is an integer satisfying \( 0 \leq r \leq p-2 \). The sequences in \( \Omega^*_r \) take on values that are \( p(p-1) \)th roots of unity except for one element per period, which is zero. By changing these zeros to ones, we obtain a new sequence family \( \Omega_r \), which now has maximum correlation at most \( 2 + (r+1)\sqrt{p} \) and comprises polyphase sequences whose alphabet size is \( p-1 \) for \( r = 0 \) and \( p(p-1) \) for \( r > 0 \). The sequences in \( \Omega^*_r \) are derived from multiplicative and additive characters of polynomials over a prime field. Bounds on the magnitude of hybrid character sums with polynomial arguments are then used to estimate the maximum correlation.

Sequence family \( \Omega^*_r \) generalizes \( \Omega^*_0 \), which was previously proposed by Scholtz and Welch [SW78]. The related sequence family \( \Omega_0 \) was also studied by Kim et al. [KSGC06]. In view of (1), the maximum correlation of \( \Omega_0 \) and \( \Omega^*_0 \) is asymptotically best possible. Sequence family \( \Omega^*_2 \) was recently
constructed by Wang and Gong [WG, Construction A] following earlier work by Gurevich, Hadani, and Sochen [GHS08]. Using methods from representation theory, the authors obtained the bound
\[ \theta(\Omega^*_2) \leq 4\sqrt{p}, \]
and asked for a more direct proof of this fact. Such a proof is provided here along with the improvement \( \theta(\Omega^*_2) \leq 3\sqrt{p} \). Wang and Gong also proved further properties of \( \Omega^*_2 \), such as low magnitude of the Fourier transform and bounded ambiguity function of the sequences in \( \Omega^*_2 \). These properties can also be proved and improved similarly to the proof of the main result of this paper. Indeed, it is also possible to obtain corresponding bounds for \( \Omega^*_r \) in general.

2 Characters and Character Sums

Given a group \( G \), a \textit{character} is a group homomorphism from \( G \) to the complex numbers. Let \( p \) be a prime, let \( \mathbb{F}_p \) be the finite field containing \( p \) elements, and write \( \mathbb{F}_p^* := \mathbb{F}_p \setminus \{0\} \). Whenever convenient, we treat integers after reduction modulo \( p \) as elements in \( \mathbb{F}_p \). We are interested in characters defined on the additive group \((\mathbb{F}_p, +)\) and on the multiplicative group \((\mathbb{F}_p^*, \cdot)\).

For positive integer \( n \) write
\[ e_n(x) := e^{\sqrt{-1}2\pi x/n}. \]
Given \( b \in \mathbb{F}_p \), the mapping \( \psi_b : \mathbb{F}_p \to \mathbb{C} \), defined by
\[ \psi_b(x) = e_p(bx), \]
is called an \textit{additive character} of \( \mathbb{F}_p \). For \( b = 0 \), the character \( \psi_b \) is called \textit{trivial}, otherwise it is called \textit{nontrivial}. It is readily verified that an additive character \( \psi \) of \( \mathbb{F}_p \) is indeed a homomorphism:
\[ \psi(x + y) = \psi(x)\psi(y) \quad \text{for all } x, y \in \mathbb{F}_p. \tag{2} \]

Now let \( g \) be a generator for the cyclic group \((\mathbb{F}_p^*, \cdot)\). Then, for integer \( a \), the mapping \( \chi_a : \mathbb{F}_p^* \to \mathbb{C} \), given by
\[ \chi_a(g^i) = e_p(ai), \]
is called a \textit{multiplicative character} of \( \mathbb{F}_p \). For \( a \equiv 0 \pmod{p-1} \), the character \( \chi_a \) is called \textit{trivial}, otherwise it is called \textit{nontrivial}. It is convenient to extend a multiplicative character \( \chi \) to a mapping acting on \( \mathbb{F}_p \) by putting \( \chi(0) = 0 \). This extension preserves the homomorphism property, so that for each multiplicative character \( \chi \) of \( \mathbb{F}_p \) we have
\[ \chi(xy) = \chi(x)\chi(y) \quad \text{for all } x, y \in \mathbb{F}_p. \tag{3} \]

The \textit{order} of a multiplicative character \( \chi_a \) is defined to be the least positive integer \( d \) such that \( da \equiv 0 \pmod{p-1} \). Equivalently, \( d = (p-1)/\gcd(a, p-1) \). Multiplicative characters of \( \mathbb{F}_p \) having order \( p-1 \) will be called \textit{primitive}. We say that a polynomial \( g(x) \in \mathbb{F}_p[x] \) is not a \textit{dth power} if \( g(x) \neq c[f(x)]^d \) for each \( c \in \mathbb{F}_p \) and each \( f(x) \in \mathbb{F}_p[x] \).

The key tools of this paper are the following bounds on sums involving characters with polynomial arguments. These results trace back to Weil, who provided the foundations of their proofs using deep methods from algebraic geometry. More elementary proofs were later established. Our first result was proved in [LN97, Thm. 5.38] (see also [Sch76, p. 44, Thm. 2E]).
\textbf{Result 1 ([LN97, Thm. 5.38])}. Let $\psi$ be a nontrivial additive character of $\mathbb{F}_p$, and let $f(x) \in \mathbb{F}_p[x]$ be of degree $n \geq 1$ with $\gcd(n, p) = 1$. Then
\begin{equation*}
\left| \sum_{x \in \mathbb{F}_p} \psi(f(x)) \right| \leq (n-1)\sqrt{p}.
\end{equation*}

Our second result was proved in [NW02, Lem. 2.2] by relaxing the conditions of [Sch76, p. 45, Thm. 2G].

\textbf{Result 2 ([NW02, Lem. 2.2])}. Let $\chi$ be a nontrivial multiplicative character of $\mathbb{F}_p$ of order $d$, and let $\psi$ be a nontrivial additive character of $\mathbb{F}_p$. Suppose that $g(x) \in \mathbb{F}_p[x]$ has $m$ distinct roots in its splitting field and that $g(x)$ is not a $d$th power. Suppose further that $f(x) \in \mathbb{F}_p[x]$ has degree $n$. Then
\begin{equation*}
\left| \sum_{x \in \mathbb{F}_p} \chi(g(x))\psi(f(x)) \right| \leq (m+n-1)\sqrt{p}.
\end{equation*}

For $m = 2$ and $n = 0$, Result 2 can be strengthened as follows (see [LN97, Exercise 5.54], for example).

\textbf{Result 3}. Let $\chi$ be a nontrivial multiplicative character of $\mathbb{F}_p$ of order $d$. Let $u$ and $v$ be distinct elements of $\mathbb{F}_p$, and let $h$ be an integer satisfying $0 < h < d$. Then
\begin{equation*}
\sum_{x \in \mathbb{F}_p} \chi((x + v)^h(x + u)^{d-h}) = -1.
\end{equation*}

\section{The Construction}

Given a prime $p > 3$ and a nonnegative integer $r$, let $i$ be an integer satisfying $0 \leq i < (p-2)p^r$. Then $i$ admits the unique decomposition
\begin{equation*}
i = (a-1)p^r + b_r p^{r-1} + b_{r-1} p^{r-2} + \cdots + b_1,
\end{equation*}
where $a$ and $b_j$ are integers satisfying $1 \leq a < p-1$ and $0 \leq b_j < p$ for $j = 1, 2, \ldots, r$. Let $\chi$ be a primitive multiplicative character of $\mathbb{F}_p$, let $\psi$ be a nontrivial additive character of $\mathbb{F}_p$, and consider the sequence $s_i$ given by
\begin{equation}
s_i(k) = \chi(k^a)\psi(b_r k^r + b_{r-1} k^{r-1} + \cdots + b_1k). \quad (4)
\end{equation}
It is immediate that the period of $s_i$ equals $p$. For $r = 0, 1, \ldots, p-2$, we define sequence family $\Omega^*_r$ of period $p$ to be the multiset
\begin{equation*}
\Omega^*_r := \{s_i : 0 \leq i < (p-2)p^r\}.
\end{equation*}
These sequence families form a nested chain of increasing size:
\begin{equation*}
\Omega^*_0 \subset \Omega^*_1 \subset \cdots \subset \Omega^*_{p-2}.
\end{equation*}
In order to establish the correlation properties of sequence family $\Omega^*_r$, we first prove that, for $0 \leq i < (p-2)p^r$, all sequences $s_i$ are distinct.
Lemma 4. \( \Omega^*_r \) contains \((p - 2)p^r\) distinct sequences.

Proof. Consider two sequences \( s, t \in \Omega^*_r \). Then there exist integers \( a, a' \) and polynomials \( b(x), b'(x) \in \mathbb{F}_p[x] \) such that

\[
\begin{align*}
    s(k) &= \chi(k^a)\psi(b(k)) \\
    t(k) &= \chi(k^{a'})\psi(b'(k))
\end{align*}
\]

for each \( k \in \mathbb{Z} \). By definition, \( a, a' \) satisfy \( 1 \leq a, a' < p - 1 \) and \( b(x), b'(x) \) have degree strictly less than \( p - 1 \) and satisfy \( b(0) = b'(0) = 0 \). We show that \( s = t \) forces \( a = a' \) and \( b(x) = b'(x) \), which will prove the lemma.

Consider the product \( s(k)t(k) \) and use (2) and (3) to obtain

\[
\begin{align*}
    s(k)t(k) &= \chi(k^a)\chi(k^{a'})\psi(b(k))\psi(b'(k)) \\
    &= \chi(k^{a-a'})\psi(b(k) - b'(k)).
\end{align*}
\]

By the definition of characters acting on \( \mathbb{F}_p \), there exist integer-valued functions \( A \) and \( B \) such that for \( k \not\equiv 0 \pmod{p} \)

\[
\begin{align*}
    \chi(k^{a-a'}) &= e_{p-1}(A(k)) \\
    \psi(b(k) - b'(k)) &= e_p(B(k)).
\end{align*}
\]

Hence,

\[
s(k)t(k) = e_{(p-1)p}(pA(k) + (p - 1)B(k)) \quad \text{for} \quad k \not\equiv 0 \pmod{p}.
\]

Now suppose that \( s = t \). Then \( s(k)t(k) = 1 \) for each \( k \not\equiv 0 \pmod{p} \). Since \( \gcd(p, p - 1) = 1 \), the Chinese Remainder Theorem implies for \( k \not\equiv 0 \pmod{p} \)

\[
A(k) \equiv 0 \pmod{p-1}
\]

and

\[
B(k) \equiv 0 \pmod{p}.
\]

Substitution into (5) and (6) gives for \( k \not\equiv 0 \pmod{p} \)

\[
\chi(k^{a-a'}) = 1
\]

and

\[
\psi(b(k) - b'(k)) = 1.
\]

Now, since \( \chi \) is primitive, (7) implies \( a \equiv a' \pmod{p - 1} \), which forces \( a = a' \) since \( 1 \leq a, a' < p - 1 \). Since \( b(0) = b'(0) \), we conclude from (8) that \( b(x) \equiv b'(x) \pmod{p} \). This forces \( b(x) = b'(x) \) because \( b(x) \) and \( b'(x) \) have degree at most \( p - 2 \), and the lemma is proved.

The correlation properties of sequence family \( \Omega^*_r \) are summarized in the following theorem.
Theorem 5. We have $\theta(\Omega_r^*) \leq (r + 1)\sqrt{p}$. In particular,

$$\theta_A(\Omega_r^*) \leq \begin{cases} 1 & \text{for } r \in \{0, 1\} \\ r\sqrt{p} & \text{otherwise} \end{cases}$$

(9)

and

$$\theta_C(\Omega_r^*) \leq (r + 1)\sqrt{p}.$$  

(10)

Proof. Given two sequences $s, t \in \Omega_r^*$, we can write

$$s(k) = \chi(k^a)\psi(b(k))$$
$$t(k) = \chi(k^{a'})\psi(b'(k))$$

for each $k \in \mathbb{Z}$, where $1 \leq a, a' < p - 1$ and $b(x), b'(x) \in \mathbb{F}_p[x]$ have degree at most $r$ and satisfy $b(0) = b'(0) = 0$. Using the homomorphism properties (2) and (3) of $\psi$ and $\chi$ and Fermat’s little theorem $x^{p-1} \equiv 1 \pmod{p}$ for $x \not\equiv 0 \pmod{p}$, we then find that

$$C_{s,t}(u) = \sum_{k=0}^{p-1} s(k)t(k + u)$$
$$= \sum_{k=0}^{p-1} \chi(k^a)\psi(b(k))\chi((k + u)^a')\psi(b'(k + u))$$
$$= \sum_{x \in \mathbb{F}_p} \chi(g(x))\psi(f(x)),$$

(11)

where $g(x), f(x) \in \mathbb{F}_p[x]$ are given by

$$g(x) = x^a(x + u)^{p-1-a'}$$
$$f(x) = b(x) - b'(x + u).$$

Suppose first that $u \not\equiv 0 \pmod{p}$ and $s = t$, so by Lemma 4, $a = a'$ and $b(x) = b'(x)$. Then $g(x)$ has precisely two distinct zeros and cannot be a $(p - 1)$th power. Moreover, for $r > 0$, $f(x)$ has degree at most $r - 1$. Application of Result 2 to (11) then shows that $|C_s(u)| \leq r\sqrt{p}$ for $r > 0$. If $r \in \{0, 1\}$, then $\deg f(x) = 0$ and $\psi(f(x)) \equiv c$ for some complex $c$ with $|c| = 1$. In this case we apply Result 3 with $h = a$ to (11) to show that $|C_s(u)| = 1$. This proves (9).

Now suppose that $s \neq t$. We distinguish the following two cases.

- **Case 1: $g(x)$ is a $(p - 1)$th power.** Here, we have $\chi(g(x)) = 0$ for $x = 0$ and $\chi(g(x)) = c$ for some complex $c$ with $|c| = 1$ otherwise. Therefore, from (11),

$$|C_{s,t}(u)| = \left| \sum_{x \in \mathbb{F}_p} \psi(f(x)) \right|$$
$$= \left| -\psi(f(0)) + \sum_{x \in \mathbb{F}_p} \psi(f(x)) \right|$$
$$\leq 1 + \left| \sum_{x \in \mathbb{F}_p} \psi(f(x)) \right|.$$  

(12)
Since \( g(x) \) is a \((p - 1)\)th power, we must have \( a = a' \) and \( u \equiv 0 \pmod{p} \). Then \( s \neq t \) forces \( b(x) \neq b'(x) \). By assumption, \( b(0) = b'(0) = 0 \), hence \( f(x) \) has degree at least 1. But \( f(x) \) can have degree at most \( r \), which is less than \( p \), so that \( \gcd(\deg f(x), p) = 1 \). Application of Result 1 to (12) therefore gives
\[
|C_{s,t}(u)| \leq 1 + (r - 1)\sqrt{p}.
\]

- **Case 2:** \( g(x) \) is not a \((p - 1)\)th power. Here, \( g(x) \) has at most two distinct zeros and \( f(x) \) has degree at most \( r \). Application of Result 2 to (11) then gives
\[
|C_{s,t}(u)| \leq (r + 1)\sqrt{p}.
\]

This proves (10). \( \square \)

Note that \( s_i \), as defined in (4), satisfies \(|s_i(k)| = 1 \) for \( k \not\equiv 0 \pmod{p} \) and \( s_i(k) = 0 \) for \( k \equiv 0 \pmod{p} \). In practise however it is desirable to use polyphase sequences. We therefore modify \( s_i \) and define the sequence \( s'_i \) by
\[
s'_i(k) = \begin{cases} 1 & \text{for } k \equiv 0 \pmod{p} \\ s_i(k) & \text{otherwise} \end{cases}
\]
for \( 0 \leq i < (p - 2)p^r \). The corresponding sequence family is defined to be
\[
\Omega_r := \{s'_i : 0 \leq i < (p - 2)p^r \}
\]
for \( r = 0, 1, \ldots, p - 2 \). By Lemma 4, \( \Omega_r \) contains again \((p - 2)p^r\) distinct sequences. But now the sequences in \( \Omega_r \) are polyphase sequences whose alphabet size is \( p - 1 \) for \( r = 0 \) and \( p(p - 1) \) for \( r > 0 \). Observe that for all \( s, t \in \Omega_r^* \),
\[
C_{s',t'}(u) = C_{s,t}(u) + t'(u) + s'(-u).
\]
We therefore have \(|C_{s',t'}(u)| \leq 2 + |C_{s,t}(u)|\) and obtain the following corollary.

**Corollary 6.** We have \( \theta(\Omega_r) \leq 2 + (r + 1)\sqrt{p} \). In particular,
\[
\theta_A(\Omega_r) \leq \begin{cases} 3 & \text{for } r \in \{0, 1\} \\ 2 + r\sqrt{p} & \text{otherwise} \end{cases}
\]
and
\[
\theta_C(\Omega_r) \leq 2 + (r + 1)\sqrt{p}.
\]

Notice that Corollary 6 gives a nontrivial bound for \( \theta(\Omega_r) \) only if \( r \) is less than \((p - 2)/\sqrt{p} - 1\).

We close this section with an example. Take \( p = 5 \), and write \( \omega := \sqrt{-1} \) and \( \zeta := e^{\pi \sqrt{-2}/5} \). Let \( \psi \) be the additive character of \( \mathbb{F}_5 \) given by \( \psi(k) = \zeta^k \), and let \( \chi \) be the primitive multiplicative character of \( \mathbb{F}_5 \) given by \( \chi(2^j) = \omega^j \). Then the sequences in \( \Omega_1^* \) have period 5 and are of the form
\[
s_{5(a-1)+b}(k) = \chi(k^a)\psi(bk) \quad \text{for } a \in \{1, 2, 3\} \text{ and } b \in \{0, 1, 2, 3, 4\},
\]

where

\[
(\chi(k^a) : 0 \leq k < 5) = \begin{cases} 
(0, 1, \omega, -\omega, -1) & \text{for } a = 1 \\
(0, 1, -1, -1, 1) & \text{for } a = 2 \\
(0, 1, -\omega, \omega, -1) & \text{for } a = 3 
\end{cases}
\]

and

\[
(\psi(bk) : 0 \leq k < 5) = \begin{cases} 
(1, 1, 1, 1, 1) & \text{for } b = 0 \\
(1, \zeta, \zeta^2, \zeta^3, \zeta^4) & \text{for } b = 1 \\
(1, \zeta^2, \zeta^4, \zeta, \zeta^3) & \text{for } b = 2 \\
(1, \zeta^3, \zeta^4, \zeta^4, \zeta^2) & \text{for } b = 3 \\
(1, \zeta^4, \zeta^3, \zeta^2, \zeta) & \text{for } b = 4.
\end{cases}
\]

Direct inspection gives \( \theta_A(\Omega^*_1) = 1 \) and \( \theta_C(\Omega^*_1) \simeq 2.90 \), which should be compared with the bounds \( \theta_A(\Omega^*_1) \leq 1 \) and \( \theta_C(\Omega^*_1) \leq 2\sqrt{5} \) in Theorem 5. We also have \( \theta_A(\Omega_1) = 3 \) and \( \theta_C(\Omega_1) \simeq 4.52 \), which should be compared with the bounds \( \theta_A(\Omega_1) \leq 3 \) and \( \theta_C(\Omega_1) \leq 2(1 + \sqrt{5}) \) in Corollary 6.

References


