Multiplicative Characters, The Weil Bound, and Polyphase Sequence Families With Low Correlation

Nam Yul Yu* and Guang Gong[†]

*Department of Electrical Engineering, Lakehead University

[†]Department of Electrical and Computer Engineering, University of Waterloo

Abstract

Power residue and Sidelnikov sequences are polyphase sequences with low correlation and variable alphabet sizes, represented by multiplicative characters. In this paper, sequence families constructed from the shift and addition of the polyphase sequences are revisited. Initially, $\psi(0) = 1$ is assumed for multiplicative characters ψ to represent power residue and Sidelnikov sequences in a simple form. The Weil bound on multiplicative character sums is refined for the assumption, where the character sums are equivalent to the correlations of sequences represented by multiplicative characters. General constructions of polyphase sequence families that produce some of known families as the special cases are then presented. The refined Weil bound enables the efficient proofs on the maximum correlation magnitudes of the sequence families. From the constructions, it is shown that M-ary known sequence families with large size can be partitioned into $(M+1)$ disjoint subsequence families with smaller maximum correlation magnitudes. More generalized constructions are also considered by the addition of multiple cyclic shifts of power residue and Sidelnikov sequences.

Index Terms

Correlation, Multiplicative characters, Polyphase sequences, Power residue sequences, Sequence family, Sidelnikov sequences, Weil bound.

I. Introduction

Sequences with low correlation find many applications in wireless communications for acquiring the correct timing information and distinguishing multiple users or channels with low mutual interference.

It is desirable that sequences have variable alphabet sizes for adaptive modulation schemes which allow variable data rates in wireless systems according to channel characteristics. In addition, a large number of distinct sequences are also required for supporting as many distinct users or channels as possible.

Power residue and Sidelnikov sequences introduced in [21] are polyphase sequences with low correlation and variable alphabet sizes, represented by multiplicative characters. For odd prime p and a positive integer $M \mid p-1$, M-ary *power residue sequences* of period p have the out-of-phase autocorrelation magnitude of at most 3, which has been also studied in [5]. For prime p and positive integers m and $M \mid p^m-1$, on the other hand, M-ary *Sidelnikov sequences* of period p^m-1 have the maximum out-of-phase autocorrelation magnitude of 4. The binary case of the sequences has been also discussed in [17]. Moreover, it is shown in [11] that the magnitude of the cross-correlation of distinct M-ary power residue sequences of period p is bounded by $\sqrt{p}+2$. Kim and Song [12] further showed that the cross-correlation of an M-ary Sidelnikov sequence of period p^m-1 and its constant multiple has the maximum magnitude of $\sqrt{p^m}+3$.

To obtain a large number of distinct sequences with low correlation, power residue and Sidelnikov sequences can be employed in constructing a polyphase sequence family. The efforts on the family have been initiated by Guohua and Quan's observation [6] on the binary sequences obtained by the *shift-and-addition* of Legendre sequences of prime period p, where the Legendre sequence is a binary version of a power residue sequence. In [20], Rushanan applied the Weil bound to theoretically prove that the correlation magnitude of the sequences is bounded by $2\sqrt{p}+5$. Han and Yang [7] then generalized the construction for M-ary sequence families from the shift and addition of power residue sequences. Also, Kim *et al.* [13] constructed M-ary sequence families from the shift and addition of Sidelnikov sequences. Recently, Han and Yang [8] summarized the known constructions, and using the same technique $-$ shift and addition, they further constructed M-ary sequence families with larger size than the known ones, but the same maximum correlation magnitude.

In this paper, we revisit the polyphase sequence families constructed from the shift and addition of constant multiples of power residue and Sidelnikov sequences. First of all, we assume $\psi(0) = 1$ in multiplicative characters ψ, contrary to the conventional assumption [18], in order to represent the sequences without the indicator function used in previous researches [8], [12], and [13]. For the assumption, we make a refinement to the Weil bound on multiplicative character sums which are equivalent to the correlations of sequences represented by the characters. We then present general constructions of polyphase sequence families by determining the maximum correlation magnitudes and the family sizes, where the constructions produce some of known sequence families as the special cases. The refined Weil bound enables more efficient proofs on the maximum correlation magnitudes than the proofs in [13] and [8]. From the constructions, we show that M-ary known sequence families with large size can be partitioned into $(M+1)$ disjoint subsequence families with smaller maximum correlation magnitudes, which is similar to partitions (or decompositions) to multiple signal sets discussed in [3] and [4]. We also consider more generalized constructions by the addition of multiple cyclic shifts of power residue and Sidelnikov sequences.

The rest of this paper is organized as follows. In Section II, we give preliminaries for this work by describing definitions and concepts. Section III introduces the Weil bound on multiplicative character sums and makes a refinement for the bound to support the assumption $\psi(0)=1$. Section IV presents general constructions of polyphase sequence families from power residue and Sidelnikov sequences, where the constructions produce some of known families as the special cases. We determine the maximum correlation magnitudes by employing the refined Weil bound. Partitioning and more generalizing known sequence families are also discussed. Concluding remarks are given in Section V.

II. Preliminaries

This section describes basic definitions and concepts for understanding the work in this paper. The following notations will be used throughout this paper.

- $\omega_M = e^{j\frac{2\pi}{M}}$ is a primitive M-th root of unity, where $j=\sqrt{-1}$.
- $\mathbb{F}_q = \mathrm{GF}(q)$ is a finite field with q elements and $\mathbb{F}_q^*$ denotes a multiplicative group of $\mathbb{F}_q$.
- $\mathbb{F}_q[x]$ is a polynomial ring over $\mathbb{F}_q$, where each coefficient of $f(x)\in\mathbb{F}_q[x]$ is an element of $\mathbb{F}_q$.
- For an element x in $\mathbb{F}_q$, a *logarithm* over $\mathbb{F}_q$ is defined by

$$\log_\alpha x = \begin{cases} t, & \text{if } x=\alpha^t,\ 0\le t\le q-2, \\ 0, & \text{if } x=0 \end{cases}$$

where α is a primitive element in $\mathbb{F}_q$.

A. Multiplicative characters

Let α be a primitive element of $\mathbb{F}_q$ and M a divisor of $q-1$, i.e., $M \mid q-1$. A *multiplicative character* [18] of $\mathbb{F}_q$ of order M is defined by

$$\psi(x) = \begin{cases} \exp\left(j\frac{2\pi t}{M}\right), & \text{if } x=\alpha^t,\ 0\le t\le q-2 \\ 0, & \text{if } x=0 \end{cases} \tag{1}$$

where it is the convention to assume $\psi(0)=0$ [18]. If $M=1$, then $\psi(\alpha^t)=1$ for any integer t, which is trivial. Thus, we assume the order $M>1$ for *nontrivial* multiplicative characters. For an integer c, $1 \leq c \leq M-1$, note that $\psi^c(x) = \psi_1(x)$ is also a nontrivial multiplicative character of $2 \leq \mathrm{ord}(\psi_1) \leq M$, where $\mathrm{ord}(\psi_1)$ denotes the order of ψ_1, or the smallest positive integer d such that $\psi_1^d(x) = 1$ for all $x \in \mathbb{F}_q^*$. For the general definition of a multiplicative character, see Theorem 5.8 in [18].

The multiplicative character is also defined by a logarithm over finite fields.

Definition 1: A multiplicative character of $\mathbb{F}_q$ of order M is defined by

$$\psi(x) = \exp\left(j\frac{2\pi \log_\alpha x}{M}\right), \quad x \in \mathbb{F}_q \tag{2}$$

where $\psi(0) = 1$ by definition of the log operation.

Throughout this paper, $\psi(x)$ may be denoted as ψ if the context is clear. In (2), note that $\psi(0) = 1$, which contradicts the conventional assumption in (1). In this paper, however, we keep the assumption of $\psi(0) = 1$ to maintain the definition of (2), which will be useful in representing power residue and Sidelnikov sequences in a simple form by multiplicative characters.

From basic log operations, multiplicative characters have some properties as follows.

a) $\psi(x^c) = \psi^c(x)$, where $x \in \mathbb{F}_q$ and c is an integer,

b) $\psi(x)\psi(y) = \psi(xy)$, where $x, y \in \mathbb{F}_q^*$,

c) $\psi(x)\psi^{-1}(y) = \psi\left(\frac{x}{y}\right)$, where $x, y \in \mathbb{F}_q^*$

where we assume $0^c = 0$ for any integer c.

B. Power residue and Sidelnikov sequences

Sidelnikov [21] introduced two types of polyphase sequences with low periodic autocorrelation. For the sequences, we present the definitions by logarithm as well as the original ones.

Definition 2: Let p be an odd prime and M a divisor of $p-1$, i.e., $M \mid p-1$. Let α be a primitive root modulo p. Let $U_k = \{\alpha^{Mi+k} \mid 0 \leq i < \frac{p-1}{M}\}$ for $0 \leq k \leq M-1$. The M-ary power residue sequence $\mathbf{r} = \{r(t) \mid 0 \leq t \leq p-1\}$ of period p is defined by

$$r(t) = \begin{cases} 0, & \text{if } t = 0 \\ k, & \text{if } t \in U_k. \end{cases}$$

By the log operation, $r(t)$ is equivalently defined by

$$r(t) \equiv \log_\alpha t \mod M, \quad 0 \leq t \leq p-1. \tag{3}$$

By (2) and (3), the modulated sequence of $r(t)$ is represented by

$$\omega_M^{r(t)} = \psi(t), \quad 0 \le t \le p-1 \tag{4}$$

where $\psi(0) = 1$. (4) represents the power residue sequences in a simple form by multiplicative characters without the indicator function $I(x)$ used in [8] and [13].

Definition 3: Let $\mathbb{F}_q$ be a finite field with $q = p^m$ and M a divisor of $q-1$, i.e., $M \mid p^m - 1$, where p is prime and m is a positive integer. Let α be a primitive element in $\mathbb{F}_q$. Let $V_k = \{\alpha^{Mi+k} - 1 \mid 0 \le i < \frac{p^m-1}{M}\}$ for $0 \le k \le M-1$. The M-ary Sidelnikov sequence $\mathbf{s} = \{s(t) \mid 0 \le t \le p^m - 2\}$ of period $p^m - 1$ is defined by

$$s(t) = \begin{cases} 0, & \text{if } \alpha^t = -1 \\ k, & \text{if } \alpha^t \in V_k. \end{cases}$$

Equivalently, $s(t)$ is defined by

$$s(t) \equiv \log_\alpha(\alpha^t + 1) \mod M, \quad 0 \le t \le p^m - 2. \tag{5}$$

By (2) and (5), the modulated sequence of $s(t)$ is represented by

$$\omega_M^{s(t)} = \psi(\alpha^t + 1), \quad 0 \le t \le p^m - 2 \tag{6}$$

where $\psi(0) = 1$. (6) represents the Sidelnikov sequences in a simple form by multiplicative characters without the indicator function $I(x)$ in [8] and [13].

C. Correlations and sequence families

Let $\mathbf{a} = \{a(t)\}$ and $\mathbf{b} = \{b(t)\}$ be M-ary sequences of period L, where $0 \le t \le L-1$. A (periodic) correlation of sequences $\mathbf{a}$ and $\mathbf{b}$ is defined by

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{t=0}^{L-1} \omega_M^{a(t)-b(t+\tau)}, \quad 0 \le \tau \le L-1 \tag{7}$$

where the indices is computed modulo L. If $\mathbf{a}$ and $\mathbf{b}$ are *cyclically equivalent*, i.e., $a(t) = b(t+l)$ for all t's and an integer l, then $C_{\mathbf{a},\mathbf{b}}(\tau) = C_{\mathbf{a}}(\tau)$ becomes the *autocorrelation* of $\mathbf{a}$. Otherwise, if $\mathbf{a}$ and $\mathbf{b}$ are *cyclically distinct*, then $C_{\mathbf{a},\mathbf{b}}(\tau)$ is the *cross-correlation* of $\mathbf{a}$ and $\mathbf{b}$.

Let $\mathcal{S} = \{\mathbf{s}^{(0)}, \cdots, \mathbf{s}^{(N-1)}\}$ be a set of N cyclically distinct M-ary sequences of period L, and $C_{\max}(\mathcal{S})$ be defined by

$$C_{\max}(\mathcal{S}) = \max \left| C_{\mathbf{s}^{(i)},\mathbf{s}^{(j)}}(\tau) \right| \text{ for any } 0 \le \tau \le L-1,\ 0 \le i, j \le N-1$$

where $\tau \neq 0$ if $i = j$. Clearly, $C_{\max}(\mathcal{S})$ is the maximum of all nontrivial auto- and cross-correlations of the sequences in $\mathcal{S}$. Then, the set $\mathcal{S}$ is called an *M-ary sequence family* of period L, where N is the *family size* and $C_{\max}(\mathcal{S})$ is the *maximum correlation magnitude* of $\mathcal{S}$. The sequence family $\mathcal{S}$ is said to have *low correlation* if $C_{\max}(\mathcal{S}) \leq v\sqrt{L}$ for a small constant v. For more details on correlation and sequence families, see [1] and [10].

III. The Weil bound and The Refinement

The Weil bound [25] gives the upper bound on the magnitude of character sums (or exponential sums). It has been widely employed in determining the maximum correlation magnitude of a sequence family since the correlation of sequences is ultimately equivalent to a character sum. For the applications of exponential sums to sequence and coding theory, see [19].

We introduce one of the various versions of the Weil bound, which is useful for this work.

Theorem 1: [24] Let $f_1(x), \cdots, f_l(x)$ be l monic polynomials in $\mathbb{F}_q[x]$ whose largest square free divisors have positive degrees $d_1, \cdots, d_l$, respectively. Let $\psi_1, \cdots, \psi_l$ be multiplicative characters of $\mathbb{F}_q$, where $\psi_i(0) = 0,\ 1 \leq i \leq l$. Assume that the product character $\prod_{i=1}^{l} \psi_i(f_i(x))$ is nontrivial, i.e., $\prod_{i=1}^{l} \psi_i(f_i(x)) \neq 1$ for all $x \in \mathbb{F}_q$. Then, for every $a_i \in \mathbb{F}_q^*$, we have

$$\left| \sum_{x \in \mathbb{F}_q} \psi_1\left(a_1 f_1(x)\right) \cdots \psi_l\left(a_l f_l(x)\right) \right| \leq (\sum_{i=1}^{l} d_i - 1)\sqrt{q}.$$

In particular, if $\prod_{i=1}^{l} \psi_i^{d_i}(x) = 1$ for all $x \in \mathbb{F}_q^*$, then

$$\left| \sum_{x \in \mathbb{F}_q} \psi_1\left(a_1 f_1(x)\right) \cdots \psi_l\left(a_l f_l(x)\right) \right| \leq (\sum_{i=1}^{l} d_i - 2)\sqrt{q} + 1. \tag{8}$$

Theorem 1 contains some straightforward generalizations from Corollary 2.3 in [24], where the bounds generally hold under the condition of the nontrivial product character. The bounds become tighter under the original condition of Corollary 2.3 that $f_i(x)$'s are pairwise prime and $\psi_i(f_i(x))$'s are nontrivial, which may occur in the worst case of sequence correlations in our analysis. Also, the sufficient condition for (8) is slightly different from the original one of Corollary 2.3 in [24]. From the proof and Theorem 2.1 in [24], however, it is easy to see that $\prod_{i=1}^{l} \psi_i^{d_i}(x) = 1$ for all $x \in \mathbb{F}_q^*$ is sufficient for achieving (8).

In the original Weil bound, $\psi_i(0) = 0$ is conventionally assumed. However, it is more convenient to have $\psi_i(0) = 1$ in our analysis as it conforms to (4) and (6). The assumption of $\psi_i(0) = 1$ then requires a slight change to the original Weil bound. Thus, we make a refinement to the Weil bound such that it can support $\psi_i(0) = 1$.

Corollary 1: In Theorem 1, let e_i be the number of distinct roots in $\mathbb{F}_q$ of $f_i(x)$, where $i = 1, \cdots, l$. If $\psi_i(0) = 1$ is assumed for each i, then

$$\left| \sum_{x \in \mathbb{F}_q} \psi_1(a_l f_1(x)) \cdots \psi_l(a_l f_l(x)) \right| \le (\sum_{i=1}^{l} d_i - 1)\sqrt{q} + \sum_{i=1}^{l} e_i. \tag{9}$$

In particular, if $\prod_{i=1}^{l} \psi_i^{d_i}(x) = 1$ for all $x \in \mathbb{F}_q^*$, then

$$\left| \sum_{x \in \mathbb{F}_q} \psi_1(a_1 f_1(x)) \cdots \psi_l(a_l f_l(x)) \right| \le (\sum_{i=1}^{l} d_i - 2)\sqrt{q} + 1 + \sum_{i=1}^{l} e_i. \tag{10}$$

Proof: Let Ω_i be a set of distinct roots of $f_i(x)$ in $\mathbb{F}_q$, and $\Omega = \bigcup_{i=1}^{l} \Omega_i = \{x \in \mathbb{F}_q \mid f_i(x) = 0,\ 1 \le i \le l\}$, where $|\Omega| \le \sum_{i=1}^{l} e_i$. Then,

$$\begin{aligned}
&\sum_{x \in \mathbb{F}_q, \psi_i(0)=1} \psi_1(a_1 f_1(x)) \cdots \psi_l(a_l f_l(x)) \\
&= \sum_{x \notin \Omega, \psi_i(0)=1} \psi_1(a_1 f_1(x)) \cdots \psi_l(a_l f_l(x)) + \sum_{x \in \Omega, \psi_i(0)=1} \psi_1(a_1 f_1(x)) \cdots \psi_l(a_l f_l(x)) \\
&= \sum_{x \in \mathbb{F}_q, \psi_i(0)=0} \psi_1(a_1 f_1(x)) \cdots \psi_l(a_l f_l(x)) + \sum_{x \in \Omega, \psi_i(0)=1} \psi_1(a_1 f_1(x)) \cdots \psi_l(a_l f_l(x)).
\end{aligned}$$

With $|\psi_i| = 1$, it is straightforward that $\left|\sum_{x \in \Omega, \psi_i(0)=1} \psi_1(a_1 f_1(x)) \cdots \psi_l(a_l f_l(x))\right| \le |\Omega|$. Therefore,

$$\begin{aligned}
&\left| \sum_{x \in \mathbb{F}_q, \psi_i(0)=1} \psi_1(a_1 f_1(x)) \cdots \psi_l(a_l f_l(x)) \right| \\
&\le \left| \sum_{x \in \mathbb{F}_q, \psi_i(0)=0} \psi_1(a_1 f_1(x)) \cdots \psi_l(a_l f_l(x)) \right| + \left| \sum_{x \in \Omega, \psi_i(0)=1} \psi_1(a_1 f_1(x)) \cdots \psi_l(a_l f_l(x)) \right| \\
&\le \left| \sum_{x \in \mathbb{F}_q, \psi_i(0)=0} \psi_1(a_1 f_1(x)) \cdots \psi_l(a_l f_l(x)) \right| + |\Omega| \\
&\le (\sum_{i=1}^{l} d_i - 1)\sqrt{q} + \sum_{i=1}^{l} e_i.
\end{aligned}$$

Similar to this approach, (10) is immediate. □

In Corollary 1, if some of $f_i(x)$'s share common roots in $\mathbb{F}_q$, there may be a case of $|\Omega| < \sum_{i=1}^{l} e_i$, which allows tighter bounds than (9) and (10). However, the upper bounds in Corollary 1 are always true, including the worst case of $|\Omega| = \sum_{i=1}^{l} e_i$. Corollary 1 turns out to be very useful in determining the maximum correlation magnitudes of sequence families represented by multiplicative characters, where we only need to take into account the degrees and the number of roots in $\mathbb{F}_q$ of each $f_i(x)$, which is a polynomial corresponding to a sequence or its cyclic shift.

IV. The Refined Weil Bound and Polyphase Sequence Families

In this section, we revisit polyphase sequence families constructed from the shift and addition of constant multiples of power residue and Sidelnikov sequences. General constructions are presented producing some of known sequence families as the special cases. We provide the efficient proofs on the maximum correlation magnitudes by employing the refined Weil bound described in Section III. Also, we discuss how to partition M-ary known sequence families with large size into $(M+1)$ disjoint subsequence families. Finally, we consider more generalized constructions by the addition of multiple cyclic shifts of power residue and Sidelnikov sequences.

A. M-ary power residue sequence families

Construction 1: Let $\mathbf{r} = \{r(t) \mid 0 \le t \le p-1\}$ be an M-ary power residue sequence of period p, where p is an odd prime and $M \mid p-1$. Let

$$\begin{aligned} \mathcal{I}_{\mathbf{r}} &= \{cr(t) \mid 1 \le c \le M-1\}, \\ \mathcal{A}_{\mathbf{r}}^{(\delta)} &= \left\{ c_0 r(t) + c_1 r(t+l) \mod M \mid 1 \le l \le \frac{p-1}{2},\ c_0 + c_1 \equiv \delta \mod M \right\} \end{aligned}$$

where δ is a constant in $0 \le \delta \le M-1$ and $1 \le c_0, c_1 \le M-1$. A polyphase sequence family $\mathcal{S}_{\mathbf{r}}^{(\delta)}$ of period p is defined by

$$\mathcal{S}_{\mathbf{r}}^{(\delta)} = \mathcal{I}_{\mathbf{r}} \cup \mathcal{A}_{\mathbf{r}}^{(\delta)}$$

where all sequences are cyclically distinct. The maximum correlation magnitude and the family size of $\mathcal{S}_{\mathbf{r}}^{(\delta)}$ are shown in Theorems 2 and 3, respectively.

It is straightforward that $\mathcal{S}_{\mathbf{r}}^{(\delta)}$ is a general sequence family including $\mathcal{F}_{\mathbf{r}}^{(a)}, \mathcal{F}_{\mathbf{r}}^{(c_1,c_2)}$, and $\tilde{\mathcal{F}}_{\mathbf{r}}$ in [8] as the special cases, where $c_0 = c_1 = a$ and $\delta = 2a$ for a constant a in $\mathcal{F}_{\mathbf{r}}^{(a)}$, and $\delta = c_1 + c_2$ for fixed integers c_1 and c_2 in $\mathcal{F}_{\mathbf{r}}^{(c_1,c_2)}$. In $\tilde{\mathcal{F}}_{\mathbf{r}}$, $c_0 = c,\ c_1 = M - c$ and $\delta = 0$ for an integer $c,\ 1 \le c \le M-1$. Obviously, $\mathcal{S}_{\mathbf{r}}^{(\delta)}$ is a subset of a larger sequence family $\mathcal{F}_{\mathbf{r}}$ in [8] where all sequences are cyclically distinct. (see (13) for $\mathcal{F}_{\mathbf{r}}$.) Therefore, the sequences in $\mathcal{S}_{\mathbf{r}}^{(\delta)}$ are also cyclically distinct.

We now determine the maximum correlation magnitude of $\mathcal{S}_{\mathbf{r}}^{(\delta)}$ by employing the refined Weil bound.

Theorem 2: For any $\delta,\ 0 \le \delta \le M-1$, the maximum correlation magnitude of $\mathcal{S}_{\mathbf{r}}^{(\delta)}$ in Construction 1 is given by

$$C_{\max}(\mathcal{S}_{\mathbf{r}}^{(\delta)}) = 2\sqrt{p} + 5.$$

Proof: Let α be a primitive root in $\mathbb{F}_p$. We derive the upper bound on the correlation magnitude of a pair of sequences $\mathbf{a} = \{a(t)\}$ and $\mathbf{b} = \{b(t)\}$ in $\mathcal{S}_{\mathbf{r}}^{(\delta)}$ for the following cases, where we use the notations of Corollary 1 in the character sums. In each case, we exclude a trivial in-phase autocorrelation of $\tau = 0$ at $\mathbf{a} = \mathbf{b}$, which drives each product character in $C_{\mathbf{a},\mathbf{b}}(\tau)$ to be nontrivial.

Case 1. $\mathbf{a}, \mathbf{b} \in \mathcal{I}_{\mathbf{r}}$: Let $a(t) = cr(t)$ and $b(t) = c'r(t)$, where $1 \le c, c' \le M-1$. From (7) and (4), the correlation of $\mathbf{a}$ and $\mathbf{b}$ is given by

$$\begin{aligned} C_{\mathbf{a},\mathbf{b}}(\tau) &= \sum_{t=0}^{p-1} \omega_M^{cr(t)-c'r(t+\tau)} \\ &= \sum_{x\in\mathbb{F}_p} \psi^{c}(x)\psi^{-c'}(x+\tau). \end{aligned}$$

Let $f_1(x) = x$ and $f_2(x) = x + \tau$, which are the monic polynomials in $\mathbb{F}_p$ corresponding to $r(t)$ and $r(t+\tau)$, respectively. Then, the degrees of $f_1(x)$ and $f_2(x)$ are $d_1 = d_2 = 1$, respectively. Also, the number of roots of $f_1(x)$ and $f_2(x)$ in $\mathbb{F}_p$ are $e_1 = e_2 = 1$, respectively. Let $\psi_1 = \psi^c$ and $\psi_2 = \psi^{-c'} = \psi^{M-c'}$. Note that the product character $\psi_1(f_1(x)) \cdot \psi_2(f_2(x))$ is nontrivial if we exclude $\tau = 0$ at $\mathbf{a} = \mathbf{b}$. With these notations, we are now able to apply the refined Weil bound of (9) in Corollary 1, i.e.,

$$|C_{\mathbf{a},\mathbf{b}}(\tau)| \le \left| \sum_{x\in\mathbb{F}_p} \psi_1(x)\psi_2(x+\tau) \right| \le (d_1 + d_2 - 1)\sqrt{p} + e_1 + e_2 = \sqrt{p} + 2$$

which confirms the upper bound of the cross-correlation magnitude of distinct power residue sequences [11].

In particular, if $c = c'$, then $\prod_{i=1}^{2} \psi_i^{d_i}(x) = \psi^{c-c'}(x) = 1$ for all $x \in \mathbb{F}_p^*$. In this case, we can apply the improved bound in (10) to obtain

$$|C_{\mathbf{a},\mathbf{b}}(\tau)| \le (d_1 + d_2 - 2)\sqrt{p} + 1 + e_1 + e_2 = 3, \quad \tau \ne 0$$

which is obvious from the out-of-phase autocorrelation of power residue sequences.

Case 2. $\mathbf{a} \in \mathcal{I}_{\mathbf{r}}$ and $\mathbf{b} \in \mathcal{A}_{\mathbf{r}}^{(\delta)}$ (or vice versa.): Let $a(t) = cr(t)$ and $b(t) = c_0 r(t) + c_1 r(t+l)$, where $1 \le c, c_0, c_1 \le M-1$ and $1 \le l \le \frac{p-1}{2}$. Then,

$$\begin{aligned} C_{\mathbf{a},\mathbf{b}}(\tau) &= \sum_{t=0}^{p-1} \omega_M^{cr(t)-c_0r(t+\tau)-c_1r(t+l+\tau)} \\ &= \sum_{x\in\mathbb{F}_p} \psi^{c}(x)\psi^{-c_0}(x+\tau)\psi^{-c_1}(x+l+\tau). \end{aligned}$$

In Corollary 1, $f_1(x) = x,\ f_2(x) = x + \tau$, and $f_3(x) = x + l + \tau$, which are in $\mathbb{F}_p$. Therefore, $d_1 = d_2 = d_3 = 1$ and $e_1 = e_2 = e_3 = 1$. Let $\psi_1 = \psi^c$, $\psi_2 = \psi^{-c_0} = \psi^{M-c_0}$, and $\psi_3 = \psi^{-c_1} = \psi^{M-c_1}$.

The cyclic distinctness of $\mathbf{a}$ and $\mathbf{b}$ guarantees that the product character $\prod_{i=1}^{3}\psi_i(f_i(x))$ is nontrivial. From (9), we have

$$|C_{\mathbf{a},\mathbf{b}}(\tau)| \leq \left|\sum_{x\in\mathbb{F}_p}\psi_1(x)\psi_2(x+\tau)\psi_3(x+\tau+l)\right| \leq (d_1+d_2+d_3-1)\sqrt{p}+e_1+e_2+e_3 = 2\sqrt{p}+3.$$

In particular, if $c \equiv c_0+c_1 \pmod{M}$, then $\prod_{i=1}^{3}\psi_i^{d_i}(x) = \psi^{c-c_0-c_1}(x) = 1$ for all $x\in\mathbb{F}_p^*$. From (10),

$$|C_{\mathbf{a},\mathbf{b}}(\tau)| \leq (d_1+d_2+d_3-2)\sqrt{p}+1+e_1+e_2+e_3 = \sqrt{p}+4.$$

Case 3. $\mathbf{a},\mathbf{b}\in\mathcal{A}_{\mathbf{r}}^{(\delta)}$: Let $a(t) = c_0r(t)+c_1r(t+l)$ and $b(t) = c_0'r(t)+c_1'r(t+l')$, where $1\leq c_0,c_1,c_0',c_1' \leq M-1$ and $1\leq l,l' \leq \frac{p-1}{2}$. Then,

$$\begin{aligned}C_{\mathbf{a},\mathbf{b}}(\tau) &= \sum_{t=0}^{p-1}\omega_M^{c_0r(t)+c_1r(t+l)-c_0'r(t+\tau)-c_1'r(t+l'+\tau)}\\ &= \sum_{x\in\mathbb{F}_p}\psi^{c_0}(x)\psi^{c_1}(x+l)\psi^{-c_0'}(x+\tau)\psi^{-c_1'}(x+l'+\tau).\end{aligned}$$

In Corollary 1, $f_1(x)=x,\ f_2(x)=x+l,\ f_3(x)=x+\tau$, and $f_4(x)=x+l'+\tau$, which are in $\mathbb{F}_p$. Thus, $d_1=d_2=d_3=d_4=1$ and $e_1=e_2=e_3=e_4=1$. Let $\psi_1=\psi^{c_0}$, $\psi_2=\psi^{c_1}$, $\psi_3=\psi^{-c_0'}=\psi^{M-c_0'}$, and $\psi_4=\psi^{-c_1'}=\psi^{M-c_1'}$. Obviously, the product character $\prod_{i=1}^{4}\psi_i(f_i(x))$ is nontrivial for the cyclically distinct sequences $\mathbf{a}$ and $\mathbf{b}$. With $c_0+c_1=c_0'+c_1'\equiv\delta \pmod{M}$,

$$\prod_{i=1}^{4}\psi_i^{d_i}(x) = \psi^{c_0+c_1-c_0'-c_1'}(x) = 1$$

for all $x\in\mathbb{F}_p^*$. From (10), therefore,

$$\begin{aligned}|C_{\mathbf{a},\mathbf{b}}(\tau)| &\leq \left|\sum_{x\in\mathbb{F}_p}\psi_1(x)\psi_2(x+l)\psi_3(x+\tau)\psi_4(x+l'+\tau)\right|\\ &\leq (d_1+d_2+d_3+d_4-2)\sqrt{p}+1+e_1+e_2+e_3+e_4 = 2\sqrt{p}+5.\end{aligned}$$

From Cases $1-3$, the proof is completed. □

Theorem 3: The family size of the M-ary sequence family $\mathcal{S}_{\mathbf{r}}^{(\delta)}$ in Construction 1 is given by

$$\left|\mathcal{S}_{\mathbf{r}}^{(\delta)}\right| = \begin{cases}\binom{\frac{p+1}{2}}{}\cdot(M-1), & \text{if } \delta=0,\\ \binom{\frac{p+1}{2}}{}\cdot(M-1)-\binom{\frac{p-1}{2}}{}, & \text{if } 1\leq\delta\leq M-1.\end{cases} \quad (11)$$

Therefore, $\mathcal{S}_{\mathbf{r}}^{(\delta)}$ has the largest family size when $\delta=0$, where $\mathcal{S}_{\mathbf{r}}^{(0)}=\tilde{\mathcal{F}}_{\mathbf{r}}$ in [8].

Before proving Theorem 3, we consider the following lemma.

Lemma 1: Let c_0 and c_1 be positive integers such that $c_0+c_1 \equiv \delta \pmod{M}$ where $1 \leq c_0, c_1 \leq M-1$. For a given integer $\delta,\ 0 \leq \delta \leq M-1$, the number of the (c_0, c_1) pairs is given by

$$N_{c_0,c_1}^{(\delta)} = \begin{cases} M-1, & \text{if } \delta = 0 \\ M-2, & \text{if } 1 \leq \delta \leq M-1. \end{cases} \tag{12}$$

Proof: If $\delta = 0$, then the (c_0, c_1) pairs are listed by

$$\Delta_0 = \{(1, M-1), (2, M-2), \cdots, (M-1, 1)\}.$$

Thus, the number of the pairs is $N_{c_0,c_1}^{(0)} = |\Delta_0| = M-1$. If $1 \leq \delta \leq M-1$, on the other hand, the pairs of (c_0, c_1) for $c_0 + c_1 \equiv \delta \pmod{M}$ are

$$\Delta_\delta = \{(1, \delta-1), (2, \delta-2), \cdots, (\delta-1, 1), (\delta+1, M-1), \cdots, (M-1, \delta-M+1)\}$$

where only a valid pair with $1 \leq c_0, c_1 \leq M-1$ exist. The number of possible pairs is therefore $N_{c_0,c_1}^{(\delta)} = |\Delta_\delta| = M-1-1 = M-2$. □

Proof of Theorem 3: First of all, $|\mathcal{I}_\mathbf{r}| = M-1$. From Construction 1, the size of $\mathcal{A}_\mathbf{r}^{(\delta)}$ is $|\mathcal{A}_\mathbf{r}^{(\delta)}| = N_{c_0,c_1}^{(\delta)} \cdot \left(\frac{p-1}{2}\right)$ from l and (c_0, c_1) pairs. Therefore, the family size of $\mathcal{S}_\mathbf{r}^{(\delta)}$, $0 \leq \delta \leq M-1$, is determined by $|\mathcal{S}_\mathbf{r}^{(\delta)}| = |\mathcal{I}_\mathbf{r}| + |\mathcal{A}_\mathbf{r}^{(\delta)}|$, which results in (11). □

In [7] and [8], an M-ary sequence family $\mathcal{F}_\mathbf{r}$ of large size has been introduced. In this paper, we denote it as $\mathcal{L}_\mathbf{r}$ that is defined by

$$\begin{aligned} \mathcal{L}_\mathbf{r} = \mathcal{I}_\mathbf{r} \cup \mathcal{B}_\mathbf{r} = & \{cr(t) \mid 1 \leq c_0 \leq M-1\} \\ & \cup \left\{ c_0 r(t) + c_1 r(t+l) \mod M \mid 1 \leq l \leq \frac{p-1}{2},\ 1 \leq c_0, c_1 \leq M-1 \right\} \end{aligned} \tag{13}$$

where $\mathbf{r} = \{r(t)\}$ is an M-ary power residue sequence of period p. As studied in [8], its correlation magnitude is bounded by $3\sqrt{p}+4$. In next lemma, we discuss the partition of $\mathcal{L}_\mathbf{r}$ into subsequence families $\mathcal{A}_\mathbf{r}^{(\delta)}$ in Construction 1 with the smaller maximum correlation magnitude of $2\sqrt{p}+5$.

Lemma 2: For an M-ary power residue sequence $\mathbf{r} = \{r(t) \mid 0 \leq t \leq p-1\}$ of period p, consider a sequence family $\mathcal{L}_\mathbf{r}$ in (13) with the maximum correlation magnitude of $3\sqrt{p}+4$. Compared to $\mathcal{S}_\mathbf{r}^{(\delta)}$ in Construction 1, we have

$$\mathcal{L}_\mathbf{r} = \mathcal{I}_\mathbf{r} \cup \mathcal{A}_\mathbf{r}^{(0)} \cup \mathcal{A}_\mathbf{r}^{(1)} \cup \cdots \cup \mathcal{A}_\mathbf{r}^{(M-1)} = \mathcal{I}_\mathbf{r} \cup \left(\bigcup_{\delta=0}^{M-1} \mathcal{A}_\mathbf{r}^{(\delta)} \right) \tag{14}$$

where all sequences are cyclically distinct among the subsequence families. In other words, $\mathcal{L}_\mathbf{r}$ is partitioned into $(M+1)$ disjoint subsequence families of $\mathcal{I}_\mathbf{r}$ and $\mathcal{A}_\mathbf{r}^{(\delta)},\ 0 \leq \delta \leq M-1$, where $\mathcal{I}_\mathbf{r}$ and $\mathcal{A}_\mathbf{r}^{(\delta)}$ have the correlation magnitudes bounded by $\sqrt{p}+2$ and $2\sqrt{p}+5$, respectively.

Proof: Apparently, the union of (c_0, c_1) pairs in $\mathcal{A}_{\mathbf{r}}^{(\delta)}$ over all δ's forms all possible (c_0, c_1) pairs of $\mathcal{B}_{\mathbf{r}}$ in (13). Since all sequences in $\mathcal{L}_{\mathbf{r}}$ are cyclically distinct [8] and we can easily check from (11) and (13) that

$$|\mathcal{I}_{\mathbf{r}}| + \sum_{\delta=0}^{M-1} \left|\mathcal{A}_{\mathbf{r}}^{(\delta)}\right| = |\mathcal{L}_{\mathbf{r}}|,$$

it is obvious that $\mathcal{L}_{\mathbf{r}}$ is partitioned into disjoint subsequence families as in (14). □

Remark 1: In code-division multiple access (CDMA) systems, we will be able to assign each subsequence family $\mathcal{I}_{\mathbf{r}}$ and $\mathcal{A}_{\mathbf{r}}^{(\delta)}$, $0 \le \delta \le M-1$ to a group of users, where each group has $|\mathcal{I}_{\mathbf{r}}|$ and $|\mathcal{A}_{\mathbf{r}}^{(\delta)}|$ users, respectively. There are total $(M+1)$ user groups supported by the sequence family $\mathcal{L}_{\mathbf{r}}$. If two users in the same group access to the system simultaneously, the *intra-group interference* is bounded by the maximum correlation magnitude $\sqrt{p}+2$ or $2\sqrt{p}+5$. On the other hand, if they belong to different groups, the *inter-group interference* is limited by $3\sqrt{p}+4$. From the partition of $\mathcal{L}_{\mathbf{r}}$ in Lemma 2, the user grouping is therefore possible for different intra- and inter-group interferences. Similar techniques of partition (or decomposition) to multiple signal sets have been discussed in [3] and [4].

Remark 2: The refined Weil bound has been employed in Theorem 2 to determine $C_{\max}(\mathcal{S}_{\mathbf{r}}^{(\delta)})$ by providing the more efficient proof on the bound than the ones used in [7] and [8]. Similar to the proof of Theorem 2, it can be also used to determine the maximum correlation magnitude of $\mathcal{L}_{\mathbf{r}}$, where $d_i = 1$ and $e_i = 1$ for $1 \le i \le 4$ in the worst case, and thus $C_{\max}(\mathcal{L}_{\mathbf{r}}) = 3\sqrt{p}+4$ by (9).

B. M-ary Sidelnikov sequence families

Construction 2: Let $\mathbf{s} = \{s(t) \mid 0 \le t \le p^m - 2\}$ be an M-ary Sidelnikov sequence of period $p^m - 1$, where p is prime, m is a positive integer, and $M \mid p^m - 1$. Let

$$\begin{aligned}
\mathcal{I}_{\mathbf{s}} &= \{cs(t) \mid 1 \le c \le M-1\}, \\
\mathcal{A}_{\mathbf{s}}^{(\delta)} &= \left\{c_0 s(t) + c_1 s(t+l) \mod M \mid 1 \le l \le \left\lfloor \frac{p^m-1}{2} \right\rfloor,\ c_0 + c_1 \equiv \delta \mod M \right\}
\end{aligned}$$

where δ is a constant in $0 \le \delta \le M-1$ and $1 \le c_0, c_1 \le M-1$. In $\mathcal{A}_{\mathbf{s}}^{(\delta)}$, note that $c_0 < c_1$ if $l = \frac{p^m-1}{2}$ for odd prime p. A polyphase sequence family $\mathcal{S}_{\mathbf{s}}^{(\delta)}$ of period $p^m - 1$ is defined by

$$\mathcal{S}_{\mathbf{s}}^{(\delta)} = \mathcal{I}_{\mathbf{s}} \cup \mathcal{A}_{\mathbf{s}}^{(\delta)}$$

where all sequences are cyclically distinct. The maximum correlation magnitude and the family size of $\mathcal{S}_{\mathbf{s}}^{(\delta)}$ are shown in Theorems 4 and 5, respectively.

$\mathcal{S}_{\mathbf{s}}^{(\delta)}$ is a general sequence family including $\mathcal{F}_{\mathbf{s}}^{(a)}$, $\mathcal{F}_{\mathbf{s}}^{(c_1,c_2)}$, and $\tilde{\mathcal{F}}_{\mathbf{s}}$ in [8] as the special cases, where $c_0 = c_1 = a$ and $\delta = 2a$ for a constant a in $\mathcal{F}_{\mathbf{s}}^{(a)}$, and $\delta = c_1 + c_2$ for fixed integers c_1 and c_2 in $\mathcal{F}_{\mathbf{s}}^{(c_1,c_2)}$. In $\tilde{\mathcal{F}}_{\mathbf{s}}$, $c_0 = c,\ c_1 = M - c$ and $\delta = 0$ for an integer $c,\ 1 \le c \le M-1$. Although the cyclic distinctness of the known families has not been clearly proven in [8], it is obvious because those are the subsets of a larger family $\mathcal{L}$ in [13] (or $\mathcal{F}_{\mathbf{s}}$ in [8]) where all sequences are cyclically distinct. (see (19) for $\mathcal{L}$.) For the same reason, all sequences in $\mathcal{S}_{\mathbf{s}}^{(\delta)}$ are cyclically distinct.

Theorem 4: For any $\delta,\ 0 \le \delta \le M-1$, the maximum correlation magnitude of $\mathcal{S}_{\mathbf{s}}^{(\delta)}$ in Construction 2 is given by

$$C_{\max}(\mathcal{S}_{\mathbf{s}}^{(\delta)}) = 2\sqrt{p^m} + 6.$$

Proof: Let α be a primitive element in $\mathbb{F}_{p^m}$. We derive the upper bound on the correlation of a pair of sequences $\mathbf{a} = \{a(t)\}$ and $\mathbf{b} = \{b(t)\}$ in $\mathcal{S}_{\mathbf{s}}^{(\delta)}$ for the following cases, where we use the notations of Corollary 1 in the character sums. In each case, we exclude a trivial in-phase autocorrelation of $\tau = 0$ at $\mathbf{a} = \mathbf{b}$, which drives each product character in $C_{\mathbf{a},\mathbf{b}}(\tau)$ to be nontrivial.

Case 1. $\mathbf{a}, \mathbf{b} \in \mathcal{I}_{\mathbf{s}}$: Let $a(t) = cs(t)$ and $b(t) = c's(t)$, where $1 \le c, c' \le M-1$. From (7) and (6), the correlation of $\mathbf{a}$ and $\mathbf{b}$ is given by

$$\begin{aligned} C_{\mathbf{a},\mathbf{b}}(\tau) &= \sum_{t=0}^{p^m-2} \omega_M^{cs(t)-c's(t+\tau)} \\ &= \sum_{x\in\mathbb{F}_{p^m}^*} \psi^c(x+1)\psi^{-c'}(\theta x+1) \\ &= \sum_{x\in\mathbb{F}_{p^m}} \psi^c(x+1)\psi^{-c'}\left(\theta\cdot(x+\theta^{-1})\right) - 1 \end{aligned}$$

where $\theta = \alpha^\tau,\ 0 \le \tau \le p^m - 2$. Let $f_1(x) = x+1$ and $f_2(x) = x + \theta^{-1}$, which are the monic polynomials in $\mathbb{F}_{p^m}$ corresponding to $s(t)$ and $s(t+\tau)$, respectively. Then, the degrees of $f_1(x)$ and $f_2(x)$ are $d_1 = d_2 = 1$, respectively, and the number of roots of $f_1(x)$ and $f_2(x)$ in $\mathbb{F}_{p^m}$ are $e_1 = e_2 = 1$, respectively. Let $\psi_1 = \psi^c$ and $\psi_2 = \psi^{-c'} = \psi^{M-c'}$. Note that the product character $\psi_1(f_1(x))\cdot\psi_2(\theta f_2(x))$ is nontrivial if we exclude $\tau = 0$ at $\mathbf{a} = \mathbf{b}$. With these notations, we are now able to apply the refined Weil bound of (9) in Corollary 1, i.e.,

$$|C_{\mathbf{a},\mathbf{b}}(\tau)| \le \left|\sum_{x\in\mathbb{F}_{p^m}} \psi_1\left(f_1(x)\right)\psi_2\left(\theta\cdot f_2(x)\right)\right| + 1 \le (d_1+d_2-1)\sqrt{p^m} + e_1 + e_2 + 1 = \sqrt{p^m} + 3$$

which confirms the cross-correlation of a Sidelnikov sequence and its constant multiple [12].

In particular, if $c = c'$, then $\prod_{i=1}^{2} \psi_i^{d_i}(x) = \psi^{c-c'}(x) = 1$ for all $x \in \mathbb{F}_{p^m}^*$. In this case, we can apply the improved bound in (10) to obtain

$$|C_{\mathbf{a},\mathbf{b}}(\tau)| \leq (d_1 + d_2 - 2)\sqrt{p^m} + 1 + e_1 + e_2 + 1 = 4, \quad \tau \neq 0$$

which is obvious from the out-of-phase autocorrelation of Sidelnikov sequences.

Case 2. $\mathbf{a} \in \mathcal{I}_{\mathbf{s}}$ and $\mathbf{b} \in \mathcal{A}_{\mathbf{s}}^{(\delta)}$ (or vice versa.): Let $a(t) = cs(t)$ and $b(t) = c_0 s(t) + c_1 s(t+l)$, where $1 \leq c, c_0, c_1 \leq M-1$ and $1 \leq l \leq \left\lfloor \frac{p^m-1}{2} \right\rfloor$. Then,

$$\begin{aligned} C_{\mathbf{a},\mathbf{b}}(\tau) &= \sum_{t=0}^{p^m-2} \omega_M^{cs(t)-c_0 s(t+\tau)-c_1 s(t+l+\tau)} \\ &= \sum_{x \in \mathbb{F}_{p^m}^*} \psi^c(x+1)\psi^{-c_0}(\theta x+1)\psi^{-c_1}(\sigma\theta x+1) \\ &= \sum_{x \in \mathbb{F}_{p^m}} \psi^c(x+1)\psi^{-c_0}\left(\theta \cdot (x+\theta^{-1})\right)\psi^{-c_1}\left(\sigma\theta \cdot (x+(\sigma\theta)^{-1})\right) - 1 \end{aligned}$$

where $\sigma = \alpha^l$ and $\theta = \alpha^\tau$. In Corollary 1, $f_1(x) = x+1,\ f_2(x) = x+\theta^{-1}$, and $f_3(x) = x+(\sigma\theta)^{-1}$, which are in $\mathbb{F}_{p^m}$. Therefore, $d_1 = d_2 = d_3 = 1$ and $e_1 = e_2 = e_3 = 1$. Let $\psi_1 = \psi^c$, $\psi_2 = \psi^{-c_0} = \psi^{M-c_0}$, and $\psi_3 = \psi^{-c_1} = \psi^{M-c_1}$. The cyclic distinctness of $\mathbf{a}$ and $\mathbf{b}$ guarantees that the product character $\prod_{i=1}^{3} \psi_i(a_i f_i(x))$ is nontrivial, where $a_1 = 1,\ a_2 = \theta$, and $a_3 = \sigma\theta$. From (9), we have

$$\begin{aligned} |C_{\mathbf{a},\mathbf{b}}(\tau)| &\leq \left| \sum_{x \in \mathbb{F}_{p^m}} \psi_1\left(f_1(x)\right)\psi_2\left(\theta \cdot f_2(x)\right)\psi_3\left(\sigma\theta \cdot f_3(x)\right) \right| + 1 \\ &\leq (d_1 + d_2 + d_3 - 1)\sqrt{p} + e_1 + e_2 + e_3 + 1 = 2\sqrt{p^m} + 4. \end{aligned}$$

In particular, if $c \equiv c_0 + c_1 \pmod{M}$, then $\prod_{i=1}^{3} \psi_i^{d_i}(x) = \psi^{c-c_0-c_1}(x) = 1$ for all $x \in \mathbb{F}_{p^m}^*$. In this case, from (10),

$$|C_{\mathbf{a},\mathbf{b}}(\tau)| \leq (d_1 + d_2 + d_3 - 2)\sqrt{p^m} + 1 + e_1 + e_2 + e_3 + 1 = \sqrt{p^m} + 5.$$

Case 3. $\mathbf{a}, \mathbf{b} \in \mathcal{A}_{\mathbf{s}}^{(\delta)}$: Let $a(t) = c_0 s(t) + c_1 s(t+l)$ and $b(t) = c_0' s(t) + c_1' s(t+l')$, where $1 \leq c_0, c_1, c_0', c_1' \leq M-1$ and $1 \leq l, l' \leq \left\lfloor \frac{p^m-1}{2} \right\rfloor$. Then,

$$\begin{aligned} C_{\mathbf{a},\mathbf{b}}(\tau) &= \sum_{t=0}^{p^m-2} \omega_M^{c_0 s(t)+c_1 s(t+l)-c_0' s(t+\tau)-c_1' s(t+l'+\tau)} \\ &= \sum_{x \in \mathbb{F}_{p^m}^*} \psi^{c_0}(x+1)\psi^{c_1}(\sigma x+1)\psi^{-c_0'}(\theta x+1)\psi^{-c_1'}(\sigma'\theta x+1) \\ &= \sum_{x \in \mathbb{F}_{p^m}} \psi^{c_0}(x+1)\psi^{c_1}\left(\sigma \cdot (x+\sigma^{-1})\right)\psi^{-c_0'}\left(\theta \cdot (x+\theta^{-1})\right)\psi^{-c_1'}\left(\sigma'\theta \cdot (x+(\sigma'\theta)^{-1})\right) - 1 \end{aligned}$$

where $\sigma = \alpha^l$, $\sigma' = \alpha^{l'}$, and $\theta = \alpha^\tau$. In Corollary 1, $f_1(x) = x + 1,\ f_2(x) = x + \sigma^{-1},\ f_3(x) = x + \theta^{-1},\ f_4(x) = x + (\sigma'\theta)^{-1}$, which are in $\mathbb{F}_{p^m}$. Then, $d_1 = d_2 = d_3 = d_4 = 1$ and $e_1 = e_2 = e_3 = e_4 = 1$. Let $\psi_1 = \psi^{c_0}$, $\psi_2 = \psi^{c_1}$, $\psi_3 = \psi^{-c_0'} = \psi^{M-c_0'}$, and $\psi_4 = \psi^{-c_1'} = \psi^{M-c_1'}$. Obviously, the product character $\prod_{i=1}^4 \psi_i(a_i f_i(x))$ is nontrivial for the cyclically distinct sequences $\mathbf{a}$ and $\mathbf{b}$, where $a_1 = 1,\ a_2 = \sigma,\ a_3 = \theta$, and $a_4 = \sigma'\theta$. With $c_0 + c_1 = c_0' + c_1' \equiv \delta \pmod{M}$,

$$\prod_{i=1}^{4} \psi_i^{d_i}(x) = \psi^{c_0+c_1-c_0'-c_1'}(x) = 1$$

for all $x \in \mathbb{F}_{p^m}^*$. From (10), therefore,

$$\begin{aligned}|C_{\mathbf{a},\mathbf{b}}(\tau)| &\le \left| \sum_{x\in\mathbb{F}_{p^m}} \psi_1\left(f_1(x)\right)\psi_2\left(\sigma\cdot f_2(x)\right)\psi_3\left(\theta\cdot f_3(x)\right)\psi_4\left(\sigma'\theta\cdot f_4(x)\right)\right| + 1\\ &\le (d_1+d_2+d_3+d_4-2)\sqrt{p^m} + 1 + e_1+e_2+e_3+e_4+1 = 2\sqrt{p^m}+6.\end{aligned}$$

From Cases $1-3$, the proof is completed. □

For the family size of $\mathcal{S}_{\mathbf{s}}^{(\delta)}$, Lemma 1 has already discussed the number of (c_0, c_1) pairs for $1 \le l < \left\lfloor \frac{p^m-1}{2} \right\rfloor$, where $c_0 + c_1 \equiv \delta \pmod{M}$ for $1 \le c_0, c_1 \le M-1$. Now, we examine the number of (c_0, c_1) pairs for $l = \frac{p^m-1}{2}$ for odd prime p in the following lemma.

Lemma 3: Let c_0 and c_1 be positive integers such that $c_0 + c_1 \equiv \delta \pmod{M}$ where $1 \le c_0 < c_1 \le M-1$. For an integer $\delta,\ 0 \le \delta \le M-1$, the number of the (c_0, c_1) pairs is given by

$$N_{c_0<c_1}^{(\delta)} = \begin{cases} \left\lfloor \frac{M-1}{2} \right\rfloor, & \text{if } (\delta = 0) \text{ or } (M \text{ is even and } \delta \text{ is odd})\\ \left\lfloor \frac{M-1}{2} \right\rfloor - 1, & \text{if } (M \text{ is odd}) \text{ or } (M \text{ is even and } \delta \text{ is even}).\end{cases} \tag{15}$$

Proof: For a given integer, $\delta,\ 0 \le \delta \le M-1$, the set of the (c_0, c_1) pairs ($c_0 < c_1$) is given by

$$\begin{aligned}\Gamma &= \{(c_0, \delta - c_0) \mid 1 \le c_0 < \delta - c_0 \text{ and } \delta - c_0 \le M-1\}\\ &\quad \cup \{(c_0, M+\delta-c_0) \mid 1 \le c_0 < M+\delta-c_0 \text{ and } M+\delta-c_0 \le M-1\}\\ &= \left\{(c_0, \delta-c_0) \mid 1 \le c_0 < \frac{\delta}{2}\right\} \cup \left\{(c_0, M+\delta-c_0) \mid \delta+1 \le c_0 < \frac{M+\delta}{2}\right\}\\ &= \Gamma_1 \cup \Gamma_2\end{aligned} \tag{16}$$

where $\Gamma_1 \cap \Gamma_2 = \phi$.

Case 1. $\delta = 0$: In this case, $|\Gamma_1| = 0$ and $|\Gamma_2| = \left|\left\{1 \le c_0 < \frac{M}{2}\right\}\right| = \left\lfloor \frac{M-1}{2} \right\rfloor$. Thus, the number of (c_0, c_1) pairs is given by $N_{c_0<c_1}^{(\delta)} = |\Gamma_1| + |\Gamma_2| = \left\lfloor \frac{M-1}{2} \right\rfloor$.

Case 2. M is even and δ is odd: From (16), it is easy to see that $|\Gamma_1| = \frac{\delta-1}{2}$ and $|\Gamma_2| = \frac{M+\delta-1}{2} - \delta$. Thus, $N_{c_0<c_1}^{(\delta)} = |\Gamma_1| + |\Gamma_2| = \frac{M}{2} - 1 = \left\lfloor \frac{M-1}{2} \right\rfloor$.

Case 3. M is even and δ is even: $|\Gamma_1| = \frac{\delta}{2} - 1$ and $|\Gamma_2| = \frac{M+\delta}{2} - \delta - 1$ from (16). Thus, $N_{c_0<c_1}^{(\delta)} = |\Gamma_1| + |\Gamma_2| = \frac{M}{2} - 2 = \left\lfloor \frac{M-1}{2} \right\rfloor - 1$.

Case 4. M is odd and δ is even: $|\Gamma_1| = \frac{\delta}{2} - 1$ and $|\Gamma_2| = \frac{M+\delta-1}{2} - \delta$ from (16). Thus, $N_{c_0<c_1}^{(\delta)} = |\Gamma_1| + |\Gamma_2| = \frac{M-1}{2} - 1 = \left\lfloor \frac{M-1}{2} \right\rfloor - 1$.

Case 5. M is odd and δ is odd: $|\Gamma_1| = \frac{\delta-1}{2}$ and $|\Gamma_2| = \frac{M+\delta}{2} - \delta - 1$ from (16). Thus, $N_{c_0<c_1}^{(\delta)} = |\Gamma_1| + |\Gamma_2| = \frac{M-1}{2} - 1 = \left\lfloor \frac{M-1}{2} \right\rfloor - 1$.

From Cases $1-5$, the proof is completed. □

We are now ready to show the family size of $\mathcal{S}_{\mathbf{s}}^{(\delta)}$.

Theorem 5: The family size of the M-ary sequence family $\mathcal{S}_{\mathbf{s}}^{(\delta)}$ in Construction 2 is determined by

$$\left|\mathcal{S}_{\mathbf{s}}^{(\delta)}\right| = \begin{cases} M - 1 + \left(\frac{p^m-1}{2} - 1\right) \cdot N_{c_0,c_1}^{(\delta)} + N_{c_0<c_1}^{(\delta)}, & \text{if } p > 2, \\ M - 1 + (2^{m-1} - 1) \cdot N_{c_0,c_1}^{(\delta)}, & \text{if } p = 2 \end{cases} \tag{17}$$

where $N_{c_0,c_1}^{(\delta)}$ and $N_{c_0<c_1}^{(\delta)}$ are given in (12) and (15), respectively. In particular, $\mathcal{S}_{\mathbf{s}}^{(\delta)}$ has the largest family size when $\delta = 0$, where $\mathcal{S}_{\mathbf{s}}^{(0)} = \tilde{\mathcal{F}}_{\mathbf{s}}$ in [8].

Proof: First of all, $|\mathcal{I}_{\mathbf{s}}| = M - 1$. From Construction 2, the size of $\mathcal{A}_{\mathbf{s}}^{(\delta)}$ is

$$|\mathcal{A}_{\mathbf{s}}^{(\delta)}| = \begin{cases} \left(\frac{p^m-1}{2} - 1\right) \cdot N_{c_0,c_1}^{(\delta)} + N_{c_0<c_1}^{(\delta)}, & \text{if } p > 2 \\ \left(2^{m-1} - 1\right) \cdot N_{c_0,c_1}^{(\delta)} & \text{if } p = 2 \end{cases} \tag{18}$$

from l and (c_0, c_1) pairs. The family size of $\mathcal{S}_{\mathbf{s}}^{(\delta)}$, $0 \le \delta \le M-1$, is determined by $|\mathcal{S}_{\mathbf{s}}^{(\delta)}| = |\mathcal{I}_{\mathbf{r}}| + |\mathcal{A}_{\mathbf{s}}^{(\delta)}|$, which results in (17). □

Table I summarizes the parameters of $\mathcal{S}_{\mathbf{r}}^{(\delta)}$ and $\mathcal{S}_{\mathbf{s}}^{(\delta)}$ in Constructions 1 and 2, respectively, for various p, δ, and M. In the table, note that $|\mathcal{S}_{\mathbf{r}}^{(0)}| = |\tilde{\mathcal{F}}_{\mathbf{r}}|$ and $|\mathcal{S}_{\mathbf{s}}^{(0)}| = |\tilde{\mathcal{F}}_{\mathbf{s}}|$ in [8].

In [13], an M-ary sequence family $\mathcal{L}$ of large size has been presented, which has been also introduced as $\mathcal{F}_{\mathbf{s}}$ in [8]. In this paper, we denote it as $\mathcal{L}_{\mathbf{s}}$, i.e.,

$$\begin{aligned} \mathcal{L}_{\mathbf{s}} = \mathcal{I}_{\mathbf{s}} \cup \mathcal{B}_{\mathbf{s}} = &\{cs(t) \mid 1 \le c \le M - 1\} \\ &\cup \left\{ c_0 s(t) + c_1 s(t+l) \mod M \mid 1 \le l \le \left\lfloor \frac{p^m - 1}{2} \right\rfloor \right\} \end{aligned} \tag{19}$$

where $\mathbf{s} = \{s(t)\}$ is an M-ary Sidelnikov sequence of period $p^m - 1$, and $1 \le c_0, c_1 \le M - 1$. Note that $c_0 < c_1$ if $l = \frac{p^m-1}{2}$ for odd prime p. As studied in [13], its correlation magnitude is bounded by $3\sqrt{p^m}+5$. In next lemma, we discuss the partition of $\mathcal{L}_{\mathbf{s}}$ into subsequence families $\mathcal{A}_{\mathbf{s}}^{(\delta)}$ in Construction 2 with the smaller maximum correlation magnitude of $2\sqrt{p^m} + 6$.

TABLE I

THE PARAMETERS OF $\mathcal{S}_{\mathbf{r}}^{(\delta)}$ AND $\mathcal{S}_{\mathbf{s}}^{(\delta)},\ 0 \le \delta \le M-1$

	Period	$C_{\max}$	Family size	
$\mathcal{S}_{\mathbf{r}}^{(\delta)}$	p	$2\sqrt{p}+5$	$\left(\frac{p+1}{2}\right)\cdot(M-1)$	$\delta=0$ [8]
			$\left(\frac{p+1}{2}\right)\cdot(M-1)-\left(\frac{p-1}{2}\right)$	$\delta \neq 0$
$\mathcal{S}_{\mathbf{s}}^{(\delta)},\ p>2$	p^m-1	$2\sqrt{p^m}+6$	$(M-1)\cdot\left(\frac{p^m-1}{2}\right)+\left\lfloor\frac{M-1}{2}\right\rfloor$	$\delta=0$ [8]
			$(M-1)\cdot\left(\frac{p^m-1}{2}\right)+\frac{M-1}{2}-\left(\frac{p^m-1}{2}\right)$	$\delta\neq 0,\ M$ odd
			$(M-1)\cdot\left(\frac{p^m-1}{2}\right)+\frac{M}{2}-\left(\frac{p^m-1}{2}\right)$	δ odd, M even
			$(M-1)\cdot\left(\frac{p^m-1}{2}\right)+\frac{M}{2}-1-\left(\frac{p^m-1}{2}\right)$	δ even $(\neq 0)$, M even
$\mathcal{S}_{\mathbf{s}}^{(\delta)},\ p=2$	2^m-1	$2\sqrt{2^m}+6$	$2^{m-1}\cdot(M-1)$	$\delta=0$ [8]
			$2^{m-1}\cdot(M-1)-(2^{m-1}-1)$	$\delta\neq 0$

Lemma 4: For an M-ary Sidelnikov sequence $\mathbf{s}=\{s(t)\mid 0\le t\le p^m-2\}$ of period p^m-1, consider a sequence family $\mathcal{L}_{\mathbf{s}}$ in (19) with the maximum correlation magnitude of $3\sqrt{p^m}+5$. Compared to $\mathcal{S}_{\mathbf{s}}^{(\delta)}$ in Construction 2,

$$\mathcal{L}_{\mathbf{s}}=\mathcal{I}_{\mathbf{s}}\cup\mathcal{A}_{\mathbf{s}}^{(0)}\cup\mathcal{A}_{\mathbf{s}}^{(1)}\cup\cdots\cup\mathcal{A}_{\mathbf{s}}^{(M-1)}=\mathcal{I}_{\mathbf{s}}\cup\left(\bigcup_{\delta=0}^{M-1}\mathcal{A}_{\mathbf{s}}^{(\delta)}\right)\tag{20}$$

where all sequences are cyclically distinct among the subsequence families. In other words, $\mathcal{L}_{\mathbf{s}}$ is partitioned into $(M+1)$ disjoint subsequence families of $\mathcal{I}_{\mathbf{s}}$ and $\mathcal{A}_{\mathbf{s}}^{(\delta)},\ 0\le\delta\le M-1$, where $\mathcal{I}_{\mathbf{s}}$ and $\mathcal{A}_{\mathbf{s}}^{(\delta)}$ have the correlation magnitude bounded by $\sqrt{p^m}+3$ and $2\sqrt{p^m}+6$, respectively.

Proof: It is clear that the (c_0,c_1) pairs in $\mathcal{A}_{\mathbf{s}}^{(\delta)}$ belong to the set of the pairs in $\mathcal{B}_{\mathbf{s}}$. Since all sequences in $\mathcal{L}_{\mathbf{s}}$ are cyclically distinct [13] and we can easily check from (18) and (19) that

$$|\mathcal{I}_{\mathbf{s}}|+\sum_{\delta=0}^{M-1}\left|\mathcal{A}_{\mathbf{s}}^{(\delta)}\right|=|\mathcal{L}_{\mathbf{s}}|\,,$$

it is obvious that $\mathcal{L}_{\mathbf{s}}$ is partitioned into disjoint subsequence families as in (20). □

Remark 3: Similar to Remark 1, each subsequence family $\mathcal{I}_{\mathbf{s}}$ and $\mathcal{A}_{\mathbf{s}}^{(\delta)},\ 0\le\delta\le M-1$ can be assigned to a group of users in CDMA systems, where total $(M+1)$ user groups are supported by the sequence family $\mathcal{L}_{\mathbf{s}}$. The intra-group interference is bounded by the maximum correlation magnitude $\sqrt{p^m}+3$ or $2\sqrt{p^m}+6$, whereas the inter-group interference is limited by $3\sqrt{p^m}+5$. Hence, the partition of $\mathcal{L}_{\mathbf{s}}$ in Lemma 4 allows the user grouping for different intra- and inter-group interferences.

Remark 4: Similar to the proof of Theorem 4, the refined Weil bound can provide a more efficient proof than the one in [13] to determine the maximum correlation magnitude of $\mathcal{L}_{\mathbf{s}}$, where $d_i = 1$ and $e_i = 1$ for $1 \leq i \leq 4$ in the worst case, and thus $C_{\max}(\mathcal{L}_{\mathbf{s}}) = 3\sqrt{p^m} + 5$ by (9).

C. Generalized constructions

In [13], Kim *et al.* attempted to generalize the construction of $\mathcal{L}$ by the addition of multiple cyclic shifts of Sidelnikov sequences. From the similar approach, we generalize the constructions from power residue and Sidelnikov sequences. The detailed proofs on the cyclic distinctness, the maximum correlation magnitudes, and the family sizes of the generalized families are described in Appendix.

Construction 3: Let $\mathbf{r} = \{r(t) \mid 0 \leq t \leq p-1\}$ be an M-ary power residue sequence of period p, where p is an odd prime and $M \mid p-1$. Let $2 \leq k \leq \frac{p-1}{2}$ be a positive integer. A polyphase sequence family $\mathcal{H}_{\mathbf{r}}^{(k)}$ of period p is defined by

$$\begin{aligned}\mathcal{H}_{\mathbf{r}}^{(k)} = \mathcal{I}_{\mathbf{r}} \cup \mathcal{E}_{\mathbf{r}}^{(k)} = &\{cr(t) \mid 1 \leq c \leq M-1\} \\ &\cup \{c_0 r(t) + c_1 r(t+l_1) + \cdots + c_k r(t+l_k) \mod M \mid 1 \leq c_0, \cdots, c_k \leq M-1\}\end{aligned}$$

where $1 \leq l_1 < l_2 < \cdots < l_k \leq \frac{p-1}{2}$.

In particular, if $\sum_{i=0}^{k} c_i \equiv \delta \pmod M$ for a given integer δ, $0 \leq \delta \leq M-1$ in $\mathcal{H}_{\mathbf{r}}^{(k)}$, the sequence family, denoted by $\mathcal{G}_{\mathbf{r}}^{(\delta,k)}$, is defined by

$$\begin{aligned}\mathcal{G}_{\mathbf{r}}^{(\delta,k)} = \mathcal{I}_{\mathbf{r}} \cup \mathcal{D}_{\mathbf{r}}^{(\delta,k)} = &\{cr(t) \mid 1 \leq c \leq M-1\} \\ &\cup \left\{ c_0 r(t) + c_1 r(t+l_1) + \cdots + c_k r(t+l_k) \mod M \mid \sum_{i=0}^{k} c_i \equiv \delta \mod M \right\}.\end{aligned}$$

where $1 \leq l_1 < l_2 < \cdots < l_k \leq \frac{p-1}{2}$ and $1 \leq c_0, \cdots, c_k \leq M-1$.

Theorem 6: In Construction 3, all sequences in $\mathcal{H}_{\mathbf{r}}^{(k)}$ are cyclically distinct, and as its subset, all sequences in $\mathcal{G}_{\mathbf{r}}^{(\delta,k)}$ are also cyclically distinct. The maximum correlation magnitudes of $\mathcal{H}_{\mathbf{r}}^{(k)}$ and $\mathcal{G}_{\mathbf{r}}^{(\delta,k)}$ are given by

$$C_{\max}(\mathcal{H}_{\mathbf{r}}^{(k)}) = (2k+1)\sqrt{p} + 2k + 2,$$

$$C_{\max}(\mathcal{G}_{\mathbf{r}}^{(\delta,k)}) = 2k\sqrt{p} + 2k + 3.$$

Also, the family sizes of $\mathcal{H}_{\mathbf{r}}^{(k)}$ and $\mathcal{G}_{\mathbf{r}}^{(\delta,k)}$ are determined by

$$\begin{aligned}\left|\mathcal{H}_{\mathbf{r}}^{(k)}\right| &= (M-1) + \binom{\frac{p-1}{2}}{k} \cdot (M-1)^{k+1}, \\ \left|\mathcal{G}_{\mathbf{r}}^{(\delta,k)}\right| &= \begin{cases} T_k - (-1)^k \cdot \binom{\frac{p-1}{2}}{k}, & \text{if } \delta = 0 \\ T_k, & \text{if } \delta \neq 0 \end{cases}\end{aligned} \tag{21}$$

where $T_k = (M-1) + \binom{\frac{p-1}{2}}{k} \cdot \left(\frac{(M-1)^{k+1}+(-1)^k}{M}\right)$.

Construction 4: Let $\mathbf{s} = \{s(t) \mid 0 \leq t \leq p^m - 2\}$ be an M-ary Sidelnikov sequence of period $p^m - 1$, where p is prime, m is a positive integer, and $M \mid p^m - 1$. Let $2 \leq k \leq \left\lfloor \frac{p^m-2}{2} \right\rfloor$ be a positive integer. A polyphase sequence family $\mathcal{H}_{\mathbf{s}}^{(k)}$ of period $p^m - 1$ is defined by

$$\begin{aligned}\mathcal{H}_{\mathbf{s}}^{(k)} = \mathcal{I}_{\mathbf{s}} \cup \mathcal{E}_{\mathbf{s}}^{(k)} = &\{cs(t) \mid 1 \leq c \leq M-1\} \\ &\cup \{c_0 s(t) + c_1 s(t+l_1) + \cdots + c_k s(t+l_k) \mod M \mid 1 \leq c_0, \cdots, c_k \leq M-1\}\end{aligned}$$

where $1 \leq l_1 < l_2 < \cdots < l_k \leq \left\lfloor \frac{p^m-2}{2} \right\rfloor$.

In particular, if $\sum_{i=0}^{k} c_i \equiv \delta \pmod M$ for a given integer δ, $0 \leq \delta \leq M-1$ in $\mathcal{H}_{\mathbf{s}}^{(k)}$, the sequence family, denoted by $\mathcal{G}_{\mathbf{s}}^{(\delta,k)}$, is defined by

$$\begin{aligned}\mathcal{G}_{\mathbf{s}}^{(\delta,k)} = \mathcal{I}_{\mathbf{s}} \cup \mathcal{D}_{\mathbf{s}}^{(\delta,k)} = &\{cs(t) \mid 1 \leq c \leq M-1\} \\ &\cup \left\{c_0 s(t) + c_1 s(t+l_1) + \cdots + c_k s(t+l_k) \mod M \mid \sum_{i=0}^{k} c_i \equiv \delta \mod M \right\}.\end{aligned}$$

where $1 \leq l_1 < l_2 < \cdots < l_k \leq \left\lfloor \frac{p^m-2}{2} \right\rfloor$ and $1 \leq c_0, \cdots, c_k \leq M-1$.

Theorem 7: In Construction 4, all sequences in $\mathcal{H}_{\mathbf{s}}^{(k)}$ are cyclically distinct, and as its subset, all sequences in $\mathcal{G}_{\mathbf{s}}^{(\delta,k)}$ are also cyclically distinct. The maximum correlation magnitudes of $\mathcal{H}_{\mathbf{s}}^{(k)}$ and $\mathcal{G}_{\mathbf{s}}^{(\delta,k)}$ are given by

$$\begin{aligned}C_{\max}(\mathcal{H}_{\mathbf{s}}^{(k)}) &= (2k+1)\sqrt{p^m} + 2k + 3, \\ C_{\max}(\mathcal{G}_{\mathbf{s}}^{(\delta,k)}) &= 2k\sqrt{p^m} + 2k + 4.\end{aligned} \tag{22}$$

Also, the family sizes of $\mathcal{H}_{\mathbf{s}}^{(k)}$ and $\mathcal{G}_{\mathbf{s}}^{(\delta,k)}$ are determined by

$$\begin{aligned}\left|\mathcal{H}_{\mathbf{s}}^{(k)}\right| &= (M-1) + \binom{\left\lfloor \frac{p^m-2}{2} \right\rfloor}{k} \cdot (M-1)^{k+1}, \\ \left|\mathcal{G}_{\mathbf{s}}^{(\delta,k)}\right| &= \begin{cases} T'_k - (-1)^k \cdot \binom{\lfloor \frac{p^m-2}{2} \rfloor}{k}, & \text{if } \delta = 0 \\ T'_k, & \text{if } \delta \neq 0 \end{cases}\end{aligned}$$

where $T'_k = (M-1) + \binom{\lfloor \frac{p^m-2}{2} \rfloor}{k} \cdot \left(\frac{(M-1)^{k+1}+(-1)^k}{M}\right)$.

Table II compares the parameters of some known polyphase sequence families.

Remark 5: In Construction 4, we remove the case of $l_i = \frac{p^m-1}{2}$, $1 \leq i \leq k$ for odd prime p, for simplicity in our analysis of $\mathcal{G}_{\mathbf{s}}^{(\delta,k)}$ and $\mathcal{H}_{\mathbf{s}}^{(k)}$. From Constructions 3 and 4, we discover that if k is even, then $\mathcal{G}_{\mathbf{r}}^{(\delta,k)}$ (or $\mathcal{G}_{\mathbf{s}}^{(\delta,k)}$) provides more sequences in $\delta \neq 0$ than in $\delta = 0$, contrary to $\mathcal{S}_{\mathbf{r}}^{(\delta,k)}$ (or $\mathcal{S}_{\mathbf{s}}^{(\delta,k)}$).

TABLE II

THE COMPARISON OF WELL KNOWN POLYPHASE SEQUENCE FAMILIES (p IS AN ODD PRIME)

	Period L	Alphabet	$C_{\max}$	Family size
Trachtenberg [23]	p^m-1, m odd	p	$\sqrt{p(L+1)}+1$	$L+2$
Helleseth [9]	p^m-1, m even $p^{m/2}\not\equiv 2 \pmod 3$	p	$2\sqrt{L+1}+1$	$L+2$
Sidelnikov [22]	p^m-1	p	$\sqrt{L+1}+1$	$L+1$
Bent [14]	p^m-1, m even	p	$\sqrt{L+1}+1$	$\sqrt{L+1}$
Kumar, Moreno [16]	p^m-1	p	$\sqrt{L+1}+1$	$L+1$
Gong [2]	$(p^m-1)^2$	p	$2\sqrt{L}+3$	$\sqrt{L}$
$\mathbb{Z}_4$ Family $S(0)$ [15]	2^m-1	4	$\sqrt{L+1}+1$	$L+2$
$\mathbb{Z}_4$ Family $S(1)$ [15]	2^m-1	4	$2\sqrt{L+1}+1$	$\geq L^2+3L+2$
$\mathbb{Z}_4$ Family $S(2)$ [15]	2^m-1	4	$4\sqrt{L+1}+1$	$\geq L^3+4L^2+5L+2$
$\mathcal{S}_{\mathbf{r}}^{(0)}$ (or $\tilde{\mathcal{F}}_{\mathbf{r}}$ [8])	p	M	$2\sqrt{L}+5$	$\left(\frac{L+1}{2}\right)\cdot(M-1)$
$\mathcal{L}_{\mathbf{r}}$ (or $\mathcal{F}_{\mathbf{r}}$ [8])	p	M	$3\sqrt{L}+4$	$M-1+\frac{(M-1)^2(L-1)}{2}$
$\mathcal{G}_{\mathbf{r}}^{(\delta,2)}, \delta\neq 0$ (in this paper)	p	M	$4\sqrt{L}+7$	$(M-1)+\frac{(L-1)(L-3)}{8}\cdot(M^2-3M+3)$
$\mathcal{H}_{\mathbf{r}}^{(2)}$ (in this paper)	p	M	$5\sqrt{L}+6$	$(M-1)+\frac{(L-1)(L-3)}{8}\cdot(M-1)^3$
$\mathcal{S}_{\mathbf{s}}^{(0)}$ (or $\tilde{\mathcal{F}}_{\mathbf{s}}$ [8])	p^m-1	M	$2\sqrt{L+1}+6$	$(M-1)\cdot\left(\frac{L}{2}\right)+\left\lfloor\frac{M-1}{2}\right\rfloor$
$\mathcal{L}_{\mathbf{s}}$ (or $\mathcal{L}$ [13])	p^m-1	M	$3\sqrt{L+1}+5$	$\frac{(M-1)^2(L-2)}{2}+\frac{M(M-1)}{2}$
$\mathcal{G}_{\mathbf{s}}^{(\delta,2)}, \delta\neq 0$ (in this paper)	p^m-1	M	$4\sqrt{L+1}+8$	$(M-1)+\frac{(L-2)(L-4)}{8}\cdot(M^2-3M+3)$
$\mathcal{H}_{\mathbf{s}}^{(2)}$ (in this paper)	p^m-1	M	$5\sqrt{L+1}+7$	$(M-1)+\frac{(L-2)(L-4)}{8}\cdot(M-1)^3$

Remark 6: A similar generalization as $\mathcal{H}_{\mathbf{s}}^{(k)}$ has been discussed in Remark 2 of [13], where it was shown that the maximum correlation magnitude is $(2k+1)\sqrt{p^m}+(k+2)^2$. However, it is not clear how to construct a sequence family from the generalization. In this paper, we presented a specific sequence family $\mathcal{H}_{\mathbf{s}}^{(k)}$ by determining the cyclic distinctness, the maximum correlation magnitude, and the family size. Moreover, we obtain the improved bound on the correlation magnitude given by (22).

V. CONCLUSION

This paper has revisited polyphase sequence families constructed from the shift and addition of power residue and Sidelnikov sequences. Initially, we assumed $\psi(0)=1$ to represent the sequences without the indicator function. In order to support the assumption, a refinement has been made to the Weil bound on multiplicative character sums, which enables the efficient proofs on the maximum correlation magnitudes of the sequence families. We then presented general constructions of $\mathcal{S}_{\mathbf{r}}^{(\delta)}$ and $\mathcal{S}_{\mathbf{s}}^{(\delta)}$ that produce the known families in [8] as the special cases, and determined the maximum correlation magnitudes and the family sizes. Moreover, we showed that the known M-ary sequence families $\mathcal{F}_{\mathbf{r}}$ in [8] and $\mathcal{L}$ in [13] (or $\mathcal{F}_{\mathbf{s}}$ in [8]) with large size could be partitioned into $(M+1)$ disjoint subsequence families with smaller maximum correlation magnitudes. Finally, more generalized constructions have been provided by the addition of multiple cyclic shifts of power residue and Sidelnikov sequences.

Appendix
Proof of Theorem 6

This section briefly describes the proof of the cyclic distinctness, the maximum correlation magnitudes, and the family sizes of the power residue sequence families of $\mathcal{G}_{\mathbf{r}}^{(\delta,k)}$ and $\mathcal{H}_{\mathbf{r}}^{(k)}$ introduced in Construction 3. The proof of Theorem 7 for the Sidelnikov sequence families $\mathcal{G}_{\mathbf{s}}^{(\delta,k)}$ and $\mathcal{H}_{\mathbf{s}}^{(k)}$ in Construction 4 are straightforward from the similar approaches made to $\mathcal{G}_{\mathbf{r}}^{(\delta,k)}$ and $\mathcal{H}_{\mathbf{r}}^{(k)}$. In what follows, we keep the notations in Construction 3.

A. Cyclic distinctness

We prove the cyclic distinctness of sequences in the large sequence family $\mathcal{H}_{\mathbf{r}}^{(k)}$, which then implies the cyclic distinctness of sequences in $\mathcal{G}_{\mathbf{r}}^{(\delta,k)}$, a subset of $\mathcal{H}_{\mathbf{r}}^{(k)}$. We first consider a sequence pair $\mathbf{a}$ and $\mathbf{b}$ existing in $\mathcal{E}_{\mathbf{r}}^{(k)}$, where $E_{\mathbf{a},\mathbf{b}}(\tau)$ is defined by

$$\begin{aligned} E_{\mathbf{a},\mathbf{b}}(\tau) &= \omega_M^{c_0 r(t)+c_1 r(t+l_1)+\cdots c_k r(t+l_k)-c'_0 r(t+\tau)-c'_1 r(t+l'_1+\tau)-\cdots-c'_k(t+l'_k+\tau)} \\ &= \psi^{c_0}(x)\psi^{c_1}(x+l_1)\cdots\psi^{c_k}(x+l_k)\psi^{-c'_0}(x+\tau)\psi^{-c'_1}(x+l'_1+\tau)\cdots\psi^{-c'_k}(x+l'_k+\tau) \end{aligned} \tag{23}$$

where $x \in \mathbb{F}_p$ and $0 \le \tau \le p-1$. In (23), let $\Lambda = \{0, -l_1, \cdots, -l_k, -\tau, -l'_1-\tau, \cdots, -l'_k-\tau\}$ be a set of roots of the polynomials in the argument of each ψ. For $x \notin \Lambda$, (23) is represented as

$$\begin{aligned} E_{\mathbf{a},\mathbf{b}}(\tau) &= \psi\left(x^{c_0}(x+l_1)^{c_1}\cdots(x+l_k)^{c_k}(x+\tau)^{M-c'_0}(x+l'_1+\tau)^{M-c'_1}\cdots(x+l'_k+\tau)^{M-c'_k}\right) \\ &= \psi\left(g(x)\right), \quad x \in \mathbb{F}_p \setminus \Lambda. \end{aligned}$$

For given c_i, c'_j, l_i, l'_j, and τ, if the sequence pair $\mathbf{a}$ and $\mathbf{b}$ are cyclically equivalent, then $g(x) = h(x)^M$ so that $\psi\left(g(x)\right)$ may be a trivial character for all x's in $\mathbb{F}_p \backslash \Lambda$, where $h(x) \in \mathbb{F}_p[x]$. For the cyclic distinctness, therefore, we need to show $g(x) \neq h(x)^M$ for the pair $\mathbf{a}$ and $\mathbf{b}$. From $1 \le c_0, \cdots, c_k, c'_0, \cdots, c'_k \le M-1$, note that any factor $(x+l_i)^{c_i}$ or $(x+\tau+l'_j)^{M-c'_j}$ of $g(x)$ is not of the form $h'(x)^M$ for $h'(x) \in \mathbb{F}_p[x]$, where $0 \leq i, j \leq k$ and $l_0 = l'_0 = 0$ is assumed. Thus, if it remains in $g(x)$, not combined to the others, then the isolated factor causes $g(x) \neq h(x)^M$.

Case 1. $\tau = 0$: Since $l_1 < l_2 < \cdots < l_k$ and $l'_1 < l'_2 < \cdots < l'_k$, no factors remain isolated in $g(x)$ if and only if $l_1 = l'_1, l_2 = l'_2, \cdots, l_k = l'_k$. In this case, $g(x) = x^{c_0+M-c'_0}(x+l_1)^{c_1+M-c'_1} \cdots (x+l_k)^{c_k+M-c'_k}$, where each exponent $c_i + M - c'_i \equiv 0 \pmod{M},\ 0 \leq i \leq k$, if and only if $c_0 = c'_0, c_1 = c'_1, \cdots, c_k = c'_k$. Clearly, $g(x) = h(x)^M$ if and only if $l_1 = l'_1, l_2 = l'_2, \cdots, l_k = l'_k$ and $c_0 = c'_0, c_1 = c'_1, \cdots, c_k = c'_k$, where $\mathbf{a} = \mathbf{b}$, a trivial case.

Case 2. $\tau \neq 0$: Let $1 \leq l_i, l'_j \leq \frac{p-1}{2}$ where $1 \leq i, j \leq k$. Obviously, $l_i + l'_j \not\equiv 0 \pmod{p}$ for any i and j, which never allows $l_i \equiv \tau \pmod{p}$ and $l'_j \equiv -\tau \pmod{p}$ at the same time. In other words, for a given $\tau \neq 0$,

$$l_i \not\equiv \tau \pmod{p} \text{ for any } i, \quad \text{ or } \quad l'_j + \tau \not\equiv 0 \pmod{p} \text{ for any } j. \tag{24}$$

If $l'_j + \tau \not\equiv 0 \pmod{p}$ for any j, then the factor x cannot be identical to $(x + l'_j + \tau)$ for any j. On the other hand, if $l_i \not\equiv \tau \pmod{p}$ for any i, then the factor $(x+\tau)$ cannot be identical to $(x + l_i)$ for any i. Since one case of (24) always occurs for a given $\tau \neq 0$, at least one factor x^{c_0} (or $(x+\tau)^{c'_0}$) remains isolated in $g(x)$, not combined to the others, which causes $g(x) \neq h(x)^M$ from $1 \leq c_0, c'_0 \leq M-1$.

From Cases 1 and 2, it is clear that $\psi(g(x))$ is nontrivial and $E_{\mathbf{a},\mathbf{b}}(\tau) \neq 1$ for all x's in $\mathbb{F}_p$. Thus, each sequence pair in $\mathcal{E}_{\mathbf{r}}^{(k)}$ is cyclically distinct. If $\mathbf{a} \in \mathcal{I}_{\mathbf{r}}$ and $\mathbf{b} \in \mathcal{E}_{\mathbf{r}}^{(k)}$ (or vice versa), we make the similar approach to $E_{\mathbf{a},\mathbf{b}}(\tau)$, which leads to the cyclic distinctness. Finally, all sequences in $\mathcal{H}_{\mathbf{r}}^{(k)}$ are cyclically distinct, which induces the cyclic distinctness of sequences in $\mathcal{G}_{\mathbf{r}}^{(\delta,k)}$, a subset of $\mathcal{H}_{\mathbf{r}}^{(k)}$.

B. Maximum correlation magnitude

The worst case of the correlation of a pair of sequences in $\mathcal{H}_{\mathbf{r}}^{(k)}$ (or $\mathcal{G}_{\mathbf{r}}^{(\delta,k)}$) occurs when $\mathbf{a}, \mathbf{b} \in \mathcal{E}_{\mathbf{r}}^{(k)}$ (or $\mathcal{D}_{\mathbf{r}}^{(\delta,k)}$). Then, the correlation is given by

$$\begin{aligned} C_{\mathbf{a},\mathbf{b}}(\tau) &= \sum_{t=0}^{p-1} \omega_M^{c_0 r(t) + c_1 r(t+l_1) + \cdots c_k r(t+l_k) - c'_0 r(t+\tau) - c'_1 r(t+l'_1+\tau) - \cdots - c'_k (t+l'_k+\tau)} \\ &= \sum_{x \in \mathbb{F}_p} \psi_0(x)\psi_1(x+l_1)\cdots\psi_k(x+l_k)\psi_{k+1}(x+\tau)\psi_{k+2}(x+l'_1+\tau)\cdots\psi_{2k+1}(x+l'_k+\tau) \end{aligned}$$

where $\psi_0 = \psi^{c_0},\ \psi_1 = \psi^{c_1}, \cdots, \psi_k = \psi^{c_k},\ \psi_{k+1} = \psi^{-c'_0} = \psi^{M-c'_0}, \cdots, \psi_{2k+1} = \psi^{-c'_k} = \psi^{M-c'_k}$, and $f_0(x) = x,\ f_1(x) = x + l_1, \cdots, f_k(x) = x + l_k,\ f_{k+1}(x) = x + \tau, \cdots, f_{2k+1}(x) = x + l'_k + \tau$. Assume $\tau \neq 0$ if $\mathbf{a} = \mathbf{b}$. Then, the cyclic distinctness of $\mathbf{a}$ and $\mathbf{b}$ guarantees that the product character $\prod_{i=0}^{2k+1} \psi_i(f_i(x))$ is nontrivial. From the notations of Corollary 1, $d_i = 1$ and $e_i = 1$ for $0 \leq i \leq 2k+1$.

If $\mathbf{a},\mathbf{b} \in \mathcal{E}_{\mathbf{r}}^{(k)}$, from (9),

$$|C_{\mathbf{a},\mathbf{b}}(\tau)| \leq (\sum_{i=0}^{2k+1} d_i - 1)\sqrt{p} + \sum_{i=0}^{2k+1} e_i = (2k+1)\cdot\sqrt{p} + 2k + 2 = C_{\max}(\mathcal{H}_{\mathbf{r}}^{(k)}).$$

If $\mathbf{a},\mathbf{b} \in \mathcal{D}_{\mathbf{r}}^{(\delta,k)}$, on the other hand, then $\sum_{i=0}^{k} c_i \equiv \sum_{i=0}^{k} c_i' \equiv \delta \pmod{M}$, and thus

$$\prod_{i=0}^{2k+1} \psi_i^{d_i}(x) = \psi^{c_0+c_1+\cdots+c_k-c_0'-c_1'-\cdots-c_k'}(x) = 1$$

for all $x \in \mathbb{F}_p^*$. From (10), therefore,

$$|C_{\mathbf{a},\mathbf{b}}(\tau)| \leq (\sum_{i=0}^{2k+1} d_i - 2)\sqrt{p} + \sum_{i=0}^{2k+1} e_i + 1 = 2k\sqrt{p} + 2k + 3 = C_{\max}(\mathcal{G}_{\mathbf{r}}^{(\delta,k)}).$$

C. Family size

The family size of $\mathcal{H}_{\mathbf{r}}^{(k)}$ in (21) is straightforward from the possible number of $(l_1,\cdots,l_k)$ and $(c_0,\cdots,c_k)$, where $1 \leq l_1 < l_2 < \cdots < l_k \leq \frac{p-1}{2}$ and $1 \leq c_0,\cdots,c_k \leq M-1$. Before proving the family size of $\mathcal{G}_{\mathbf{r}}^{(\delta,k)}$ in (21), we consider the following lemma.

Lemma 5: For a positive integer $k \geq 1$, let $c_i,\ 0 \leq i \leq k$ be positive integers such that $\sum_{i=0}^{k} c_i = c_0 + c_1 + \cdots + c_k \equiv \delta \pmod{M}$ where $1 \leq c_0,\cdots,c_k \leq M-1$. For a given integer $\delta,\ 0 \leq \delta \leq M-1$, the number of the $(c_0, c_1,\cdots,c_k)$ pairs is given by

$$N_k^{(\delta)} = \begin{cases} \frac{(M-1)^{k+1}+(-1)^k}{M} - (-1)^k, & \text{if } \delta = 0 \\ \frac{(M-1)^{k+1}+(-1)^k}{M}, & \text{if } 1 \leq \delta \leq M-1. \end{cases}$$

Proof: **Case 1.** $\delta = 0$: If $k = 1$, then $N_1^{(0)} = M-1$ from Lemma 1. If $k > 1$, then $c_0 + c_1 + \cdots c_k \equiv 0 \pmod{M}$ and thus $c_k \equiv -c_0 - c_1 - \cdots - c_{k-1} \pmod{M}$, where the case of $c_0 + c_1 + \cdots + c_{k-1} \equiv 0 \pmod{M}$ must be excluded to avoid $c_k = 0$. Clearly, if $k > 1$,

$$N_k^{(0)} = (M-1)^k - N_{k-1}^{(0)}.$$

Starting from $N_1^{(0)} = M-1$, we easily get

$$\begin{aligned} N_k^{(0)} &= (M-1)^k - (M-1)^{k-1} + (M-1)^{k-2} - \cdots - (-1)^k \cdot (M-1) \\ &= \frac{(M-1)^{k+1} - (-1)^k \cdot (M-1)}{M} \\ &= \frac{(M-1)^{k+1} + (-1)^k}{M} - (-1)^k. \end{aligned}$$

If $k = 1$, then $N_1^{(0)} = \frac{(M-1)^2-1}{M} + 1 = M - 1 = N_{c_0,c_1}^{(0)}$ in (12).

Case 2. $1 \le \delta \le M-1$: If $k=1$, then $N_1^{(\delta)} = M-2$ from Lemma 1. Similar to Case 1, the case of $c_0 + \cdots + c_{k-1} \equiv 0 \pmod{M},\ k>1$ must be excluded in considering $c_0 + c_1 + \cdots + c_k \equiv 0 \pmod{M}$. From this,

$$N_k^{(\delta)} = (M-1)^k - N_{k-1}^{(\delta)}.$$

Starting from $N_1^{(0)} = M-2$, $N_k^{(\delta)}$ is determined by

$$\begin{aligned} N_k^{(\delta)} &= (M-1)^k - (M-1)^{k-1} + (M-1)^{k-2} - \cdots - (-1)^k \cdot (M-1) + (-1)^k \\ &= N_k^{(0)} + (-1)^k = \frac{(M-1)^{k+1} + (-1)^k}{M}. \end{aligned}$$

If $k=1$, then $N_1^{(\delta)} = \frac{(M-1)^2-1}{M} = M-2 = N_{c_0,c_1}^{(\delta)}$ in (12).

From Cases 1 and 2, the proof is completed. □

In Construction 3, $\left|\mathcal{G}_{\mathbf{r}}^{(\delta,k)}\right| = |\mathcal{I}_{\mathbf{r}}| + \left|\mathcal{D}_{\mathbf{r}}^{(\delta,k)}\right|$, where $\left|\mathcal{D}_{\mathbf{r}}^{(\delta,k)}\right| = N_k^{(\delta)} \cdot \binom{\frac{p-1}{2}}{k}$ from Lemma 5 and $1 \le l_1 < l_2 < \cdots < l_k \le \frac{p-1}{2}$. Hence, the family size of $\mathcal{G}_{\mathbf{r}}^{(\delta,k)}$ in (21) is immediate.

References

[1] S. W. Golomb and G. Gong, *Signal Design for Good Correlation - for Wireless Communication, Cryptography and Radar*. Cambridge University Press, 2005.

[2] G. Gong, "New designs for signal sets with low cross correlation, balance property, and large linear span: GF(p) case," *IEEE Trans. Inf. Theory*, vol. 48, no. 11, pp. 2847-2867, Nov. 2002.

[3] G. Gong, "Constructions of multiple shift-distinct signal sets with low correlation," *Proceedings of International Symposium on Information Theory (ISIT 2007)*, pp. 2306-2310, Nice, France, June 2007.

[4] G. Gong, "Correlation of multiple bent function signal sets," *Proceedings of 2007 IEEE Information Theory Workshop on Information Theory for Wireless Networks*, pp. 1-5, Bergen, Norway, July 2007.

[5] D. H. Green and P. R. Green, "Polyphase related-prime sequences," *IEE Proceedings, Compute. Digit. Tech.*, vol. 148, no. 2, pp. 53-62, Mar. 2001.

[6] Z. Guohua and Z. Quan, "Pseudonoise codes constructed by Legendre sequence," *Electron. Lett.*, vol. 38, pp. 376-377, Apr. 2002.

[7] Y. K. Han and K. Yang, "New M-ary power residue sequence families with low correlation," *in Proc. of IEEE Int. Symp. Information Theory (ISIT2007)*, pp. 2616-2620, Nice, France, Jun. 2007.

[8] Y. K. Han and K. Yang, "New M-ary sequence families with low correlation and large size," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1815-1823, Apr. 2009.

[9] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discrete Math.*, vol. 16, pp. 209-232, 1976.

[10] T. Helleseth and P. V. Kumar, *Sequences with Low Correlation*. A chapter in *Handbook of Coding Theory*. Edited by V. Pless and C. Huffman. Elsevier Science Publishers, 1998.

[11] Y.-J. Kim, H.-Y. Song, G. Gong, and H. Chung, "Crosscorrelation of q-ary power residue sequences of period p," *in Proc. of IEEE Int. Symp. Information Theory (ISIT2006)*, pp. 311-315, Seattle, WA, Jul. 2006.

[12] Y.-J. Kim and H.-Y. Song, “Cross correlation of Sidel’nikov sequences and their constant multiples,” *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 1220-1224, Mar. 2007.

[13] Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, “New families of M-ary sequences with low correlation constructed from Sidel’nikov sequences,” *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3768-3774, Aug. 2008.

[14] P. V. Kumar, *On Bent Sequences and Generalized Bent Functions*, Ph. D. Dissertation, Univ. Southern Calif., Los Angeles, CA, 1983.

[15] P. V. Kumar, T. Helleseth, A. R. Calderbank, and A. R. Hammons Jr., “Large families of quaternary sequences with low correlation,” *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 579-592, Mar. 1996.

[16] P. V. Kumar and O. Moreno, “Prime-phase sequqences with periodic correlation properties better than binary sequences,” *IEEE Trans. Inf. Theory*, vol. 37, no. 3, pp. 603-616, May 1991.

[17] A. Lempel, M. Cohn, and W. Eastman, “A class of balanced binary sequences with optimal autocorrelation property,” *IEEE Trans. Inf. Theory*, vol. IT-23, no. 1, pp. 38-42, Jan. 1977.

[18] R. Lidl and H. Niederreiter, *Finite Fields*, in *Encyclopedia of Mathematics and Its Applications*, vol. 20, Cambridge University Press, 1997.

[19] K. G. Paterson, “Applications of exponential sums in communication theory,” *Lecture Notes in Computer Sciences (LNCS)*, vol. 1746, Springer-Verlag, pp. 1-24, 1999.

[20] J. J. Rushanan, “Weil sequences: A family of binary sequences with good correlation properties,” *in Proc. of IEEE Int. Symp. Information Theory (ISIT2006)*, pp. 1648-1652, Seattle, WA, Jul. 2006.

[21] V. M. Sidelnikov, “Some k-valued pseudo-random sequences and nearly equidistant codes,” *Probl. Inf. Transm.*, vol. 5, pp. 12-16, 1969.

[22] V. M. Sidelnikov, “On mutual correlation of sequences,” *Soviet Math. Dokl.*, vol. 12, no. 1, pp. 197-201, 1971.

[23] H. M. Trachtenberg, *On the Cross-Correlation Functions of Maximal Linear Sequences*, Ph. D. Dissertation, Univ. Southern Calif., Los Angeles, CA, 1970.

[24] D. Wan, “Generators and irreducible polynomials over finite fields,” *Math. Comput.*, vol. 66, no. 219, pp. 1195-1212, Jul. 1997.

[25] A. Weil, *Basic Number Theory*, 3rd. Ed., Springer-Verlag, 1974.