New Polyphase Sequence Families with Low Correlation Derived from the Weil Bound of Exponential Sums

Zilong Wang[1], Guang Gong[1] and Nam Yul Yu[2]
[1]Department of Electrical and Computer Engineering, University of Waterloo
Waterloo, ON. N2L 3G1, Canada
[2]Department of Electrical Engineering, Lakehead University
Thunder Bay, ON, Canada
Email: wzlmath@gmail.com ggong@uwaterloo.ca nam.yu@lakeheadu.ca

Abstract

In this paper, the sequence families of which maximum correlation is determined by the Weil bound of exponential sums are revisited. Using the same approach, two new constructions with large family sizes and low maximum correlation are given. The first construction is an analogue of one recent result derived from the interleaved structure of Sidel'nikov sequences. For a prime p and an integer $M|(p-1)$, the new M-ary sequence families of period p are obtained from irreducible quadratic polynomials and known power residue-based sequence families. The new sequence families increase family sizes of the known power residue-based sequence families, but keep the maximum correlation unchanged. In the second construction, the sequences derived from the Weil representation are generalized, where each new sequence is the element-wise product of a modulated Sidel'nikov sequence and a modulated trace sequence. For positive integers $d < p$ and $M|(p^n-1)$, the new family consists of $(M-1)p^{nd}$ sequences with period p^n-1, alphabet size Mp, and the maximum correlation bounded by $(d+1)\sqrt{p^n}+3$.

Index Terms. Character, correlation, exponential sum, m-sequences, power residue sequences, Sidel'nikov sequences, Weil bound.

1 Introduction

Sequences with low correlation are widely used in wireless communications for acquiring the correct timing information as well as distinguishing multiple users or channels with low mutual interference. It is desirable for sequences to have variable alphabet sizes for adaptive modulation schemes. This would 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.

The trade-offs among the different parameters of a sequence family, such as period, alphabet size, family size and the maximum correlation were studied by Welch [1] and Sidel'nikov [2]. The research for constructing sequences with the desired parameters has flourished in the literature. A brief review

is referred to Kumar and Helleseth's chapter [3], and Golomb and Gong's book [4].

For sequence families with large size and low correlation determined by the Weil bound [5][6] of exponential sums over finite fields, we can classify them into the following two classes according to the types of exponential sums.

The first class is derived from the bound of additive character sums, such as Frank-Zadoff-Chu (FZC) sequences [7, 8], Alltop sequences [9], and p-ary trace sequences. An in-depth review of the applications of character sums for binary trace sequences was given by Paterson in [10]. Furthermore, the general applications to p-ary trace sequences have also been considered, where the correlation properties are improved for $p > 2$. An analogue of the Weil bound over Galois rings was studied by Kumar, Helleseth and Calderbank in [11]. Also, Kumar, Helleseth, Calderbank, and Hammons designed $\mathbb{Z}_4$ sequence families in [12], which provide the largest family sizes for the given maximum correlation among all known sequence families.

The second class is derived from the bound of multiplicative character sums, such as power residue and Sidel'nikov sequences [13]. After the studies of correlation properties of M-ary power residue and Sidel'nikov sequences by scaling in [14, 15], power residue-based and Sidel'nikov-based sequence families were constructed in [16, 17, 18]. Recently, Yu and Gong [19] studied the interleaved structure of Sidel'nikov sequences, and constructed the sequence families which have lager family sizes than the Sidel'nikov-based sequence families in [16, 17] with the same maximum correlation. In this paper, we propose analogous families constructed from irreducible quadratic polynomials and known power residue-based sequence families, where the new families have the larger family sizes than known ones in [17] with the identical maximum correlation.

By utilizing the Weil representation, a sequence family with desired properties such as low correlation, flat Fourier spectra, and low ambiguity function was proposed by Gurevich, Hadina and Sochen [20]. Later on, Wang and Gong [21] found a simple construction for these sequences by the element-wise product of the modulated power residue and FZC sequences. Shortly after that, Schmidt [22] gave a direct proof for this construction by the Weil bound of hybrid character sums. One drawback of this sequence family is that the alphabet size, Mp, is larger than the period p where $M|(p-1)$. In this paper, we generalize this construction by extending the finite field $\mathbb{F}_p$ to $\mathbb{F}_{p^n}$, where each new sequence is the element-wise product of a modulated Sidel'nikov sequence and a modulated trace sequence. For positive integers $d < p$ and $M|(p^n-1)$, the new family consists of $(M-1)p^{nd}$ sequences with period p^n-1, alphabet size Mp, and the maximum correlation is bounded by $(d+1)\sqrt{p^n}+3$.

The rest of the paper is organized as follows. In Section 2, we introduce some basic notations, definitions and the Weil bound of additive, multiplicative, and hybrid character sums with polynomial arguments. In Section 3, we provide an interpretation of polyphase sequence families with low correlation and their corresponding polynomials in character sums. In Section 4, we present two new

constructions along with proofs of their properties on correlation and family sizes. In Section 5, comparisons between the constructions in this paper and various related sequence families are given. The maximum magnitudes of discrete Fourier spectra and ambiguity functions are also obtained by using the Weil bound in this section. Section 6 concludes the paper.

2 Preliminaries

This section introduces some basic definitions and concepts used in this paper.

2.1 Notations and Definitions

- $q = p^n$ where p is prime and n is a positive integer. $\mathbb{F}_q$ is a finite field with q elements, and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ is the multiplicative group of $\mathbb{F}_q$. α is a primitive element in $\mathbb{F}_q$. The algebraic closure of $\mathbb{F}_q$ is denoted by $\overline{\mathbb{F}}_q$.

- Define the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ as $Tr(x) = x + x^p + x^{p^2} \cdots + x^{p^{n-1}}$ for $x \in \mathbb{F}_{p^n}$.

- A *logarithm* over $\mathbb{F}_q^*$ is defined by

$$\log_\alpha x = t \text{ (for } x = \alpha^t,\ 0 \le t \le q-2),$$

  or simply as $\log x$ if the context is clear. We extend the definition to $\log 0 = 0$ in this paper.

- For a positive integer M, $\mathbb{Z}_M$ is a residue ring modulo M, and $\omega_M = e^{\frac{2\pi\sqrt{-1}}{M}}$ is a primitive complex M-th root of unity.

- $\mathbf{a} = \{a(t)\}_{t \geqslant 0}$ where $a(t) \in \mathbb{Z}_M$, is called an M-ary sequence. If $M = p$, it is called a p-ary sequence. $\mathbf{a}' = \{a'(t)\}_{t \geqslant 0} = \{\omega_M^{a(t)}\}_{t \geqslant 0}$ is called the *modulated sequence* of $\mathbf{a}$.

- Denote $\mathbb{F}_q[x]$ as the polynomial ring over field $\mathbb{F}_q$, and $\deg(f)$ as the degree of polynomial $f(x) \in \mathbb{F}_q[x]$.

The operators of *decimation* D_s and *(time) shift* L_τ on sequence $\mathbf{a} = \{a(t)\}$ are defined as $D_s(\mathbf{a}) = \{a(st)\}$ and $L_\tau(\mathbf{a}) = \{a(t+\tau)\}$ respectively. For a pair of sequences $\mathbf{a} = \{a(t)\}$ and $\mathbf{b} = \{b(t)\}$ with period N, the correlation function between $\mathbf{a}$ and $\mathbf{b}$ is defined by

$$C_{\mathbf{a},\mathbf{b}}(\tau) = < \mathbf{a}', L_\tau(\mathbf{b}') > = \sum_{t=0}^{N-1} a'(t)\overline{b'(t+\tau)}, \quad 0 \leqslant \tau \leqslant N-1. \tag{1}$$

If $\mathbf{a} = \mathbf{b}$, then the correlation function becomes the *autocorrelation* function, denoted as $C_{\mathbf{a}}(\tau)$. We call $C_{\mathbf{a}}(\tau)$ the *out-of-phase autocorrelation* of $\mathbf{a}$ for $\tau \neq 0$. Let $\mathcal{S}$ be a set consisting of L distinct M-ary sequences of period N. The maximum correlation of $\mathcal{S}$ is defined by

$$C_{\max}(\mathcal{S}) = \max\{|C_{\mathbf{a},\mathbf{b}}(\tau)| : \mathbf{a}, \mathbf{b} \in \mathcal{S}, 0 \leqslant \tau \leqslant N-1, \tau \neq 0 \text{ if } \mathbf{a} = \mathbf{b}\}. \tag{2}$$

Then, the set $\mathcal{S}$ is called an M-ary sequence family of period N with the family size L and the maximum correlation $C_{\max}(\mathcal{S})$. Note that the maximum correlation of $\mathcal{S}$ is defined as the maximum magnitude of correlation values of any pair of sequences in $\mathcal{S}$.

2.2 Characters and Weil Bounds over Finite Fields

Definition 1 *(**Additive character**) For each $\beta \in \mathbb{F}_q^*$, a nontrivial additive character of $\mathbb{F}_q$ is defined by*

$$\psi(x) = \omega_p^{Tr(\beta \cdot x)}, \ \forall x \in \mathbb{F}_q.$$

Definition 2 *(**Multiplicative Character**) For $M|(q-1)$ and each $j = 1, 2, \cdots, M-1$, a nontrivial multiplicative character of $\mathbb{F}_q^*$ of order M is defined by*

$$\chi(\alpha^k) = \omega_M^{jk}, \ \forall \alpha^k \in \mathbb{F}_q^*,$$

which is equivalent to

$$\chi(x) = \omega_M^{(j \log_\alpha x) \bmod M}, \ \forall x \in \mathbb{F}_q^*.$$

The definition is conventionally extended to $\chi(0) = 0$ for every nontrivial χ.

The following Weil bounds of exponential sums are presented in [5, 6]. The special case for $M|\deg(g)$ is improved in [23].

Fact 1 *Let ψ be a nontrivial additive character of $\mathbb{F}_q$ and $f(x) \in \mathbb{F}_q[x]$ with $deg(f) = d \geqslant 1$ and* $\gcd(d, q) = 1$. *Then*

$$\left| \sum_{x \in \mathbb{F}_q} \psi(f(x)) \right| \leqslant (d-1)\sqrt{q}.$$

Fact 2 *Let χ be a nontrivial multiplicative character of $\mathbb{F}_q$ with order M. For $g(x) \in \mathbb{F}_q[x]$ where $g(x) \neq c \cdot h^M(x)$ for some $c \in \mathbb{F}_q$ and $h(x) \in \mathbb{F}_q[x]$, let s be the number of distinct roots of $g(x)$ in $\overline{\mathbb{F}}_q$. Then*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(g(x)) \right| \leqslant \begin{cases} (s-1)\sqrt{q}, \\ (s-2)\sqrt{q} + 1, & \text{if } M|deg(g). \end{cases}$$

Fact 3 *Let ψ be a nontrivial additive character of $\mathbb{F}_q$, and χ be a nontrivial multiplicative character of $\mathbb{F}_q$ with order M. Let $f(x) \in \mathbb{F}_q[x]$ with degree d, and $g(x) \in \mathbb{F}_q[x]$ with $g(x) \neq c \cdot h^M(x)$ and s distinct roots in $\overline{\mathbb{F}}_q$. Then*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(g(x))\psi(f(x)) \right| \leqslant (d+s-1)\sqrt{q}.$$

2.3 Bounds for Correlation of Sequences

In this paper, we will apply Facts 1-3 to determine the maximum correlation of sequences. For Facts 2 and 3, we will adopt the definition $\chi(0) = 1$ as shown in [18] which agrees with our assumption $\log 0 = 0$. Then the results in Facts 2 and 3 can be refined as follows to support $\chi(0) = 1$.

Corollary 1 *([18]) With the notations in Fact 2 and the assumption $\chi(0) = 1$, let e be the number of distinct roots of $g(x)$ in $\mathbb{F}_q$. Then*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(g(x)) \right| \leqslant \begin{cases} (s-1)\sqrt{q} + e, \\ (s-2)\sqrt{q} + e + 1, & \text{if } M | deg(g). \end{cases} \tag{3}$$

Considering the exponential sum for $x \in \mathbb{F}_q^*$, we have

$$\left| \sum_{x \in \mathbb{F}_q^*} \chi(g(x)) \right| \leqslant \begin{cases} (s-1)\sqrt{q} + e - 1, \\ (s-2)\sqrt{q} + e, & \text{if } M | deg(g), \end{cases} \tag{4}$$

where $x | g(x)$, and

$$\left| \sum_{x \in \mathbb{F}_q^*} \chi(g(x)) \right| \leqslant \begin{cases} (s-1)\sqrt{q} + e + 1, \\ (s-2)\sqrt{q} + e + 2, & \text{if } M | deg(g), \end{cases} \tag{5}$$

where $x \nmid g(x)$.

Corollary 2 *With the notations in Fact 3 and the assumption $\chi(0) = 1$, let e be the number of distinct roots of $g(x)$ in $\mathbb{F}_q$. Then*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(g(x))\psi(f(x)) \right| \leqslant \ (d+s-1)\sqrt{q} + e. \tag{6}$$

Considering the exponential sum for $x \in \mathbb{F}_q^*$, we have

$$\left| \sum_{x \in \mathbb{F}_q^*} \chi(g(x))\psi(f(x)) \right| \leqslant \begin{cases} (d+s-1)\sqrt{q} + e - 1, & \text{if } x | g(x), \\ (d+s-1)\sqrt{q} + e + 1, & \text{if } x \nmid g(x). \end{cases} \tag{7}$$

3 Revisit to Known Sequences

In this section, we present the relationships among the correlation of sequences, their associated polynomials and exponential sums, and then revisit known polyphase sequence families according to the Weil bound of exponential sums.

3.1 Sequences, Polynomials and Correlation

The sequence $\{a(t)\}_{t\geqslant 0}$ associated with polynomial $f(x) \in \mathbb{F}_q[x]$ ($q = p$ or $q = p^n$) can be classified into the following two cases. Recall that ψ is a nontrivial additive character of $\mathbb{F}_q$, and χ is a nontrivial multiplicative character of $\mathbb{F}_q$ with order M.

The first class is derived from the additive character of finite field $\mathbb{F}_q$.

A-1. $f(x) \in \mathbb{F}_p[x]$: $a(t) = f(t)$ and $a'(t) = \omega_p^{f(t)} = \psi(f(t))$ represent the t-th element of a p-ary sequence of period p and its modulated version, respectively. For example, Alltop sequences [9] of period $N = p$ have $f(x) = cx^2, c \in \mathbb{F}_p^*$. Note that this is equivalent to FZC sequences [7, 8] of period $N = p$.

A-2. $f(x) \in \mathbb{F}_q[x]$: $a(t) = Tr(f(\alpha^t))$ and $a'(t) = \omega_p^{Tr(f(\alpha^t))} = \psi(f(\alpha^t))$ represent the t-th element of a p-ary sequence of period $q-1$ and its modulated version, respectively. For example, m-sequences have $f(x) = cx, c \in \mathbb{F}_q^*$.

The second class is derived from the multiplicative character of finite field $\mathbb{F}_q$.

M-1. $f(x) \in \mathbb{F}_p[x]$: $a(t) \equiv \log_\alpha(f(t)) \pmod M$ and $a'(t) = \omega_M^{\log(f(t))} = \chi(f(t))$ represent the t-th element of an M-ary sequence of period p and its modulated version, respectively, where α is a primitive element in $\mathbb{F}_p$ and $M|(p-1)$. For example, power residue sequences [13] have $f(x) = x$.

M-2. $f(x) \in \mathbb{F}_q[x]$: $a(t) \equiv \log_\alpha(f(\alpha^t)) \pmod M$ and $a'(t) = \omega_M^{\log(f(\alpha^t))} = \chi(f(\alpha^t))$ represent the t-th element of an M-ary sequence of period $q-1$ and its modulated version, respectively, where α is a primitive element in $\mathbb{F}_q$ and $M|(q-1)$. For example, Sidel'nikov sequences [13] have $f(x) = x+1$.

We can define another class of sequences by element-wise product of modulated version of sequences in class A-1 and M-1, or class A-2 and M-2. Let $\{a(t)\}_{t\geqslant 0}$ be a sequence associated with polynomials $g(x), f(x) \in \mathbb{F}_q[x]$.

H-1. $g(x), f(x) \in \mathbb{F}_p[x]$: $a'(t) = \chi(g(t))\psi(f(t))$ represents the t-th element of a modulated sequence of period p where $M|(p-1)$.

H-2. $g(x), f(x) \in \mathbb{F}_q[x]$: $a'(t) = \chi(g(\alpha^t))\psi(f(\alpha^t))$ represents the t-th element of a modulated sequence of period $q-1$ where $M|(q-1)$.

Note that H-2 is a general form of the sequences in our second new construction which will be introduced in Subsection 4.2.

Table 1: Polynomials, Sequences and Correlation

Class	Field	Alphabet	Period	Modulated sequence	$C_{\mathbf{a},\mathbf{b}}(\tau)$
A-1	$\mathbb{F}_p$	p	p	$\psi(f(t))$	$\sum_{x\in\mathbb{F}_p}\psi(f(x)-g(x+\tau))$
A-2	$\mathbb{F}_q$	p	$q-1$	$\psi(f(\alpha^t))$	$\sum_{x\in\mathbb{F}_q^*}\psi(f(x)-g(\alpha^\tau x))$
M-1	$\mathbb{F}_p$	$M\|(p-1)$	p	$\chi(f(t))$	$\sum_{x\in\mathbb{F}_p}\chi(f(x)g(x+\tau)^{M-1})$
M-2	$\mathbb{F}_q$	$M\|(p^n-1)$	$q-1$	$\chi(f(\alpha^t))$	$\sum_{x\in\mathbb{F}_q^*}\chi(f(x)g(\alpha^\tau x)^{M-1})$
H-1	$\mathbb{F}_p$	pM	p	$\chi(g(t))\psi(f(t))$	$\sum_{x\in\mathbb{F}_p}\chi(g_1(x)g_2(x+\tau)^{M-1})\cdot\psi(f_1(x)-f_2(x+\tau))$
H-2	$\mathbb{F}_q$	pM	$q-1$	$\chi(g(\alpha^t))\psi(f(\alpha^t))$	$\sum_{x\in\mathbb{F}_q^*}\chi(g_1(x)g_2(\alpha^\tau x)^{M-1})\cdot\psi(f_1(x)-f_2(\alpha^\tau x))$

Table 1 describes how the correlation of a pair of sequences in each class can be represented by the exponential sum of their associated polynomials. Note that in the last column of Table 1, the relationships between sequences and polynomials are given as follows. For the classes A-1, A-2, M-1 and M-2, sequences $\mathbf{a}$ and $\mathbf{b}$ are associated with polynomials $f(x)$ and $g(x)$, respectively. For the classes H-1 and H-2, sequence $\mathbf{a}$ is associated with polynomials $g_1(x)$ and $f_1(x)$, while sequence $\mathbf{b}$ is associated with polynomials $g_2(x)$ and $f_2(x)$. Then an upper bound of $|C_{\mathbf{a},\mathbf{b}}(\tau)|$ can be obtained by Fact 1 or Corollaries 1 and 2.

3.2 Known Sequence Families with Low Correlation

In this subsection, we revisit known sequence families of which maximum correlation are obtained by the Weil bound.

A. Trace sequences

For a positive integer $d \ll \sqrt{q}$, the sequence family $\mathcal{S}_d$ [2] is represented by

$$\mathcal{S}_d = \{\{Tr(f(\alpha^t)\}_{t\geqslant 0} | f(x) \in \mathcal{F}_d\}$$

where $\mathcal{F}_d = \{\sum_{k=2}^{d} a_k x^k + x | a_k \in \mathbb{F}_q, a_k = 0 \text{ if } p|k\}$. A p-ary trace sequence $\{Tr(f(\alpha^t))\}$ associated with polynomial $f(x) \in \mathbb{F}_q[x]$ can be achieved by decimation, shift and addition of an m-sequence $\{Tr(\alpha^t)\}$. According to the class A-2 in Table 1 and Fact 1, $\mathcal{S}_d$ is a family consisting of $q^{d-1-\lfloor \frac{d}{p} \rfloor}$ sequences with period $q-1$, and $C_{\max}(\mathcal{S}_d) \leqslant (d-1)\sqrt{q}+1$ [2].

B. Scaling, shift-and-addition of power residue and Sidel'nikov sequences

Let $\{u(t)\}$ be an M-ary power residue sequence with period p. Let

$$\mathcal{A}_{1,p} = \{\{cu(t) \pmod M\} | c \in \mathbb{Z}_M \backslash \{0\}\},$$

$$\mathcal{A}_{2,p} = \left\{\{c_0 u(t) + c_1 u(t+l) \pmod M\} | 1 \leqslant l \leqslant \frac{p-1}{2}, c_0, c_1 \in \mathbb{Z}_M \backslash \{0\}\right\}, \text{ and}$$

$$\mathcal{A}_{2,p,\delta} = \{\{c_0 u(t) + c_1 u(t+l)\} \in \mathcal{A}_{2,p} | c_0 + c_1 \equiv \delta \pmod M\}.$$

The modulated version of each sequence in $\mathcal{A}_{2,p}$ is represented by $\{\chi(t^{c_0}(t+l)^{c_1})\}$ which corresponds to polynomial $f(x) = x^{c_0}(x+l)^{c_1}$. Note that $f(x)$ has 2 distinct roots in $\mathbb{F}_p$. According to the class M-1 in Table 1 and Corollary 1-(3), we have $C_{\max}(\mathcal{A}_{1,p}) \leqslant \sqrt{p} + 2$ [14], $C_{\max}(\mathcal{A}_{1,p} \cup \mathcal{A}_{2,p}) \leqslant 3\sqrt{p} + 4$ [17], and $C_{\max}(\mathcal{A}_{1,p} \cup \mathcal{A}_{2,p,\delta}) \leqslant 2\sqrt{p} + 5$ [17].

Let $\{v(t)\}$ be an M-ary Sidel'nikov sequence with period $q-1$. Let

$$\mathcal{C}_{1,q} = \{\{cv(t) \pmod M\} | c \in \mathbb{Z}_M \backslash \{0\}\},$$

$$\mathcal{C}_{2,q} = \left\{\{c_0 v(t) + c_1 v(t+l) \pmod M\} | 1 \leqslant l \leqslant \lfloor \frac{q-1}{2} \rfloor, c_0, c_1 \in \mathbb{Z}_M \backslash \{0\}, c_0 < c_1 \text{ if } l = \frac{q-1}{2}\right\}, \text{ and}$$

$$\mathcal{C}_{2,q,\delta} = \{\{c_0 v(t) + c_1 v(t+l)\} \in \mathcal{C}_{2,q} | c_0 + c_1 \equiv \delta \pmod M\}.$$

The modulated version of each sequence in $\mathcal{C}_{2,q}$ is given by $\{\chi((\alpha^t+1)^{c_0}(\alpha^l\alpha^t+1)^{c_1})\}$ corresponding to polynomial $f(x) = (x+1)^{c_0}(\alpha^l x+1)^{c_1}$ with 2 distinct roots in $\mathbb{F}_q$. According to the class M-2 in Table 1 and Corollary 1-(5), we have $C_{\max}(\mathcal{C}_{1,q}) \leqslant \sqrt{q} + 3$ [15], $C_{\max}(\mathcal{C}_{1,q} \cup \mathcal{C}_{2,q}) \leqslant 3\sqrt{q} + 5$ [16], and $C_{\max}(\mathcal{C}_{1,q} \cup \mathcal{C}_{2,q,\delta}) \leqslant 2\sqrt{q} + 6$ [17].

These power residue-based (or Sidel'nikov-based) sequence families were generalized in [18] where the sequences are associated with polynomials $f(x) = \prod_{i=0}^{d-1}(x+l_i)^{c_i}$ (or $f(x) = \prod_{i=0}^{d-1}(\alpha^{l_i}x+1)^{c_i}$) with d distinct roots in $\mathbb{F}_p$ (or $\mathbb{F}_q$). More details on how to choose proper values of c_i and l_i to obtain low maximum correlation, see [18].

C. The inverse of Sidel'nikov sequences

The inverse of Sidel'nikov sequences was considered in [25]. Let

$$\mathcal{Z}_{1,q} = \{\{cv(-t) \pmod M\} | c \in \mathbb{Z}_M \backslash \{0\}\}, \text{ and}$$

$$\mathcal{Z}_{2,q} = \left\{\{c_0 v(t) + c_1 v(-t+l) \pmod M\} | 1 \leqslant l \leqslant \lfloor \frac{q-1}{2} \rfloor, c_0, c_1 \in \mathbb{Z}_M \backslash \{0\}, c_0 \neq c_1 \text{ if } l = \frac{q-1}{2}\right\}.$$

The modulated version of each sequence in $\mathcal{Z}_{2,q}$ is represented by $\{\chi((\alpha^t)^{M-c_1}(\alpha^t+1)^{c_0}(\alpha^t+\alpha^l)^{c_1})\}$ which corresponds to polynomial $f(x) = x^{M-c_1}(x+1)^{c_0}(x+\alpha^l)^{c_1}$. Note that $f(x)$ has 3 distinct roots in

$\mathbb{F}_q$. According to the class M-2 in Table 1 and Corollary 1-(4), we have $C_{\max}(\mathcal{C}_{1,q} \cup \mathcal{C}_{2,q} \cup \mathcal{Z}_{1,q} \cup \mathcal{Z}_{2,q}) \leqslant 4\sqrt{q} + 4$. (Note that this bound is tighter than the original bound $4\sqrt{q} + 5$ given in [25].) More general sequence families corresponding to polynomials with 3 roots in $\mathbb{F}_q$ were studied in [18] where the family sizes are significantly larger than that in [25].

D. Sequence families constructed by irreducible polynomials over $\mathbb{F}_q$

Yu and Gong [19] studied the interleaved structure of Sidel'nikov sequences. (For interleaved sequences, see [24].) By writing an M-ary Sidel'nikov sequence of period $q^2 - 1$ as a $(q-1) \times (q+1)$ array, they discovered that the column sequences can be generated by irreducible polynomials over $\mathbb{F}_q$. Note that α and β are primitive elements in $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$, respectively. Let

$$\mathcal{D}_{2,q} = \left\{ \{ d \log_\alpha(g_j(\alpha^t)) \pmod M \} | d \in \mathbb{Z}_M \backslash \{0\}, 1 \leqslant j \leqslant \lfloor \frac{q}{2} \rfloor \right\},$$

$$\mathcal{D}_{2,q,0} = \left\{ \{ \frac{M}{2} \log_\alpha(g_j(\alpha^t)) \} \right\} \subset \mathcal{D}_{2,q} \text{ for } M \text{ even, and}$$

$$\mathcal{D}_{2,q,\delta} = \left\{ \{ 2^{-1} \delta \log_\alpha(g_j(\alpha^t)) \} \right\} \subset \mathcal{D}_{2,q} \text{ for } M \text{ odd}, 2^{-1} \in \mathbb{Z}_M, \delta \neq 0,$$

where

$$g_j(x) = (\beta^j x - 1)(\beta^{jq} x - 1) = \beta^{(q+1)j} x^2 - (\beta^j + \beta^{jq}) \cdot x + 1. \tag{8}$$

Then each sequence in $\mathcal{D}_{2,q}$ is associated with polynomial $g_j(x)^d$ with two roots in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. According to the class M-2 in Table 1 and Corollary 1-(5), we have $C_{\max}(\mathcal{C}_{1,q} \cup \mathcal{C}_{2,q} \cup \mathcal{D}_{2,q}) \leqslant 3\sqrt{q} + 5$, and $C_{\max}(\mathcal{C}_{1,q} \cup \mathcal{C}_{2,q,\delta} \cup \mathcal{D}_{2,q,\delta}) \leqslant 2\sqrt{q} + 6$ [24].

E. Sequences from hybrid character of $\mathbb{F}_p$

Using the Weil representation, a sequence family with desired properties was proposed in [20]. Then a simple construction for these sequences which avoids costly group-theoretic computations was found by Wang and Gong [21]. Later on, Schmidt [22] found a direct proof by the Weil bound and gave a generalized construction which can be defined as follows. For positive integers $d \ll \sqrt{p}$ and $M|(p-1)$, the modulated version of a sequence family is given by

$$\Omega_{d,p} = \{ \{ \chi(t^c) \psi(f(t)) \}_{t \geqslant 0} | 1 \leqslant c \leqslant M-1, f(x) \in \mathcal{F}_{d,p} \} \tag{9}$$

where $\mathcal{F}_{d,p} = \{ \sum_{k=1}^{d} a_k x^k | a_k \in \mathbb{F}_p \}$. (Note that $M = p - 1$ in [20][21][22].) $\Omega_{d,p}$ is a sequence family with period p, alphabet size Mp, family size $(M-1)p^d$ and $C_{\max}(\Omega_{d,p}) \leqslant (d+1)\sqrt{p} + 2$ by the class H-1 in Table 1 and Corollary 2-(6).

No known constructions have been reported for the class H-2. We will give a new sequence family which is similar to $\Omega_{d,p}$ in Subsection 4.2.

4 New Constructions

In this section, we present two new constructions of sequence families with good correlation, which are analogous cases to the sequence families presented in Subsection 3.2-(D) and (E).

4.1 Construction 1

Sequences in $\mathcal{C}_{1,q}$, $\mathcal{C}_{2,q}$ and $\mathcal{D}_{2,q}$ defined in Subsection 3.2-(B) and (D) correspond to polynomials in $\mathbb{F}_q[x]$ with one root, two distinct roots in $\mathbb{F}_q$, and two distinct roots in quadratic extension field $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$, respectively. Similar to sequences in $\mathcal{D}_{2,q}$, we employ irreducible quadratic polynomials in $\mathbb{F}_p[x]$ to generate new sequences. Note that α and β are primitive elements in $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$, respectively.

Construction 1: For odd prime p and $M|(p-1)$, define M-ary sequence families of period p as follows.

$$\mathcal{B}_{2,p} = \left\{ \{d \log_\alpha(f_j(t)) \pmod M\} | d \in \mathbb{Z}_M \setminus \{0\}, 1 \leqslant j \leqslant \frac{p-1}{2} \right\},$$

$$\mathcal{B}_{2,p,0} = \left\{ \{\frac{M}{2} \log_\alpha(f_j(t))\} \right\} \subset \mathcal{B}_{2,p} \text{ for even } M, \text{ and}$$

$$\mathcal{B}_{2,p,\delta} = \left\{ \{2^{-1}\delta \log_\alpha(f_j(t))\} \right\} \subset \mathcal{B}_{2,p} \text{ for odd } M, 2^{-1} \in \mathbb{Z}_M, \delta \in \mathbb{Z}_M \setminus \{0\},$$

where

$$f_j(x) = (x - j\beta)(x - j\beta^p) = x^2 - j(\beta + \beta^p)x + j^2\beta^{p+1}. \tag{10}$$

Let $\mathcal{U}_p = \mathcal{A}_{1,p} \cup \mathcal{A}_{2,p} \cup \mathcal{B}_{2,p}$ and $\mathcal{U}_{p,\delta} = \mathcal{A}_{1,p} \cup \mathcal{A}_{2,p,\delta} \cup \mathcal{B}_{2,p,\delta}$ where $\mathcal{A}_{1,p}, \mathcal{A}_{2,p}$ and $\mathcal{A}_{2,p,\delta}$ are defined in Subsection 3.2-(B). Then $\mathcal{U}_p$ and $\mathcal{U}_{p,\delta}$ are new M-ary sequence families with period p.

The modulated version of each sequence in $\mathcal{B}_{2,p}$ is $\{\chi(f_j(t)^d)\}$ corresponding to polynomial $f_j(x)^d$. The maximum correlation of $\mathcal{U}_p$ and $\mathcal{U}_{p,\delta}$ can be obtained by class M-1 in Table 1 and Corollary 1 as shown below.

Theorem 1 *In Construction 1,*

(1) $\mathcal{U}_p$ is an M-ary sequence family of period p with family size $(\frac{p-1}{2}M + 1)(M-1)$ and maximum correlation $C_{\max}(\mathcal{U}_p) \leqslant 3\sqrt{p} + 4$, and

(2) $\mathcal{U}_{p,\delta}$ is an M-ary sequence family of period p with maximum correlation $C_{\max}(\mathcal{U}_{p,\delta}) \leqslant 2\sqrt{p} + 5$. The family size of $\mathcal{U}_{p,\delta}$ is $(\frac{p+1}{2}M - 1)$ for even M and $\delta = 0$, or $\frac{p+1}{2}(M-1)$ for odd M and $\delta \neq 0$.

Proof: We will first derive the maximum correlation of families $\mathcal{U}_p$ and $\mathcal{U}_{p,\delta}$, and then determine their respective family sizes.

(1) Let $f(x)$ and $g(x)$ be polynomials associated with sequences $\mathbf{a}$ and $\mathbf{b}$ in $\mathcal{U}_p$, respectively. According to the class M-1 in Table 1, the correlation of $\mathbf{a}$ and $\mathbf{b}$ at shift τ can be presented as

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{x\in\mathbb{F}_p} \chi(f(x)g(x+\tau)^{M-1}). \tag{11}$$

To determine an upper bound of $C_{\max}(\mathcal{U}_p)$, there are four cases that we need to consider, i.e.,

- Case 1: $\mathbf{a}, \mathbf{b} \in \mathcal{A}_{1,p} \cup \mathcal{A}_{2,p}$. Then $f(x) = x^{d_0}(x+l_1)^{d_1}$ and $g(x) = x^{c_0}(x+l_2)^{c_1}$.
- Case 2: $\mathbf{a} \in \mathcal{B}_{2,p}$, $\mathbf{b} \in \mathcal{A}_{2,p}$. Then $f(x) = f_j(x)^d$ where $f_j(x)$ is defined in (10) and $g(x) = x^{c_0}(x+l)^{c_1}$ for $1 \leqslant c_0, c_1, d \leqslant M-1$.
- Case 3: $\mathbf{a} \in \mathcal{B}_{2,p}$, $\mathbf{b} \in \mathcal{A}_{1,p}$. Then $f(x) = f_j(x)^d$ and $g(x) = x^c$ for $1 \leqslant c, d \leqslant M-1$.
- Case 4: $\mathbf{a}, \mathbf{b} \in \mathcal{B}_{2,p}$. Then $f(x) = f_j(x)^{d_1}$ and $g(x) = f_k(x)^{d_2}$ where $1 \leqslant j, k \leqslant \frac{p-1}{2}$ and $1 \leqslant d_1, d_2 \leqslant M-1$.

Next, we discuss the maximum correlation for each case.

Case 1: This case is a result discussed in [17]. Thus $|C_{\mathbf{a},\mathbf{b}}(\tau)| \leqslant 3\sqrt{p}+4$ for $\mathbf{a} \neq \mathbf{b}$ or $\mathbf{a} = \mathbf{b}, \tau \neq 0$.

Case 2: The correlation function (11) can be rewritten as

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{x\in\mathbb{F}_p} \chi(f_j(x)^d(x+\tau)^{M-c_0}(x+l+\tau)^{M-c_1}). \tag{12}$$

The polynomial argument $f_j(x)^d(x+\tau)^{M-c_0}(x+l+\tau)^{M-c_1}$ in (12) has 4 distinct roots in $\overline{\mathbb{F}}_p$, i.e., $x = j\beta, j\beta^p, -\tau$ and $-l-\tau$ with multiplicities $d, d, M-c_0$ and $M-c_1$, respectively, so $f_j(x)^d(x+\tau)^{M-c_0}(x+l+\tau)^{M-c_1}$ can never be an M-th power of a polynomial. Notice that only two roots $x = -\tau$ and $x = -l-\tau$ are in $\mathbb{F}_p$. Then $|C_{\mathbf{a},\mathbf{b}}(\tau)|$ is upper bounded by $3\sqrt{p}+2$ according to Corollary 1-(3).

Case 3: The proof is similar to Case 2. Polynomial $f_j(x)^d(x+\tau)^{M-c}$ has 3 distinct roots in $\overline{\mathbb{F}}_p$, i.e., $x = j\beta, j\beta^p$ and $-\tau$ with multiplicities d, d and $M-c$, respectively, so we have $|C_{\mathbf{a},\mathbf{b}}(\tau)| \leqslant 2\sqrt{p}+1$.

Case 4: The correlation function (11) can be rewritten as

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{x\in\mathbb{F}_p} \chi(f_j(x)^{d_1} f_k(x+\tau)^{M-d_2}). \tag{13}$$

In what follows, we show that $f_j(x)^{d_1} f_k(x+\tau)^{M-d_2}$ in (13) can never be an M-th power of a polynomial in $\mathbb{F}_p[x]$ for $f_j(x)^{d_1} \neq f_k(x)^{d_2}$ or $f_j(x)^{d_1} = f_k(x)^{d_2}, \tau \neq 0$.

Case 4-(1): For $\tau = 0$, it is obvious that $f_j(x)^{d_1} f_k(x)^{M-d_2}$ is an M-th power of a polynomial if and only if $j = k$ and $d_1 = d_2$.

Case 4-(2): For $\tau \neq 0$, in order to prove that $f_j(x)^{d_1} f_k(x)^{M-d_2}$ is not an M-th power of a polynomial, we only need to show $f_j(x) \neq f_k(x+\tau)$, or alternatively, $f_j(x)$ and $f_k(x+\tau)$ do not have a common root in $\overline{\mathbb{F}}_p$. Note that the roots of $f_j(x)$ are $j\beta$ and $j\beta^p$, while the roots of $f_k(x+\tau)$ are $k\beta-\tau$ and $k\beta^p-\tau$. It is obvious that $j\beta \neq k\beta-\tau$ and $j\beta^p \neq k\beta^p-\tau$ for $\tau \neq 0$. If $j\beta = k\beta^p-\tau$, then we have $(j+k)\beta = k\beta + k\beta^p - \tau = kTr(\beta) - \tau \in \mathbb{F}_p$ which contradicts with $(j+k)\beta \notin \mathbb{F}_p$. Similarly, we can prove $j\beta^p \neq k\beta - \tau$. Thus $f_j(x)$ and $f_k(x+\tau)$ cannot have a common root in $\overline{\mathbb{F}}_p$.

By cases 4-(1) and 4-(2), we know that polynomial $f_j(x)^{d_1} f_k(x+\tau)^{M-d_2}$ is not an M-th power of a polynomial, and has no root in $\mathbb{F}_p$. Hence $C_{\max}(\mathcal{B}_{2,p}) \leqslant 3\sqrt{p}$ according to Corollary 1-(3).

From the above discussion in cases 1-4, we have $C_{\max}(\mathcal{U}_p) \leqslant 3\sqrt{p}+4$.

(2) Let $f(x)$ and $g(x)$ be polynomials associated with sequences $\mathbf{a}$ and $\mathbf{b}$ in $\mathcal{U}_{p,\delta}$, respectively. The correlation of $\mathbf{a}$ and $\mathbf{b}$ at shift τ is given in (11). Since the family $\mathcal{U}_{p,\delta}$ is a subset of $\mathcal{U}_p$, the proof for correlation of sequences in $\mathcal{U}_p$ is still valid. Thus $f(x)g(x+\tau)^{M-1}$ in (11) is not an M-th power of a polynomial.

If at least one of the sequences $\mathbf{a}$ and $\mathbf{b}$ are in $\mathcal{A}_{1,p}$, polynomial $f(x)g(x+\tau)^{M-1}$ has at most 3 distinct roots in $\mathbb{F}_p$. According to Corollary 1-(3), $|C_{\mathbf{a},\mathbf{b}}(\tau)| \leqslant 2\sqrt{p}+3$ follows. If neither $\mathbf{a}$ nor $\mathbf{b}$ is in $\mathcal{A}_{1,p}$, we have $\deg(f(x)) \equiv \deg(g(x+\tau)) \equiv \delta \pmod{M}$. Then the degree of polynomial argument in (11) is given by $\deg(f(x)g(x+\tau)^{M-1}) \equiv \delta + \delta(M-1) \equiv 0 \pmod{M}$, i.e., $M|\deg(f(x)g(x+\tau)^{M-1})$. Notice that $f(x)g(x+\tau)^{M-1}$ has at most 4 distinct roots in $\mathbb{F}_p$. Then we have $|C_{\mathbf{a},\mathbf{b}}(\tau)| \leqslant 2\sqrt{p}+5$ according to Corollary 1-(3). Hence, $C_{\max}(\mathcal{U}_{p,\delta}) \leqslant 2\sqrt{p}+5$.

Finally, we determine their respective sizes of sequence families $\mathcal{U}_p$ and $\mathcal{U}_{p,\delta}$. Since $\mathcal{A}_{1,p}$, $\mathcal{A}_{2,p}$ and $\mathcal{B}_{2,p}$ are disjoint subsets of $\mathcal{U}_p$, we have $|\mathcal{U}_p| = |\mathcal{A}_{1,p}| + |\mathcal{A}_{2,p}| + |\mathcal{B}_{2,p}|$ where $|\mathcal{A}_{1,p}| = M-1$, $|\mathcal{A}_{2,p}| = \frac{p-1}{2}(M-1)^2$, and $|\mathcal{B}_{2,p}| = \frac{p-1}{2}(M-1)$, respectively. Similarly, we have $|\mathcal{U}_{p,\delta}| = |\mathcal{A}_{1,p}| + |\mathcal{A}_{2,p,\delta}| + |\mathcal{B}_{2,p,\delta}|$ where $|\mathcal{A}_{2,p,0}| = \frac{p-1}{2}(M-1)$ for even M, $|\mathcal{A}_{2,p,\delta}| = \frac{p-1}{2}(M-2)$ for odd M and $\delta \neq 0$, and $|\mathcal{B}_{2,p,\delta}| = \frac{p-1}{2}$ for every δ, respectively. Then the assertions on the family sizes of $\mathcal{U}_p$ and $\mathcal{U}_{p,\delta}$ follow immediately. □

4.2 Construction 2

We now turn our attention to the sequences derived from the Weil representation revisited in Subsection 3.2-(E). One drawback of the sequence family $\Omega_{d,p}$ defined in (9) is that the alphabet size Mp is larger than the period p. In this subsection, we generalize this construction by extending the finite field from $\mathbb{F}_p$ to $\mathbb{F}_{p^n}$, which gives a new sequence family in class H-2. Each sequence in the new family has period $q-1$ and alphabet size Mp where $q = p^n$ and $M|(q-1)$.

Construction 2: For $d \ll \sqrt{q}$ and $M|(q-1)$, the modulated version of a new sequence family is defined

by

$$\Gamma_{d,q} = \left\{ \{\chi((\alpha^t+1)^c)\psi(f(\alpha^t))\}_{t\geqslant 0} | 1 \leqslant c \leqslant M-1, f(x) \in \mathcal{F}_{d,q} \right\} \tag{14}$$

where $\mathcal{F}_{d,q} = \{\sum_{k=1}^{d} a_k x^k | a_k \in \mathbb{F}_q, a_k = 0 \text{ if } p|k\}$.

Note that our new sequence is the element-wise product of a modulated Sidel'nikov sequence and a modulated trace sequence with period $q-1$.

Example 1 *For $p=3$ and $n=2$, let α be a primitive element of $\mathbb{F}_{3^2}$ satisfying $\alpha^2+2\alpha+2=0$. For a given m-sequence $\{Tr(\alpha^t)\} = (0,1,1,2,0,2,2,1)$ and a 4-ary Sidel'nikov sequence $\{\log(\alpha^t+1) \pmod 4\} = (0,2,3,2,0,3,1,1)$, $\Gamma_{2,3^2}$ can be constructed as follows.*

Table 2: Example of Construction 2

$\{\chi((\alpha^t+1)^c)\}$	$\{\psi(a_2\alpha^{2t})\}$	$\{\psi(a_1\alpha^t)\}$
$\sqrt{-1}^{(0,2,3,2,0,3,1,1)}$	$\omega_3^{(0,1,0,2,0,1,0,2)}$	$\omega_3^{(0,1,1,2,0,2,2,1)}$
$\sqrt{-1}^{(0,0,2,0,0,2,2,2)}$	$\omega_3^{(1,0,2,0,1,0,2,0)}$	$\omega_3^{(1,1,2,0,2,2,1,0)}$
$\sqrt{-1}^{(0,2,1,2,0,1,3,3)}$	$\omega_3^{(0,2,0,1,0,2,0,1)}$	$\omega_3^{(1,2,0,2,2,1,0,1)}$
	$\omega_3^{(2,0,1,0,2,0,1,0)}$	$\omega_3^{(2,0,2,2,1,0,1,1)}$
	$\omega_3^{(1,2,2,1,1,2,2,1)}$	$\omega_3^{(0,2,2,1,0,1,1,2)}$
	$\omega_3^{(2,2,1,1,2,2,1,1)}$	$\omega_3^{(2,2,1,0,1,1,2,0)}$
	$\omega_3^{(2,1,1,2,2,1,1,2)}$	$\omega_3^{(2,1,0,1,1,2,0,2)}$
	$\omega_3^{(1,1,2,2,1,1,2,2)}$	$\omega_3^{(1,0,1,1,2,0,2,2)}$

In Table 2, the columns $\{\psi(a_1\alpha^t)\}$ and $\{\psi(a_2\alpha^{2t})\}$ exhibit all the modulated sequences derived from m-sequence $\{0,1,1,2,0,2,2,1\}$ and 2-decimation of m-sequence $\{0,1,0,2,0,1,0,2\}$ by shift, respectively, while the column $\{\chi((\alpha^t+1)^c)\}$ shows all the modulated sequences derived from Sidel'nikov sequence $\{0,2,3,2,0,3,1,1\}$ by scaling. Then the sequences in $\Gamma_{2,3^2}$ are constructed by the element-wise products of the sequences $\{\chi((\alpha^t+1)^c)\}$, $\{\psi(a_2\alpha^{2t})\}$ and $\{\psi(a_1\alpha^t)\}$.

Theorem 2 *In Construction 2, $\Gamma_{d,q}$ is a sequence family of period $q-1$ with alphabet size Mp, family size $(M-1)q^{d-\lfloor \frac{d}{p} \rfloor}$ and maximum correlation $C_{\max}(\Gamma_{d,q}) \leqslant (d+1)\sqrt{q}+3$.*

Proof: Since $\chi((\alpha^t+1)^c)$ and $\psi(f(\alpha^t))$ are complex M-th and p-th roots of unity, respectively, then $\chi((\alpha^t+1)^c)\psi(f(\alpha^t))$ is an (Mp)-th root of unity in complex field. Thus, the alphabet size of sequence family $\Gamma_{d,q}$ is Mp. For the family size, we have $|\Gamma_{d,q}| = (M-1)|\mathcal{F}_{d,q}| = (M-1)q^{d-\lfloor \frac{d}{p} \rfloor}$ where $d - \lfloor \frac{d}{p} \rfloor = |\{k | 1 \leqslant k \leqslant d, (k,p)=1\}|$.

For a pair of modulated sequences $\mathbf{a}', \mathbf{b}' \in \Gamma_{d,q}$, let $a'(t) = \chi((\alpha^t+1)^c)\psi(f_1(\alpha^t))$ and $b'(t) = \chi((\alpha^t+1)^d)\psi(f_2(\alpha^t))$ respectively, where $1 \leqslant c,d \leqslant M-1$ and $f_1(x), f_2(x) \in \mathcal{F}_{d,q}$. According to the

class H-2 in Table 1, we have

$$C_{\mathbf{a}',\mathbf{b}'}(\tau) = \sum_{x\in\mathbb{F}_q^*} \chi((x+1)^c(\alpha^\tau x+1)^{M-d})\psi(f_1(x) - f_2(\alpha^\tau x)). \tag{15}$$

Case 1: If $\tau \neq 0$, polynomial $(x+1)^c(\alpha^\tau x+1)^{M-d}$ in (15) has the root $x=-1$ of multiplicity c and the root $x=\alpha^{-\tau}$ of multiplicity $M-d$, so it cannot be an M-th power of a polynomial. Since $(x+1)^c(\alpha^\tau x+1)^{M-d}$ has 2 distinct roots and $\deg(f_1(x)-f_2(\alpha^\tau x)) \leqslant d$, we have $|C_{\mathbf{a}',\mathbf{b}'}(\tau)| \leqslant (d+1)\sqrt{q}+3$ according to Corollary 2-(7).

Case 2: If $\tau = 0$ and $c \neq d$, polynomial $(x+1)^c(\alpha^\tau x+1)^{M-d} = (x+1)^{M+c-d}$ has only one root $x=-1$ of multiplicity $M+c-d$, so it cannot be an M-th power of a polynomial. Since $\deg(f_1(x)-f_2(\alpha^\tau x)) \leqslant d$, we have $|C_{\mathbf{a}',\mathbf{b}'}(\tau)| \leqslant (d+1)\sqrt{q}+2$ by Corollary 2-(7).

Case 3: If $\tau = 0$, $c = d$ and $f_1(x) \neq f_2(x)$, the above hybrid character sum will be reduced to an additive character sum, i.e., $C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{x\in\mathbb{F}_q^*} \psi(f_1(x)-f_2(x))$. Notice that $1 \leqslant \deg(f_1(x)-f_2(x)) \leqslant d$ and $(\deg(f_1(x)-f_2(x)), q) = 1$. Then we have $|C_{\mathbf{a},\mathbf{b}}(\tau)| \leqslant (d-1)\sqrt{q}+1$ according to Fact 1.

From Cases 1-3, we have $C_{\max}(\Gamma_{d,q}) \leqslant (d+1)\sqrt{q}+3$. □

5 Comparisons and Discussions

In this section, we compare our new constructions with various known sequence families in terms of family size and maximum correlation. We then discuss their discrete Fourier transform and ambiguity function by the Weil bound.

5.1 Family Size and Maximum Correlation

Table 3 presents the comparison data of the parameters of known polyphase sequence families with low correlation, where $\mathcal{U}_p$, $\mathcal{U}_{p,0}$ and $\Gamma_{d,q}$ are the new sequence families found in this paper. We have the following observations.

(1) Compared to [17], $\mathcal{U}_p$ and $\mathcal{U}_{p,0}$ provide more M-ary sequences of period p than the known power residue-based sequence families $\mathcal{A}_{1,p} \cup \mathcal{A}_{2,p}$ and $\mathcal{A}_{1,p} \cup \mathcal{A}_{2,p,0}$, respectively, where $C_{\max}(\mathcal{U}_p) = C_{\max}(\mathcal{A}_{1,p} \cup \mathcal{A}_{2,p})$ and $C_{\max}(\mathcal{U}_{p,0}) = C_{\max}(\mathcal{A}_{1,p} \cup \mathcal{A}_{2,p,0})$. Specially, for $M=2$, the family sizes of $\mathcal{U}_p$ and $\mathcal{U}_{p,0}$ are almost twice of sizes of $\mathcal{A}_{1,p} \cup \mathcal{A}_{2,p}$ and $\mathcal{A}_{1,p} \cup \mathcal{A}_{2,p,0}$, respectively.

(2) Sequence families $\Gamma_{d,q}$ is an analogue of $\Omega_{d,p}$. Sequences in $\Omega_{d,p}$ have period p and alphabet size Mp for $M|(p-1)$, while sequences in $\Gamma_{d,q}$ have period p^n-1 and alphabet size Mp for $M|(p^n-1)$.

Table 3: Comparisons of Known Polyphase Sequence Families

Family $\mathcal{S}$	Period N	Alphabet	$C_{\max}(\mathcal{S})$	Family size
Chu [8, 7]	N	$2N$	$\sqrt{N}$	$p-1^{(1)}$
Alltop [9]	odd N	N	$\sqrt{N}$	$p-1^{(1)}$
Kumar and Moreno[26]	p^n-1	p	$\sqrt{N+1}+1$	$N+1$
$\mathbb{Z}_4(0)$ [12]	2^n-1	4	$\sqrt{N+1}+1$	$N+2$
$\mathbb{Z}_4(1)$ [12]	2^n-1	4	$2\sqrt{N+1}+1$	$\geqslant N^2+3N+2$
$\mathbb{Z}_4(2)$ [12]	2^n-1	4	$4\sqrt{N+1}+1$	$\geqslant N^3+4N^2+5N+2$
$\mathcal{A}_{1,p}$ [14]	p	M	$\sqrt{N}+2$	$M-1$
$\mathcal{A}_{1,p}\cup\mathcal{A}_{2,p,0}$[17]	p	M	$2\sqrt{N}+5$	$\frac{(M-1)(N+1)}{2}$
$\mathcal{U}_{p,0}$ in this paper	p	M	$2\sqrt{N}+5$	$\frac{M(N+1)}{2}-1$
$\mathcal{A}_{1,p}\cup\mathcal{A}_{2,p}$[17]	p	M	$3\sqrt{N}+4$	$(M-1)(\frac{(N-1)(M-1)}{2}+1)$
$\mathcal{U}_p$ in this paper	p	M	$3\sqrt{N}+4$	$(M-1)(\frac{N-1}{2}M+1)$
$\mathcal{C}_{1,q}$ [15]	p^n-1	M	$\sqrt{N+1}+3$	$M-1$
$\mathcal{C}_{1,q}\cup\mathcal{C}_{2,q,0}$[17]	p^n-1	M	$2\sqrt{N+1}+6$	$\frac{(M-1)(N+1)}{2}^{(2)}$
$\mathcal{C}_{1,q}\cup\mathcal{C}_{2,q,0}\cup\mathcal{D}_{2,q,0}$[19]	p^n-1	M	$2\sqrt{N+1}+6$	$\frac{M(N+1)}{2}^{(2)}$
$\mathcal{C}_{1,q}\cup\mathcal{C}_{2,q}$[17]	p^n-1	M	$3\sqrt{N+1}+5$	$(M-1)(\frac{(N-1)(M-1)}{2}+1)^{(2)}$
$\mathcal{C}_{1,q}\cup\mathcal{C}_{2,q}\cup\mathcal{D}_{2,q}$[19]	p^n-1	M	$3\sqrt{N+1}+5$	$(M-1)(\frac{N-1}{2}M+2)^{(2)}$
$\mathcal{C}_{1,q}\cup\mathcal{C}_{2,q}\cup\mathcal{Z}_{1,q}\cup\mathcal{Z}_{2,q}$[25]	p^n-1	M	$4\sqrt{N+1}+4$	$(M-1)((M-1)N+2)^{(2)}$
$\mathcal{S}_{d+2}$[2]	p^n-1	p	$(d+1)\sqrt{N+1}+1$	$(N+1)^{d+1}$ $^{(3)}$
$\Omega_{d,p}$[20, 21, 22]	p	pM	$(d+1)\sqrt{N}+2$	$(M-1)N^d$
$\Gamma_{d,q}$ in this paper	p^n-1	pM	$(d+1)\sqrt{N+1}+3$	$(M-1)(N+1)^d$ $^{(3)}$

(1) p is the smallest prime divisor of N.

(2) For the family size, we only consider the case $p=2$, since it is convenient to compare the parameters of the sequence families in class M-1 and M-2 in this table. For odd p, please refer to the tables in [17, 19, 25] for the family sizes, which are slightly different from the case $p=2$.

(3) We only consider $d \ll \sqrt{p}$ to compare these 3 sequence families.

5.2 Discrete Fourier Transform and Ambiguity Function

The purpose of sequence design by the Weil representation proposed by Gurevich, Hadina and Sochen [20] is not only to obtain good correlation property, but also to have some other desired properties, such as flat Fourier spectra and low valued ambiguity function.

The N-point *discrete Fourier transform* (DFT) of a modulated sequence $\mathbf{a}' = \{a'(t)\}$ with period N

is defined by $DFT[\mathbf{a}'](k) = \sum_{t=0}^{N-1} a'(t)\omega_N^{-tk}$ for $0 \leqslant k \leqslant N-1$. The maximum magnitude of discrete Fourier spectra can be used to determine the *peak-to-average power ratio* (PAPR) [27] of multicarrier transmission employing the sequence [28] [29]. The discrete Fourier spectra of trace codes were studied by the Weil bound in [10]. By extending the idea in [10], Table 4 gives the DFT of sequences in Table 1. Then the magnitudes of their respective discrete Fourier spectra can be bounded by Facts 1-3 and Corollaries 1-2. Note that in Tables 4 and 5, χ_1 is a multiplicative character of order $q-1$, i.e., $\chi_1(\alpha^k) = w_{q-1}^k$ for all $\alpha^k \in \mathbb{F}_q^*$ and $\chi_1(0) = 1$ by our assumption.

Table 4: DFT Spectra

Class	Sequence $a'(t)$	$DFT[\mathbf{a}'](k)$	$\mathbf{b}$ ∈Example $\mathcal{S}$	$\lvert DFT[\mathbf{b}'](k)\rvert$
A-1	$\psi(f(t))$	$\sum_{x\in\mathbb{F}_p} \psi(f(x)-kx)$	Alltop [9]	$\sqrt{p}$
A-2	$\psi(f(\alpha^t))$	$\sum_{x\in\mathbb{F}_q^*} \chi_1(x^{-k})\psi(f(x))$	$\mathcal{S}_d$[2]	$\leqslant d\sqrt{q}$
M-1	$\chi(f(t))$	$\sum_{x\in\mathbb{F}_p} \chi(f(x))\psi(-kx)$	$\mathcal{U}_p$ in this paper	$\leqslant 2\sqrt{p}+2$
M-2	$\chi(f(\alpha^t))$	$\sum_{x\in\mathbb{F}_q^*} \chi_1(x^{-k}f(x)^{\frac{q-1}{M}})$	$\mathcal{C}_{1,q}\cup\mathcal{C}_{2,q}\cup\mathcal{D}_{2,q}$[19]	$\leqslant 2\sqrt{q}+2$
H-1	$\chi(g(t))\psi(f(t))$	$\sum_{x\in\mathbb{F}_p} \chi(g(x))\psi(f(x)-kx)$	$\Omega_{d,p}$[20, 21, 22]	$\leqslant d\sqrt{p}+1$
H-2	$\chi(g(\alpha^t))\psi(f(\alpha^t))$	$\sum_{x\in\mathbb{F}_q^*} \chi_1(x^{-k}g(x)^{\frac{q-1}{M}})\psi(f(x))$	$\Gamma_{d,q}$ in this paper	$\leqslant (d+1)\sqrt{q}+1$

In [20], the (linear) doppler shift P_w on a modulated sequence $\mathbf{a}' = \{a'(t)\}$ with period N is defined by $P_w[\mathbf{a}'](t) = \omega_N^{wt}a'(t)$ for $0 \leqslant w \leqslant N-1$. By taking both time delay and doppler shift into consideration, the *ambiguity function* of $\mathbf{a}$ and $\mathbf{b}$ is defined as two-dimensional correlation function, given by $G_{\mathbf{a},\mathbf{b}}(\tau, w) =< \mathbf{a}', P_w L_t \mathbf{b}' >$. The maximum ambiguity function of sequence family $\mathcal{S}$ is defined by

$$G_{\max}(\mathcal{S}) = \max\{|G_{\mathbf{a},\mathbf{b}}(\tau, w)| : \mathbf{a}, \mathbf{b} \in \mathcal{S}, (\tau, w) \neq (0,0) \text{ if } \mathbf{a} = \mathbf{b}\}. \tag{16}$$

Note that the concept of ambiguity function is strongly related to Costas array, introduced by Costas in [30], and extensively studied in the literature, e.g., [31, 32, 33].

The ambiguity functions of sequences in Table 1 are given in Table 5, where their respective maximum ambiguity function can be bounded by Facts 1-3 and Corollaries 1-2. Note that though $G_{\max}(\Omega_{d,p}) = p$, we can choose a subset of $\Omega_{d,p}$, namely, $\Omega_{d,p}^0 = \left\{\{\chi(t^c)\psi(f(t))\}_{t\geqslant 0} | f(x) = \sum_{k=2}^{d} a_k x^k \in \mathbb{F}_p[x]\right\} \subset \Omega_{d,p}$, such that the maximum ambiguity function of $\Omega_{d,p}^0$ is bounded by $(d+1)\sqrt{p}+2$. For some experimental results on other properties of the new sequence which is an element-wise product of a ternary Sidel'nikov sequence and a binary m-sequence from Construction 2, see [35].

Table 5: Ambiguity Function

Class	Sequence $a'(t)$	Ambiguity function $G_{\mathbf{a},\mathbf{b}}(\tau, w)$	Example $\mathcal{S}$	$G_{\max}(\mathcal{S})$
A-1	$\psi(f(t))$	$\sum_{x\in\mathbb{F}_p}\psi(f(x)-g(x+\tau)-wx)$	Alltop [9]	p
A-2	$\psi(f(\alpha^t))$	$\sum_{x\in\mathbb{F}_q^*}\chi_1(x^{-w})\psi(f(x)-g(\alpha^\tau x))$	$\mathcal{S}_d$[2]	$d\sqrt{q}$
M-1	$\chi(f(t))$	$\sum_{x\in\mathbb{F}_p}\chi(f(x)g(x+\tau)^{M-1})\psi(-wx)$	$\mathcal{U}_p$ in this paper	$4\sqrt{p}+4$
M-2	$\chi(f(\alpha^t))$	$\sum_{x\in\mathbb{F}_q^*}\chi_1(x^{-w}(f(x)g(\alpha^\tau x)^{M-1})^{\frac{q-1}{M}}))$	$\mathcal{C}_{1,q}\cup\mathcal{C}_{2,q}\cup\mathcal{D}_{2,q}$[19]	$4\sqrt{q}+4$
H-1	$\chi(g(t))\psi(f(t))$	$\sum_{x\in\mathbb{F}_p}\chi(g_1(x)g_2(x+\tau)^{M-1})$ $\cdot\psi(f_1(x)-f_2(x+\tau)-wx)$	$\Omega^0_{d,p}$[20, 21, 22]	$(d+1)\sqrt{p}+2$
H-2	$\chi(g(\alpha^t))\psi(f(\alpha^t))$	$\sum_{x\in\mathbb{F}_q^*}\chi_1(x^{-w}(g_1(x)g_2(\alpha^\tau x)^{M-1})^{\frac{q-1}{M}})$ $\cdot\psi(f_1(x)-f_2(\alpha^\tau x))$	$\Gamma_{d,q}$ in this paper	$(d+2)\sqrt{q}+2$

6 Concluding Remarks

In this paper, we revisited sequence families of which maximum correlation is determined by the Weil bound. With the same technique, we presented two new constructions with large family sizes and low correlation. In the first construction, a new sequence family consists of $(\frac{p-1}{2}M+1)(M-1)$ (or $(\frac{p+1}{2}M-1)$) shift distinct M-ary sequences of period p having maximum correlation $3\sqrt{p}+4$ (or $2\sqrt{p}+5$), obtained by adding the sequences from irreducible quadratic polynomials in $\mathbb{F}_p[x]$ to the known power residue-based sequence families while the maximum correlation remains unchanged. In the second construction, the sequences derived from the Weil representation are generalized. Each new sequence is the element-wise product of a modulated Sidel'nikov sequence and a modulated trace sequence. For a given prime p, an integer d and $M|(p^n-1)$, a new sequence family consists of $(M-1)q^{d-\lfloor\frac{d}{p}\rfloor}$ distinct sequences with alphabet size Mp, period p, and maximum correlation $(d+1)\sqrt{q}+3$. The discrete Fourier spectra and ambiguity functions are also derived.

From the revisit to the known sequence families and new constructed sequence families in this paper, we observed that their maximum values of correlation, discrete Fourier spectra and ambiguity function can be determined by the Weil bounds of the exponential sums because their associated polynomials have low degree. However, there are known sequence families [3] derived from additive characters that have smaller maximum correlation than predicted by the Weil bound. For example, the Gold pair [36] sequence family, given by $Tr(ax+x^3), a\in\mathbb{F}_{2^n}$ where n is odd has the maximum correlation $\sqrt{2}\sqrt{2^n}$. However, the maximum correlation obtained using the Weil bound is $2\sqrt{2^n}$. Thus, one open question is to investigate whether there exist some sequence families using multiplicative characters or hybrid charters for which their associated polynomials have high degree, but the maximum correlation is better

than those given by the Weil bounds.

Acknowledgment

The first author would like to thank Prof. Daqing Wan for communication of his paper [23]. The authors would like to thank the anonymous reviewers for their helpful and valuable comments and suggestions.

References

[1] L. R. Welch, "Lower bounds on the minimum correlation of signal," *IEEE Trans. Inf. Theory*, vol. 20, no. 3, pp. 397-399, May 1974.

[2] V. M. Sidel'nikov, "On mutual correlation of sequences," *Soviet Math. Dokl*, vol. 12, no. 1, pp. 197-201, 1971.

[3] T. Helleseth and P. V. Kumar, "Sequences with low correlation,"a chapter in *Handbook of Coding Theory*, V. Pless and C. Huffman, Ed., Elsevier Science Publishers, 1998, pp. 1765-1853.

[4] S. W. Golomb and G. Gong, *Signal Design with Good Correlation: for Wireless Communications, Cryptography and Radar Applications*, Cambridge University Press, 2005.

[5] A. Weil, "On some exponential sums," *Proc. Natl. Acad. Sci. USA*, vol. 34, no. 5, pp. 204-207, 1948.

[6] P. Deligne, "La conjecture de Weil I," *Publ. Math. IHES*, vol. 43, no. 1, pp. 273-307, 1974.

[7] R. Frank, S. Zadoff and R. Heimiller, "Phase shift pulse codes with good periodic correlation properties," *IRE Trans. Inf. Theory*, vol. 8, no. 6, pp. 381-382, Oct. 1962.

[8] C. Chu, "Polyphase codes with good periodic correlation properties," *IEEE Trans. Inf. Theory*, vol. 18, no. 4, pp. 531-532, Jul. 1972.

[9] W. O. Alltop, "Complex sequences with low periodic correlations," *IEEE Trans. Inf. Theory*, vol. 26, no. 3, pp. 350-354, May 1980.

[10] K. G. Paterson, "Applications of exponential sums in communication theory," *Cryptography and Coding*, M. Walker, Ed., LNCS vol. 1746, Springer, pp.1-24, 1999.

[11] P. V. Kumar, T. Helleseth, and A. R. Calderbank, "An upper bound for Weil exponential sums over Galois rings and applications," *IEEE Trans. Inf. Theory*, vol. 41, no. 2, pp. 456-468, Mar. 1995.

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

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

[14] Y. J. Kim, H. Y. Song, G. Gong and H. Chung, "Crosscorrelation of q-ary power residue sequences of period p,"in *Proc. IEEE ISIT*, 2006, pp.311-315.

[15] 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.

[16] Y. Kim, J. 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

[17] 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.

[18] N. Y. Yu and G. Gong, "Multiplicative characters, the Weil Bound, and polyphase sequence families with low correlation," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6376–6387, Dec. 2010.

[19] N. Y. Yu and G. Gong, "New construction of M-ary sequence families with low correlation from the structure of Sidelnikov sequences," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 4061 - 4070, Aug. 2010.

[20] S. Gurevich, R. Hadani and N. Sochen, "The finite harmonic oscillator and its applications to sequences, communication and radar," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4239-4253, Sep. 2008.

[21] Z. Wang and G. Gong, "New sequences design from Weil representation with low two-dimensional correlation in both time and phase shifts," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4600-4611, Jul. 2011.

[22] K. U. Schmidt, "Sequence families with low correlation derived from multiplicative and additive characters," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2291-2294, Apr. 2011.

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

[24] G. Gong, "Theory and applications of q-ary interleaved sequences," *IEEE Trans. Inf. Theory*, vol. 41, no. 2, pp. 400-411, Mar. 1995.

[25] J. S. Chung, J. S. No and H. Chung, "A construction of a new family of M-ary sequences with low correlation from Sidel'nikov sequences," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2301-2305, Apr. 2011.

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

[27] S. Litsyn, *Peak Power Control in Multi-carrier Communications*, Cambridge University Press, 2007.

[28] K. G. Paterson and V. Tarokh, "On the existence and construction of good codes with low peak-to-average power ratios," *IEEE Trans. Inf. Theory*, vol. 46, no. 6, pp. 1974-1987. Jun. 2000.

[29] S. Litsyn and A. Yudin, "Discrete and continuous maxima in multicarrier communications," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 919-928 , Mar. 2005.

[30] J. P. Costas, "A study of a class of detection waveforms having nearly ideal range-doppler ambiguity properties," *Proc. IEEE*, vol. 72, no. 8, pp. 996-1009, 1984.

[31] S. W. Golomb, "Algebraic constructions for Costas arrays," *Journal of Combinatorics Theory (A)*, vol. 37, no. 1, pp. 13-21, 1984.

[32] T. Etzion, "Combinatorial designs derived from Costas arrays," *Discrete Mathematics*, vol. 93, no. 2- 3, pp. 143-154, 1991.

[33] S. W. Golomb and G. Gong, "The status of Costas arrays," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4260 - 4265, Nov. 2007.

[34] S. D. Howard, A. R. Calderbank and W. Moran, "The finite Heisenberg- Weyl groups in radar and communications," *EURASIP J. Appl. Signal Process*, pp. 1-12, 2006.

[35] F. Huo, *Sequences design for OFDM and CDMA systems. Master Thesis*, University of Waterloo, 2011.

[36] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Trans. Inf. Theory*, vol. 14, no. 1, pp. 154-156. Jan. 1968.