Correlation of Binary Sequence Families Derived from Multiplicative Character of Finite Fields

Zilong Wang and Guang Gong
Department of Electrical and Computer Engineering, University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA
Email: wzlmath@gmail.com ggong@uwaterloo.ca

Abstract

In this paper, new constructions of binary sequence families of period $q-1$ with large family size and low correlation, derived from multiplicative character of finite fields for an odd prime power q, are proposed. For $m \geqslant 2$, the maximum correlation magnitudes of new sequence families $\mathcal{S}_m$ are bounded by $(2m-2)\sqrt{q}+2m+2$, and the family sizes of $\mathcal{S}_m$ are given by $q-1$ for $m=2$, $2(q-1)-1$ for $m=3$, $(q^2-1)q^{\frac{m-4}{2}}$ for m even, $m>2$, and $2(q-1)q^{\frac{m-3}{2}}$ for m odd, $m>3$. It is shown that the known binary Sidel'nikov-based sequence families are equivalent to the new constructions for the case $m=2$.

Index Terms. Binary sequences, multiplicative character, correlation, Weil bound.

1 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 to construct sequence families with large family size and low correlation.

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 [14] and Sidel'nikov [11]. 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 [8], and Golomb and Gong's book [2], where a majority of sequences are constructed by the trace function and their correlation functions are presented by the additive character sums. The sequence families providing the largest family sizes for the given maximum correlation magnitudes among all known are $\mathbb{Z}_4$ sequence families designed by Kumar, Helleseth, Calderbank, and Hammons in [9], where the sequences are constructed by the trace function of Galois rings.

There is another class of sequences whose correlation functions are determined by the multiplicative character sums, such as M-ary power residue sequences (also called Legendre sequence for $M=2$)

[0] 2000 Mathematics Subject Classification. Primary: 94B25, 11T24.

of period p and Sidel'nikov sequences of period $q-1$ ($q = p^n$) introduced in [10]. The out-of-phase autocorrelation of power residue sequences and Sidel'nikov sequences are bounded by 3 and 4, respectively. Moreover, M-ary power residue-based and Sidel'nikov-based sequence families were constructed in [7, 6, 5, 4, 17, 16]. It was shown that the families of power residue and Sidel'nikov sequences by scaling have the maximum correlation $\sqrt{p}+2$ in [7] and $\sqrt{q}+3$ in [6], respectively, and the families of power residue and Sidel'nikov sequences by shift-and-addition [5, 4, 17] have maximum correlation $2\sqrt{p}+5$ and $2\sqrt{q}+6$, respectively. These power residue-based and Sidel'nikov-based sequence families were generalized in [16] which provided larger families sizes at the cost of larger maximum correlation.

In this paper, we are only interested in the binary sequences derived from the multiplicative character of finite fields. We point out that, for the binary case $M = 2$, it was shown in [3] that a large number of binary sequences of this type have good pseudo-random properties. However, for binary case $M = 2$, the sizes of sequence families constructed in [7, 6, 5, 4, 17] are all small. We provide a polynomial-based approach, which is different from the method in [16], to obtain binary sequence families with low correlation and large size. Furthermore, for $2 \leqslant m \ll \sqrt{q}$, new sequence families $\mathcal{S}_m$ of period $q-1$ with maximum correlation $(2m-2)\sqrt{q}+2m+2$ are proposed. The family sizes of $\mathcal{S}_m$ are given by $q-1$ for $m=2$, $2(q-1)-1$ for $m=3$, $(q^2-1)q^{\frac{m-4}{2}}$ for m even, $m>2$, and $2(q-1)q^{\frac{m-3}{2}}$ for m odd, $m>3$. We also show that the known binary Sidel'nikov-based sequence family in [6, 5, 4, 17] and power residue-based sequence family in [7, 5, 4, 13] are equivalent to our constructions $\mathcal{S}_2$ and $\mathcal{L}_2$, respectively.

The rest of the paper is organized as follows. In Section 2, we introduce some basic notations, definitions, and the Weil bound of multiplicative character sum with polynomial arguments. In Section 3, we present our new constructions along with proofs of their properties on correlation and family sizes. In Section 4, the relationships between the known binary sequence families derived from multiplicative character and the new constructions are discussed. Section 5 concludes the paper.

2 Preliminaries

2.1 Basic Concepts and Notations

- *Finite Fields.* $q = p^n$ where p is an odd 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 $\mathbb{F}_q$.

- *Logarithm.* A logarithm in $\mathbb{F}_q^*$ is defined by $\log_\alpha x = i$ for $x = \alpha^i, 0 \le i \le q-2$, or simply as $\log x$ if the context is clear. In this paper, we are only interested in the least significant bit of $\log x$, i.e., $\log x \pmod 2$. If we extend the definition to $\log 0 = 0$, we have

$$\log x \equiv \begin{cases} 0 \pmod 2, & \text{if } x \text{ is a square in } \mathbb{F}_q, \\ 1 \pmod 2, & \text{if } x \text{ is a nonsquare in } \mathbb{F}_q. \end{cases}$$

- *Sequence and Correlation.* $\mathbf{a} = \{a(i)\}_{i\geqslant 0}$ where $a(i) \in \{0,1\}$, is called a binary sequence. For $\tau \in \mathbb{N}$, the shift operator L_τ on sequence $\mathbf{a} = \{a(i)\}_{i\geqslant 0}$ is defined by $L_\tau(\mathbf{a}) = \{a(t+\tau)\}_{i\geqslant 0}$. The correlation of a pair of binary sequences $\mathbf{a}$ and $\mathbf{b}$ of period N at shift τ is defined by

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{i=0}^{N-1} (-1)^{a_i - b_{i+\tau}}, \quad 0 \leqslant \tau \leqslant N-1.$$

If $\mathbf{b} = L_\tau(\mathbf{a})$ for some τ, $\mathbf{b}$ and $\mathbf{a}$ are called *shift equivalent*. Otherwise, they are called *shift-distinct*.

- *Binary Sequence Family.* For a set $\mathcal{S}$ consisting of L shift-distinct binary sequences of period N, the maximum correlation of $\mathcal{S}$ is defined by

$$C_{\max}(\mathcal{S}) = \max\{|C_{\mathbf{a},\mathbf{b}}(\tau)| : \mathbf{a},\mathbf{b} \in \mathcal{S}, \text{either } \mathbf{a} \neq \mathbf{b} \text{ or } \tau \neq 0\}. \tag{1}$$

Then the set $\mathcal{S}$ is called an $(N, L, C_{\max}(\mathcal{S}))$ sequence family.

2.2 Quadratic Multiplicative Character

Definition 1 *The quadratic multiplicative character of $\mathbb{F}_q^*$ is defined by*

$$\chi(\alpha^i) = (-1)^i, \ \forall \alpha^i \in \mathbb{F}_q^*,$$

which is equivalent to

$$\chi(x) = (-1)^{(\log_\alpha x) \pmod 2}, \ \forall x \in \mathbb{F}_q^*,$$

The definition is conventionally extended to $\chi(0) = 0$.

For the quadratic multiplicative character sum with polynomial arguments, we have the following Weil bound [15, 1], where the special case for $2|\deg(f(x))$ is improved in [12].

Fact 1 *Let χ be the quadratic multiplicative character of $\mathbb{F}_q$. For $f(x) \in \mathbb{F}_q[x]$ where $f(x) \neq c \cdot h^2(x)$ for some $c \in \mathbb{F}_q$ and $h(x) \in \mathbb{F}_q[x]$, let s be the number of distinct roots of $f(x)$ in $\overline{\mathbb{F}}_q$ (the algebraic closure of $\mathbb{F}_q$), then*

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

In the rest of the paper, we will adopt the definition $\chi(0) = 1$ as shown in [16] which agrees with our assumption $\log 0 = 0$. Then Fact 1 can be refined as follows to support $\chi(0) = 1$.

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

$$\left|\sum_{x\in\mathbb{F}_q}\chi(f(x))\right| \leqslant \begin{cases} (s-1)\sqrt{q}+e, \\ (s-2)\sqrt{q}+e+1, & \textit{if } \; 2|\mathit{deg}(f(x)), \end{cases} \tag{2}$$

and

$$\left|\sum_{x\in\mathbb{F}_q^*}\chi(f(x))\right| \leqslant \begin{cases} (s-1)\sqrt{q}+e+1, \\ (s-2)\sqrt{q}+e+2, & \textit{if } \; 2|\mathit{deg}(f(x)). \end{cases} \tag{3}$$

2.3 Sequences, Polynomials and Correlation

For a given polynomial $f(x) \in \mathbb{F}_q[x]$, define a sequence $\mathbf{a}$ corresponding to $f(x)$ by

$$a(i) \equiv \log(f(\alpha^i)) \pmod 2,$$

or alternatively,

$$a(i) = \begin{cases} 0, & \text{if } f(\alpha^i) \text{ is a square in } \mathbb{F}_q, \\ 1, & \text{if } f(\alpha^i) \text{ is a nonsquare in } \mathbb{F}_q. \end{cases}$$

Then $\mathbf{a} = \{a(i)\}_{i\geqslant 0}$ is a binary sequence of period $q-1$. For example, the polynomial corresponding to Sidel'nikov sequence is given by $f(x) = x+1$. From the definition of the sequences and quadratic characters, the correlation of sequences $\mathbf{a}$ and $\mathbf{b}$ corresponding to polynomials $f(x)$ and $g(x)$ is presented by

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{i=0}^{q-2}(-1)^{a(i)-b(i+\tau)} = \sum_{i=0}^{q-2}(-1)^{\log(f(\alpha^i)g(\alpha^{i+\tau}))} = \sum_{x\in\mathbb{F}_q^*}\chi(f(x)g(\alpha^\tau x)), \tag{4}$$

where χ is the quadratic multiplicative character of $\mathbb{F}_q$ with assumption $\chi(0) = 1$. Therefore, an upper bound of $|C_{\mathbf{a},\mathbf{b}}(\tau)|$ can be obtained by Corollary 1.

3 New Constructions

In this section, we propose several new sequence families with large size and low correlation derived from quadratic multiplicative character of $\mathbb{F}_q$.

Construction 1: $\mathcal{S}_2 = \{\{\log(f(\alpha^i)) \pmod 2\}_{i\geqslant 0} | f(x) = ax^2+x+1 \in \mathbb{F}_q[x], a \neq (2^{-1})^2\}$.

Theorem 1 *For Construction 1, $\mathcal{S}_2$ is a $(q-1, q-1, 2\sqrt{q}+6)$ sequence family.*

Proof: Let $f(x)$ and $g(x)$ be polynomials corresponding to sequences $\mathbf{a}$ and $\mathbf{b}$ in $\mathcal{S}_2$, respectively. According to (4), the correlation of $\mathbf{a}$ and $\mathbf{b}$ at shift τ can be presented by

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{x \in \mathbb{F}_q^*} \chi(f(x)g(\alpha^\tau x)). \tag{5}$$

We show $f(x)g(\alpha^\tau x) \neq c \cdot h^2(x)$ for either $f \neq g$ or $\tau \neq 0$ below.

Case 1: If $f(x) = g(x) = x+1$, then $f(x)g(\alpha^\tau x) = (x+1)(\alpha^\tau x + 1)$ has two distinct roots in $\mathbb{F}_q$ for $\tau \neq 0$.

Case 2: If $\deg(f(x)) = 1$ and $\deg(g(x)) = 2$, then we have $\deg(f(x)g(\alpha^\tau x)) = 3$.

Case 3: If $\deg(f(x)) = \deg(g(x)) = 2$, since $ax^2 + x + 1$ has two distinct roots for $a \neq (2^{-1})^2$, both $f(x)$ and $g(\alpha^\tau x)$ have two distinct roots in $\overline{\mathbb{F}}_q$. Then $f(x)g(\alpha^\tau x) = c \cdot h^2(x)$, if and only if $g(\alpha^\tau x) = c' \cdot f(x)$ for some $c' \in \mathbb{F}_q^*$, if and only if $f(x) = g(x)$ and $\tau = 0$ by comparing coefficients method.

From the discussions above, $f(x)g(\alpha^\tau x)$ can never be the form of $c \cdot h^2(x)$. According to Corollary 1, we have $|C_{\mathbf{a},\mathbf{b}}(\tau)| \leqslant 2\sqrt{q} + 6$ for either $\mathbf{a} \neq \mathbf{b}$ or $\tau \neq 0$. □

The degrees of polynomials corresponding to sequences in $\mathcal{S}_2$ are 2 and 1. In what follows, we generalize the construction $\mathcal{S}_2$, and obtain new constructions $\mathcal{S}_m$ for $2 \leqslant m \ll \sqrt{q}$, which contain two disjoint subsets $\mathcal{S}'_m$ and $\mathcal{S}'_{m-1}$, i.e., $\mathcal{S}_m = \mathcal{S}'_m \cup \mathcal{S}'_{m-1}$, where the degrees of polynomials corresponding to sequences are m and $m-1$, respectively. The definitions of sequence families $\mathcal{S}'_m$ depend on m even or odd. We present $\mathcal{S}'_m$ in Construction 2 for $m = 2d$ even and in Construction 3 for $m = 2d+1$ odd, respectively.

Construction 2: $\mathcal{S}'_{2d} = \{\{\log(f(\alpha^i)) \pmod 2\}_{i \geqslant 0} | f(x) = \sum_{i=1}^d a_i x^{2i} + x + 1 \in \mathbb{F}_q[x], a_d \neq 0\}$ for $2 \leqslant d \ll \sqrt{q}$.

Theorem 2 *For Construction 2, S'_{2d} is a $(q-1, (q-1)q^{d-1}, (4d-2)\sqrt{q} + 4d + 2)$ sequence family.*

Proof: First, for a polynomial $f(x) = \sum_{i=1}^d a_i x^{2i} + x + 1 \in \mathbb{F}_q[x]$ ($a_d \neq 0$), we show that $f(x) \neq c \cdot h^2(x)$ for any $c \in \mathbb{F}_q$ and $h(x) \in \mathbb{F}_q[x]$. Otherwise, assume

$$\sum_{i=1}^d a_i x^{2i} + x + 1 = c(\sum_{i=1}^d b_i x^i + b_0)^2. \tag{6}$$

By comparing the constant terms of both sides of equation (6), we have $cb_0^2 = 1$, so c is a square in $\mathbb{F}_q$. Without loss of generality, we suppose $c = b_0 = 1$. By comparing the coefficients of linear term in both sides of equation (6), we have $b_1 = 2^{-1}$. By comparing the coefficients of odd-degree terms in both sides of equation (6), we have the following two cases. If d is even, we have $b_{2i-1} = 0$ for $1 \leqslant i \leqslant \frac{d}{2}$ which contradicts to $b_1 = 2^{-1}$. If d is odd, we have $b_{2i} = 0$ for $0 \leqslant i \leqslant \frac{d-1}{2}$ which contradicts to $b_0 = 1$.

Then, for polynomials $f(x)$ and $g(x)$ of the form $\sum_{i=1}^{d} a_i x^{2i} + x + 1 \in \mathbb{F}_q[x]$ $(a_d \neq 0)$, we show that $f(x)g(\alpha^\tau x) \neq c \cdot h^2(x)$ for either $f(x) \neq g(x)$ or $\tau \neq 0$. Otherwise, assume $f(x) = c_f k(x)(f_0(x))^2$ and $g(\alpha^\tau x) = c_g k(x)(g_0(x))^2$ where $k(x) = (f(x), g(\alpha^\tau x))$, the great common divisor of $f(x)$ and $g(\alpha^\tau x)$, $c_f, c_g \in \mathbb{F}_q^*$, and $f_0(x), g_0(x)$ and $k(x)$ are all monic polynomials in $\mathbb{F}_q[x]$. Then we have $\deg(k(x)) \geqslant 2$.

Let $k(x)(f_0(x))^2 = f_1(x) + c_1 x$ and $k(x)(g_0(x))^2 = g_1(x) + c_2 x$, where $f_1(x)$ and $g_1(x)$ are both even polynomials and $c_1, c_2 \in \mathbb{F}_q^*$. Then we have

$$k(x)f_0(x)^2 k(-x)g_0(-x)^2 = (f_1(x) + c_1 x)(g_1(-x) - c_2 x) = (f_1(x) + c_1 x)(g_1(x) - c_2 x), \tag{7}$$

and

$$k(-x)f_0(-x)^2 k(x)g_0(x)^2 = (f_1(-x) - c_1 x)(g_1(x) + c_2 x) = (f_1(x) - c_1 x)(g_1(x) + c_2 x). \tag{8}$$

From (7)-(8), we obtain

$$k(x)k(-x)(f_0(x)^2 g_0(-x)^2 - f_0(-x)^2 g_0(x)^2) = 2x(c_2 f_1(x) - c_1 g_1(x)). \tag{9}$$

If $c_2 f_1(x) - c_1 g_1(x) = 0$, then

$$c_2 k(x)(f_0(x))^2 - c_1 k(x)(g_0(x))^2 = c_2(f_1(x) + c_1 x) - c_1(g_1(x) + c_2 x) = 0,$$

which induces that $g(\alpha^\tau x) = c' \cdot f(x)$ for some $c' \in \mathbb{F}_q^*$. By comparing the coefficients of linear and constant terms of $f(x)$ and $g(\alpha^\tau x)$, we have $f(x) = g(x)$ and $\tau = 0$.

If $c_2 f_1(x) - c_1 g_1(x) \neq 0$, we consider the degrees of the polynomials in both sides of equation (9). For the right side of (9), it is clear

$$\deg(2x(c_2 f_1(x) - c_1 g_1(x))) \leqslant 2d + 1.$$

Decompose the polynomial in the left side of (9), we get

$$k(x)k(-x)(f_0(x)^2 g_0(-x)^2 - f_0(-x)^2 g_0(x)^2) = k(x)k(-x)(f_0(x)g_0(-x) + f_0(-x)g_0(x))(f_0(x)g_0(-x) - f_0(-x)g_0(x)).$$

Let $\deg(k(x)) = r$. Then $\deg(f_0(x)) = \deg(g_0(x)) = \frac{1}{2}(2d - r)$. Since the degree of polynomial

$$2f_0(x)g_0(-x) = (f_0(x)g_0(-x) + f_0(-x)g_0(x)) + (f_0(x)g_0(-x) - f_0(-x)g_0(x))$$

is $2d - r$, the degree of $(f_0(x)g_0(-x) + f_0(-x)g_0(x))$ or $(f_0(x)g_0(-x) - f_0(-x)g_0(x))$ is greater than or equal to $2d - r$. Then a lower bound of the degree of polynomial in the left side of (9) is given by

$$\deg(k(x)k(-x)(f_0(x)^2 g_0(-x)^2 - f_0(-x)^2 g_0(x)^2)) \geqslant r + r + (2d - r) = 2d + r.$$

Comparing the degrees of polynomials in the both sides of equation (9), we have $2d+r \leqslant 2d+1$, which contradicts to $r \geqslant 2$.

Let $f(x)$ and $g(x)$ discussed above be polynomials corresponding to sequences $\mathbf{a}$ and $\mathbf{b}$ in $\mathcal{S}'_{2d}$, respectively. According to (4) and Corollary 1, we have $|C_{\mathbf{a},\mathbf{b}}(\tau)| \leqslant (4d-2)\sqrt{q}+4d+2$ for either $\mathbf{a} \neq \mathbf{b}$ or $\tau \neq 0$. □

Construction 3: $\mathcal{S}'_{2d+1} = \{\{\log(f(\alpha^i)) \pmod 2\}_{i\geqslant 0} | f(x) = \sum_{i=1}^{d} a_i x^{2i+1} + x + 1 \in \mathbb{F}_q[x], a_d \neq 0\}$ for $1 \leqslant d \ll \sqrt{q}$.

Theorem 3 *For Construction 3, S'_{2d+1} is a $(q-1, (q-1)q^{d-1}, 4d\sqrt{q}+4d+4)$ sequence family.*

Proof: Every polynomial corresponding to sequence in Construction 2 is the summation of a even polynomial and term x, while that in Construction 3 is the summation of an odd polynomial and constant term 1. Following the process of proof for Theorem 2, we prove Theorem 3 below.

For polynomials $f(x)$ and $g(x)$ of the form $\sum_{i=1}^{d} a_i x^{2i+1} + x + 1 \in \mathbb{F}_q[x]$ $(a_d \neq 0)$, we show that $f(x)g(\alpha^\tau x) \neq c \cdot h^2(x)$ for either $f(x) \neq g(x)$ or $\tau \neq 0$. Otherwise, assume $f(x) = c_f k(x)(f_0(x))^2$ and $g(\alpha^\tau x) = c_g k(x)(g_0(x))^2$ where $k(x) = (f(x), g(\alpha^\tau x))$, $c_f, c_g \in \mathbb{F}_q^*$, and $f_0(x), g_0(x)$ and $k(x)$ are all monic polynomials in $\mathbb{F}_q[x]$. Then we have $\deg(k(x)) \geqslant 1$.

Let $k(x)(f_0(x))^2 = f_1(x) + c_1$ and $k(x)(g_0(x))^2 = g_1(x) + c_2$, where $f_1(x)$ and $g_1(x)$ are both odd polynomials and $c_1, c_2 \in \mathbb{F}_q^*$. Then we have

$$k(x)f_0(x)^2 k(-x)g_0(-x)^2 = (f_1(x)+c_1)(g_1(-x)+c_2) = (f_1(x)+c_1)(-g_1(x)+c_2), \tag{10}$$

and

$$k(-x)f_0(-x)^2 k(x)g_0(x)^2 = (f_1(-x)+c_1)(g_1(x)+c_2) = (-f_1(x)+c_1)(g_1(x)+c_2). \tag{11}$$

From(10)-(11), we obtain

$$k(x)k(-x)(f_0(x)^2 g_0(-x)^2 - f_0(-x)^2 g_0(x)^2) = 2(c_2 f_1(x) - c_1 g_1(x)). \tag{12}$$

If $c_2 f_1(x) - c_1 g_1(x) = 0$, then

$$c_2 k(x)(f_0(x))^2 - c_1 k(x)(g_0(x))^2 = c_2(f_1(x)+c_1) - c_1(g_1(x)+c_2) = 0,$$

which induces that $g(\alpha^\tau x) = c' \cdot f(x)$ for some $c' \in \mathbb{F}_q^*$. By comparing the coefficients of linear and constant terms of $f(x)$ and $g(\alpha^\tau x)$, we have $f(x) = g(x)$ and $\tau = 0$.

If $c_2 f_1(x) - c_1 g_1(x) \neq 0$, we consider the degrees of the polynomials in both sides of equation (12). For the right side of (12), it is obvious

$$\deg(2(c_2 f_1(x) - c_1 g_1(x))) \leqslant 2d+1.$$

Decompose the polynomial in the left side of (12), we get

$$k(x)k(-x)(f_0(x)^2g_0(-x)^2-f_0(-x)^2g_0(x)^2) = k(x)k(-x)(f_0(x)g_0(-x)+f_0(-x)g_0(x))(f_0(x)g_0(-x)-f_0(-x)g_0(x)).$$

Let $\deg(k(x)) = r$. Then $\deg(f_0(x)) = \deg(g_0(x)) = \frac{1}{2}(2d - r + 1)$. Since the degree of polynomial

$$2f_0(x)g_0(-x) = (f_0(x)g_0(-x) + f_0(-x)g_0(x)) + (f_0(x)g_0(-x) - f_0(-x)g_0(x))$$

is $2d-r+1$, the degree of $(f_0(x)g_0(-x)+f_0(-x)g_0(x))$ or $(f_0(x)g_0(-x) - f_0(-x)g_0(x))$ is greater than or equal to $2d - r + 1$. Then a lower bound of the degree of polynomial in the left side of (12) is given by

$$\deg(k(x)k(-x)(f_0(x)^2g_0(-x)^2 - f_0(-x)^2g_0(x)^2)) \geqslant r + r + (2d - r + 1) = 2d + r + 1.$$

Comparing the degrees of polynomials in the both sides of equation (12), we have $2d + r + 1 \leqslant 2d + 1$, which contradicts to $r \geqslant 1$.

Let $f(x)$ and $g(x)$ discussed above be polynomials corresponding to sequences $\mathbf{a}$ and $\mathbf{b}$ in $\mathcal{S}'_{2d+1}$, respectively. According to (4) and Corollary 1, we have $|C_{\mathbf{a},\mathbf{b}}(\tau)| \leqslant 4d\sqrt{q} + 4d + 4$ for either $\mathbf{a} \neq \mathbf{b}$ or $\tau \neq 0$. □

Construction 4: $\mathcal{S}_{2d} = \mathcal{S}'_{2d} \cup \mathcal{S}'_{2d-1}$ for $2 \leqslant d \ll \sqrt{q}$.

Theorem 4 *For Construction 4, $\mathcal{S}_{2d}$ is a $(q-1, (q^2-1)q^{d-2}, (4d-2)\sqrt{q} + 4d + 2)$ sequence family.*

Proof: There are three cases for the sequence $\mathbf{a}$ and $\mathbf{b}$ in $\mathcal{S}_{2d}$ which are shown below.

Case 1: For $\mathbf{a}, \mathbf{b} \in \mathcal{S}'_{2d}$, it was shown that $|C_{\mathbf{a},\mathbf{b}}(\tau)| \leqslant (4d-2)\sqrt{q} + 4d + 2$ for either $\mathbf{a} \neq \mathbf{b}$ or $\tau \neq 0$ in Theorem 2.

Case 2: For $\mathbf{a}, \mathbf{b} \in \mathcal{S}'_{2d-1}$, it was shown that $|C_{\mathbf{a},\mathbf{b}}(\tau)| \leqslant 4(d-1)\sqrt{q} + 4d$ for either $\mathbf{a} \neq \mathbf{b}$ or $\tau \neq 0$ in Theorem 3.

Case 3: For $\mathbf{a} \in \mathcal{S}'_{2d}$ and $\mathbf{b} \in \mathcal{S}'_{2d-1}$, let $f(x)$ and $g(x)$ be their respective associated polynomials. Then $\deg(f(x)g(\alpha^\tau x)) = 4d - 1$ which implies that $f(x)g(\alpha^\tau x) \neq c \cdot h^2(x)$ for any $c \in \mathbb{F}_q^*$ and $h(x) \in \mathbb{F}_q[x]$. According to (4) and Corollary 1, we have $|C_{\mathbf{a},\mathbf{b}}(\tau)| \leqslant (4d-2)\sqrt{q} + 4d$ for every τ.

From the discussions above, the assertion follows immediately. □

Construction 5: $\mathcal{S}_{2d+1} = \mathcal{S}'_{2d+1} \cup \mathcal{S}'_{2d}$ for $1 \leqslant d \ll \sqrt{q}$, where $\mathcal{S}'_2 = \mathcal{S}_2 \setminus \{\{\log(\alpha^i + 1) \pmod 2\}_{i \geqslant 0}\}$.

Theorem 5 *For Construction 5, $\mathcal{S}_{2d+1}$ is a sequence family with maximum correlation $4d\sqrt{q} + 4d + 4$. The family sizes of $\mathcal{S}_{2d+1}$ are given by $2(q-1)q^{d-1}$ for $d \geqslant 2$, and $2(q-1) - 1$ for $d = 1$.*

Proof: The proof is similar to that of Theorem 4. □

We make a summary of the constructions in this section. For $2 \leqslant m \ll \sqrt{q}$, new sequence families $\mathcal{S}_m$ were proposed in Constructions 1 for $m = 2$, in Construction 4 for $m > 2$, m even, and in Construction 5 for m odd. Combined Theorems 1, 4 and 5 together, we get that $\mathcal{S}_m$ are sequence families of period $q-1$ with maximum correlation $(2m-2)\sqrt{q}+2m+2$, and the family sizes of $\mathcal{S}_m$ are given by $q-1$ for $m = 2$, $2(q-1)-1$ for $m = 3$, $(q^2-1)q^{\frac{m-4}{2}}$ for m even, $m > 2$, and $2(q-1)q^{\frac{m-3}{2}}$ for m odd, $m > 3$.

4 Relations to Sidel'nikov-Based and Power Residue-Based Sequence Families

In this section, we discuss the relationships between the known binary Sidel'nikov-based and power residue-based sequence families and the new constructions in this paper.

4.1 Sidel'nikov-Based Sequence Families and $\mathcal{S}_2$

There have been a few constructions of M-ary sequences of period $q-1$ derived from multiplicative character of $\mathbb{F}_q$ in the literature, e.g., [10, 6, 5, 4, 17]. For $M = 2$, we list the results in the above references below.

The construction in [6] consists only one binary sequence of period $q-1$. We denote it as

$$\mathcal{C}_1 = \{\{\log(\alpha^i+1) \pmod 2\}_{i\geqslant 0}\}$$

which contains only a Sidel'nikov sequence corresponding to polynomial $x+1$. We denote the binary sequence family of period $q-1$ in [5, 4] as

$$\mathcal{C}_2 = \{\{\log(f(\alpha^i)) \pmod 2\}_{i\geqslant 0} | f(x) = (x+1)(\alpha^l x+1), 1 \leqslant l < \frac{q-1}{2}\}.$$

Then $\mathcal{C}_1 \cup \mathcal{C}_2$ is a $(q-1, \frac{q-1}{2}, 2\sqrt{q}+6)$ sequence family [5, 4]. The interleaved structure of Sidel'nikov sequences was studied in [17]. By writing a Sidel'nikov sequence of period q^2-1 as a $(q-1)\times(q+1)$ array, it was 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. We denote the binary sequence family in [17] as

$$\mathcal{D}_2 = \{\{\log(f(\alpha^i)) \pmod 2\}_{i\geqslant 0} | f(x) = \beta^{(q+1)j}x^2 - (\beta^j + \beta^{qj}) \cdot x + 1, 1 \leqslant j \leqslant \frac{q-1}{2}\}.$$

Then $\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{D}_2$ is a $(q-1, q-1, 2\sqrt{q}+6)$ sequence family [17].

Actually, sequence family $\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{D}_2$ is equivalent to $\mathcal{S}_2$ in our Construction 1, i.e., for every sequence $\mathbf{a} \in \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{D}_2$, there exists one sequence $\mathbf{b} \in \mathcal{S}_2$ such that $\mathbf{b} = L_\tau(\mathbf{a})$ for some τ, and vise versa. Let $\mathbf{a}$ be a sequence in $\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{D}_2$ corresponding to polynomial $f(x)$. Then the polynomial corresponding to $L_\tau(\mathbf{a})$ is given by $f(a^\tau x)$. Note that the coefficient of linear term in $f(x)$ is nonzero. Thus there exists τ such that the coefficient of linear term in $f(a^\tau x)$ equals 1, which induces that there exists sequence $\mathbf{b} \in \mathcal{S}_2$ such that $\mathbf{b} = L_\tau(\mathbf{a})$. From the above discussions, together with the facts $|\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{D}_2| = |\mathcal{S}_2| = q-1$ and $C_{\max}(\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{D}_2) = C_{\max}(\mathcal{S}_2) = 2\sqrt{q}+6$, we know these two sequence families are equivalent.

From the observation above, $\mathcal{S}_2$ in our Construction 1 can be regarded as the binary sequence family in [6, 5, 4, 17] with uniform expression. And by a nontrivial generalization of the sequence family $\mathcal{S}_2$, we obtain new binary sequence families $\mathcal{S}_m$ for $m \geqslant 2$.

Besides, there is another generalization of sequence family $\mathcal{C}_1 \cup \mathcal{C}_2$ based on shift-and-addition of Sidel'nikov sequences in [16]. However, the basic ideas of constructions in [16] and this paper are totally different. Generally speaking, the method in [16] can be regarded as Sidel'nikov sequence-based generalization, while that in this paper is a polynomial-based generalization.

4.2 An Union Set of Power Residue-Based Sequence Families

For $q = p$, there exists another method for indexing the elements of $\mathbb{F}_p$, so there exists another method to define sequences. For a given polynomial $f(x) \in \mathbb{F}_p[x]$, define a sequence $\mathbf{a}$ corresponding to $f(x)$ by

$$a(i) \equiv \log(f(i)) \pmod 2,$$

or alternatively,

$$a(i) = \begin{cases} 0, & \text{if } f(i) \text{ is a square in } \mathbb{F}_p, \\ 1, & \text{if } f(i) \text{ is a nonsquare in } \mathbb{F}_p. \end{cases}$$

Then $\mathbf{a} = \{a(i)\}_{i \geqslant 0}$ is a binary sequence of period p. For example, the polynomial corresponding to Legendre sequence is given by $f(x) = x$. From the definition of the sequences and quadratic characters, the correlation of the sequences $\mathbf{a}$ and $\mathbf{b}$ corresponding to $f(x)$ and $g(x)$, respectively, is presented by

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{i=0}^{p-1} (-1)^{a(i)-b(i+\tau)} = \sum_{i=0}^{p-1} (-1)^{\log(f(i)g(i+\tau))} = \sum_{x \in \mathbb{F}_p} \chi(f(x)g(\alpha^\tau x)), \tag{13}$$

where χ is the quadratic multiplicative character of $\mathbb{F}_p$ with assumption $\chi(0) = 1$. Therefore, an upper bound of $|C_{\mathbf{a},\mathbf{b}}(\tau)|$ can be obtained by Corollary 1. There have been a few constructions of M-ary sequences of period p derived from multiplicative character of $\mathbb{F}_p$ in [7, 5, 4, 13]. When $M = 2$, we list the results in the above references below.

The construction in [7] consists only one binary sequence of period p. We denote it as

$$\mathcal{A}_1 = \{\{\log(i) \pmod 2\}_{i \geqslant 0}\}$$

which contains only a Legendre sequence corresponding to polynomial x. We denote the binary sequence family of period p in [5, 4] as

$$\mathcal{A}_2 = \{\{\log(f(i)) \pmod 2\}_{i\geqslant 0} | f(x) = x(x+l), 1 \leqslant l \leqslant \frac{p-1}{2}\}.$$

Then $\mathcal{A}_1 \cup \mathcal{A}_2$ is a $(p, \frac{p+1}{2}, 2\sqrt{p}+5)$ sequence family [5, 4]. Note that α and β are primitive elements in $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$, respectively. We denote the binary sequence family in [13] as

$$\mathcal{B}_2 = \{\{\log_\alpha(f(i)) \pmod 2\}_{i\geqslant 0} | f(x) = x^2 - j(\beta+\beta^p)\cdot x + j^2\beta^{p+1}, 1 \leqslant j \leqslant \frac{p-1}{2}\}.$$

Then $\mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{B}_2$ is a $(p, p, 2\sqrt{p}+5)$ sequence family [13].

Inspired by our construction $\mathcal{S}_2$, we give a sequence family which is equivalent to $\mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{B}_2$ with uniform expression as follows.

Construction 6: $\mathcal{L}_2 = \{\{\log(f(\alpha^i)) \pmod 2\}_{i\geqslant 0} | f(x) = x$ or $f(x) = x^2 + x + a \in \mathbb{F}_p[x], a \neq (2^{-1})^2\}$.

Theorem 6 *For Construction 6, $\mathcal{L}_2$ is equivalent to $\mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{B}_2$, so $\mathcal{L}_2$ is a $(p, p, 2\sqrt{p}+5)$ sequence family.*

Proof: Let $\mathbf{a}$ be a sequence in $\mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{B}_2$ corresponding to polynomial $f(x)$ of degree 2. Then the polynomial corresponding to $L_\tau(\mathbf{a})$ is given by $f(x+\tau)$. There exists τ such that the coefficient of linear term in $f(x+\tau)$ equals 1, which induces that there exists sequence $\mathbf{b} \in \mathcal{L}_2$ such that $\mathbf{b} = L_\tau(\mathbf{a})$. From the above discussions, together with the facts $|\mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{B}_2| = |\mathcal{L}_2| = q-1$ and $C_{\max}(\mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{B}_2) = 2\sqrt{p}+5$, we know these two sequence families are equivalent. Then the result follows. □

5 Conclusions

In this paper, binary sequences derived form the multiplicative character of finite fields were studied. For $2 \leqslant m \ll \sqrt{q}$, new sequence families $\mathcal{S}_m$ of period $q-1$ with maximum correlation $(2m-2)\sqrt{q}+2m+2$ were constructed. The family sizes of $\mathcal{S}_m$ are given by $q-1$ for $m=2$, $2(q-1)-1$ for $m=3$, $(q^2-1)q^{\frac{m-4}{2}}$ for m even, $m>2$, and $2(q-1)q^{\frac{m-3}{2}}$ for m odd, $m>3$. We showed that the known binary Sidel'nikov-based sequence family in [6, 5, 4, 17] is equivalent to family $\mathcal{S}_2$ where the sequences are presented in the uniform expression. We also showed binary power residue-based sequence family in [7, 5, 4, 13] is equivalent to our construction $\mathcal{L}_2$.

Acknowledgment

The first author would like to thank Prof. Daqing Wan for communication of his paper [12].

References

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

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

[3] L. Goubin, C. Mauduit and A. S*á*rk*ö*zy, “Construction of large families of pseudorandom binary sequences,” *J. Number Theory*, vol. 106, pp.56-69, 2004.

[4] 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.

[5] 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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

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

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

[13] Z. Wang and G. Gong, “New polyphase sequence families with low correlation derived from the Weil bound of exponential sums,” Preprint.

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

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

[16] 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.

[17] 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.