Character Sums and Polyphase Sequence Families with Low Correlation, DFT and Ambiguity

Guang Gong
Department of Electrical and Computer Engineering
University of Waterloo, Waterloo, Ontario, Canada
Email: ggong@uwaterloo.ca

Abstract

We present a survey on the current status of the constructions of polyphase sequences with low correlation, discrete Fourier transform (DFT), and ambiguity in both time and phase domain, including some new insights and results. Firstly, we systematically introduce the concepts of phase-shift operators and ambiguity functions of sequences, and give a new construction of polyphase sequences from combinations of different indexing field elements and hybrid characters. We then present the constructions, some known and some new, of polyphase sequences with low degree polynomials, for their low correlation, DFT and ambiguity can be bounded by directly applying the Weil bounds. Thirdly, we introduce the Hadamard equivalence, restate the conjectured new ternary 2-level autocorrelation sequences, and present their Hadamard equivalence relations. Some open problems are presented.

Key words: Polyphase sequence, character sum, finite field, time shift, phase shift, correlation, discrete Fourier transform, ambiguity function, 2-level autocorrelation.

1 Introduction

Sequences with good correlation properties find many applications in wireless communications. In particular, low correlation is used for acquiring the correct timing information and distinguishing multiple users or channels, minimized discrete Fourier transform (DFT) spectra are for getting low peak-to-average power ratio (PAPR) for orthogonal frequency division multiplexing (OFDM) systems, and low ambiguity functions are for radar systems and signal processing schemes.

Correlation, DFT and ambiguity of polyphase sequences are three properties used in practical systems for evaluating the performance of a communication system which employs polyphase sequences. We will give formal definitions for these three concepts in the later sections. However, mathematically, those three properties of polyphase sequences are determined by some exponential sums. Thus, sequences with low correlation, DFT and ambiguity can be constructed directly using low degree polynomials where the Weil bounds are applicable. However, using additive character

sums, there are many known sequences with low correlation or 2-level autocorrelation which correspond to high degree polynomials, whose correlation cannot be bounded by the Weil bound, neither their DFT nor their ambiguity.

In this survey, Section 2 is an introduction to basic definitions and concepts of sequences, and additive, multiplicative, and hybrid character sums. Section 3 introduces phase-shift operators, ambiguity functions, ambiguity signal sets, and the optimality of correlation, DFT, and ambiguity. Section 4 introduces polyphase sequences defined by the additive group $\mathbb{Z}_N$ and by additive and multiplicative characters under different indexing methods, and their corresponding exponential sums of the correlation, DFT and ambiguity. Section 5 shows the constructions of three types of polyphase signal sets with low three metrics, namely, polyphase sequences defined by odd degree polynomials, polyphase sequences from power residue and Sidel'nikov sequences, and polyphase sequences from Weil representation and from general hybrid characters. In Section 6, we present four conjectures on ternary 2-level autocorrelation sequences, Hadamard equivalence of those conjectured sequences, and the exponential sums in terms of iterative decimation Hadamard transform. Section 7 addresses some open problems.

2 Basic Definitions and Concepts

2.1 Notations

The following notations will be used throughout this paper.

- $\mathbb{C}$ is the complex field, M a positive integer, $\mathbb{Z}_M = \{0, 1, \ldots, M-1\}$, and $\omega_M = e^{i\frac{2\pi}{M}}$ is a primitive complex M-th root of unity where $i = \sqrt{-1}$.
- p is a prime, n a positive integer, $q = p^n$, $\mathbb{F}_q$ the finite field with q elements, $\mathbb{F}_q^*$ the multiplicative group of $\mathbb{F}_q$, α a primitive element in $\mathbb{F}_q$, $\overline{\mathbb{F}}_q$ the algebraic closure of $\mathbb{F}_q$ and $Tr_r^n(x) = x + x^{q_1} + \ldots + x^{q_1^{n/r-1}}$ $(q_1 = p^r)$ the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^r}$ with $r \,|\, n$ where $Tr_1^n(x)$ is denoted by $Tr(x)$ for simplicity.
- For $x \in \mathbb{F}_q$, *the discrete logarithm* to the base α is defined by

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

  or simply as $\log x$ if the context is clear.
- $\mathbf{a} = \{a(t)\}_{t\ge 0}$ where $a(t) \in \mathbb{Z}_M$, is called an M-ary sequence. If $a(t+N) = a(t)$, for all $t = 0, 1, \ldots$, then we say that N is a *period* of $\{a(t)\}$. The smallest integer with this property is called the *least period* of the sequence. Throughout this paper, when we say *the period* of the sequence we mean that it is the least period of the sequence for simplicity. If $\mathbf{a}$ has period N, then we use $(a(0), \ldots, a(N-1))$, a vector of dimension N, to represent the sequence.

- U is the set consisting of all complex sequences whose entries have magnitude 1, i.e., $\mathbf{a} = (a(0), a(1), \ldots) \in U$, $|a(t)| = 1$, for $t = 0, 1, \ldots$. Let $\mathbf{x} = (x_0, \ldots, x_{N-1})$ and $\mathbf{y} = (y_0, \ldots, y_{N-1})$ be two sequences in $\mathbb{C}^N$, the inner product of $\mathbf{x}$ and $\mathbf{y}$ is defined by $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{j=0}^{N-1} x_i y_j^*$ where y^* is the conjugate of the complex number y.

2.2 Polynomial Functions over $\mathbb{F}_q$

Any polynomial in $\mathbb{F}_q[x] = \{\sum_i c_i x^i, c_i \in \mathbb{F}_q\}$ is considered as a polynomial function mapping from $\mathbb{F}_q$ to $\mathbb{F}_q$. We may assume that their (algebraic) degrees of these polynomials are less than or equal to $q-1$ because of $x^q = x, x \in \mathbb{F}_q$.

Property 1 *Let $f(x) = \sum_{i=0}^{q-1} c_i x^i$ and $g(x) = \sum_{i=0}^{q-1} d_i x^i$ be polynomials in $\mathbb{F}_q[x]$. Then $f(x) = g(x)$ for all $x \in \mathbb{F}_q$ if and only if $c_i = d_i$, for $i = 0, 1, \ldots, q-1$.*

For a function mapping from $\mathbb{F}_q$ to $\mathbb{F}_p$ where $q = p^n, n > 1$, we need some concepts on (cyclotomic) cosets. A coset containing r modulo $q-1$ is defined as $C_r = \{r, rp, \ldots, rp^{n_r-1}\} \subset \mathbb{Z}_{q-1}$ where n_r is the smallest positive integer such that $r \equiv rp^{n_r} \bmod (q-1)$. The smallest integer in C_r is called the *coset leader* of C_r. Note that $n_r \,|\, n$. Let $\Gamma(q)$ be the set consisting of all coset leaders modulo $(q-1)$.

Let $\xi(x)$ be a mapping from $\mathbb{F}_q$ to $\mathbb{F}_p$, then $\xi(x)$ can be represented by

$$\xi(x) = \sum_{r \in \Gamma(q)} Tr_1^{n_r}(\beta_r x^r) \tag{1}$$

where $\beta_r \in \mathbb{F}_{p^{n_r}}$ and $n_r = |C_r|$, the size of the coset containing r. This is called the *trace representation* of a function from $\mathbb{F}_q$ to $\mathbb{F}_p$. It can be computed in terms of the discrete Fourier transform (DFT) over $\mathbb{F}_q$ (see [14]). The trace representation of a function from $\mathbb{F}_q$ to $\mathbb{F}_p$ is unique.

Property 2 *The trace representation (1) of ξ satisfies $\xi(x) = 0$ for all $x \in \mathbb{F}_q$ if and only if $\beta_r = 0$ for all $r \in \Gamma(q)$.*

Note that for any function $\xi(x)$ from $\mathbb{F}_q$ to $\mathbb{F}_p$, we can find a polynomial $f(x)$ in $\mathbb{F}_q[x]$ with exponents being coset leaders modulo $(q-1)$, i.e.,

$$f(x) = \sum_{r \in \Gamma(q)} c_r x^r, \text{ such that } \xi(x) = Tr(f(x)), x \in \mathbb{F}_q. \tag{2}$$

However, this representation is not unique except for the following case.

Property 3 *For $f(x) = \sum_{r \in \Gamma(q)} c_r x^r, c_r \in \mathbb{F}_q$, if for all $c_r \neq 0$, the coset leaders r have the full length n (i.e., $|C_r| = n$), then $f(x) = 0$ if and only if $c_r = 0$ for all $r \in \Gamma(q)$.*

In this paper, in order to easily incorporate the process for directly applying the Weil bound, we use the form given in (2) for a function from $\mathbb{F}_q$ to $\mathbb{F}_p$. For the theory of finite fields and the basics of sequences with good correlation properties, the reader is referred to [14, 34].

2.3 Characters of Finite Fields

Let G be a finite abelian group with identity 1. A character χ of G is a homomorphism from G into U (recalled that U is the multiplicative group of complex numbers with magnitude 1), i.e., a mapping from G into U with $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$ for all $g_1, g_2 \in G$.

Definition 1 *(**Additive character**) For each $j = 0, 1, \ldots, p-1$, the function ψ_j, given by*

$$\psi_j(x) = e^{2\pi i j Tr(x)/p} = \omega_p^{jTr(x)}, x \in \mathbb{F}_q$$

defines an additive character of $\mathbb{F}_q$ as a character of the additive group of $\mathbb{F}_q$. We also denote it as $\psi(x)$ when $j = 1$. Furthermore,

$$\psi_j(x+y) = \psi_j(x)\psi_j(y), \forall x, y \in \mathbb{F}_q.$$

Definition 2 *(**Multiplicative Character**) Let $M \,|\, (q-1)$. For each $j = 0, 1, \ldots, M-1$, a multiplicative character χ_j of order $M/\gcd(j, M)$, as a character of the multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$, is defined by*

$$\chi_j(\alpha^k) = e^{2\pi i j k/M} = \omega_M^{jk},\ \alpha^k \in \mathbb{F}_q^*$$

or equivalently

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

We extend the definition of χ_j at zero by $\chi_j(0) = 1$ throughout this paper if not stated otherwise. We denote χ^0 as the trivial multiplicative character, i.e., $\chi^0(x) = 1$ for all $x \in \mathbb{F}_q^*$, and $\chi_1(x)$ as $\chi^1(x)$ when we emphasize the case that $M = q-1$ and $j = 1$. Furthermore,

$$\chi_j(x \cdot y) = \chi_j(x)\chi_j(y),\ \textit{for all } x, y \in \mathbb{F}_q^*.$$

2.4 The Weil Bounds on Character Sums

The following three lemmas are in [54, 55] and Corollary 1 is improved from a variation in [50].

Lemma 1 *Let ψ be a nontrivial additive character over $\mathbb{F}_q$ and $f(x) = c_r x^r + \ldots + c_1 x + c_0 \in \mathbb{F}_q[x]$ with $deg(f) = r \geq 1$, $\gcd(r, q) = 1$ and $f \neq g^p - g + c$ for all $g(x) \in \mathbb{F}_q[x]$ and $c \in \mathbb{F}_q$, then*

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

Lemma 2 *Let χ be a multiplicative character of $\mathbb{F}_q$ of order $M > 1$ and $\chi(0) = 0$. For $g \in \mathbb{F}_q[x]$, $g(x) \neq c \cdot h^M(x)$ for some $h \in \mathbb{F}_q[x]$, let d be the number of distinct roots of g in the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$, then*

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

However, in sequence design, it is more convenient to define $\chi(0) = 1$, as shown in [59]. Thus, the above lemma can be rewritten as follows in order to easily determine the correlation related properties of sequences, which is the version that we use in this paper.

Corollary 1 *With the notation in Lemmas 1 and 2, if we define $\chi(0) = 1$ and let e be the number of distinct roots of $g(x)$ in $\mathbb{F}_q$. Then*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(g(x)) \right| \leq \begin{cases} (d-1)\sqrt{q} + e \\ (d-2)\sqrt{q} + 1 + e \quad \text{if } M | deg(g). \end{cases}$$

From Corollary 1 and the hybrid sum in [55], the following result follows immediately.

Lemma 3 *Let ψ be a nontrivial additive character of $\mathbb{F}_q$ and χ a nontrivial multiplicative character of $\mathbb{F}_q$ of order $M > 1$ with $\chi(0) = 1$. Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of degree r with the condition in Lemma 1, and $g(x) \in \mathbb{F}_q[x]$ with $g(x) \neq c \cdot h^M(x)$ and d distinct roots in $\overline{\mathbb{F}}_q$ and e distinct roots in $\mathbb{F}_q$. Then*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(g(x)) \psi(f(x)) \right| \leq \ (r + d - 1)\sqrt{q} + e. \tag{3}$$

We call the sum of (3) *a hybrid character sum.*

3 Correlation, DFT, and Ambiguity Functions

3.1 Operators on Sequences

We first define four operators on U, namely, decimation D_s, the time-shift L_τ, (linear) M phase-shift P_w, and discrete Fourier transform (DFT) F. Given $\mathbf{a} = \{a(t)\} \in U$ and a fixed positive integer $H > 1$, for s, τ, w arbitrary integers, and $t = 0, 1, \ldots$, we define

Decimation	$D_s[\mathbf{a}](t) := a(st)$
Time-shift	$L_\tau[\mathbf{a}](t) := a(t + \tau)$
Phase-shift	$P_w[\mathbf{a}](t) := \omega_H^{wt} a(t)$

The N points $(\widetilde{a}(0), \widetilde{a}(1), \ldots, \widetilde{a}(N-1))$ of the DFT of $(a(0), \ldots, a(N-1))$ are defined as follows:

$$\widetilde{a}(k) = F[\mathbf{a}](k) := \sum_{t=0}^{N-1} a(t)\omega_N^{-tk} \tag{4}$$

where we use the notation $\widetilde{a}$ for $F[\mathbf{a}]$ for simplicity. The inverse DFT (IDFT) is given by

$$a(t) = \frac{1}{N}\sum_{k=0}^{N-1} \widetilde{a}(k)\omega_N^{tk}.$$

The time-shift and phase-shift operators capture the characteristic of signals when they are transmitted through physical channels. At the receiver's side, due to the possible Doppler's effect and multipath propagation of the channel, the received signal (or sequence) could be both time shifted and phase shifted. Also, one could receive multiple shifted signals. For the phase shift, the received signal could have nonlinear phase shifts. However, it is difficult to build a model which captures all these factors in real communication systems. Thus, we simplify the scenario to only considering the linear phase shift.

Furthermore, in sequence design, the choice of H for the phase-shift operator is determined by the algebraic structure over which the sequence is defined. In other words, we restrict the values of H to N, q, p, $q-1$ or $p-1$ depending on the sequences defined over $\mathbb{Z}_N$, $\mathbb{F}_p$ or $\mathbb{F}_q$, additively or multiplicatively. Those phenomena will be elaborated clearly in the next section. Note that this restriction is convenient for theoretical studies. However, it may be not the case in practice.

It is worth to point out that sequence $\mathbf{a}$ may not be periodic and N may not be the period of $\mathbf{a}$ when the DFT is applied. The definition of DFT is very general, which is applied to any finite segment of a sequence with an infinite length in U. This is the typical case in the application of orthogonal frequency division multiplexing (OFDM) communications. However, in this paper, we assume that $\mathbf{a}$ has the period N. For the theory of digital communications, the reader is referred to [41, 42].

Definition 3 *For two sequences* $\mathbf{a}$ *and* $\mathbf{b}$ *with period* N*, if* $\mathbf{b} = D_s\mathbf{a}$ *with* $\gcd(s, N) = 1$ *or* $\mathbf{b} = L_\tau\mathbf{a}$ *or* $\mathbf{b} = P_w\mathbf{a}$*, then we say that* $\mathbf{a}$ *and* $\mathbf{b}$ *are* decimation equivalent *or* time-shift equivalent *or* phase-shift equivalent*. We denote them as* $\mathbf{b} \sim_T \mathbf{a}$*,* $T \in \{D_s, L_\tau, P_w\}$*. Otherwise, they are* decimation distinct *or* time-shift distinct *or* phase-shift distinct*.*

3.2 Correlation Functions

Let $\mathcal{S} \subset U$ consist of the sequences with period N. For two sequences $\mathbf{a} = \{a(t)\}$ and $\mathbf{b} = \{b(t)\}$ in $\mathcal{S}$, the *crosscorrelation* between $\mathbf{a}$ and $\mathbf{b}$ is defined by

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{t=0}^{N-1} a(t)b(t+\tau)^*, \tag{5}$$

or equivalently,

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \langle \mathbf{a}, L_\tau \mathbf{b} \rangle. \tag{6}$$

If $\mathbf{a} = \mathbf{b}$, then the crosscorrelation function becomes the *autocorrelation function*, denoted as $C_{\mathbf{a}}(\tau)$. The maximum correlation of $\mathcal{S}$ is defined by

$$C_{\max} := \max\{AC_{\max}, CC_{\max}\}$$

where the maximum autocorrelation is

$$AC_{\max} := \max\{|C_{\mathbf{a}}(\tau)| : \mathbf{a} \in \mathcal{S}, 1 \le \tau \le N-1\}$$

and the maximum crosscorrelation is

$$CC_{\max} := \max\{|C_{\mathbf{a},\mathbf{b}}(\tau)| : \mathbf{a}, \mathbf{b} \in \mathcal{S}, \mathbf{a} \ne \mathbf{b}, 0 \le \tau \le N-1\}.$$

We call $C_{\mathbf{a}}(\tau)$ for $\tau \not\equiv 0 \bmod N$ *out-of-phase autocorrelation* of $\mathbf{a}$.

Definition 4 *Let* $\mathbf{a} = \{a(t)\}$ *where* $a(t) \in \mathbb{Z}_{M'}$*, then a* modulated polyphase sequence *of* $\mathbf{a}$*, denoted as* $\omega^{\mathbf{a}}$*, is defined as* $\omega_M^{\mathbf{a}}$*, i.e.,*

$$\omega^{\mathbf{a}} := \omega_M^{\mathbf{a}} = (\omega_M^{a(0)}, \omega_M^{a(1)}, \ldots, \omega_M^{a(N-1)})$$

where M *and* M' *are not necessary to be equal. If both* $\mathbf{a}$ *and* $\mathbf{b}$ *are* M'*-ary sequences, then the crosscorrelation of* $\mathbf{a}$ *and* $\mathbf{b}$ *is defined through their modulated sequences, given as*

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{t=0}^{N-1} \omega_M^{a(t)-b(t+\tau)}.$$

Furthermore, the phase-shift operator is applied to the modulated sequence of $\mathbf{a}$*, i.e.,* $P_w(\mathbf{a}) = \{\omega_H^{wt}\omega_M^{a(t)}\}$.

Note that the decimation and time-shift operators do not change the image sets of the autocorrelation functions provided some conditions are satisfied. Specifically, we have the following results.

Property 4 *For* $\gcd(s, N) = 1$*,* $D_s(\mathbf{a})$*,* $L_\tau(\mathbf{a})$*, and* $\mathbf{a} + c$ *where* c *is constant have the same autocorrelation properties as* $\mathbf{a}$*. Furthermore, the autocorrelation function of* $\mathbf{b} := P_w(\mathbf{a})$ *is given by* $C_{\mathbf{b}}(\tau) = \omega_H^{-w\tau} C_{\mathbf{a}}(\tau)$.

We say that sequence $\mathbf{a}$ is a *perfect sequence* if $C_{\mathbf{a}}(\tau) = 0$ for $\tau \not\equiv 0 \bmod N$ and $\mathbf{a}$ is an *(ideal) 2-level autocorrelation sequence* if $C_{\mathbf{a}}(\tau) = -1$ for $\tau \not\equiv 0 \bmod N$.

According to Property 4, if $\mathbf{a}$ is a perfect or 2-level autocorrelation sequence, then $D_s\mathbf{a}$, $L_\tau\mathbf{a}$, and $\mathbf{a} + c$ are perfect or 2-level autocorrelation sequences where $1 \le s < N$ with $\gcd(s, N) = 1$. Furthermore, if $\mathbf{a}$ is perfect then $P_w(\mathbf{a})$ is perfect.

Example 1 We consider one binary sequence and one ternary sequence.

(a) Let $M = M' = 2$, $H = 3$ and $\mathbf{a} = (1101100)$. We denote ω_3 by ω for simplicity. Then $D_3(\mathbf{a})$, $L_2(\mathbf{a})$, and $P_2(\mathbf{a})$ are given as follows.

$\mathbf{a} = (1101100)$	
$(-1)^{\mathbf{a}} = (-1,-1,1,-1,-1,1,1)$	$\{C_{\mathbf{a}}(\tau)\} = (7,-1,-5,3,3,-5,-1)$
$D_3(\mathbf{a}) = (1100011)$	$\{C_{D_3(\mathbf{a})}(\tau)\} = (7,3,-1,-5,-5,-1,3)$
$L_2(\mathbf{a}) = (0110011)$	$C_{L_2(\mathbf{a})}(\tau) = C_{\mathbf{a}}(\tau)$
$P_2(\mathbf{a}) = (-1,-\omega^2,\omega,-1,-\omega^2,\omega,1)$	$\{C_{P_2(\mathbf{a})}(\tau)\} = (7,-\omega,-5\omega^2,3,3\omega,-5\omega^2,-1)$

(b) Let $M = M' = 3$, $H = 3$ and $\mathbf{a} = (1,0,1,1,2,0,2,2)$ where $a_i \in \mathbb{Z}_3$. Then $D_3(\mathbf{a})$, $L_2(\mathbf{a})$, and $P_2(\mathbf{a})$ are given as follows.

$\mathbf{a} = (1,0,1,1,2,0,2,2)$
$\omega^{\mathbf{a}} = (\omega,1,\omega,\omega,\omega^2,1,\omega^2,\omega^2)$
$D_3(\mathbf{a}) = (1,1,2,0,2,2,1,0)$
$L_2(\mathbf{a}) = (1,1,2,0,2,2,1,0)$
$P_2(\mathbf{a}) = (\omega,\omega^2,\omega^2,\omega,\omega,\omega,\omega^2,\omega)$

They all have the same autocorrelation as $\mathbf{a}$:

$$C_{\mathbf{a}}(\tau) = \begin{cases} 8 & \tau \equiv 0 \bmod 8 \\ -1 & \tau \not\equiv 0 \bmod 8. \end{cases}$$

3.3 Ambiguity Functions

Definition 5 *The* auto and cross ambiguity functions *of* $\mathbf{a}$ *and* $\mathbf{b}$ *of period* N *in* U *are defined as two-dimensional autocorrelation and crosscorrelation functions in both time and phase, given by*

$$G_{\mathbf{a}}(\tau, w) = \langle \mathbf{a}, P_w L_\tau \mathbf{a} \rangle \text{ and } G_{\mathbf{a},\mathbf{b}}(\tau, w) = \langle \mathbf{a}, P_w L_\tau \mathbf{b} \rangle, 0 \le \tau < N, 0 \le w < H.$$

Thus, the autocorrelation and crosscorrelation functions are equal to their respective auto and cross ambiguity functions for the case $w = 0$.

Definition 6 *A set* S *is called an* (N, r, σ) (correlation) signal set *if each sequence in* S *has period* N*, there are* r *time-shift distinct sequences in* S*, and both the maximum magnitude of out-of-phase autocorrelation values and crosscorrelation values are upper bounded by* σ*.*

Definition 7 *A set S is called an (N, r, σ, ρ)* ambiguity signal set *if it is an (N, r, σ) correlation signal set, all r sequences are both time-shift distinct and phase-shift distinct, and both the maximum magnitude of out-of-phase auto ambiguity functions and cross ambiguity functions are upper bounded by ρ, i.e.,*

$$|G_{\mathbf{a}}(\tau, w)| \leqslant \rho, \quad (\tau, w) \neq (0, 0),$$
$$|G_{\mathbf{a},\mathbf{b}}(\tau, w)| \leqslant \rho, \quad \mathbf{a} \neq \mathbf{b} \in S.$$

For $(\tau, w) \neq (0, 0)$, $G_{\mathbf{a}}(\tau, w)$ is referred to as the *out-of-phase auto ambiguity*. Similar to the correlation, we denote by $AG_{\max}$ the maximum magnitude of the out-of-phase auto ambiguity and by $CG_{\max}$ the maximum magnitude of the cross ambiguity functions of any two distinct sequences in S. If we define $G_{\max} = \max\{AG_{\max}, CG_{\max}\}$, then $G_{\max} \leq \rho$.

Definition 8 *If $\mathbf{u} = \{u(t)\} \in U$ and there exists an M-ary sequence $\mathbf{a} = \{a(t)\}, a(t) \in \mathbb{Z}_M$ such that $u(t) = \omega_M^{a(t)} v(t)$ where $\mathbf{v} \in U$, then we say that $\mathbf{u}$ has an M-*ary factor sequence.

According to this definition, the phase-shifted sequence of $\mathbf{u}$ is a sequence in U which has an H-ary factor sequence $\{\omega_H^{wt}\}$. In other words, the phase-shifted sequence of $\mathbf{u}$ is the term-by-term product sequence of $\{\omega_H^{wt}\}$ and $\{u(t)\}$.

Example 2 We assume that $\mathbf{a} = (1, 0, 1, 1, 2)$, $M' = M = 3$, $H = 3$ and $\omega = \omega_3$. Then we list a few values of auto ambiguity function of $\mathbf{a}$ in the following table.

$\mathbf{a}$	=	$(1, 0, 1, 1, 2)$	$G_{\mathbf{a}}(\tau, w) = \langle \mathbf{a}, P_w L_\tau \mathbf{a} \rangle$
$\omega^{\mathbf{a}}$	=	$(\omega, 1, \omega, \omega, \omega^2)$	
$P_1(\mathbf{a})$	=	$(\omega, \omega, 1, \omega, 1)$	$G_{\mathbf{a}}(0, 1) = -\omega$
$P_2(\mathbf{a})$	=	$(\omega, \omega^2, \omega^2, \omega, \omega)$	$G_{\mathbf{a}}(0, 2) = -\omega^2$
$L_1(\omega^{\mathbf{a}})$	=	$(1, \omega, \omega, \omega^2, \omega)$	$G_{\mathbf{a}}(1, 0) = -1$
$P_1 L_1(\omega^{\mathbf{a}})$	=	$(1, \omega^2, 1, \omega^2, \omega^2)$	$G_{\mathbf{a}}(1, 1) = 2\omega$
$P_2 L_1(\omega^{\mathbf{a}})$	=	$(1, 1, \omega^2, \omega^2, \omega)$	$G_{\mathbf{a}}(1, 2) = -1$

Property 5 *Let S_1 be an (N, r, σ, ρ) ambiguity signal set and let $S_2 = \{P_w \mathbf{u} = \{\omega_H^{wt} u(t)\} \,|\, w \in \mathbb{Z}_H, \mathbf{u} \in S_1\}$. Then S_2 is an (N, Hr, ρ) correlation signal set.*

Note that the concept of ambiguity functions is strongly related to Costas arrays, introduced by Costas in [6], and extensively studied in the literature, see [9, 13, 15], just to list a few. Up to now, systematically, there are only two constructions. One is the Welch construction using $\mathbb{F}_p$ and the other is the Lempel-Golomb construction using $\mathbb{F}_{2^n}$, which correspond to power residue and Sidel'nikov sequences, respectively. In the remainder of the paper, we restrict ourselves to a subset of U in which each sequence has at most two different M-ary factor sequences. From Property 5, given an ambiguity signal set, we can obtain a correlation signal set with the same correlation and the size increased to a multiple of the size of the given ambiguity signal set.

3.4 Convolution and Correlation

For $\mathbf{a}, \mathbf{b} \in U$ with period N, the correlation function between $\mathbf{a}$ and $\mathbf{b}$ is equal to convolution between $\mathbf{a}$ and $\mathbf{b}$, denoted as $\mathbf{a} * \mathbf{b}$, i.e.,

$$(\mathbf{a} * \mathbf{b})(\tau) = C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{t=0}^{N-1} a(t)b(t+\tau)^*. \tag{7}$$

From the signals and systems in digital communication [41], we have the following relation with their respective DFTs.

Property 6 *Let* $\mathbf{a}$ *and* $\mathbf{b}$ *be two complex sequences in* U*. Then*

$$\begin{array}{ll} \textit{DFT of the convolution:} & \widetilde{C}_{\mathbf{a},\mathbf{b}}(-k) = \widetilde{a}(k)\widetilde{b}(k)^* \\ \textit{Parseval Identity:} & \sum_{t=0}^{N-1} |a(t)|^2 = \frac{1}{N}\sum_{k=0}^{N-1} |\widetilde{a}(k)|^2 = N. \end{array}$$

3.5 Optimal Correlation, DFT and Ambiguity

From the Welch bound [56], an (N, r, σ, ρ) ambiguity signal set S where $r > 1$ has the maximum correlation, maximum DFT spectra $F_{\max} = \max\{|\widetilde{a}(k)| : \forall \mathbf{a} \in S, \forall k\}$ (it can be considered as crosscorrelation of two sequences), and maximum ambiguity being at least the square root of N, i.e.,

$$C_{\max}, F_{\max}, G_{\max} \geq \sqrt{N}, \text{for large } N.$$

Thus the best we aim for is to find signal sets for which those values are upper bounded by $c\sqrt{N}$ for a small constant $c \geq 1$.

Thus, we have the following criteria for measuring correlation, DFTs and ambiguity properties of ambiguity signal sets:

$$C_{\max} \leq c_1\sqrt{N} \tag{8}$$

$$F_{\max} \leq c_2\sqrt{N} \tag{9}$$

$$G_{\max} \leq c_3\sqrt{N} \tag{10}$$

where the c_is are constants satisfying $1 \leq c_i < \log\log N$ which do not depend on N. Therefore, in order to avoid repeatedly saying that the maximum of correlation functions, DFTs and ambiguity functions of the sequences in an ambiguity signal set satisfy (8)-(10), we simply refer each inequality above as a *metric*. For example, a metric for good correlation of a signal set means its maximum correlation is upper bounded by (8).

4 Polyphase Sequences for Three Metrics

In this section, we introduce polyphase sequences constructed from the additive group $\mathbb{Z}_N$ or finite fields. We will separate the sequences obtained from $\mathbb{F}_p$ additive and multiplicative characters and $\mathbb{F}_q$ additive and multiplicative characters, since their constructions are slightly different and easily confused. For polyphase sequences over a Galois ring, the reader is referred to [25] and references listed there.

4.1 Sequences from Additive Group of $\mathbb{Z}_N$ and Additive Group of $\mathbb{Z}_p$

Let

$$f(x) = c_r x^r + \ldots + c_1 x + c_0, c_i \in \mathbb{Z}_N.$$

An N-ary sequence $\mathbf{a} = \{a(t)\}_{t\geq 0}$ with period N from $\mathbb{Z}_N$ additive group and its modulated sequence are defined below.

$a(t) = f(t) \in \mathbb{Z}_N$	$\omega^{a(t)} = \omega_{kN}^{a(t)}$
an N-ary sequence	a (kN)-phase modulated sequence

(11)

where k is a positive integer. When $N = p$, a p-ary sequence $a(t)$ and its modulated sequence are defined as follows.

$a(t) = f(t) \in \mathbb{F}_p$	$\omega^{a(t)} = \psi_1(a(t)) = \omega_p^{a(t)}$
a p-ary sequence	a p-phase modulated sequence

(12)

where $\psi_1(x) = \omega^x, x \in \mathbb{F}_p$, an additive character defined in Section 2. We say that the sequence $\mathbf{a}$ is an *additive sequence over* $\mathbb{Z}_N$ or an *additive sequence over* $\mathbb{F}_p$ if $N = p$. Note that the modulated sequence given in (12) is a special case of (11) when $N = p$ and $k = 1$.

4.1.1 Frank-Zadoff-Chu (FZC) sequences

Proposition 1 *(Frank, Zadoff, Chu [4, 10]) For $c \in \mathbb{Z}_N$ with $\gcd(c, N) = 1$, we define $\mathbf{a}_c = \{a_c(t)\}$ and its modulated sequence, denoted as $\mathbf{b}_c = \{b_c(t)\}$ as follows*

$$a_c(t) = f(t), t \in Z_N \text{ and } b_c(t) := \omega_{2N}^{a_c(t)}$$

where

$$f(x) = \begin{cases} cx^2, & N \text{ even} \\ cx(x+1), & N \text{ odd.} \end{cases}$$

Then $\{a_c(t)\}$ is a perfect sequence, called a Frank-Zadoff-Chu (FZC) sequence. *If $N = p$, let $f(x) = c_2x^2 + c_1x, c_i \in \mathbb{F}_p$ where $c_2 \neq 0$ and $p > 2$, then the p-ary sequence $\mathbf{a}$ defined in (12) is a perfect sequence.*

A modulated FZC sequence $\{\omega^{a_c(t)}\}$ can be obtained by another way for N odd, which is presented by Sarwate [44].

Proposition 2 *(Sarwate [45]) Let N be odd.*

1. *The modulated FZC sequence $\mathbf{b}_c$ can be represented by*

$$b_c(t) = (-1)^{ct}\omega_{2N}^{ct^2}. \tag{13}$$

2. *In the following, we assume $S = \{\mathbf{b}_c \mid \gcd(c, N) = 1\}$.*

   (a) $\widetilde{b}_c(k) = b_1(c^{-1}k)^* \cdot \widetilde{b}_c(0), \forall k$.

   (b) $|\widetilde{b}_c(k)| = \sqrt{N}, k = 0, 1, \ldots$.

   (c) *If $c \neq d$ and $\gcd(c - d, N) = 1$, then the crosscorrelation between $\mathbf{b}_c$ and $\mathbf{b}_d$ is given by* $|C_{\mathbf{b}_c,\mathbf{b}_d}(\tau)| = \sqrt{N}$.

   (d) *Let p be the smallest prime divisor of N and $S_1 = \{\mathbf{b}_{c^{-1}} \mid 1 \leq c \leq p - 1, \gcd(c, N) = 1\}$. Then S_1 is an $(N, p - 1, \sqrt{N})$ correlation signal in which each sequence is perfect and $F_{\max} = \sqrt{N}$.*

Note that in [45] the condition in (c) is listed as $\gcd(d^{-1} - c^{-1}, N) = 1$, which is equivalent to the condition listed here.

Assertion (i) is straightforward. The proof for Assertion (ii) is to first prove (a) which can be obtained by directly expanding the DFT, then using the Parseval identity presented in Property 6 and together with (a) to obtain (b). Taking DFT of the correlation together with (b) to get (c), then (d) follows from (c) directly. The proof given by Sarwate was an earlier work to compute the correlation of sequences using transform, i.e., use of DFT. In the work by Dillon and Dobbertin [8] for proving the validity of the conjectured binary 2-level sequences also used this technique.

It is worth to point out that the results in Propositions 1 and 2 cannot be obtained by the Weil bound if N is not prime. Furthermore, the ambiguity of the FZC sequences can reach N. However, up to now, this is the only class of perfect sequences with optimal correlation and DFT for an arbitrary odd integer N (see [45] for its optimality).

Remark 1 The result of (c) in Proposition 2-(ii) shows that the crosscorrelation of two different FZC sequences with some condition is equal to $\sqrt{N}$. Sarwate proved this by showing that the DFT of the crosscorrelation of two FZC sequences is equal to an FZC sequence up to a scalar factor $\pm N$. If the definition of DFT in (4) had a factor $\frac{1}{\sqrt{N}}$, then the DFT of the crosscorrelation of two FZC sequences were equal to an FZC sequence. This is the reason that FZC sequences are considered superior than the other known sequences with good correlation. Note that the elements of an FZC sequence belong to $\mathbb{Z}_N$ and its modulated sequence is defined by the $(2N)$th primitive complex root of unity.

Remark 2 From the identity (13) in Proposition 2-(i), an FZC sequence for odd N can be considered as being defined by a kind of hybrid characters, which resembles a new type of sequences constructed from the Weil representation (see Section 5).

4.1.2 Another Class for $\mathbb{Z}_N$

Another class of quadratic phase sequences is defined by Alltop [1].

Proposition 3 *Let N be odd, p be the smallest prime factor of N, $f_c(x) = cx^2$ with $1 \le c < p$, $a(t) = ct^2 \in \mathbb{Z}_N$, and the modulated sequence is defined by*

$$b_c(t) = \omega_N^{a(t)} = \omega_N^{ct^2}.$$

Let $S = \{\{b_c(t)\} \mid 1 \le c < p\}$. Then $C_{\max} = F_{\max} = \sqrt{N}$.

Note that the ambiguity of this set can reach N no matter whether N is a prime or not.

4.1.3 Sequences from $\mathbb{F}_p$ Additive Characters

For $\mathbb{F}_p$ additive sequences, its phase-shift operator is defined by additive characters. If the defining polynomials over $\mathbb{F}_p$ have degrees at most d, then all their correlations, DFTs, and phase-shifts are determined by a polynomial with degree at most d. Thus, the three metrics can be bounded directly by the Weil bound, Lemma 1, on the additive characters. This is straightforward, so we omit them here. However, there is one special case, given below.

Alltop sequences ([1,37]): Let S consist of all $\mathbb{F}_p$ additive sequences given by $f_c(x) = cx^3 + x$, $c \in \mathbb{F}_p^*$ and $p > 3$. Then $C_{\max} = \sqrt{p}$ given in [1], which is better than the bound given by Lemma 1. From Lemma 1, we have $F_{\max}, G_{\max} \le 2\sqrt{p}$.

4.2 Sequences from $\mathbb{F}_p$ Multiplicative Characters

Let $M \mid (p-1)$, $f(x) \in \mathbb{F}_p[x]$, and χ be a multiplicative character of order M with $\chi(0) = 1$. An M-ary sequence $\mathbf{u} = \{u(t)\}$ with period p from the multiplicative structure of $\mathbb{F}_p$ and its modulated sequence are defined as follows:

$u(t) = c \log_\alpha f(t) \mod M, c \ne 0 \in \mathbb{Z}_M$	$\omega_M^{u(t)} = \chi_c(f(t))$
an M-ary sequence	a modulated sequence

(14)

(Recall that $\log_\alpha 0 = 0$, defined in the beginning of Section 2.) The sequence $\mathbf{u}$ is called an $\mathbb{F}_p$ *multiplicative sequence*. It has period p, the same as the additive case. If $f(x) = x$, then $\{u(t)\}$ is called a *power residue* sequence. If $M = 2$ and $p \equiv 3 \bmod 4$, then the complement of $u(t)$ is a *quadratic residue sequence (or Legendre sequence)* with 2-level autocorrelation.

Example 3 Let $p = 7$ and $\alpha = 3$ be a primitive element in $\mathbb{F}_7$. Then we have sequences from $\mathbb{F}_7$ additive and multiplicative structures listed in the following table (note that $\log_\alpha 0 = 0$):

Additive	$a(t) = t^2$	$\{a(t)\} = (0, 1, 4, 2, 2, 4, 1)$
Multiplicative: $M = 6$	$u(t) = \log_3 t$	$\{u(t)\} = (0, 0, 2, 1, 4, 5, 3)$
$M = 3$	$u_1(t) = \log_3 t \bmod 3$	$\{u_1(t)\} = (0, 0, 2, 1, 1, 2, 0)$
$M = 2$	$u_2(t) = \log_3 t \bmod 2$	$\{u_2(t)\} = (0, 0, 0, 1, 0, 1, 1)$ $1 + \mathbf{u}_2 = (1, 1, 1, 0, 1, 0, 0)$ a quadratic residue sequence of period 7

A phase shift of $\mathbf{u}$ is defined in terms of multiplicative characters of $\mathbb{F}_p$ with order M, given by

$$P_w[\mathbf{u}](t) = \omega_M^{w \log_\alpha t} \omega_M^{u(t)} = \chi_w(t)\chi(f(t)), t, w \in \mathbb{F}_p. \tag{15}$$

We have the following relationship of correlation, DFT and ambiguity with character sums.

Proposition 4 *For $\mathbb{F}_p$ multiplicative sequences $\mathbf{u}$, defined in (14), and $\mathbf{v}$, given by $v(t) = d \log_\alpha g(t) \bmod M, 1 \le d < M$ where $g(x) \in \mathbb{F}_p[x]$, their correlation, DFT, and ambiguity function are given by*

$$C_{\mathbf{u},\mathbf{v}}(\tau) = \sum_{t \in \mathbb{F}_p} \chi_c(f(t))\chi_d(g(t+\tau))^* = \sum_{t \in \mathbb{F}_p} \chi(h_0(t)) \tag{16}$$

$$\text{where } h_0(x) = f(x)^c g(x+\tau)^{M-d}$$

$$\widetilde{u}(k) = \sum_{t \in \mathbb{F}_p} \chi_c(f(t))\omega_p^{-tk} = \sum_{t \in \mathbb{F}_p} \chi_c(f(t))\psi(-tk) \tag{17}$$

$$G_{\mathbf{u},\mathbf{v}}(\tau, w) = \sum_{t \in \mathbb{F}_p} \chi_c(f(t))[\chi_d(g(t+\tau))\chi_w(t)]^* = \sum_{t \in \mathbb{F}_p} \chi(d_0(t)) \tag{18}$$

$$\text{where } d_0(x) = h_0(x)x^{M-w}.$$

From Proposition 4, we know that both correlation and ambiguity can be bounded by the Weil bound on multiplicative characters when both f and g have low degrees, and their DFTs can be bounded by the Weil bound on hybrid character sums as long as f has low degree. For a power residue sequence with $f(x) = x$, from (17), both $f(x)$ and $(-kx)$ have degree 1. According to Lemma 3, the DFT of a power residue sequence is bounded by $\sqrt{p} + 1$.

In order to facilitate a quicker assessment for the condition in Corollary 1 and Lemma 3, we introduce the following concepts (see [22]), which will be also used in the $\mathbb{F}_q$ case. For $f \in \mathbb{F}_q[x]$ ($q = p$ or $q = p^n$), if $f(x) = c \cdot h^M(x)$, then we say that $f(x)$ is an *M-th power multiple* in $\mathbb{F}_q[x]$. Thus, the following assertions are equivalent.

(i) $f(x)$ is an M-th power multiple in $\mathbb{F}_q[x]$.

(ii) The factorization of $f(x)$ is $f(x) = c(x-\gamma_1)^{e_1} \dots (x-\gamma_s)^{e_s}$ where $\gamma_i \in \overline{\mathbb{F}}_q, c \in \mathbb{F}_q$ where $M \mid e_i$ for all i's.

Using this result, we can easily see that ambiguity of a power residue sequence cannot be bounded since $d_0(x)$ in (18) could be an M-th power multiple. In detail, $d_0(x) = x^c(x+\tau)^{M-d}x^{M-w}$ where $1 \le c, d, w < M$. By choosing $c = d + w \bmod M$ with $c \ne d \bmod M$ and $\tau = 0$ we have $d_0(x) = x^{2M}$, an M-th power multiple. So, $G_{\mathbf{u},\mathbf{v}}(0, w) = p$.

In the following, we summarize the correlation, DFT, ambiguity of power residue sequences in a theorem where the last two results are from [53].

Theorem 1 *Let $M \mid (p-1)$, an M-ary power residue sequence $\mathbf{u}_c = \{u_c(t)\}$ whose elements are defined by $u_c(t) = c \log_\alpha t \bmod M, t \in \mathbb{F}_p, M \mid (p-1)$, and let $S = \{\mathbf{u}_c : 1 \le c < M\}$. Then $\mathbf{u}_c$ has the period p.*

1. *For any sequence $\mathbf{u} \in S$, the autocorrelation function of $\mathbf{u}$ is bounded by (Sidel'nikov [48], Lempel* et. al. *[33], Sarwate [44])*

$$|C_{\mathbf{u}}(\tau)| \le 3, \tau \not\equiv 0 \bmod p.$$

In particular, for $M = 2$,

$$C_{\mathbf{u}}(\tau) \in \begin{cases} \{-1\} & \tau \not\equiv 0 \bmod p \quad \text{if } p \equiv 3 \bmod 4 \\ \{1, -3\} & \tau \not\equiv 0 \bmod p \quad \text{if } p \equiv 1 \bmod 4. \end{cases}$$

2. *For any two sequences $\mathbf{u} \in S$ and $\mathbf{v} \in S$, their crosscorrelation function is bounded by $|C_{\mathbf{u},\mathbf{v}}(\tau)| \le \sqrt{p} + 2$ (Kim* et al. *[29]).*

3. *The DFT is bounded by $|\widetilde{u}(k)| \le \sqrt{p} + 1$.*

4. *The cross ambiguity function has a peak value p.*

4.3 Sequences from $\mathbb{F}_q$ Additive Characters

We now introduce sequences defined by $Tr(f(x))$, a function from $\mathbb{F}_q$ to $\mathbb{F}_p$ in (2), which are the most popular sequences in both theory and practice. We assume that $f(0) = 0$ in this case. Let $\mathbf{a} = \{a(t)\}$ whose elements are defined by

$$a(t) = Tr(f(\alpha^t)), t = 0, 1, \dots. \tag{19}$$

Then $\mathbf{a}$ is a sequence over $\mathbb{F}_p$ with period $N \mid (q-1)$ where α is a primitive element in $\mathbb{F}_q$, and we also say that $\mathbf{a} = \{a(t)\}$ is defined by $f(x)$. The equation (1) is also called a *trace representation* of

the sequence $\{a(t)\}$. If $f(x) = x^d$ with $(d, q-1) = 1$, then $\mathbf{a}$ is an *m-sequence* over $\mathbb{F}_p$ with period $p^n - 1$, i.e.,

$$m\text{-sequence} \longleftrightarrow Tr(x^d), \gcd(d, q-1) = 1.$$

Any m-sequence has a 2-level autocorrelation function. If $\mathbf{b} = \{b(t)\}$ where $b(t) = a(dt)$, then $\mathbf{b}$ is a d-decimation of $\mathbf{a}$. Thus, any sequence of period $N \mid (q-1)$ can be obtained by summing up different decimations on a shifted m-sequence with trace representation $Tr(x)$.

The study of correlation of the sequences defined in (19) has been around for more than 5 decades. Since the polynomials considered here usually have high degrees, they cannot be bounded by the Weil bounds. Each case with low correlation was found by a special method for manipulating the exponential sums (see [25]). In general, DFT and ambiguity for those sequences with low correlation are unknown. One exceptional example is the Kasami small set of the sequences of period $2^n - 1$ (n even), which are defined by polynomials $Tr(x + cx^d), c \in \mathbb{F}_q$ where $d = 2^{n/2} + 1$ having very high degree, but the DFT is bounded, see [32].

We may write $f(x) = \sum_{r \in \Gamma(q)} c_r x^r, c_r \in \mathbb{F}_{p^{n_r}}$ (recall that $\Gamma(q)$ consists of all the coset leaders modulo q in Section 2.2). Let

$$S = \{\{a(t)\} : c_r \in \mathbb{F}_{p^{n_r}}\}$$

where $a(t)$'s are defined by (19). The set S corresponds to a cyclic code. To determine maximum correlation is equivalent to find the minimum distance of this code. This connection also indicates the hardness for determining the three metrics of this set if $f(x)$ is too general. Starting now, for the sequences defined by (19), we restrict ourselves to the case that the sequences have period $N = q - 1$.

The sequences defined here are p-ary sequences, so the phase shift is defined through an additive character $\psi(x) = \omega_p^{Tr(x)}$ (see Section 2), given by

$$\begin{aligned} P_w[\mathbf{a}](t) &= \psi(Tr(\alpha^{t+w}))\omega_p^{a(t)} = \psi(\alpha^{t+w} + a(t)) \\ &= \psi(\alpha^{t+w} + f(\alpha^t)), t, w = 0, 1, \ldots \end{aligned} \tag{20}$$

where the last identity comes from (19). The following proposition presents correlation, DFT and ambiguity of an $\mathbb{F}_q$ additive sequence using character sums.

Proposition 5 *With $f(x)$ and $\mathbf{a}$ above, let $b(t) = Tr(g(\alpha^t))$ where $g(x) \in \mathbb{F}_q[x]$ with $g(0) = 0$ and the exponents of x in g belong to $\Gamma(q)$. Recall that χ^1 is a multiplicative character of order $q-1$.*

$$\begin{aligned} C_{\mathbf{a},\mathbf{b}}(\tau) &= \sum_{x \in \mathbb{F}_q} \psi(f(x))\psi(g(\alpha^\tau x))^* - 1 = \sum_{x \in \mathbb{F}_q} \psi(h_1(x)) - 1 \\ &\quad \textit{where } h_1(x) = f(x) - g(\alpha^\tau x), \tau \in \mathbb{Z}_{q-1}. \end{aligned} \tag{21}$$

$$\widetilde{a}(k) = \sum_{t=0}^{q-2} \omega_p^{Tr(f(\alpha^t))}\omega_{q-1}^{-tk} = \sum_{x \in \mathbb{F}_q} \psi(f(x))\chi^1(x^{-k}) - 1, k \in \mathbb{Z}_{q-1}. \tag{22}$$

$$\begin{aligned} G_{\mathbf{a},\mathbf{b}}(\tau, w) &= \sum_{t=0}^{q-2} \psi(f(\alpha^t))[\psi(g(\alpha^{t+\tau}))\psi(\alpha^{t+k})]^* \\ &= \sum_{x\in\mathbb{F}_q} \psi(d_1(x)) - 1 \qquad (23) \\ &\quad \textit{where } d_1(x) = h_1(x) - \alpha^w x,\ \tau, w \in \mathbb{Z}_{q-1}. \end{aligned}$$

From (22), when $f(x) = x$ we immediately see that the DFT is less than or equal to $\sqrt{q}$ by the Weil hybrid sum in Lemma 3. In other words, the DFT of an m-sequence defined by $Tr(x)$ is upper bounded by $\sqrt{q}$. This is reported in several papers, say [40]. From Proposition 5, three metrics can be obtained using the Weil bounds only when the polynomials have low degrees.

The sequence $\mathbf{a}$ has 2-level autocorrelation if and only if the exponential sum in (21) is equal to zero. For the binary case, i.e., $p = 2$, all known 2-level autocorrelation sequences with period $2^n - 1$ are presented in [14]. For nonbinary cases, i.e., $p > 2$, there are not so many constructions known. We will introduce them in Section 6 and present some conjectures on zero exponential sums.

4.4 Sequences from $\mathbb{F}_q$ Multiplicative Characters

Let $f(x) \in \mathbb{F}_q[x]$. For $M \,|\, (q-1)$, and $1 \le c < M$, recall that the definition of a multiplicative character $\chi_c(\alpha^x) = \omega_M^{cx}$ from Definition 2. An M-ary $\mathbb{F}_q$ multiplicative sequence $\mathbf{u}_c = \{u_c(t)\}$ and its modulated sequence are defined as

$$u_c(t) = c \log_\alpha f(\alpha^t) \bmod M, \text{ and } \omega_M^{u_c(t)} = \chi_c(f(\alpha^t)),\ t = 0, 1, \ldots.$$

Let $S = \{\mathbf{u}_c : 1 \le c < M\}$. Then each sequence in S has period $q-1$ and $|S| = M$. If $f(x) = x+1$, we have

$$u_c(t) = c \log_\alpha(\alpha^t + 1) \bmod M \text{ and } \omega_M^{u_c(t)} = \chi_c(\alpha^t + 1),\ t = 0, 1, \ldots. \qquad (24)$$

$\{u(t)\}$ is called a *Sidel'nikov sequence* and $\{\omega_M^{u_c(t)}\}$ is its modulated sequence.

Example 4 Let $p = 2$, $n = 4$ and $\mathbb{F}_{2^4}$ be defined by a primitive polynomial $t(x) = x^4 + x + 1$, and let α be a primitive element in $\mathbb{F}_{2^4}$ with $t(\alpha) = 0$. We list below a binary m-sequence defined by $Tr(x)$ and three Sidel'nikov sequences for $M = 15, 5, 3$.

Additive	$\mathbf{a} = (000100110101111)$, $a(t) = Tr(\alpha^t)$	$f_1(x) = x$
Multiplicative	$u(t) = \log(\alpha^t + 1) \bmod M$	$f_2(x) = x + 1$
$M = 15$	$\mathbf{u} = (0, 4, 8, 14, 1, 10, 13, 9, 2, 7, 5, 12, 11, 6, 3)$	
$M = 5$	$\mathbf{u}_1 = (0, 4, 3, 4, 1, 0, 3, 4, 2, 2, 0, 2, 1, 1, 3)$	
$M = 3$	$\mathbf{u}_2 = (0, 1, 2, 2, 1, 1, 1, 0, 2, 1, 2, 2, 2, 0, 0)$	

The phase shift of an $\mathbb{F}_q$ multiplicative sequence is defined by multiplicative characters of order M, i.e.,

$$P_w[\mathbf{u}](t) = \omega_M^{wt}\omega_M^{u(t)} = \chi_w(\alpha^t)\chi(f(\alpha^t)),\ 0 \le t < q-1, 1 \le w < M.$$

We now present the correlation, DFT and ambiguity of an $\mathbb{F}_q$ multiplicative sequence in terms of character sums.

Proposition 6 *With $f(x)$ as above, let $g(x) \in \mathbb{F}_q[x]$ and $v(t) = d\log_\alpha g(\alpha^t) \bmod M$. Then*

$$C_{\mathbf{u},\mathbf{v}}(\tau) = \sum_{x\in\mathbb{F}_q} \chi_c(f(x))\chi_d(g(\alpha^\tau x))^* - 1 = \sum_{x\in\mathbb{F}_q} \chi(h_2(x)) - 1 \tag{25}$$

$$\textit{where } h_2(x) = f(x)^c g(\alpha^\tau x)^{M-d}.$$

$$\widetilde{u}(k) = \sum_{t=0}^{q-2} \chi_c(f(\alpha^t))\omega_{q-1}^{-tk} = \sum_{x\in\mathbb{F}_q} \chi_c(f(x))\chi^1(x^{-k}) - 1. \tag{26}$$

$$\begin{aligned} G_{\mathbf{u},\mathbf{v}}(\tau, w) &= \sum_{t=0}^{q-2} \chi_c(f(\alpha^t))[\chi_d(g(\alpha^{t+\tau}))\chi_w(\alpha^t)]^* \\ &= \sum_{x\in\mathbb{F}_q} \chi(d_2(x)) - 1 \textit{ where } d_2(x) = h_2(x)x^{M-w}. \end{aligned} \tag{27}$$

From Proposition 6, all three metrics can be obtained by the Weil bound on multiplicative characters by Corollary 1 when both f and g have low degrees. Thus, for $f(x) = x + 1$, i.e., the Sidel'nikov case, from (26), the polynomial $f(x)$ has -1 as a root and the polynomial x has zero as a root, but both in $\mathbb{F}_p$. Applying Lemma 2, the magnitude of the DFT is upper bounded by $\sqrt{q}+1$. Similarly, from (27), $d_2(x)$ has three distinct roots where two are in $\mathbb{F}_p$ and it is not an M-th power multiple in $\mathbb{F}_q[x]$. Again using Corollary 1, the magnitude of the auto and cross ambiguity functions are upper bounded by $2\sqrt{q} + 3$. We summarize these results in the following theorem where the last part is taken from [53].

Theorem 2 *With the notation defined above, then each Sidel'nikov sequence has period $q-1$ and S is an $(q-1, M, \sqrt{q}+3, 2\sqrt{q}+2)$ ambiguity set, whose properties are listed below in details.*

1. *The autocorrelation function is bounded by (Sidel'nikov [48], Lempel* et al. *[33], Sarwate [44])*

$$|C_{\mathbf{u}}(\tau)| \le 4, \tau \not\equiv 0 \mod (q-1).$$

In particular, for $M = 2$,

$$C_{\mathbf{u}}(\tau) \in \begin{cases} \{-2, 2\} & \tau \not\equiv 0 \mod (q-1) \quad \textit{if } q \equiv 3 \bmod 4 \\ \{0, -4\} & \tau \not\equiv 0 \mod (q-1) \quad \textit{if } q \equiv 1 \bmod 4. \end{cases}$$

2. *The crosscorrelation is bounded by* $\sqrt{q}+3$ *(Kim* et al. *[28]).*

3. *The DFT is bounded by* $|\widetilde{u}(k)| \leq \sqrt{q}+1$ *(Yu* et al. *[57]).*

4. *Ambiguity are bounded by* $|G_{\mathbf{u},\mathbf{v}}(\tau,w)| \leq 2\sqrt{q}+2$ *for any* (τ,w) *when* $\mathbf{u} \neq \mathbf{v}$ *and* $(\tau,w) \neq (0,0)$ *when* $\mathbf{u}=\mathbf{v}$.

We summarize these four types of sequences and their corresponding characters in Table 1 where ψ is a nontrivial additive character, χ is a multiplicative character of $\mathbb{F}_p$ or $\mathbb{F}_q$ of order M, and χ^1 is a multiplicative character of $\mathbb{F}_q$ of order $q-1$.

Table 1: Four types of sequences and characters

	$\mathbb{F}_p$	$\mathbb{F}_q$
Additive: p-ary sequence		
Sequence	$a(t)=f(t)$	$a(t)=Tr(f(\alpha^t))$
Correlation	$\psi(f_0(x))$	$\psi(h_1(x))$
DFT	$\psi(f_1(x))$	$\psi(f(x))\chi^1(x^{-k})$
Ambiguity	$\psi(f_2(x))$	$\psi(h_1(x)+\alpha^w x)$
	f_i's have the same degree	$h_1(x)=f(x)-g(\alpha^\tau x)$
Multiplicative: M-ary sequence		
Sequence	$u(t)=\log_\alpha f(t) \bmod M$	$u(t)=\log_\alpha f(\alpha^t) \bmod M$
Correlation	$\chi(h_0(x))$	$\chi(h_2(x))$
DFT	$\chi_c(f(x))\psi(-kx)$	$\chi_c(f(x))\chi^1(x^{-k})$
Ambiguity	$\chi(h_0(x)x^{M-w})$	$\chi(h_2(x)x^{M-w})$
	$h_0(x)=f(x)^c g(x+\tau)^{M-d}$	$h_2(x)=f(x)^c g(\alpha^\tau x)^{M-d}$

Note that $\mathbb{F}_p$ or $\mathbb{F}_q$ additive sequences have p phases in their modulated sequences. On the other hand, $\mathbb{F}_p$ or $\mathbb{F}_q$ multiplicative sequences have M phases in their modulated sequences. For $\mathbb{F}_p$ additive and $\mathbb{F}_q$ multiplicative sequences, correlation, DFT and ambiguity only involve $\mathbb{F}_p$ additive characters and $\mathbb{F}_q$ multiplicative characters, respectively. However, for $\mathbb{F}_p$ multiplicative and $\mathbb{F}_q$ additive sequences, their DFTs are hybrid characters sums.

Remark 3 The auto and cross ambiguity functions of an $\mathbb{F}_q$ additive sequence are equal to the Hadamard transform of their respective autocorrelation and crosscorrelation functions. We will come back to the Hadamard transform in Section 6.

4.5 Sequences Defined by Indexing Field Elements Alternatively

For $\mathbb{F}_p$ sequences, regardless they are additive or multiplicative, the elements are indexed by $0, 1, \ldots, p-1$ in the additive group of $\mathbb{F}_p$. On the other hand, for $\mathbb{F}_q$ sequences, both additive or multiplicative cases, the elements are indexed by $1, \alpha, \ldots, \alpha^{q-1}$ in the multiplicative group of $\mathbb{F}_q$. Thus, for the $\mathbb{F}_p$ case, we have two different indexing methods to define the sequences: the field elements are indexed by $0, 1, \ldots, p-1$, as shown in Sections 4.2 and 4.3, or indexed by $1, \alpha, \ldots, \alpha^{p-2}$ where α is a primitive element of $\mathbb{F}_p$, as shown in Sections 4.4 and 4.5 when $q = p$. However, for the $\mathbb{F}_q$ case with $q > p$, we also have an alternative definition for indexing $\mathbb{F}_q$ elements. In order to do so, we need a one-to-one correspondence between a p-adic integer $t = 0, 1, \ldots, q-1$ $(q = p^n)$, and the elements in $\mathbb{F}_q$ as shown below.

$$t = \sum_{i=0}^{n-1} t_i p^i, t_i \in \mathbb{F}_p \longleftrightarrow \alpha_t = \sum_{i=0}^{n-1} t_i \alpha^i \longleftrightarrow \mathbf{t} = (t_{n-1}, \ldots, t_0).$$

These four alternative definitions of sequences are given in Table 2.

Table 2: Four types of sequences by indexing the elements of $\mathbb{F}_p$ and $\mathbb{F}_q$ alternatively

	$\mathbb{F}_p$	$\mathbb{F}_q$
Additive	$b(t) = f(\alpha^t)$	$b(t) = Tr(f(\alpha_t))$
Multiplicative	$v(t) = \log_\alpha f(\alpha^t) \bmod M$ $t = 0, \ldots, p-2$	$v(t) = \log_\alpha f(\alpha_t) \bmod M$ $t = 0, 1, \ldots, q-1$
Period	$p-1$	q

For example, Golay sequences are ordered by the additive group of $\mathbb{F}_{2^n}$ [7, 39].

Example 5 Let $n = 3$ and $f(x_0, x_1, x_2) = x_0x_1 + x_1x_2$. Then a binary Golay sequence, denoted by $\mathbf{b} = \{b(t)\}$ is defined as follows:

$$\begin{aligned} b(t) &= f(t) \text{ where } t = t_2 2^2 + t_1 2 + t_0, \mathbf{t} = (t_2, t_1, t_0), t = 0, 1, \ldots, 7, \text{ and} \\ f &= (f(0,0,0), f(1,0,0), f(0,1,0), f(1,1,0), \\ &\quad f(0,0,1), f(1,0,1), f(0,1,1), f(1,1,1)) \\ &= (0,0,0,1,0,0,1,0). \end{aligned}$$

In other words, the sequence $\mathbf{b}$ consists of the values of f in the truth table in Table 5.

Let F_{2^3} be the finite field defined by a primitive polynomial $g(x) = x^3 + x + 1$ over $\mathbb{F}_2$, α be a primitive element of F_{2^3} satisfying $g(\alpha) = 0$. Using the finite field discrete Fourier transform

(DFT) (see [14]), we can obtain the trace presentation of **b**, which is given by

$$B(x) = Tr(h(x)) \quad \text{where} \quad h(x) = \alpha^6 x + \alpha^3 x^3 \tag{28}$$

and $Tr(x) = x + x^2 + x^4$ is the trace function of F_{2^3}. Then $b(t) = Tr(h(\alpha_t)), t = 0, 1, \cdots, 7$ where the conversions between t and α_t are given in Table 5.

Table 3: Truth table of the Golay sequence **b**

Index t	α_t	x_2	x_1	x_0	f
0	$\alpha_0 = 0$	0	0	0	0
1	$\alpha_1 = 1 = \alpha^0$	0	0	1	0
2	$\alpha_2 = \alpha$	0	1	0	0
3	$\alpha_3 = \alpha^3$	0	1	1	1
4	$\alpha_4 = \alpha^2$	1	0	0	0
5	$\alpha_5 = \alpha^6$	1	0	1	0
6	$\alpha_6 = \alpha^4$	1	1	0	1
7	$\alpha_7 = \alpha^5$	1	1	1	0

If we evaluate $B(x) = Tr(h(x))$ over $\{\alpha^t : t = 0, 1, \ldots, 6\}$, i.e., let $a(t) = B(\alpha^t)$, then we obtain $\{a(t)\} = (0001100)$. In other words, for a given function $B(x)$ in (28), using the additive character, we have two sequences:

Indexed in the additive group of $\mathbb{F}_{2^3}$	Indexed in the multiplicative group of $\mathbb{F}_{2^3}$
$b(t) = B(t)$	$a(t) = B(\alpha^t)$
$\{(-1)^{b(t)}\} = (1, 1, 1, -1, 1, 1, -1, 1)$	$\{(-1)^{a(t)}\} = (1, 1, 1, -1 - 1, 1, 1)$
Period: 8	Period: 7
Autocorrelation	
$\{C_{\mathbf{b}}(\tau)\} = (8, 0, 0, 4, 0, 4, 0, 0)$	$\{C_{\mathbf{a}}(\tau)\} = (7, 3, -1, -1, -1, -1, 3)$

In general, the sequences indexed in the additive group of $\mathbb{F}_{2^n}$ have period 2^n or a factor of 2^n. However, it is not easy to find the polynomials or boolean functions such that the sequences defined through the additive group of $\mathbb{F}_q$ for having low correlation, DFT and ambiguity, since no known bounds can be applied to those cases. Even for the Golay sequences, the autocorrelation of an individual sequence is unknown, although the sum of the autocorrelation functions of a Golay pair sequences is equal to zero. Some preliminary treatments about correlation of the sequences defined by $\mathbb{F}_q$ additive group order can be found in [14]. It could be interesting to see whether some new sequences with good correlation, DFT and ambiguity could arise from those classes.

5 Sequences with Low Degree Polynomials

From Propositions 4, 5, and 6 or the summaries in Table 1 in the previous section, we know three metrics can be bounded by the Weil bounds on additive character sums, multiplicative character sums, and hybrid sums when the defining polynomials have low degrees. In the last section, we have also introduced sequences with low degree polynomials from additive characters over $\mathbb{F}_p$, and $f(x) = x$ in $\mathbb{F}_p$ or $f(x) = x + 1$ in $\mathbb{F}_q$ through multiplicative characters. In this section, we continue our journey along this line with emphasis on the constructions of ambiguity signal sets with low degree polynomials.

5.1 Methods for Generating Signal Sets from A Single Sequence

For $\mathbb{F}_q$ additive sequences, a general method is to apply the decimation-and-add operation, as explained in Section 2.3, which has been attracting researchers since the end of 1950s. For those constructions, most of them are the sum of two m-sequences. Golomb constructed binary m-sequences using linear feedback shift registers in the middle of 1950's [12] and Zieler extended them to $\mathbb{F}_q$ [62] with period $q - 1$. The multi-term sequences from the decimation-and-add operations on an m-sequence have been marked by various footprints from many researchers, [56] (1974), [23] (1976), [31](1991), just to list a few.

Investigating $\mathbb{F}_q$ multiplicative sequences including $\mathbb{F}_p$ case occurs more recently. It can be classified as follows.

1. Amplitude scaling operation: $y_c(t) = cu(t)$, where c is a constant (see [29] for the case that $u(t)$ is a power residue sequence and [28] for a Sidel'nikov sequence $u(t)$).

2. Shift-and-add with/without inverse: $y_{(c,d,\tau)}(t) = cu(t) + du(\delta t + \tau)$ where $\delta = \pm 1$, c, d and τ are constant (first observed in [61], and later proved in [43] in 2006 for $\delta = 1$).

3. Interleaved method: A Sidel'nikov sequence of period $q^2 - 1$, writing it as an $q - 1$ by $q + 1$ array, then taking some columns to form a signal set. (The result in [59] shows that it can be done when $u(t)$ is a Sidel'nikov sequence.)

In the remainder of this section, we first introduce the signal sets with low odd degree polynomials, then present sequences from power or Sidel'nikov sequences using the above operations, thirdly, we present the sequences from the Weil representation and their extensions, and finally, we give a new construction of sequences from combinations of different indexing field elements and hybrid characters sums.

5.2 Sequences with Low Odd Degree Polynomials

In this subsection, we consider the following polynomial functions of odd degrees over $\mathbb{F}_q$, which have been considered extensively in the literature, for example, [38, 40, 46], for constructing signal

sets using $\mathbb{F}_q$ additive characters. Let

$$d < \begin{cases} \sqrt{q} \text{ if } p = 2 \\ \sqrt{q}/2 \text{ if } p > 2 \end{cases} \tag{29}$$

$$T_0 = \left\{ \sum_{i=2}^{d} b_i x^{2i-1} + x + 1 \mid b_i \in \mathbb{F}_q \text{ with (29)} \right\} \tag{30}$$

$$T_1 = \left\{ \sum_{i=2}^{d} b_i x^{2i-1} + x \mid b_i \in \mathbb{F}_q \text{ with (29)} \right\} \tag{31}$$

$$T_2 = \left\{ \sum_{i=3}^{d} b_i x^{2i-1} + x^3 \mid b_i \in \mathbb{F}_q \text{ with (29)} \right\}. \tag{32}$$

The polynomials in T_1 are recently considered in [11] for deterministic extractors for affine random sources. By directly applying the Weil bounds, the authors show that the character sum $\sum_{x\in\mathbb{F}_q} \eta(f(x))$ is bounded when η is an additive character where $p = 2$, or η is a multiplicative character of order 2 for $p > 2$. In the following, we investigate the size and three metrics of the signal set consisting of the sequences defined by polynomials in T_2 using $\mathbb{F}_q$ additive characters and T_0 for multiplicative characters.

5.2.1 $\mathbb{F}_q$ Additive Sequences with Low Odd Degree Polynomials

For the additive case, the exponents of the polynomials should belong to different cosets in order to generate time-shift distinct and phase-shift distinct sequences. According to Property 3 in Section 4, we need the following result. For an easy reference, we also include a proof there.

Proposition 7 *The odd integers $2i-1$'s with the condition in (30) belong to different cosets modulo $(q-1)$ for $p = 2$ and for $p > 2$ provided $2i - 1 \neq 0 \bmod p$. Furthermore, each coset of $2i - 1$ has the full size n.*

Proof. Case 1. $p = 2$. For $s = 2i - 1$, $i > 1$, since $d < \sqrt{q} = 2^{n/2}$, the binary representation of s is

$$(1, s_1, \ldots, s_{\lfloor n/2 \rfloor - 1}, \underbrace{0, \ldots, 0}_{m}), m = n - \lfloor n/2 \rfloor, s_i \in \{0, 1\}. \tag{33}$$

Thus, for any two different vectors in the form of (33), one cannot be obtained from the other by the shifting operator. Thus they are not in the same coset modulo $2^n - 1$. Furthermore, the coset containing s has the full size n, since any binary vector given in (33) does not have a period less than n.

Case 2. $p > 2$. Since $s \neq p^i$, the p-ary representation of s is given as

$$(s_0, \ldots, s_{\lfloor n/2 \rfloor - 1}, \underbrace{0, \ldots, 0}_{m}), s_i \in \mathbb{F}_p, s_0 \neq 0.$$

A similar argument can be made for this case, thus the assertion is true.

□

Let

$$a(t) = Tr(f(\alpha^t)), f \in T_2, \quad \text{and} \quad S_2 = \{\{\omega_M^{a(t)}\} \, : \, f(x) \in T_2\}. \tag{34}$$

Using the Weil bounds in Lemmas 1 and 3, and Proposition 5, the following results on binary sequences follow immediately.

Theorem 3 *For $p = 2$ and $3 \not| q - 1$, S_2 defined by (34) is an ambiguity signal set where the size of S_2 and three metrics are given by*

$$|S_2| = q^{d-2}, C_{\max}, G_{\max} \leq (2d-2)\sqrt{q} + 1, \text{ and } F_{\max} \leq (2d-1)\sqrt{q}.$$

Remark 4 For $p > 2$, $f(x)$ could contain monomial terms with even exponents. In other words, we may assume that there exists some $1 < i_0 \leq d$ such that $\gcd(i_0, q-1) = 1$, then we set

$$S_2' = \{\{a(t)\} : f(x) = \sum_{i=2, i \neq i_0}^{d} c_i x^i + x^{i_0}, c_i \in \mathbb{F}_q\}$$

where $a(t) = Tr(f(\alpha^t))$. Then the number of the phase-shift distinct sequences defined by S_2' and their three metrics are given by

$$|S_2'| = q^{d-2-\lfloor \frac{d}{p} \rfloor}, C_{\max}, G_{\max} \leq (d-1)\sqrt{q} + 1, \text{ and } F_{\max} \leq d\sqrt{q}.$$

Note that i_0 is not unique, which is used to prove the phase-shift distinctness of the sequences in the set.

Remark 5 Note that the correlation bound obtained directly by applying the Weil bound is not as good as those obtained by a special method (see [25]). The following two cases show how far the bounds of $C_{\max}$ given by Theorem 3 are from the bound proved using a special technique.

1. $f(x) = cx^3 + x, c \in \mathbb{F}_{2^n}$, and S is the set consisting of the sequences defined by all those polynomials. Then S is a Gold pair signal set (see [25]) where $C_{\max} \leq \sqrt{2q}$. However, $C_{\max}$ in Lemma 1 or Theorem 3 is bounded by $C_{\max} \leq 2\sqrt{q}$. However, the sequences in S are not phase-shift distinct. Thus, the ambiguity can reach $2^n - 1$.

2. $f(x) = c_2x^5 + c_1x^3 + x, c_i \in \mathbb{F}_{2^n}$. Then S is a triple error correction code where $C_{\max} \leq \sqrt{8q}$. From Theorem 3, it is bounded by $C_{\max} \leq 4\sqrt{q} + 1$. Note that not all sequences in S are phase-shift distinct. However, all sequences in S_2 for $d = 3$ are phase-shift distinct. Thus, the ambiguity function of the sequences in S can reach $2^n - 1$ except for $c_1 = 1$. In this case, $S = S_2$ for $d = 3$.

Note that ambiguity of the above Case 1 is not bounded and Case 2 is not bounded if $c_1 \neq 1$.

5.2.2 $\mathbb{F}_q$ Multiplicative Sequences with Low Odd Degree Polynomials

Next we look at the multiplicative case. Let

$$u(t) = c \log_\alpha f(\alpha^t) \bmod M, f \in T_0, \quad \text{and}$$
$$S_0 = \{\{\omega_M^{u(t)}\} \,|\, \forall f \in T_0, 1 \leq c < M\}.$$

We need to show that the associated polynomials are not M-th power multiples in $\mathbb{F}_q[x]$ where $M \,|\, (q-1)$. In the following, we only present the proof for the case of $M = 2$ and $d = 3$, i.e., the binary case. The proof for this case and the results on general M and d are reported in [52]. Note that the size of S_0 is equal to the number of phase-shift distinct sequences. In this case, as long as not all $d-1$ coefficients in $f(x) \in T_0$, defined in (30) are equal zero, then their corresponding sequences are phase-shift distinct. Thus $|S_0| = (q-1)q^{d-2}$. The following results are due to [52].

Theorem 4 *For any p, assume that $M = 2$ and $d < \sqrt{q}/2$. Then S_0 is an ambiguity signal set where the size and three metrics are given by*

$$|S_0| = (q-1)q^{d-2}$$
$$C_{\max} \leq (4d-4)\sqrt{q} + 4d$$
$$F_{\max} \leq (2d-1)\sqrt{q} + 2d - 1$$
$$G_{\max} \leq (4d-2)\sqrt{q} + 4d - 2.$$

Proof. According to Proposition 6 or Table 1, for $C_{\max}$, we only need to show

Claim 1: $g(x) = f_1(x)^c f_2(\alpha^\tau x)^{M-d} = f_1(x) f_2(\alpha^\tau x), f_i \in T_0$ is not a square multiple in $\mathbb{F}_q[x]$.

For $G_{\max}$, from Proposition 6 or Table 1, we only need to prove

Claim 2. $g(x)x^{M-w} = g(x)x^w$ is not a square multiple in $\mathbb{F}_q[x]$ where $g(x)$ is defined in Claim 1.

However, Claim 1 implies Claim 2. Thus, we only need to show that Claim 1 is true. We now show the case of $d = 3$. We assume that both f_1 and f_2 have degree 5. The other cases can be proved in a similar way, but much simpler. By considering the coefficient of x and constant term, $f_2(\alpha^\tau x) = c \cdot f_1(x)$ will induce $\tau = 0$ and $f_1 = f_2$. Thus $f_1(x)$ and $f_2(\alpha^\tau x)$ have at least one different root in $\overline{F}_q$. If $f_1(x)f_2(\alpha^\tau x)$ is a square multiple, then we have the following three cases where the computations are in $\overline{\mathbb{F}}_q$. Note that $M \mid q-1$ and now $M = 2$, so $p \neq 2$ in the following derivations.

Case 1. $f_1(x)$ and $f_2(\alpha^\tau x)$ share 5 roots. This case leads to $f_2(\alpha^\tau x) = c \cdot f_1(x)$, which is a contradiction.

Case 2. $f_1(x)$ and $f_2(\alpha^\tau x)$ share 3 roots, say, a, b and c. In this case, each of these two polynomials will have the form $h(x) = e(x-a)(x-b)(x-c)(x-d)^2$ since $f_1(x)f_2(\alpha^\tau x)$ is a square multiple. We now consider the coefficient of x^4 of $h(x)$, which is zero. Then we get $d = -2^{-1}(a+b+c)$ which implies that $f_1(x)$ and $f_2(\alpha^\tau x)$ share 5 roots. This is a contradiction.

Case 3. $f_1(x)$ and $f_2(\alpha^\tau x)$ share 1 root a. In this case, each of these two polynomials will have the form $t(x) = e(x-a)(x-b)^2(x-c)^2$. Since the coefficients of x^4 and x^2 of $t(x)$ are zero, we get

$$\begin{array}{ll} a + 2b + 2c = 0, & b + c = -2^{-1}a, \\ 2(b^2c + c^2b) + 4abc + b^2a + c^2a = 0. & \Longrightarrow \quad bc = -(2^{-1}a)^2. \end{array}$$

Thus b and c are the roots of equation $x^2 + 2^{-1}ax - (2^{-1}a)^2 = 0$ over $\overline{F}_q$ which imply that $f_1(x)$ and $f_2(\alpha^\tau x)$ share 5 roots. A contradiction occurs.

Every case induces a contradiction here, so $f_1(x)f_2(\alpha^\tau x)$ is not a square multiple in $\mathbb{F}_q[x]$. Hence, the assertions are true. □

The results on Theorems 3 and 4 are true for $d < \sqrt{q}/2$. When $d < \log\log_2 q$ and $d < \log_2 n$ when $p = 2$, they satisfy the bounds given in (8)-(10).

5.3 Sequences from Power Residue and Sidel'nikov Sequences

5.3.1 Interleaved Structure of Sidel'nikov Sequences

We first present a result on Sidel'nikov sequences. Yu and Gong [60] studied the interleaved structure of Sidel'nikov sequences (for interleaved sequences, see [16]). They consider the case of M-ary Sidel'nikov sequences of period q^2-1 for $M \mid (q-1)$. By investigating the $(q-1)\times(q+1)$ array structure of the Sidel'nikov sequences, they proved that half of the column sequences correspond to the polynomials

$$f_j(x) = (\alpha^j x - 1)(\alpha^{qj} x - 1) = \alpha^{(q+1)j}x^2 - Tr(\alpha^j) \cdot x + 1 \tag{35}$$

where $Tr(x) = x + x^q$, $1 \leqslant j \leqslant \frac{q}{2}$ and $f_{q+1-j} = f_j$. Then f_j is irreducible over $\mathbb{F}_q$.

Example 6 Let $q = p = 7$, $M = 6$, $q^2 = 7^2$, and a finite field $\mathbb{F}_{7^2}$ defined by a primitive polynomial $t(x) = x^2 + x + 3$. Then a 6-ary Sidel'nikov sequence $u(t)$ of period $q^2 - 1 = 48$ can be presented by a $(q-1) \times (q+1) = 6 \times 8$ array as follows.

$$(v_0, v_1, \ldots, v_7) = \begin{bmatrix} 4 & 1 & 5 & 0 & 5 & 1 & 5 & 1 \\ 2 & 4 & 4 & 2 & 2 & 2 & 5 & 4 \\ 2 & 4 & 3 & 3 & 1 & 0 & 4 & 4 \\ 0 & 5 & 0 & 3 & 5 & 2 & 3 & 5 \\ 4 & 1 & 3 & 1 & 2 & 3 & 0 & 1 \\ 0 & 0 & 5 & 2 & 1 & 3 & 3 & 0 \end{bmatrix}$$

where $v_j(t) = \log_\alpha f_j(t) \bmod M, 0 \le t \le q-1$ and $f_{8-j}(x) = f_j(x), j = 1, 2, 3$.

5.3.2 Sequences from Linear and/or Quadratic/Inverse Polynomials

Similar to (35), we formally define quadratic polynomials over $\mathbb{F}_p$ as follows, although those do not correspond to any interleaved structures of power residue sequences.

$$g_j(x) = (x - j\alpha)(x - j\alpha^p) = x^2 - j \cdot Tr(\alpha) + j^2\alpha^{p+1}, 1 \leqslant j \leqslant \frac{p-1}{2} \tag{36}$$

where α is a primitive element of $\mathbb{F}_p$. Then $g_j(x)$ is irreducible and $\deg(g_j(x)) = 2$. We now assume that $\mathbf{u}$ is defined by

$$u(t) = \begin{cases} \log_\alpha t \bmod M, M \mid (p-1) & \text{for } \mathbb{F}_p \\ \log_\alpha(\alpha^t + 1) \bmod M, M \mid (q-1) & \text{for } \mathbb{F}_q \end{cases} \tag{37}$$

and

$$v_j(t) = \begin{cases} \log_\alpha g_j(t) \bmod M, M \mid (p-1) & \text{for } \mathbb{F}_p \\ \log_\alpha f_j(\alpha^t) \bmod M, M \mid (q-1) & \text{for } \mathbb{F}_q \end{cases} \tag{38}$$

where the quadratic polynomials f_j and g_j are defined by (35) and (36), respectively. We can now write a unified set for both $\mathbb{F}_p$ and $\mathbb{F}_q$. For $r \in \{p, q\}$, we define the following signal sets where $\delta_r = p$ when $r = p$ and $\delta_r = q - 1$ when $r = q$.

Note that the sequence $\{c_0u(t) + c_1u(t+\tau)\}$ in $\mathcal{A}_{2,r}$ corresponds to polynomial $f(x) = x^{c_0}(x+\tau)^{c_1}$ and the sequences in $\mathcal{Z}_{2,r}$ correspond to polynomials $(x+1)^{c_0}(\beta x^{-1} + 1)^{c_1}$. Thus their respective correlation functions correspond to a polynomial with 4 distinct roots and a polynomial with 5 distinct roots. Note that $\mathcal{A}_{1,p}$ is only a correlation signal set, but not an ambiguity signal set (see Theorem 1 in Section 4). From Theorems 1 and 2 in Section 4, we have the results listed in Table 5.

Table 4: Signal sets from power residue and Sidel'nikov sequences

Scalar	$\mathcal{A}_{1,r} = \{c\mathbf{u} \mid 1 \le c < M\}, \mathcal{Z}_{1,r} = \{c\{u(-t)\} \mid 1 \le c < M\}$
Shift-and-Add	$\mathcal{A}_{2,r} = \left\{\{c_0u(t) + c_1u(t+\tau)\} \mid 1 \le \tau \le \lfloor \frac{\delta_r}{2} \rfloor,\ c_0, c_1 \ne 0\right\}$
	$c_0 < c_1$ if $\tau = \lfloor \frac{\delta_r}{2} \rfloor$ then $c_0 = 1$ for $r = p$,
	which are applied for all the cases below
	$\mathcal{A}_{2,0,r} = \{\{c_0u(t) + c_1u(t+\tau)\} \in \mathcal{A}_{2,r} \mid c_0 + c_1 \equiv 0\}$
	$c_0 < c_1$ if $\tau = \lfloor \frac{\delta_r}{2} \rfloor$
Shift-and-Add Inverse	$\mathcal{Z}_{2,r} = \left\{\{c_0u(t) + c_1u(-t+\tau)\} \mid 1 \le \tau \le \lfloor \frac{\delta_r}{2} \rfloor,\ c_0, c_1 \ne 0\right\}$
	$c_0 \ne c_1$ if $\tau = \lfloor \frac{\delta_r}{2} \rfloor$
Quadratic and Scalar	$\mathcal{B}_{2,r} = \left\{\{cv_j(t)\} \mid 1 \le c \le M-1, 1 \leqslant j \leqslant \frac{p-1}{2} \text{ or } \frac{q}{2}\right\}$, *and*
Quadratic	$\mathcal{B}_{2,0,r} = \left\{\{\frac{M}{2}v_j(t)\} \mid 1 \leqslant j \leqslant \frac{p-1}{2} \text{ or } \frac{q}{2}\right\}$ for M even

Table 5: Three metrics for $A_{1,r}$

$\lvert\mathcal{A}_{1,r}\rvert = M-1, C_{\max} \le \sqrt{r} + 2 + h_r$, where $h_r = \begin{cases} 0 & \text{for } r = p \\ 1 & \text{for } r = q \end{cases}$
$F_{\max} \le \sqrt{r} + 1$, and $G_{\max} \le 2\sqrt{q} + 2$.

Together with Corollary 1 in Section 2, for the signal sets in Table 4, one only needs to show that each of the corresponding polynomials for correlation, DFT and ambiguity is not an M-th power multiple in $\mathbb{F}_r[x], r \in \{p, q\}$. This can be easily done. Thus they are ambiguity signal sets where the three metrics are listed in Table 6. These ambiguity signal sets have been studied by a number of researchers. In particular, it is shown that $\mathcal{A}_{2,r}$ and $C_{\max}$ in [30] for $r = q$ and in [21] for $r = p$; $\mathcal{A}_{2,r} \cup \mathcal{Z}_{2,r}$ and $C_{\max}$ in [5] for $r = q$; $\mathcal{A}_{2,r} \cup \mathcal{B}_{2,r}$ and $C_{\max}$ in [60] for $r = q$, and $\mathcal{A}_{2,c,r}$ and $C_{\max}$ in [59] for both $r = p$ and $r = q$. The rest of the results are due to [53].

In Table 6, we use the notation P and S to indicate the sequences constructed from the power residue sequences and Sidel'nikov sequences, respectively, because the Sidel'nikov sequences can have both cases for $\mathbb{F}_q$ for $q = p^n, n > 1$ and $q = p$. The sizes of the signal sets constructed from Sidel'nikov sequences are only listed for the case $q = 2^n$ for simplicity. The sizes will be slightly different for $q = p^n$ where p is odd (see [53]). Note that the values given in Table 6 for $C_{\max}$, $F_{\max}$, and $G_{\max}$ are precise values and not bounds.

Table 6: Ambiguity signal sets with quadratic/inverse polynomials and their three metrics

Sets	$C_{\max}$	$F_{\max}$	$G_{\max}$	Sizes
$\mathcal{A}_{2,p}(P)$	$3\sqrt{p}+4$	$2\sqrt{p}+2$	$3\sqrt{p}+4$	$(M-1)\frac{p-1}{2}$
$\mathcal{A}_{1,r} \cup \mathcal{A}_{2,r}(S)$	$3\sqrt{q}+5$	$2\sqrt{q}+2$	$4\sqrt{q}+4$	$(M-1)+(M-1)^2\frac{q-2}{2}$
$\mathcal{A}_{1,r} \cup \mathcal{A}_{2,r} \cup$ $\mathcal{Z}_{1,r}(S) \cup \mathcal{Z}_{2,r}(S)$	$4\sqrt{q}+4$	$2\sqrt{q}+2$	$4\sqrt{q}+4$	$2(M-1)+$ $2(M-1)^2\frac{q-2}{2}$
$\mathcal{A}_{2,p} \cup \mathcal{B}_{2,p}(P)$	$3\sqrt{p}+4$	$2\sqrt{p}+2$	$4\sqrt{p}+2$	$(M-1)(p-1)$
$\mathcal{A}_{1,r} \cup \mathcal{A}_{2,r} \cup \mathcal{B}_{2,r}(S)$	$3\sqrt{q}+5$	$2\sqrt{q}+2$	$4\sqrt{q}+4$	$(M-1)\frac{q+2}{2}+$ $(M-1)^2\frac{q-2}{2}$
$\mathcal{A}_{2,0,p} \cup \mathcal{B}_{2,0,p}(P)$	$2\sqrt{p}+5$	$2\sqrt{p}+2$	$4\sqrt{p}+2$	$p-1$
$\mathcal{A}_{2,0,r} \cup \mathcal{B}_{2,0,r}(S)$	$2\sqrt{q}+6$	$2\sqrt{q}+2$	$4\sqrt{q}+4$	$M\frac{q-2}{2}+1$

5.4 Sequences from Hybrid Characters

5.4.1 Sequences Using Weil Representation and Their Generalizations

By using the Weil representation, a signal set was constructed by Gurevich, Hadani and Sochen [20], and three metrics of this signal set were proved by algebraic geometry. This is the first work to consider all the three metrics together for a signal set, which leads to the following new discoveries. A simple elementary construction for these sequences was found by Wang and Gong [51]. Let $g(x) = x,\ f(x) = bx^2 + x, b \in \mathbb{F}_p$, for $1 \le c < p-1$, define

$$s_{c,b}(t) = \chi_c(g(t))\psi(f(t)) = \chi_c(t)\psi(bt^2+t).$$

Let

$$\Omega_{2,p} = \{\mathbf{s}_{c,b} \mid 1 \le c < M, b \in \mathbb{F}_p\}.$$

Wang and Gong [51] showed that $\Omega_{2,p}$ is the sequences constructed using the Weil representation by Gurevich, Hadina and Sochen [20]. Shortly after that, Schmidt [47] gave a direct proof of three metrics of those sequences and the following generalized construction. Let $g(x) = x,\ f(x) = \sum_{j=2}^{d} b_j x^j + x$ where $d < p$, $1 \le c \le p-2$ and $\mathbf{b} = (b_d, \ldots, b_2, 1)$ with $b_j \in \mathbb{F}_p$ and $b_1 = 1$, define

$$s_{c,\mathbf{b}}(t) = \chi_c(g(t))\psi(f(t)) = \chi_c(t)\psi(\sum_{j=1}^{d} b_j t^j),\ \mathbf{s}_{c,\mathbf{b}} = \{s_{c,\mathbf{b}}(t)\}$$

where χ is a multiplicative character of $\mathbb{F}_p$ of order $p-1$. We may further extend the above sequences to a multiplicative character with order $M \mid (p-1)$ as follows:

$$s_{c,\mathbf{b}}(t) = \omega_M^{c \log_\alpha t}\psi(f(t)). \tag{39}$$

Let

$$\Omega_{d,p} = \{s_{c,\mathbf{b}} | 1 \le c < M, b_i \in \mathbb{F}_p\}.$$

The phase-shift operation for hybrid sequences, defined by (39), is through additive characters in $\mathbb{F}_p$. By directly applying the Weil bound in Lemma 3, we obtain that $\Omega_{d,p}$ is an ambiguity signal set with the following parameters.

Proposition 8 *With the above notation, if the phase-shift operation for hybrid sequences is defined by additive characters in $\mathbb{F}_p$, then we have the results listed in Table 8.*

Table 7: Three metrics of hybrid sequences over $\mathbb{F}_p$

$C_{\max}$	$F_{\max}$	$G_{\max}$	$\lvert\Omega_{d,p}\rvert$
$3\sqrt{p}+2$	$2\sqrt{p}+1$	$3\sqrt{p}+2$	$(M-1)p,\ d=2$
$(d+1)\sqrt{p}+2$	$d\sqrt{p}+1$	$(d+1)\sqrt{p}+2$	$(M-1)p^{d-1},\ d>2$

Remark 6 For $d = 2$ and $M = p - 1$, the result on correlation in (8), appeared in [47], actually improved the bounds originally proved by using the Weil representation in [20, 51].

5.4.2 Generalization to $\mathbb{F}_q$ Hybrid Sequences

A generalization of the construction of $\Omega_{d,p}$ to $\mathbb{F}_q$ is given in [53] and as a special case, the product of a binary m-sequence and a ternary Sidel'nikov sequence is investigated in [27]. Let $M \mid (q-1)$, $g(x) = x + 1$, $u(t)$ be an M-ary Sidel'nikov sequence, and $f(x) \in \mathbb{F}_q[x]$ be defined as

$$f(x) = bx^2 + x, b \in \mathbb{F}_q \text{ where } p > 2 \text{ or} \tag{40}$$

$$f(x) = \sum_{i=2}^{d} b_i x^{2i-1} + x \in T_1, \text{ where } T_1 \text{ is defined in (31).} \tag{41}$$

Let

$$s_{c,\mathbf{b}}(t) = \chi(\alpha^t + 1)\psi_1(f(\alpha^t)) = \omega_M^{c \log_\alpha(\alpha^t+1)} \omega_p^{Tr(f(\alpha^t))}$$

where χ is a multiplicative character of order $M \mid q-1$. We write $\mathbf{b} = (b_1, \ldots, b_d)$ where $b_1 = 1$. Let

$$\Omega_{2,q} = \{\mathbf{s}_{c,b} | 1 \le c < M, b \in \mathbb{F}_q\},\ f(x) \text{ in (40).}$$
$$\Omega_{d,q,o} = \{\mathbf{s}_{c,\mathbf{b}} | 1 \le c < M, b_j \in \mathbb{F}_q\},\ f(x) \text{ in (41).}$$

Note that the coset containing 2 modulo $q-1$ has the full size n.

Table 8: Three metrics of hybrid sequences over $\mathbb{F}_q$

Sets	$C_{\max}$	$F_{\max}$	$G_{\max}$	Sizes
$\Omega_{2,q}$	$3\sqrt{q}+3$	$2\sqrt{q}+1$	$3\sqrt{q}+3$	$(M-1)q$
$\Omega_{d,q,o}$	$2d\sqrt{q}+3$	$(2d-1)\sqrt{q}+1$	$2d\sqrt{q}+3$	$(M-1)q^{d-1}$

Proposition 9 *With the above notation and the phase-shift operator is defined through additive characters of $\mathbb{F}_q$. Then $\Omega_{d,q}$ is an ambiguity signal set where the size and three metrics are given in Table 9.*

Example 7 The signal set $\Omega_{2,q}$ is an analogue of the signal set from the Weil representation where $g(x) = x + 1$ and $f(x) = bx^2 + x$, $b \in \mathbb{F}_q$. For $\Omega_{2,3^2}$ $(q = 3^2)$, let $\mathbb{F}_9$ be defined by a primitive polynomial $t(x) = x^2+2x+2$ over $\mathbb{F}_3$ and $t(\alpha) = 0$, then α is a primitive element of $\mathbb{F}_9$. In this case, $Tr(x)$ defines the m-sequence $\{0, 1, 1, 2, 0, 2, 2, 1\}$ and and $Tr(bx^2)$ gives the shifts of 2-decimation of the m-sequence for different $b_2 \in \mathbb{F}_{3^2}$, i.e., $\{0, 1, 0, 2, 0, 1, 0, 2\}$ and $\{1, 2, 2, 1, 1, 2, 2, 1\}$.

Table 9: Component sequences for hybrid sequences from $\mathbb{F}_9$ for $M = 8$

$u(t) = \omega_8^{c\log_\alpha(\alpha^t+1)}$	$\psi(b_2t^2) = \omega_3^{Tr(b_2t^2)}$
$(-1, \omega_8^2, \omega_8^7, \omega_8^6, 1, \omega_8^3, \omega_8^5, \omega_8)$	$(1, \omega_3, 1, \omega_3^2, 1, \omega_3, 1, \omega_3^2)$
$(1, -1, \omega_8^6, -1, 1, \omega_8^6, \omega_8^2, \omega_8^2)$	$(\omega_3, 1, \omega_3^2, 1, \omega_3, 1, \omega_3^2, 1)$
$(-1, \omega_8^6, \omega_8^5, \omega_8^2, 1, \omega_8, \omega_8^7, \omega_8^3)$	$(1, \omega_3^2, 1, \omega_3, 1, \omega_3^2, 1, \omega_3)$
$(1, 1, -1, 1, 1, -1, -1, -1)$	$(\omega_3^2, 1, \omega_3, 1, \omega_3^2, 1, \omega_3, 1)$
$(-1, \omega_8^2, \omega_8^3, \omega_8^6, 1, \omega_8^7, \omega_8, \omega_8^5)$	$(\omega_3, \omega_3^2, \omega_3^2, \omega_3, \omega_3, \omega_3^2, \omega_3^2, \omega_3)$
$(1, -1, \omega_8^2, -1, 1, \omega_8^2, \omega_8^6, \omega_8^6)$	$(\omega_3^2, \omega_3^2, \omega_3, \omega_3, \omega_3^2, \omega_3^2, \omega_3, \omega_3)$
$(-1, \omega_8^6, \omega_8, \omega_8^2, 1, \omega_8^5, \omega_8^3, \omega_8^7)$	$(\omega_3^2, \omega_3, \omega_3, \omega_3^2, \omega_3^2, \omega_3, \omega_3, \omega_3^2)$
	$(\omega_3, \omega_3, \omega_3^2, \omega_3^2, \omega_3, \omega_3, \omega_3^2, \omega_3^2)$
	$(1, 1, 1, 1, 1, 1, 1, 1)$

A sequence in $\Omega_{2,9}$ is a term-by-term product of three sequences from each of the columns in Table 9 and the m-sequence. Note that this example is used only to illustrate the construction of the sequences through hybrid characters, since the bounds of the three metrics in this case is not meaningful.

Remark 7 Note that the phase-shift operation for the case for $\mathbb{F}_q$ is different from the case of $\mathbb{F}_p$. In Proposition 9, the phase shift of the $\mathbb{F}_q$ hybrid sequences is defined through additive characters of

$\mathbb{F}_q$. However, it can also be defined through multiplicative characters of $\mathbb{F}_q$, since the field elements are indexed by the order of multiplicative group of $\mathbb{F}_q$. If so, the bound on ambiguity functions in Proposition 9 will be changed to $4\sqrt{q}+2$ and $(2d+1)\sqrt{q}+2$ respectively.

The known ambiguity signal sets with the sizes in the order of q^2 are $\mathcal{A}_{2,0,q} \cup \mathcal{B}_{2,0,q}$, $\Omega_{2,p}$ and $\Omega_{2,q}$ given by Tables 6, (8) and (9) which are collectively grouped in Table 10. We denote by P the number of phases in a sequence in the table.

Table 10: Known ambiguity signal sets with the sizes in the order of q^2

Sets	$(C_{\max}, F_{\max}, G_{\max})$	Sizes	$(P,\ \min P)$
$\mathcal{A}_{2,0,q} \cup \mathcal{B}_{2,0,q}$	$(2\sqrt{q}+6, 2\sqrt{q}+2, 4\sqrt{q}+4)$	$M\frac{q-2}{2}+1$	$(M, 2)$
$\Omega_{2,p}$	$(3\sqrt{p}+2, 2\sqrt{p}+1, 3\sqrt{p}+2)$	$(M-1)p$	$(Mp, 2p)$
$\Omega_{2,q}$	$(3\sqrt{q}+3, 2\sqrt{q}+1, 3\sqrt{q}+3)$	$(M-1)q$	$(Mp, 6)$ when $p=2$

Thus $\mathbb{F}_q$ multiplicative sequences with quadratic polynomials have the best parameters in terms of correlation and DFT, and the other two are superior in terms of ambiguity.

5.5 A New Construction

As we have introduced in Section 4.5, there are alternative four classes of sequences in terms of the different methods for indexing the elements of $\mathbb{F}_p$ and $\mathbb{F}_q$. Thus a sequence defined by hybrid characters could have a number of different combinations.

Construction A. Let

$$
\begin{aligned}
&s(t) = \eta(x(t))\sigma(y(t)), \quad \text{where} \\
&\eta, \sigma \in \{\psi_i, \chi_j \,|\, 0 < i < p, 0 < j < q-1\}, \text{ and } x(t), y(t) \in \mathcal{P}, \quad \text{where} \\
&\mathcal{P} = \{a(t) \text{ and } u(t), \text{ defined in Table 1, and } b(t) \text{ and } v(t), \text{ defined in Table 2}\}.
\end{aligned}
$$

The ambiguity signal sets presented in Section 5.4 for both $\mathbb{F}_p$ and $\mathbb{F}_q$ use $x(t) = a(t)$, $y(t) = u(t)$, $\eta = \psi$ and $\sigma = \chi$. Thus, it is interesting to see whether there exist some combinations which yield ambiguity signal sets with low three metrics. An example of this new construction is the sequences considered in [49], which is obtained by flipping a few bits of the following sequence

$$
\begin{aligned}
s(t) \quad = \quad & \chi_i(u(t))\chi_j(v(t)) = (-1)^{s_1(t)}(-1)^{s_2(t)} \text{ where} \\
& s_1(t) = \log_\alpha t \mod 2 \\
& s_2(t) = \log_\alpha^{(\alpha^t+1)} \mod 2, \ t = 0, 1, \ldots
\end{aligned}
$$

where $u(t), v(t) \in \mathcal{P}$ in Construction A, and both χ_i and χ_j are multiplicative quadratic characters of $\mathbb{F}_p$. Note that $\{s_1(t)\}$ has period p and $\{s_2(t)\}$ has period $p-1$ since it uses the multiplicative group order of $\mathbb{F}_p$. Thus $\{s(t)\}$ has period $(p-1)p$.

6 Two-Level Autocorrelation Sequences and Double Exponential Sums

In this section, we look at the sequences with ideal 2-level autocorrelation. Up to now in all the known multiplicative cases, there are only polynomials with degree 1, which produce the sequences with optimal autocorrelation, i.e., power residue sequences for $\mathbb{F}_p$ multiplicative and Sidel'nikov sequences for $\mathbb{F}_q$ multiplicative. For $\mathbb{Z}_N$ additive, FZC sequences are perfect sequences with defining polynomials of degree 2. However, for $\mathbb{F}_q$ additive, there are several classes of sequences with 2-level autocorrelation with high degree polynomials. The work on binary 2-level autocorrelation sequences, i.e., $q = 2^n$, has been collected in [14] and has no new sequences coming out since then. For the ternary case, i.e., $q = 3^n$, there are several conjectured sequences, whose validity has been established recently by Arasu, Dillion and Player [3], but the proofs did not appear yet. For $p > 3$, there are only two known classes of primary constructions (we will define this concept below), one is the class of m-sequences and the other is the Helleseth-Gong (HG) class.

In this section, we first introduce the concepts on prime 2-level autocorrelation sequences and Hadamard equivalence, then we show the conjectured ternary sequences and their alternative exponential sums in terms of the 2nd order decimation-Hadamard transform. We use the trace representation of $\mathbb{F}_q$ additive sequences in this section.

6.1 Prime 2-Level Autocorrelation Sequences

Let $f(x)$ be the trace representation of a p-ary sequence $\mathbf{a} = \{a(t)\}$, i.e., $a(t) = f(\alpha^t), t = 0, 1, \ldots$, with 2-level autocorrelation, i.e., $f(x)$ is a function from $\mathbb{F}_q$ to $\mathbb{F}_p$. Let m be a proper factor of n and $h(x)$ be a function from $\mathbb{F}_q$ to $\mathbb{F}_{p^m}$. We say that $h(x)$ is $\mathbb{F}_{p^m}$ *linear* if for $y \in \mathbb{F}_{p^m}$, and $x \in \mathbb{F}_q$, we have $h(xy) = y^d h(x)$ for some d with $1 \le d < p^m - 1$. If we can write

$$f(x) = g(x) \circ h(x)$$

where $g(x)$ is a polynomial nonlinear function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ (i.e., $g(x) \neq Tr_1^m(ax), \forall a \in \mathbb{F}_p$) such that the sequence defined by $g(x)$ has 2-level autocorrelation, and $h(x)$ is an $\mathbb{F}_{p^m}$ linear function from $\mathbb{F}_q$ to $\mathbb{F}_{p^m}$, then we say that $\mathbf{a}$ is a *composited 2-level autocorrelation sequence*. Otherwise, it is said to be a *prime 2-level autocorrelation sequence*.

Currently, there are only two classes known F_{p^m} linear functions, one is given by $Tr_m^n(x^d)$ with $1 \le d < q-1$ and $\gcd(d, q-1) = 1$, and the other is HG functions, which will be defined shortly. For example, GMW sequences or generalized GMW sequences are the composited 2-level

autocorrelation sequences (see [14]). So, we only need to classify all prime 2-level autocorrelation sequences.

6.2 Hadamard Transform, 2nd Order Decimation-Hadamard Transform, and Hadamard Equivalence

The Hadamard transforms of $f(x)$ and $\mathbf{a}$ are defined by

$$\begin{aligned} \widehat{f}(\lambda) &= \sum_{x\in\mathbb{F}_q} \psi(Tr(\lambda x))\psi(f(x))^* = \sum_{x\in\mathbb{F}_q} \omega_p^{Tr(\lambda x)-f(x)}, \lambda \in \mathbb{F}_q \\ \widehat{\mathbf{a}}(\tau) &= \widehat{f}(\alpha^\tau) - 1, \tau = 0, 1, \ldots. \end{aligned} \tag{42}$$

Note that the Hadamard transform of $\mathbf{a}$ is equal to the crosscorrelation of $\mathbf{a}$ and an m-sequence defined by $Tr(x)$. From (42), the Hadamard transform of $f(x)$ and $\mathbf{a}$ are determined by each other. From now on, we focus on the Hadamard transform of functions. The inverse formula for $f(x)$ is given by

$$\psi(f(\lambda)) = \frac{1}{q}\sum_{x\in\mathbb{F}_q} \psi(Tr(\lambda x))\widehat{f}(x)^*, \lambda \in \mathbb{F}_q.$$

For $(v,t) \in \mathbb{Z}_{q-1}^2$ and $\lambda \in \mathbb{F}_q$, the first-order and second order decimation-Hadamard transforms (DHT) are defined as follows.

$$\begin{aligned} \text{1st order DFT:}\quad \widehat{f}(v)(\lambda) &= \textstyle\sum_{x\in\mathbb{F}_q} \psi(Tr(\lambda x))\psi(f(x^v))^* \\ &= \textstyle\sum_{x\in\mathbb{F}_q} \omega_p^{Tr(\lambda x)-f(x^v)}. \end{aligned}$$

$$\begin{aligned} \text{2nd order DFT:}\quad \widehat{f}(v,t)(\lambda) &= \textstyle\sum_{y\in\mathbb{F}_q} \psi(Tr(\lambda y))\widehat{f}(v)(y^t)^* \\ &= \textstyle\sum_{x,y\in\mathbb{F}_q} \omega_p^{Tr(\lambda y)-Tr(y^t x)+f(x^v)}. \end{aligned}$$

In general, for any integer pair (v,t), $x \in \mathbb{F}_q$, $\widehat{f}(v,t)(x)$ may be just a complex number. However, if it satisfies the following condition:

$$\widehat{f}(v,t)(x) \in \{q\omega_p^i \,|\, i = 0, \ldots, p-1\}, \forall x \in \mathbb{F}_q,$$

then we can construct a function, say $g(x)$, from $\mathbb{F}_q$ to $\mathbb{F}_p$, whose elements are given by

$$\psi(g(x)) = \frac{1}{q}\widehat{f}(v,t)(x), x \in \mathbb{F}_q. \tag{43}$$

In this case, we say that (v,t) is *realizable*, and $g(x)$ is a *realization* of $f(x)$ or $\mathbf{a}$. If $g(x)$ is realized by $f(x)$ with (v,t), from (43), we have

$$\widehat{g}(\lambda) = \widehat{f}(v)(\lambda^t),\ \lambda \in \mathbb{F}_q. \tag{44}$$

Definition 9 *If f and g satisfy (44), then we say that f and g are* Hadamard equivalent*, written as $f \sim_H g$.*

In order to determine the autocorrelation of the sequence defined by $g(x)$, we need the Parseval formula on the Hadadmard transform.

Property 7 (Parseval Formula)

$$\sum_{x\in\mathbb{F}_q} \psi(f(\lambda x))\psi(f(x))^* = \sum_{x\in\mathbb{F}_1} \widehat{f}(\lambda x)\widehat{f}(x)^*, \lambda \in \mathbb{F}_q.$$

From the Parseval formula, the autocorrelation of $\mathbf{a}$, defined by $f(x)$, is equal to the autocorrelation of its Hadamard transform sequence. If one of them has 2-level autocorrelation, so does the other. Formally, we have

Property 8 *Let $\mathbf{b}$ be a sequence defined by $g(x)$, i.e., $b(t) = g(\alpha^t)$, where $g(x)$ is a realization of $\mathbf{a}$. Then $\mathbf{a}$ has 2-level autocorrelation if and only if $\mathbf{b}$ has 2-level autocorrelation.*

Dillon and Dobbertin [8] used the Parseval formula to prove binary 2-level sequences. The concepts on the second order DHT are introduced in [17] by Gong and Golomb for the case that both v and t are coprime with $q-1$ and those are extended to any integers in [58].

6.3 Conjectures on Ternary 2-Level Autocorrelation Sequences

Let $p = 3$, $n = 2m+1$ and $d = 2\cdot 3^m + 1$. Lin's Conjecture [35] is stated as follows.

Conjecture 1 *(Lin [35]) Let $f(x) = Tr(x + x^d)$ and $a(t) = f(\alpha^t)$. Then $\mathbf{a} = \{a(t)\}$ has 2-level autocorrelation. In other words,*

$$\sum_{x\in\mathbb{F}_{3^n}} \omega_3^{Tr(x+x^d)-Tr(\alpha^\tau x+\alpha^{\tau d}x^d)} = 0,\ \textit{for all } \tau = 1,\ldots,q-2.$$

Conjecture 2 *(Gong* et al. *[18]) Let $f(x) = Tr(x)$ and (v,t) be defined as follows*

$$v = \begin{cases} 2(3^{m+1}-1) & \textit{for } m \textit{ even} \\ -2(3^{m+1}-3) & \textit{for } m \textit{ odd} \end{cases} \quad \textit{and } t = \frac{3^n+1}{4}.$$

Then (v,t) is a realizable pair and $\widehat{f}(v,t)(\lambda)$ realizes the conjectured 2-term sequences in Conjecture 1.

Note that in this case, $\gcd(v, q-1) \neq 1$. So the realized sequence should be computed through the multiplexing method as presented in [58].

The following two conjectures involve the HG sequences.

Theorem 5 *(Helleseth* et al. *[24]) Let $n = (2m+1)k$ and s be an integer with $1 \leq s \leq 2m$ and $\gcd(s, 2m+1) = 1$. Define $b_0 = 1$, $b_{is} = (-1)^i$ and $b_i = b_{2m+1-i}$ for $i = 1, 2, \ldots, m$, where all indices of b_i's are taken modulo $2m+1$. Let $u_0 = b_0/2 = (p+1)/2$ and $u_i = b_{2i}$ for $i = 1, 2, \ldots, m$. Define*

$$e(x) = \sum_{i=0}^{m} u_{m-i} x^{(q_1^{2i}+1)/2}, q_1 = p^k.$$

Then the sequence $\{s(t)\}$ over $\mathbb{F}_p$ whose elements are defined by $s(t) = Tr(e(\alpha^t))$ has an ideal two-level autocorrelation for any p.

This is referred to as *HG sequences*, which was discovered by Helleseth and Gong [24]. Note in [24] there are two classes of 2-level autocorrelation sequences, however, they are decimation equivalent. When $p = 3$, $k = 1$, and $s = 2$, $e(x)$ becomes

$$e(x) = Tr\left(\sum_{i=0}^{m} u_{m-i} x^{(3^{2i}+1)/2}\right).$$

Let

$$\delta = \begin{cases} 1 & m \text{ odd} \\ 2 & m \text{ even} \end{cases} \quad \text{and } \epsilon = \begin{cases} 1 & m \text{ odd} \\ 0 & m \text{ even.} \end{cases} \tag{45}$$

The following conjecture illustrates that Lin's conjectured 2-term sequences are the realizations of HG Sequences.

Conjecture 3 *(Ludkovski and Gong [36]) Let $u_0 = \frac{3^n-1}{2}$, $u_1 = \frac{3^m-1}{2}$, $f(x) = x + x^d$, defined in Conjecture 1, and $g(x) = \delta e(x)$. Then*

$$\widehat{f}(\lambda) = \widehat{g}(\lambda^{t^{-1}}), \ \forall \lambda \in \mathbb{F}_{3^n} \tag{46}$$

where $t = \epsilon u_0 + u_1$. Thus, Lin sequences and HG sequences are Hadamard equivalent. The exponential sum equality of (46) is written as

$$\sum_{x \in \mathbb{F}_q} \omega^{Tr(\lambda x - x - x^d)} = \sum_{x \in \mathbb{F}_q} \omega^{Tr(\lambda^{t^{-1}} x) - g(x)}, \ \forall \lambda \in \mathbb{F}_q.$$

The following conjecture indicates that the conjectured ternary 2-level autocorrelation sequences by Ludkovski and Gong in [36] can also be realized by HG sequences.

Conjecture 4 *Keep $g(x) = \delta e(x)$. Let*

$$v = \tfrac{3^n+1}{4} \quad \textit{and} \quad t_j = \tfrac{3^{n-1}-1}{2} - 3^j, \\ j = n-2, n-3, \ldots, \tfrac{n+1}{2}, \epsilon\tfrac{n+1}{2}, \tfrac{n-1}{2}$$

where ϵ is defined in (45) and let

$$\omega^{T_j(x)} = \frac{1}{q}\widehat{g}(v, t_j)(x), x \in \mathbb{F}_q.$$

Then $T_j(x)$ defines a 2-level autocorrelation sequence. Equivalently,

$$\sum_{x,y\in\mathbb{F}_q} \omega^{Tr(\lambda y - y^{t_j}x)+g(x^v)} \in \{q, q\omega, q\omega^2\}, \ \forall \lambda \in \mathbb{F}_q.$$

T_j contains exactly three classes B, C and D conjectured in [36].

The validity of all the conjectures has been verified for $n = 5, 7, 9, 11$ and 13 and probabilistically verified for $n = 15$. From Conjectures 2-4, we have the Hadamard equivalence relations listed in Table 11.

Table 11: Hadamard equivalence relations given by Conjectures 2-4

m-sequences	$\sim_H$	Lin conjectured 2-term sequences (Conjecture 2)
Lin conjectured 2-term sequences	$\sim_H$	HG-sequences (Conjecture 3)
HG-sequences	$\sim_H$	Ludkovski-Gong conjectured sequences (Conjecture 4)

7 Some Open Problems

In this section, we summarize some unsolved problems on polyphase sequences with good correlation, DFT and ambiguity properties, which are introduced in previous sections.

7.1 Current Status of the Conjectures on Ternary 2-Level Autocorrelation

Arasu announced in [2] the validity of the 2-level autocorrelation property of Lin conjectured sequences, and Ludkovski and Gong conjectured sequences in an unpublished paper [3]. However, the Hadamard equivalences given by Table 11 still remain open. It is not clear whether those questions could be solved by the light of their approaches.

If all Conjectures 2-4 are true, then there are only two classes of known ternary 2-level autocorrelation sequences. One is the class, denoted by $\mathcal{T}_1$, consisting of all known ternary prime 2-level autocorrelation sequences and one type of HG sequences. Note that the ternary 2-level autocorrelation sequences in [26] is a special case of HG sequences. The other class, denoted by $\mathcal{T}_2$, is the rest of HG sequences. Conjectures 2-4 state that all the sequences in $\mathcal{T}_1$ are Hadamard equivalent, which still remain unsolved.

7.2 Possibility of Multiplicative Sequences with Low Autocorrelation

It is natural to ask whether there exist $\mathbb{F}_p$ or $\mathbb{F}_q$ multiplicative sequences with low autocorrelation, but the defining polynomials have high degrees. For example, $\mathbb{F}_p$ multiplicative sequences have the same autocorrelation as the power residue sequences and $\mathbb{F}_q$ multiplicative sequences have the same autocorrelation as the Sidel'nikov sequences. Those sequences, if there exist any, should be revealed using some special techniques. This could constitute an extremely challenge task.

7.3 Problems on Four Alternative Classes of Sequences and the General Hybrid Construction

As we have shown in Section 4.5, corresponding to the four classes of sequences through $\mathbb{F}_p$ and $\mathbb{F}_q$ algebraic structures, there are the other four classes of the sequences using alternative indexing field elements of $\mathbb{F}_p$ and $\mathbb{F}_q$. Among those sequences, only Golay sequences [7], indexing the elements of $\mathbb{F}_{2^n}$ by additive group, are extensively investigated in the literature. Recently, it has been reported in [19] that Golay sequences have a large zero autocorrelation zone. However, the other out-of-phase autocorrelation values have very large peaks. We ask whether there exist some classes of those sequences with low autocorrelation or with low crosscorrelation. The other open question is to find some class of the sequences with three metrics, constructed from combinations of different indexing field elements and hybrid characters in Construction A.

8 Conclusions

We have introduced four types of polyphase sequences defined by $\mathbb{F}_p$ additive and multiplicative characters, and $\mathbb{F}_q$ additive and multiplicative characters, respectively. We considered polyphase sequences with three metrics, namely, correlation, DFT and ambiguity together. We have showed sequences with three metrics which are obtained from odd degree polynomials, power residue sequences, Sidel'nikov sequences, Weil representation sequences, and the sequences from combinations of different indexing field elements and hybrid characters. We restated conjectured ternary sequences with 2-level autocorrelation and their Hadamard equivalence relation. Some open problems were addressed.

References

[1] W.O. Alltop. Complex sequences with low periodic correlations. *IEEE Transactions on Information Theory*, 26(3):350–354, 1980.

[2] K.T. Arasu. Sequences and arrays with desirable correlation properties. arhiva.math.uniri.hr/NATO-ASI/abstracts/arasu.pdf, 2011.

[3] K.T. Arasu, J.F. Dillon, and K.J. Player. Character sum factorizations yield perfect sequences, Preprint, 2010.

[4] D.C. Chu. Polyphase codes with good periodic correlation properties. *IEEE Transactions on Information Theory*, 18(4):531–532, 1972.

[5] J.S. Chung, J.S. No, and H. Chung. A construction of a new family of M-ary sequences with low correlation from Sidelnikov sequences. *IEEE Transactions on Information Theory*, 57(4):2301–2305, 2011.

[6] J.P. Costas. A study of a class of detection waveforms having nearly ideal range of doppler ambiguity properties. *Proceedings of the IEEE*, 72(8):996–1009, 1984.

[7] J.A. Davis and J. Jedwab. Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes. *IEEE Transactions on Information Theory*, 45(7):2397–2417, 1999.

[8] J.F. Dillon and H. Dobbertin. New cyclic difference sets with Singer parameters. *Finite Fields and Their Applications*, 10(3):342–389, 2004.

[9] T. Etzion. Combinatorial designs derived from Costas arrays. *Discrete Mathematics*, 93(2-3):143–154, 1991.

[10] R. Frank, S. Zadoff, and R. Heimiller. Phase shift pulse codes with good periodic correlation properties. *IRE Transactions on Information Theory*, 8(6):381–382, 1962.

[11] A. Gabizon and R. Raz. Deterministic extractors for affine sources over large fields. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '05, pages 407–416. IEEE Computer Society, 2005.

[12] S.W. Golomb. Sequences with randomness properties. The Glenn L. Martin Company, Baltimore, MD, 1955.

[13] S.W. Golomb. Algebraic constructions for Costas arrays. *Journal of Combinatorics Theory (A)*, 37(1):13–21, 1984.

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

[15] S.W. Golomb and G. Gong. The status of Costas arrays. *IEEE Transactions on Information Theory*, 53(11):4260–4265, 2007.

[16] G. Gong. Theory and applications of q-ary interleaved sequences. *IEEE Transactions on Information Theory*, 41(2):400–411, 1995.

[17] G. Gong and S.W. Golomb. The decimation-Hadamard transform of two-level autocorrelation sequences. *IEEE Transactions on Information Theory*, 48(4):853–865, 2002.

[18] G. Gong, T. Helleseth, H.G. Hu, F. Huo, and Y. Yang. On conjectured ternary 2-level autocorrelation sequences. Progress Report, August 2011.

[19] G. Gong, F. Huo, and Y. Yang. Large zero autocorrelation zone of Golay sequences and 4^q-QAM Golay complementary sequences. Technical Report CACR 2011-16, University of Waterloo, 2011.

[20] S. Gurevich, R. Hadani, and N. Sochen. The finite harmonic oscillator and its applications to sequences, communication, and radar. *IEEE Transactions on Information Theory*, 54(9):4239–4253, 2008.

[21] Y.K. Han and K. Yang. New M-ary sequence families with low correlation and large size. *IEEE Transactions on Information Theory*, 55(4):1815–1823, 2009.

[22] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*. 5th ed., New York, Oxford University Press, 1980.

[23] T. Helleseth. Some results about the cross-correlation functions between two maximal length linear sequences. *Discrete Mathematics*, 16(3):209–232, 1976.

[24] T. Helleseth and G. Gong. New nonbinary sequences with ideal two-level autocorrelation. *IEEE Transactions on Information Theory*, 48(11):2868–2872, 2002.

[25] T. Helleseth and P.V. Kumar. Sequences with low correlation. In *Handbook of coding theory*, volume 2, pages 1765–1853. Amsterdam, The Netherlands: Elsevier, 1998.

[26] T. Helleseth, P.V. Kumar, and H. Martinsen. A new family of ternary sequences with ideal two-level autocorrelation function. *Designs, Codes and Cryptography*, 23:157–166, 2001.

[27] Fei Hou. Sequences design for ofdm and cdma systems. Master Thesis, University of Waterloo, 2011.

[28] Y.J. Kim and H.Y. Song. Cross correlation of Sidelnikov sequences and their constant multiples. *IEEE Transactions on Information Theory*, 53(3):1220–1224, 2007.

[29] Y.J. Kim, H.Y. Song, G. Gong, and H. Chung. Crosscorrelation of q-ary power residue sequences of period p. In *IEEE International Symposium on Information Theory 2006*, pages 311–315. IEEE, 2006.

[30] Y.S. Kim, J.S. Chung, J.S. No, and H. Chung. New families of M-ary sequences with low correlation constructed from Sidelnikov sequences. *IEEE Transactions on Information Theory*, 54(8):3768–3774, 2008.

[31] P.V. Kumar and O. Moreno. Prime-phase sequences with periodic correlation properties better than binary sequences. *IEEE Transactions on Information Theory*, 37(3):603–616, 1991.

[32] J. Lahtonen. On the odd and aperiodic correlation properties of the Kasami sequences. *IEEE Transactions on Information Theory*, 41(5):1506–1508, 1995.

[33] A. Lempel, M. Cohn, and W. Eastman. A class of balanced binary sequences with optimal autocorrelation properties. *IEEE Transactions on Information Theory*, 23(1):38–42, 1977.

[34] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, 1997, 2nd ed.

[35] A.H. Lin. From cyclic Hadamard difference sets to perfectly balanced sequences. In *Ph. D thesis*. University of Southern California, 1998.

[36] M. Ludkovski and G. Gong. New families of ideal 2-level autocorrelation ternary sequences from second order DHT. In *Proceedings of the second International Workshop in Coding and Cryptography*, pages 345–354. INRIA, 2001.

[37] H.D. Lüke. Large family of cubic phase sequences with low correlation. *Electronics Letters*, 31(3):163, 1995.

[38] O. Moreno and P.V. Kumar. Minimum distance bounds for cyclic codes and Deligne's theorem. *IEEE Transactions on Information Theory*, 39(5):1524–1534, 1993.

[39] K.G. Paterson. Generalized Reed-Muller codes and power control for OFDM modulation. *EEE Transactions on Information Theory*, 46(1):104–120, 2000.

[40] K.G. Paterson and V. Tarokh. On the existence and construction of good codes with low peak-to-average power ratios. *IEEE Transactions on Information Theory*, 46(6):1974–1987, 2000.

[41] J.G. Proakis. *Digital Communications, 2006*. McGraw-Hill, 2006.

[42] M.B. Pursley. *Introduction to Digital Communications*. Prentice Hall, 2005.

[43] J.J. Rushanan. Weil sequences: A family of binary sequences with good correlation properties. In *Proceedings of IEEE International Symposium on Information Theory (ISIT2006)*, pages 1648–1652. IEEE, 2006.

[44] D. Sarwate. Comments on "A class of balanced binary sequences with optimal autocorrelation properties" by Lempel *et al. IEEE Transactions on Information Theory*, 24(1):128–129, 1978.

[45] D. Sarwate. Bounds on crosscorrelation and autocorrelation of sequences. *IEEE Transactions on Information Theory*, 25(6):720–724, 1979.

[46] D.V. Sarwate and M.B. Pursley. Crosscorrelation properties of pseudorandom and related sequences. *Proceedings of the IEEE*, 68(5):593–619, 1980.

[47] K.U. Schmidt. Sequence families with low correlation derived from multiplicative and additive characters. *IEEE Transactions on Information Theory*, 57(4):2291–2294, 2011.

[48] V.M. Sidel'nikov. Some k-valued pseudo-random sequences and nearly equidistant codes. *Problemy Peredachi informatii (Problems on Information Transmission)*, 5(1):16–22, 1969.

[49] M. Su and A. Winterhof. Autocorrelation of Legendre - Sidelnikov sequences. *IEEE Transactions on Information Theory*, 56(4):1714–1718, 2010.

[50] D. Wan. Generators and irreducible polynomials over finite fields. *Mathematics of Computation*, 66(219):1195–1212, 1997.

[51] Z. Wang and G. Gong. New sequences design from Weil representation with low two-dimensional correlation in both time and phase shifts. *IEEE Transactions on Information Theory*, 57(7):4600–4611, 2011.

[52] Z.L. Wang and G. Gong. Cross correlation of binary sequence from multiplicative characters of polynomials. Preprint, March 2012.

[53] Z.L. Wang, G. Gong, and N.Y. Yu. Polyphase sequence families with low correlation from the bounds of character sums. CACR Technical Report, University of Waterloo, 2012.

[54] A. Weil. On some exponential sums. *Proceedings of the National Academy of Sciences of the United States of America*, 34(5):204–207, 1948.

[55] A. Weil. *Basic Number Theory*. 3rd ed. New York: Springer-Verlag, 3rd ed, 1974.

[56] L. Welch. Lower bounds on the maximum cross correlation of signals. *IEEE Transactions on Information Theory*, 20(3):397–399, 1974.

[57] N.Y. Yu. New near-optimal codebooks associated with binary sidel'nikov sequences. In *The proceedings of 2012 IEEE International Symposium on Information Theory Proceedings (ISIT)*, 2012.

[58] N.Y. Yu and G. Gong. Multiplexing realizations of the decimation-Hadamard transform of two-level autocorrelation sequences. In *Coding and Cryptology*, volume 5557, pages 248–258. Springer-Verlag, 2009.

[59] N.Y. Yu and G. Gong. Multiplicative characters, the Weil bound, and polyphase sequence families with low correlation. *IEEE Transactions on Information Theory*, 56(12):6376–6387, 2010.

[60] N.Y. Yu and G. Gong. New construction of M-ary sequence families with low correlation from the structure of Sidelnikov sequences. *IEEE Transactions on Information Theory*, 56(8):4061–4070, 2010.

[61] G.H. Zhang and Q. Zhou. Pseudonoise codes constructed by Legendre sequence. *Electronic Letters*, 38(8):376–377, April 2002.

[62] N. Zierler. Linear recurring sequences. *Journal of the Society for Industrial and Applied Mathematics*, 7(1):31–48, 1959.