Three new constructions of asymptotically optimal periodic quasi-complementary sequence sets with small alphabet sizes

Luo, Gaojun; Cao, Xiwang; Shi, Minjia; Helleseht, Tor

2021

Luo, G., Cao, X., Shi, M. & Helleseht, T. (2021). Three new constructions of asymptotically optimal periodic quasi-complementary sequence sets with small alphabet sizes. IEEE Transactions On Information Theory, 67(8), 5168-5177.
<https://dx.doi.org/10.1109/TIT.2021.3068474>

<https://hdl.handle.net/10356/147219>

<https://doi.org/10.1109/TIT.2021.3068474>

© 2021 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at:
<https://doi.org/10.1109/TIT.2021.3068474>.

Downloaded on 26 Apr 2023 17:23:04 SGT

Three new constructions of asymptotically optimal periodic quasi-complementary sequence sets with small alphabet sizes

Gaojun Luo Xiwang Cao Minjia Shi and Tor Helleseth

Abstract—Quasi-complementary sequence sets (QCSSs) play an important role in multi-carrier code-division multiple-access (MC-CDMA) systems. They can support more users than perfect complementary sequence sets in MC-CDMA systems. It is desirable to design QCSSs with good parameters that are a trade-off of large set size, small periodic maximum magnitude correlation and small alphabet size. The main results are to construct new infinite families of QCSSs that all have small alphabet size and asymptotically optimal periodic maximum magnitude correlation. In this paper, we propose three new constructions of QCSSs using additive characters over finite fields. Notably, these QCSSs have new parameters and small alphabet sizes. Using the properties of characters and character sums, we determine their maximum periodic correlation magnitudes and prove that these QCSSs are asymptotically optimal with respect to the lower bound.

Index Terms—Quasi-complementary sequence set (QCSS); asymptotically optimal; periodic correlation; additive character; multi-carrier code-division multiple-access (MC-CDMA).

I. INTRODUCTION

A perfect complementary sequence set (PCSS) is a collection of two-dimensional matrices in which non-trivial auto-correlations and cross-correlations of the row sequences sum to zero for any non-zero time-shift. In multi-carrier code-division multiple-access (MC-CDMA) communications, the system assigns every user a two-dimensional matrix and transfers each data symbol of a user by transmitting all the row sequences over sub-carrier channels simultaneously [1–3].

A disadvantage of PCSS is that its set size can not exceed the number of row sequences of the two-dimensional matrices. Therefore, the application of PCSSs in MC-CDMA communications is constrained if a large number of users need

to be supported. To overcome the defect, two generalizations of PCSS were proposed for supporting more users. The first one is referred to as a low-correlation zone complementary sequence set (LCZ-CSS) consisting of two-dimensional matrices, which possesses low non-trivial correlation magnitudes within a zone around the origin [4, 13, 16]. In particular, a LCZ-CSS reduces to a zero-correlation zone complementary sequence set (ZCZ-CSS) if the correlation magnitude is equal to zero. Liu et al. [10, 11] introduced the second extension of PCSS named a quasi-complementary sequence set (QCSS). A QCSS consists of two-dimensional matrices such that the maximum non-trivial correlation sum is small but nonzero for any non-zero time-shift. Since QCSSs have large set sizes and low interference performance [11, 12], they have been an increasingly important area of research. In “fractional-delay” transmission schemes with the delay of non-integral multiple of half chip duration [14], QCSSs can achieve better performance than PCSSs [21].

A. The correlation bound of periodic QCSSs

A periodic $(M, K, N, \vartheta_{max})$ -QCSS over an alphabet is a set of M two-dimensional K by N matrices over the alphabet, where each row of two-dimensional matrices is a constituent sequence of length N and K, ϑ_{max} denote the flock size and the maximum non-trivial periodic correlation sum respectively.

The maximum possible amount of multipath interference and multiuser interference is measured in terms of the maximum non-trivial periodic correlation sum ϑ_{max} . In practice, for given K and N , it is desirable to construct an $(M, K, N, \vartheta_{max})$ -QCSS with M being as large as possible and ϑ_{max} being as small as possible. However, Liu et al. [10] presented a lower bound for the maximum periodic correlation sum of a periodic $(M, K, N, \vartheta_{max})$ -QCSS as follows:

$$\vartheta_{max} \geq \vartheta_{opt} = KN \sqrt{\frac{M/K - 1}{MN - 1}}. \quad (1)$$

Furthermore, if the maximum magnitude ϑ_{max} of a periodic QCSS achieves the above bound, then it is termed an optimal QCSS. When ϑ_{max} asymptotically meets the above bound for sufficiently large N , the periodic QCSS is said to be asymptotically optimal.

B. Known results

It is noted that optimal periodic QCSSs only exist for very restrictive parameters and it seems that constructing an infinite

G. Luo is with the School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371 (e-mail: gjluo1990@163.com).

X. Cao is with the Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China, and also with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China (e-mail: xwcao@nuaa.edu.cn).

M. Shi is with the School of Mathematical Sciences, Anhui University, Hefei 230601, China. (e-mail: smjwcl.good@163.com)

T. Helleseth is with the Department of Informatics, University of Bergen, Bergen N-5020, Norway (e-mail: tor.helleseth@uib.no)

G. Luo was supported by NTU Research Grant 04INS000047C230GRT01. X. Cao was supported by the National Natural Science Foundation of China (Grant Nos. 11771007 and 61572027). M. Shi is supported by National Natural Science Foundation of China (12071001, 61672036), Excellent Youth Foundation of Natural Science Foundation of Anhui Province (1808085J20) and the Academic Fund for Outstanding Talents in Universities (gxbjZD03). T. Helleseth was supported by the Research Council of Norway (Grant No. 247742/O70 and No. 311646/O70).

family of optimal periodic QCSSs is very difficult. Up to now, the existence of an infinite family of optimal periodic QCSSs remains open. Hence, most researchers have tried to construct asymptotically optimal periodic QCSSs. Liu et al. [10] proposed a framework for establishing periodic QCSSs. With this framework, a family of asymptotically optimal periodic QCSSs was designed by employing Singer difference sets. Along this line, in [6], the authors constructed a family of periodic QCSSs by using almost difference sets instead of Singer difference sets. As a generalization of the work in [10], Li et al. [7] reported a new method for constructing periodic QCSSs. In addition, utilizing difference sets and almost difference sets, two families of asymptotically optimal periodic QCSSs were proposed. In fact, all the aforementioned research on the constructions of periodic QCSSs has been carried out by additive characters and multiplicative characters over a finite field. It is well known that additive characters and multiplicative characters over a finite field are powerful tools to construct a variety of sequences. Sequences and some frameworks with low correlation have been designed by using characters over a finite field [5, 18, 22, 23]. Very recently, Li et al. [8, 9] established several families of asymptotically optimal QCSSs by multiplicative characters and the combination of additive characters and multiplicative characters over finite fields.

Almost all previous constructions of asymptotically optimal periodic QCSSs in the literature make use of multiplicative characters over finite fields, which have suffered from large alphabet sizes. Precisely speaking, the length N , set size M and alphabet size of a QCSS from these constructions are on the same order of magnitude. Owing to the selection of phase sequences, the construction of asymptotically optimal periodic QCSSs from additive characters over finite fields, reported in [7], has the same shortcoming. Consequently, the alphabet sizes of the QCSSs mentioned earlier may limit their real applications if their lengths and set sizes are large.

C. Our contributions and techniques

Considering the drawback of the previous constructions, the main contribution of this paper is to provide three explicit constructions of asymptotically optimal periodic QCSSs with small alphabet sizes. The results and techniques of this paper can be summarized as follows.

1. Since the definition of additive characters over the finite field with characteristic p is based on a primitive p -th root of unity, periodic QCSSs established by additive characters have small alphabet sizes. Utilizing additive characters over the finite field with characteristic p , we give a new general framework of periodic $(p^n, K, p^n - 1, \vartheta_{\max})$ -QCSSs whose alphabet size is p . With this new framework, we provide three new infinite families of periodic QCSSs. It turns out that these periodic QCSSs are asymptotically optimal with respect to the bound defined in (1). Remarkably, the alphabet sizes of our constructions are very small, which is a major advantage of our constructions. As a comparison, we list the parameters of known classes of asymptotically optimal

periodic QCSSs and the new ones in Table I. For instance, to construct a periodic QCSS with length $3^6 - 1$, the alphabet sizes of known periodic QCSSs are at least $3^6 - 1$ while the alphabet sizes of periodic QCSSs from our constructions are 3. In brief, to the best of our knowledge, this is the first research on the constructions of periodic QCSSs which greatly decrease the alphabet sizes.

2. As is shown in Table I, the set sizes of all known QCSSs do not exceed the lengths of constituent sequences. However, for any periodic QCSS provided in this paper, the set size is greater than the length. To support more users in MC-CDMA communications, one would like to design QCSSs with large set size. For different requirements of MC-CDMA systems, one can select appropriate QCSSs.
3. To design an asymptotically optimal periodic QCSS with flock size $K = (p^n - 1)/2$ and length $N = p^n - 1$, there are three constructions of periodic QCSSs, namely periodic $(p^n - 2, (p^n - 1)/2, p^n - 1, \leq (p^n + 4\sqrt{p^n} + 3)/2)$ -QCSSs defined by [8], periodic $(p^n - 1, (p^n - 1)/2, p^n - 1, \leq (p^n + \sqrt{p^n})/2)$ -QCSSs in [9] and periodic $(p^n, (p^n - 1)/2, p^n - 1, (p^n + 1)/2)$ -QCSSs proposed by Theorem III.2. Among these periodic QCSSs, the periodic QCSSs constructed by Theorem III.2 have the largest set sizes, the smallest alphabet sizes and the lowest maximum periodic correlation sums in most cases. Therefore, the periodic QCSSs in [8] and [9] may be replaced by the periodic QCSSs of Theorem III.2.

In summary, in this paper, we present three new constructions of asymptotically optimal periodic QCSSs with new parameters and small alphabet sizes.

The rest of the paper is organized as follows. Section II is devoted to basic definitions and results about the QCSS, characters and character sums over finite fields. In Section III, we propose three constructions of asymptotically optimal QCSSs. Section IV concludes the paper.

II. PRELIMINARIES

In this section, we recall some basic definitions and results which will be needed in our discussion. We start with the definition of the quasi-complementary sequence set.

A. Periodic quasi-complementary sequence set

Assume that $\mathbf{s}_i = (s_i(0), s_i(1), \dots, s_i(N - 1))$ and $\mathbf{s}_j = (s_j(0), s_j(1), \dots, s_j(N - 1))$ are two complex-valued sequences of length N . The (periodic) correlation function between $\mathbf{s}_i$ and $\mathbf{s}_j$ is defined by

$$R_{\mathbf{s}_i, \mathbf{s}_j}(\tau) = \sum_{t=0}^{N-1} s_i(t) s_j^*(t + \tau), \quad 0 \leq \tau < N,$$

where a^* stands for the conjugate of a complex number a and the argument addition is counted modulo N . If $\mathbf{s}_i = \mathbf{s}_j$, we get the auto-correlation $R_{\mathbf{s}_i, \mathbf{s}_i}(\tau)$. Otherwise, $R_{\mathbf{s}_i, \mathbf{s}_j}(\tau)$ is termed cross-correlation.

Table I: The parameters of asymptotically optimal periodic QCSSs

Set size M	Flock size K	Length N	ϑ_{max}	Alphabet Size	Constraint	References
$2^n - 1$	$2^{n-1} - 1$	2^n	$(2^n + 2^{n/2})/2$	$2(2^n - 1)$	$n > 1$	[10]
p	$(p-1)/2$	p	$\leq (p + \sqrt{p})/2$	p	p is a prime	[7]
$p^n - 2$	$(p^n - 1)/2$	$p^n - 1$	$\leq (p^n + 4\sqrt{p^n} + 3)/2$	$p^n - 1$	p is an odd prime	[8]
$p^{2n} - 2$	p^n	$p^{2n} - 1$	$p^n(p^{2n} + 3)$	$p^{2n} - 1$	p is a prime	[8]
$p^n - 1$	$(p^n - 1)/2$	$p^n - 1$	$\leq (p^n + \sqrt{p^n})/2$	$p(p^n - 1)$	p is an odd prime	[9]
$p^n - 1$	p^{n-1}	$p^n - 1$	$\leq p^{n-1/2}$	$p(p^n - 1)$	p is a prime and $n > 1$	[9]
$p^{2n} - 1$	p^n	$p^{2n} - 1$	$p^{3n/2}$	$p(p^{2n} - 1)$	p is a prime	[9]
$2^n - 1$	$2^{n-1} - 1$	$2^n - 1$	2^{n-1}	$2(2^n - 1)$	$n > 1$	[9]
p^n	$(p^n - 1)/2$	$p^n - 1$	$(p^n + 1)/2$	p	p is an odd prime such that $p^n > 3$	Theorem III.2
p^n	$(p^n - p^{n-1})/2$	$p^n - 1$	$(p^n + p^{n-1})/2$	p	p is an odd prime such that $p^n > 3$	Theorem III.3
p^n	u	$p^n - 1$	v	p	p is an odd prime and $n > 1$ is an odd number	Theorem III.4

where $u = \frac{p^n - p^{n-1} + (-1)^{(p-1)(n+3)/4}(p-1)p^{(n-1)/2}}{2}$, $v = \frac{p^n + p^{n-1} - (-1)^{(p-1)(n+3)/4}(p-1)p^{(n-1)/2}}{2}$ and n is a positive integer.

For $0 \leq i < M$, let $\mathcal{C}^i$ be a two-dimensional matrix with size $K \times N$, which is defined by

$$\mathcal{C}^i = \begin{bmatrix} \mathbf{c}_0^i \\ \mathbf{c}_1^i \\ \vdots \\ \mathbf{c}_{K-1}^i \end{bmatrix} = \begin{bmatrix} c_0^i(0) & c_0^i(1) & \cdots & c_0^i(N-1) \\ c_1^i(0) & c_1^i(1) & \cdots & c_1^i(N-1) \\ \vdots & \vdots & \ddots & \vdots \\ c_{K-1}^i(0) & c_{K-1}^i(1) & \cdots & c_{K-1}^i(N-1) \end{bmatrix},$$

where $\mathbf{c}_k^i = (c_k^i(0), c_k^i(1), \dots, c_k^i(N-1))$ is the k -th constituent sequence of length N , $0 \leq k \leq K-1$.

Assume that the set $\mathfrak{C} = \{\mathcal{C}^0, \mathcal{C}^1, \dots, \mathcal{C}^{M-1}\}$. The (periodic) correlation function between two matrices $\mathcal{C}^i$ and $\mathcal{C}^j$ of $\mathfrak{C}$ is defined by

$$R_{\mathcal{C}^i, \mathcal{C}^j}(\tau) = \sum_{k=0}^{K-1} R_{\mathbf{c}_k^i, \mathbf{c}_k^j}(\tau), \quad 0 \leq \tau < N,$$

where $0 \leq i, j < M$. The maximum magnitudes of the periodic cross-correlation ϑ_c and the periodic auto-correlation ϑ_a of the matrices in $\mathfrak{C}$ are respectively given by

$$\vartheta_c = \max\{|R_{\mathcal{C}^i, \mathcal{C}^j}(\tau)| : 0 \leq i \neq j < M, 0 \leq \tau < N\},$$

$$\vartheta_a = \max\{|R_{\mathcal{C}^i, \mathcal{C}^i}(\tau)| : 0 \leq i < M, 0 < \tau < N\}.$$

Furthermore, the maximum periodic correlation magnitude (also called periodic tolerance) of $\mathfrak{C}$ is defined as $\vartheta_{max} = \max\{\vartheta_c, \vartheta_a\}$. Accordingly, $\mathfrak{C}$ is called a periodic $(M, K, N, \vartheta_{max})$ quasi-complementary sequence set (QCSS) if $\vartheta_{max} > 0$. Otherwise, $\mathfrak{C}$ is termed a periodic perfect complementary sequence set (PCSS). Particularly, a PCSS reduces to a matrix consisting of two row sequences if $M = 1$ and $K = 2$. Such a matrix is called a Golay complementary pair.

Notice that the transmission of a PCSS or a QCSS needs a multi-channel system. Therefore each matrix in a PCSS or a QCSS requires $K (\geq 2)$ non-interfering channels for the separate transmission of K row sequences.

B. Characters over finite fields

Let p be a prime and n a positive integer. Denote by $\mathbb{F}_q$ a finite field with q elements, where $q = p^n$. The trace function

from $\mathbb{F}_q$ to $\mathbb{F}_p$ is defined as

$$\text{Tr}_{q/p}(a) = a + a^p + \cdots + a^{p^{n-1}},$$

where $a \in \mathbb{F}_q$.

Let $\mathbb{F}_q^*$ denote the multiplicative group of $\mathbb{F}_q$. It is well-known that $\mathbb{F}_q^*$ is a cyclic group of order $q-1$. A generator of $\mathbb{F}_q^*$ is said to be a primitive element of the finite field $\mathbb{F}_q$. Assume that α is a primitive element of $\mathbb{F}_q$. For each integer i with $0 \leq i \leq q-2$, a multiplicative character φ_i of $\mathbb{F}_q$ is defined by

$$\varphi_i(\alpha^j) = \xi_{q-1}^{ij},$$

where $0 \leq j \leq q-2$ and $\xi_{q-1} = e^{2\pi\sqrt{-1}/(q-1)}$. Each multiplicative character of $\mathbb{F}_q$ can be obtained in this way. If $i = 0$, the multiplicative character φ_0 is called the trivial multiplicative character of $\mathbb{F}_q$. For any multiplicative character φ_i of $\mathbb{F}_q$, its conjugate φ_i^* is given by $\varphi_i^*(g) = \varphi_i(g^{-1})$, where $g \in \mathbb{F}_q^*$. All the multiplicative characters of $\mathbb{F}_q$ form a cyclic group $\widehat{\mathbb{F}_q^*}$ under the multiplication of characters defined as:

$$\chi\psi(g) = \chi(g)\psi(g),$$

for any $g \in \mathbb{F}_q^*$, where χ, ψ are multiplicative characters of $\mathbb{F}_q$. The group $\widehat{\mathbb{F}_q^*}$ is isomorphic to the multiplicative group $\mathbb{F}_q^*$. The orthogonal relations of $\mathbb{F}_q^*$ and $\widehat{\mathbb{F}_q^*}$ are

$$\sum_{g \in \mathbb{F}_q^*} \varphi(g) = \begin{cases} 0, & \text{if } \varphi \text{ is a nontrivial multiplicative character of } \mathbb{F}_q \\ q-1, & \text{if } \varphi \text{ is the trivial multiplicative character of } \mathbb{F}_q, \end{cases}$$

and

$$\sum_{\varphi \in \widehat{\mathbb{F}_q^*}} \varphi(g) = \begin{cases} 0, & \text{if } g \neq 1 \in \mathbb{F}_q^*, \\ q-1, & \text{if } g = 1. \end{cases}$$

We extend the definition of φ by putting $\varphi(0) = 1$ if φ is trivial and $\varphi(0) = 0$ if φ is nontrivial.

For each $a \in \mathbb{F}_q$, an additive character of $\mathbb{F}_q$ is given by the function

$$\chi_a(x) = \xi_p^{\text{Tr}_{q/p}(ax)},$$

where $\xi_p = e^{2\pi\sqrt{-1}/p}$. If $a = 1$, we term $\chi_1(x)$ the canonical additive character of $\mathbb{F}_q$. Let $\chi_0(x)$ denote the trivial additive character of $\mathbb{F}_q$. The additive character of $\mathbb{F}_q$ has similar properties as the multiplicative character of $\mathbb{F}_q$.

C. Character sums over finite fields

Assume that χ_a is an additive character and φ is a multiplicative character over $\mathbb{F}_q$. Then the Gauss sum over $\mathbb{F}_q$ is defined as

$$G(\varphi, \chi_a) = \sum_{x \in \mathbb{F}_q^*} \varphi(x) \chi_a(x).$$

Gauss sums have wide applications in coding theory, sequence design and cryptography. It is clear that the absolute value of the Gauss sum $G(\varphi, \chi)$ is at most $q-1$, but is in general much smaller, as the following lemma shows.

Lemma II.1. [17, Theorem 5.11] *Let the symbols be the same as above. Then the Gauss sum $G(\varphi, \chi_a)$ over $\mathbb{F}_q$ satisfies*

$$G(\varphi, \chi_a) = \begin{cases} q-1, & \text{if } \varphi = \varphi_0, \chi = \chi_0, \\ -1, & \text{if } \varphi = \varphi_0, \chi \neq \chi_0, \\ 0, & \text{if } \varphi \neq \varphi_0, \chi = \chi_0. \end{cases}$$

Additionally, if $\varphi \neq \varphi_0$ and $a \neq 0$, we have $|G(\varphi, \chi_a)| = \sqrt{q}$.

Under the transformations of additive characters and multiplicative characters, we have the following equation on Gauss sums.

Lemma II.2. [17, Theorem 5.12 and Equation (5.16)] *Let $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$. Then*

- 1) $G(\varphi, \chi_{ab}) = \varphi^*(a)G(\varphi, \chi_b)$,
- 2) $\varphi(a) = \frac{1}{q} \sum_{x \in \mathbb{F}_q} G(\varphi, \chi_x) \chi_x(a)$.

In general, we can only determine the value of Gauss sums for some special characters of finite fields. Assume that $\eta = \varphi_{\frac{q-1}{2}}$ is the quadratic multiplicative character of $\mathbb{F}_q$. The following lemma provides the explicit value of the quadratic Gauss sum $G(\eta, \chi_1)$ over $\mathbb{F}_q$.

Lemma II.3. [17, Theorem 5.15] *Let $q = p^n$, where p is an odd prime and n is a positive integer. Assume that χ_1 is the canonical additive character and $\eta = \varphi_{\frac{q-1}{2}}$ is the quadratic multiplicative character of $\mathbb{F}_q$. Then*

$$G(\eta, \chi_1) = (-1)^{n-1} \sqrt{-1}^{\left(\frac{p-1}{2}\right)^2 n} \sqrt{q}.$$

In the sequel, the following two lemmas will be needed.

Lemma II.4. [19] *Let p be an odd prime and $q = p^n$. Suppose that η and $\bar{\eta}$ are the quadratic multiplicative character of $\mathbb{F}_q$ and $\mathbb{F}_p$, respectively. If n is even, then $\eta(a) = 1$ for any $a \in \mathbb{F}_q^*$. If n is odd, then $\eta(a) = \bar{\eta}(a)$ for any $a \in \mathbb{F}_q^*$.*

Lemma II.5. [17, Theorem 5.33] *Assume that $q = p^n$, where p is an odd prime and n is a positive integer. Let χ_1 be the canonical additive character of $\mathbb{F}_q$ and $f(x) = a_2 x^2 + a_1 x + a_0 \in \mathbb{F}_q[x]$ with $a_2 \neq 0$. Then, we have*

$$\sum_{b \in \mathbb{F}_q} \chi_1(f(b)) = \chi_1(a_0 - a_1^2(4a_2)^{-1}) \eta(a_2) G(\eta, \chi_1).$$

III. MAIN RESULTS

In this section, we give a general construction of QCSSs from additive characters over finite fields. The QCSS generated by this general construction possesses small alphabet size and its set size is greater than the length of the constituent

sequences. Furthermore, we present three constructions of QCSSs and show that these are asymptotically optimal with respect to the bound of (1).

A. A general framework of periodic QCSSs from [9]

In [9], the authors proposed a general framework of periodic QCSSs from additive characters and multiplicative characters over finite fields associated with integer sets.

Let q be a prime power and $D = \{d_0, d_1, \dots, d_{K-1}\}$ be an integer set with cardinality K , where $K \leq q-1$. Suppose that α is a primitive element of $\mathbb{F}_q$. For any $0 \leq j \leq q-2$, assume that χ_1 is the canonical additive character and φ_j is a multiplicative character of $\mathbb{F}_q$. Then, define a complementary sequence set as

$$\mathcal{F} = \{\mathcal{F}^0, \mathcal{F}^1, \dots, \mathcal{F}^{q-2}\}, \quad (2)$$

where every complementary sequence $\mathcal{F}^i = \{\mathbf{f}_0^i, \mathbf{f}_1^i, \dots, \mathbf{f}_{K-1}^i\}$ is in the form of a $K \times (q-1)$ matrix. Herein,

$$\mathbf{f}_l^i = \{\varphi_{i+d_l}(\alpha^t) \chi_1(\alpha^t)\}_{t=0}^{q-2},$$

for any $0 \leq i \leq q-2$ and $0 \leq l \leq K-1$.

For any periodic QCSS deduced by (2), its set size and length of constituent sequences are equal to $q-1$. The flock size and periodic tolerance are determined by D . Precisely speaking, the flock size is equal to the cardinality of D and the periodic tolerance is

$$\sqrt{q} \max_{1 \leq \tau \leq q-2} \left| \sum_{l=0}^{K-1} \varphi_{d_l}(\alpha^{-\tau}) \right|.$$

Because of the property of multiplicative characters, the evaluation of the periodic tolerance can be converted into the calculation of $\left| \sum_{l=0}^{K-1} \varphi_{d_l}(\alpha^{-\tau}) \right|$. By designing different integer sets D , Li et al. [9] constructed four infinite families of asymptotically optimal periodic QCSSs. It is observed that the periodic QCSS constructed by (2) has large alphabet size and its set size can not exceed the length of its constituent sequences. Clearly, these drawbacks are caused by the utilization of multiplicative characters over $\mathbb{F}_q$. Hence, it is natural to consider a construction of periodic QCSSs by additive characters over finite fields.

B. A new general construction of periodic QCSSs with small alphabet sizes

Let p be a prime and n a positive integer. Write $q = p^n$. Label the elements of the finite field

$$\mathbb{F}_q = \{a_0, a_1, \dots, a_{q-1}\}.$$

Suppose that χ_b is an additive character of $\mathbb{F}_q$, where $b \in \mathbb{F}_q$. Assume that $E = \{e_0, e_1, \dots, e_{K-1}\}$ is a subset of $\mathbb{F}_q$, where K is the cardinality of the set E . For each $0 \leq i \leq q-1$ and $0 \leq l \leq K-1$, define a constituent sequence c_l^i of length $q-1$ by

$$\mathbf{c}_l^i = \{\chi_{a_i+e_l}(\alpha^t)\}_{t=0}^{q-2},$$

where α is a primitive element of $\mathbb{F}_q$. Then we obtain a complementary sequence $\mathcal{C}^i = \{\mathbf{c}_0^i, \mathbf{c}_1^i, \dots, \mathbf{c}_{K-1}^i\}$ in the form of a $K \times (q-1)$ matrix. Moreover, the set

$$\mathfrak{C} = \{\mathcal{C}^0, \mathcal{C}^1, \dots, \mathcal{C}^{q-1}\} \quad (3)$$

is a complementary sequence set.

Theorem III.1. *Let the symbols be the same as above. Then $\mathfrak{C}$ constructed by (3) is a periodic QCSS with parameters $(q, K, q-1, \vartheta_{max})$, where $\vartheta_{max} = \max\{K, q-K\}$. Furthermore, the alphabet size of $\mathfrak{C}$ is p .*

Proof: First, we determine the value of ϑ_{max} . Define a characteristic function from $\mathbb{F}_q$ to $\{0, 1\}$ as

$$I(x) = \begin{cases} 1, & \text{if } x \in E, \\ 0, & \text{if } x \notin E. \end{cases}$$

Let $\mathcal{C}^i, \mathcal{C}^j$ be any two complementary sequences of $\mathfrak{C}$ and τ be an integer with $0 \leq \tau \leq q-2$. Label the elements of $E = \{e_0, e_1, \dots, e_{K-1}\}$. Then we have

$$\begin{aligned} & R_{\mathcal{C}^i, \mathcal{C}^j}(\tau) \\ &= \sum_{l=0}^{K-1} R_{\mathbf{c}_l^i, \mathbf{c}_l^j}(\tau) \\ &= \sum_{l=0}^{K-1} \sum_{t=0}^{q-2} \chi_{a_i+e_l}(\alpha^t) \chi_{a_j+e_l}^*(\alpha^{t+\tau}) \\ &= \sum_{l=0}^{K-1} \sum_{t=0}^{q-2} \chi_1((a_i+e_l)\alpha^t) \chi_1(-(a_j+e_l)\alpha^{t+\tau}) \\ &= \sum_{t=0}^{q-2} \chi_1((a_i-a_j\alpha^\tau)\alpha^t) \sum_{l=0}^{K-1} \chi_1(e_l(1-\alpha^\tau)\alpha^t). \quad (4) \end{aligned}$$

Case 1): If $\tau = 0$ and $i \neq j$, it follows from (4) and the orthogonal relations of additive characters that

$$R_{\mathcal{C}^i, \mathcal{C}^j}(\tau) = \sum_{t=0}^{q-2} \chi_1((a_i-a_j)\alpha^t) \sum_{l=0}^{K-1} 1 = -K.$$

Case 2): If $\tau \neq 0$, according to (4) and letting $h = \frac{a_i-a_j\alpha^\tau}{1-\alpha^\tau}$, we obtain

$$\begin{aligned} & R_{\mathcal{C}^i, \mathcal{C}^j}(\tau) \\ &= \sum_{t=0}^{q-2} \chi_1((a_i-a_j\alpha^\tau)\alpha^t) \sum_{x \in \mathbb{F}_q} I(x) \chi_1((1-\alpha^\tau)\alpha^t x) \\ &= \sum_{y \in \mathbb{F}_q^*} \chi_1(hy) \sum_{x \in \mathbb{F}_q} I(x) \chi_1(yx) \\ &= \sum_{x \in \mathbb{F}_q} I(x) \sum_{y \in \mathbb{F}_q^*} \chi_1((h+x)y) \\ &= I(-h)(q-1) - \sum_{x \in \mathbb{F}_q \setminus \{-h\}} I(x) \\ &= - \sum_{x \in \mathbb{F}_q} I(x) + qI(-h) \\ &= -K + qI(-h). \end{aligned}$$

Since $a_i - a_j\alpha^\tau$ runs through the finite field $\mathbb{F}_q$, we derive that $R_{\mathcal{C}^i, \mathcal{C}^j}(\tau) \in \{-K, q-K\}$ for any $\tau \neq 0$. To summarize

Case 1) and Case 2), the periodic tolerance of $\mathfrak{C}$ is $\vartheta_{max} = \max\{K, q-K\}$. Therefore, it is easy to verify that the QCSS designed by (3) has parameters $(q, K, q-1, \max\{K, q-K\})$ and the alphabet size is p . $\square$

Remark 1. *For a fixed length of constituent sequences, the alphabet size of a periodic QCSS generated by (3) is much smaller than that of [9] and the set size is greater than that of [9].*

From Theorem III.1, it is obvious that the flock size and periodic tolerance of a periodic QCSS constructed by (3) are determined by the set E . Thus, the problem how to construct a QCSS with low periodic tolerance can be translated to the design of the set E .

C. Three constructions of asymptotically optimal periodic QCSSs

In this subsection, by selecting three suitable sets E , we present three constructions of QCSSs and show their asymptotical optimality.

Theorem III.2. *Assume that p is an odd prime and n is a positive integer with $p^n > 3$. Let $q = p^n$ and $E = \{x \in \mathbb{F}_q^* : \eta(x) = 1\}$, where η is the quadratic multiplicative character of $\mathbb{F}_q$. Then $\mathfrak{C}$ defined by (3) is a periodic $(q, \frac{q-1}{2}, q-1, \frac{q+1}{2})$ -QCSS. In addition, $\mathfrak{C}$ is asymptotically optimal with respect to the lower bound in (1).*

Proof: It follows from the definition of the set E and Theorem III.1 that $\mathfrak{C}$ is a periodic $(q, \frac{q-1}{2}, q-1, \frac{q+1}{2})$ -QCSS. The corresponding lower bound defined in (1) for $\mathfrak{C}$ is

$$\vartheta_{opt} = \frac{(q-1)^2}{2} \sqrt{\frac{q+1}{q(q-1)^2 - q + 1}}.$$

Then, we have

$$\frac{\vartheta_{max}}{\vartheta_{opt}} = \sqrt{\frac{q(q-1)^2(q+1) - q^2 + 1}{(q-1)^4}},$$

which implies that $\lim_{q \rightarrow +\infty} \frac{\vartheta_{max}}{\vartheta_{opt}} = 1$. The proof is completed. $\square$

In what follows, we exemplify Theorem III.2 by a specific example.

Example 1. *Let $p = 3$, $n = 2$ and α be a primitive element of $\mathbb{F}_9$. Put $E = \{1, 2, \alpha^2, \alpha^6\}$. Then $\mathfrak{C}$ defined by Theorem III.2 is a periodic $(9, 4, 8, 5)$ -QCSS and made up of the following complementary sequences, where every element stands for a power of $\xi_3 = e^{2\pi\sqrt{-1}/3}$.*

$$\begin{aligned} \mathcal{C}^0 &= \begin{bmatrix} 2 & 1 & 0 & 1 & 1 & 2 & 0 & 2 \\ 0 & 1 & 1 & 2 & 0 & 2 & 2 & 1 \\ 1 & 2 & 0 & 2 & 2 & 1 & 0 & 1 \\ 0 & 2 & 2 & 1 & 0 & 1 & 1 & 2 \end{bmatrix}, \\ \mathcal{C}^1 &= \begin{bmatrix} 1 & 2 & 0 & 2 & 2 & 1 & 0 & 1 \\ 2 & 2 & 1 & 0 & 1 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 2 & 2 & 1 & 0 & 1 & 1 \end{bmatrix}, \end{aligned}$$

$$\begin{aligned} \mathcal{C}^2 &= \begin{bmatrix} 0 & 1 & 1 & 2 & 0 & 2 & 2 & 1 \\ 1 & 1 & 2 & 0 & 2 & 2 & 1 & 0 \\ 2 & 2 & 1 & 0 & 1 & 1 & 2 & 0 \\ 1 & 2 & 0 & 2 & 2 & 1 & 0 & 1 \end{bmatrix}, \\ \mathcal{C}^3 &= \begin{bmatrix} 2 & 2 & 1 & 0 & 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & 1 & 0 & 1 & 1 & 2 \\ 1 & 0 & 1 & 1 & 2 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \\ \mathcal{C}^4 &= \begin{bmatrix} 0 & 2 & 2 & 1 & 0 & 1 & 1 & 2 \\ 1 & 2 & 0 & 2 & 2 & 1 & 0 & 1 \\ 2 & 0 & 2 & 2 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 2 & 0 & 2 & 2 \end{bmatrix}, \\ \mathcal{C}^5 &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 2 & 0 & 2 & 2 \\ 2 & 1 & 0 & 1 & 1 & 2 & 0 & 2 \\ 1 & 1 & 2 & 0 & 2 & 2 & 1 & 0 \end{bmatrix}, \\ \mathcal{C}^6 &= \begin{bmatrix} 1 & 1 & 2 & 0 & 2 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 & 1 & 2 & 0 & 2 \\ 0 & 2 & 2 & 1 & 0 & 1 & 1 & 2 \\ 2 & 2 & 1 & 0 & 1 & 1 & 2 & 0 \end{bmatrix}, \\ \mathcal{C}^7 &= \begin{bmatrix} 2 & 0 & 2 & 2 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 2 & 0 & 2 & 2 & 1 & 0 \\ 0 & 1 & 1 & 2 & 0 & 2 & 2 & 1 \end{bmatrix}, \\ \mathcal{C}^8 &= \begin{bmatrix} 1 & 0 & 1 & 1 & 2 & 0 & 2 & 2 \\ 2 & 0 & 2 & 2 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 & 0 & 2 & 2 & 1 \\ 2 & 1 & 0 & 1 & 1 & 2 & 0 & 2 \end{bmatrix}. \end{aligned}$$

Using the Magma System, it can be easily seen that the periodic correlation function $R_{\mathcal{C}^i, \mathcal{C}^j}(\tau)$ is equal to -4 or 5 for any $0 \leq i = j \leq 8$, $0 < \tau \leq 7$ or $0 \leq i \neq j \leq 8$, $0 \leq \tau \leq 7$. Consequently, the periodic tolerance is $\vartheta_{\max} = 5$, which verifies the result in Theorem III.2.

In order to describe the asymptotical optimality of the QCSS $\mathcal{C}$ constructed in Theorem III.2 by numerical results, some explicit values of the parameters of $\mathcal{C}$ for some given q with $3 < q \leq 60$ and the corresponding numerical data of the lower bound defined by (1) have been carried out in Table II. The numerical results indicate that the QCSS $\mathcal{C}$ is indeed asymptotically optimal.

A subset D of size k in an abelian group $(G, +)$ with order n is said to be an (n, k, λ) difference set in $(G, +)$ if every nonidentity element of G can be expressed as $d_1 - d_2$ for exactly λ pairs $(d_1, d_2) \in D \times D$. It follows from [20] that the set E defined by Theorem III.2 is a difference set in $(\mathbb{F}_q, +)$ if $q \equiv 3 \pmod{4}$. Hence, for a subset of $\mathbb{F}_q$ which is not a difference set, an asymptotically optimal periodic QCSS can be generated by Theorem III.1 as well. In the sequel, we propose two more constructions of asymptotically optimal periodic QCSSs from the subsets which are not difference sets.

Theorem III.3. Let p be an odd prime and n a positive integer such that $p^n > 3$. Suppose that $\bar{\eta}$ is the quadratic multiplicative character of $\mathbb{F}_p$ and $E = \{x \in \mathbb{F}_{p^n} :$

Table II: Parameters of the $(q, \frac{q-1}{2}, q-1, \frac{q+1}{2})$ -QCSS of Theorem III.2

q	M	K	N	$\vartheta_{\max}$	ϑ_{opt}	$\frac{\vartheta_{\max}}{\vartheta_{\text{opt}}}$
5	5	2	4	3.00000	2.24781	1.33463
7	7	3	6	4.00000	3.24601	1.23228
9	9	4	8	5.00000	4.24596	1.17759
11	11	5	10	6.00000	5.24623	1.14368
13	13	6	12	7.00000	6.24654	1.12062
17	17	8	16	9.00000	8.24710	1.09129
19	19	9	18	10.0000	9.24733	1.08139
23	23	11	22	12.0000	11.2477	1.06688
25	25	12	24	13.0000	12.2479	1.06141
27	27	13	26	14.0000	13.2480	1.05676
29	29	14	28	15.0000	14.2481	1.05277
31	31	15	30	16.0000	15.2482	1.04930
37	37	18	36	19.0000	18.2485	1.04118
41	41	20	40	21.0000	20.2486	1.03711
43	43	21	42	22.0000	21.2487	1.03536
47	47	23	46	24.0000	23.2488	1.03231
49	49	24	48	25.0000	24.2488	1.03098
53	53	26	52	27.0000	26.2489	1.02861
59	59	29	58	30.0000	29.2490	1.02568

$\bar{\eta}(\text{Tr}_{p^n/p}(x)) = 1\}$. Then $\mathcal{C}$ constructed by (3) is a periodic $(p^n, \frac{p^n - p^{n-1}}{2}, p^n - 1, \frac{p^n + p^{n-1}}{2})$ -QCSS and its periodic tolerance asymptotically meets the lower bound in (1).

Proof: It is easy to verify that the cardinality of the set E is $\frac{p^n - p^{n-1}}{2}$. By Theorem III.1, $\mathcal{C}$ is a QCSS with parameters $(p^n, \frac{p^n - p^{n-1}}{2}, p^n - 1, \frac{p^n + p^{n-1}}{2})$. Finally, we have to show its asymptotical optimality according to the bound of (1). The corresponding lower bound of (1) for the periodic tolerance of $\mathcal{C}$ is

$$\vartheta_{\text{opt}} = \frac{p^n - 1}{2} \sqrt{\frac{p^{2n} - p^{2n-2}}{p^{2n} - p^n - 1}}.$$

Thus,

$$\lim_{p \rightarrow +\infty} \frac{\vartheta_{\max}}{\vartheta_{\text{opt}}} = \lim_{p \rightarrow +\infty} \frac{p^n + p^{n-1}}{p^n - 1} \sqrt{\frac{p^{2n} - p^n - 1}{p^{2n} - p^{2n-2}}} = 1.$$

It is now obvious that the theorem holds. $\square$

In the following, an example is presented to illustrate the periodic QCSS in Theorem III.3

Example 2. Let $p = 3$ and $n = 2$. Then $E = \{2, \alpha, \alpha^3\}$, where α is a primitive element of $\mathbb{F}_9$. One can obtain a periodic QCSS $\mathcal{C}$ with parameters $(9, 3, 8, 6)$ by Theorem III.3. Moreover, all the elements of $\mathcal{C}$ are listed as follows, where every element stands for a power of $\xi_3 = e^{2\pi\sqrt{-1}/3}$.

$$\begin{aligned} \mathcal{C}^0 &= \begin{bmatrix} 1 & 0 & 1 & 1 & 2 & 0 & 2 & 2 \\ 1 & 1 & 2 & 0 & 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 2 & 2 & 1 & 0 & 1 \end{bmatrix}, \\ \mathcal{C}^1 &= \begin{bmatrix} 0 & 1 & 1 & 2 & 0 & 2 & 2 & 1 \\ 0 & 2 & 2 & 1 & 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \\ \mathcal{C}^2 &= \begin{bmatrix} 2 & 0 & 2 & 2 & 1 & 0 & 1 & 1 \\ 2 & 1 & 0 & 1 & 1 & 2 & 0 & 2 \\ 2 & 2 & 1 & 0 & 1 & 1 & 2 & 0 \end{bmatrix}, \\ \mathcal{C}^3 &= \begin{bmatrix} 1 & 1 & 2 & 0 & 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 2 & 2 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 2 & 0 & 2 & 2 \end{bmatrix}, \end{aligned}$$

$$\begin{aligned} \mathcal{C}^4 &= \begin{bmatrix} 2 & 1 & 0 & 1 & 1 & 2 & 0 & 2 \\ 2 & 2 & 1 & 0 & 1 & 1 & 2 & 0 \\ 2 & 0 & 2 & 2 & 1 & 0 & 1 & 1 \end{bmatrix}, \\ \mathcal{C}^5 &= \begin{bmatrix} 2 & 2 & 1 & 0 & 1 & 1 & 2 & 0 \\ 2 & 0 & 2 & 2 & 1 & 0 & 1 & 1 \\ 2 & 1 & 0 & 1 & 1 & 2 & 0 & 2 \end{bmatrix}, \\ \mathcal{C}^6 &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 2 & 0 & 2 & 2 & 1 \\ 0 & 2 & 2 & 1 & 0 & 1 & 1 & 2 \end{bmatrix}, \\ \mathcal{C}^7 &= \begin{bmatrix} 1 & 2 & 0 & 2 & 2 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 2 & 0 & 2 & 2 \\ 1 & 1 & 2 & 0 & 2 & 2 & 1 & 0 \end{bmatrix}, \\ \mathcal{C}^8 &= \begin{bmatrix} 0 & 2 & 2 & 1 & 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 2 & 0 & 2 & 2 & 1 \end{bmatrix}. \end{aligned}$$

By employing the Magma System, the periodic correlation function $R_{\mathcal{C}^i, \mathcal{C}^j}(\tau)$ is equal to -3 or 6 for any $0 \leq i = j \leq 8$, $0 < \tau \leq 7$ or $0 \leq i \neq j \leq 8$, $0 \leq \tau \leq 7$. Therefore, we obtain that the periodic tolerance $\vartheta_{max} = 6$, which verifies the result in Theorem III.3.

Theorem III.3 has proved that the QCSS $\mathfrak{C}$ defined by Theorem III.3 is asymptotically optimal. In Table III, we list some explicit values of the parameters of $\mathfrak{C}$ for $n = 2$ and some given p with $3 \leq p \leq 60$ and the corresponding numerical data of the lower bound given by (1) for comparison. Predictably, the numerical results show that the periodic tolerance of QCSS $\mathfrak{C}$ asymptotically meets the lower bound.

Table III: Parameters of the $(p^2, \frac{p^2-p}{2}, p^2-1, \frac{p^2+p}{2})$ -QCSS of Theorem III.3

p	M	K	N	ϑ_{max}	ϑ_{opt}	$\frac{\vartheta_{max}}{\vartheta_{opt}}$
3	9	3	8	6.00000	4.02807	1.48955
5	25	10	24	15.0000	12.0100	1.24896
7	49	21	48	28.0000	24.0051	1.16642
11	121	55	120	66.0000	60.0021	1.09996
13	169	78	168	91.0000	84.0015	1.08331
17	289	136	288	153.000	144.001	1.06249
19	361	171	360	190.000	180.001	1.05555
23	529	253	528	276.000	264.000	1.04545
29	841	406	840	435.000	420.000	1.03571
31	961	465	960	496.000	480.000	1.03333
37	1369	666	1368	703.000	684.000	1.02778
41	1681	820	1680	861.000	840.000	1.02500
43	1849	903	1848	946.000	924.000	1.02381
47	2209	1081	2208	1128.00	1104.00	1.02174
53	2809	1378	2808	1431.00	1404.00	1.01923
59	3481	1711	3480	1770.00	1740.00	1.01724

In the end, we present the third construction of asymptotically optimal periodic QCSSs.

Theorem III.4. Suppose that p is an odd prime and $n > 1$ is an odd number. Put $E = \{x \in \mathbb{F}_{p^n} : \bar{\eta}(\text{Tr}_{p^n/p}(x^2)) = 1\}$, where $\bar{\eta}$ is the quadratic multiplicative character of $\mathbb{F}_p$. Then $\mathfrak{C}$ defined by (3) is a periodic $(p^n, \frac{p^n - p^{n-1} + (-1)^{(p-1)(n+3)/4}(p-1)p^{(n-1)/2}}{2}, p^n - 1, \vartheta_{max})$ -QCSS, where

$$\vartheta_{max} = \frac{p^n + p^{n-1} - (-1)^{(p-1)(n+3)/4}(p-1)p^{(n-1)/2}}{2}.$$

Furthermore, $\mathfrak{C}$ is asymptotically optimal with respect to the lower bound in (1).

Proof: Our first goal is to evaluate the cardinality of E . Assume that $q = p^n$ and λ_b is an additive character of $\mathbb{F}_p$, where $b \in \mathbb{F}_p$. By the definition of E , Lemmas II.2, II.4 and II.5, we have

$$\begin{aligned} \#E &= \sum_{x \in \mathbb{F}_q, \text{Tr}_{q/p}(x^2) \neq 0} \frac{1 + \bar{\eta}(\text{Tr}_{q/p}(x^2))}{2} \\ &= \frac{1}{2} \sum_{x \in \mathbb{F}_q, \text{Tr}_{q/p}(x^2) \neq 0} 1 + \frac{1}{2} \sum_{x \in \mathbb{F}_q} \bar{\eta}(\text{Tr}_{q/p}(x^2)) \\ &= \frac{1}{2} \left(q - \sum_{x \in \mathbb{F}_q, \text{Tr}_{q/p}(x^2) = 0} 1 \right) \\ &\quad + \frac{1}{2p} \sum_{x \in \mathbb{F}_q} \sum_{b \in \mathbb{F}_p} G(\bar{\eta}, \lambda_b^*) \lambda_b(\text{Tr}_{q/p}(x^2)) \\ &= \frac{q}{2} - \frac{1}{2p} \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_p} \lambda_1(y \text{Tr}_{q/p}(x^2)) \\ &\quad + \frac{1}{2p} \sum_{b \in \mathbb{F}_p} G(\bar{\eta}, \lambda_b^*) \sum_{x \in \mathbb{F}_q} \chi_1(bx^2) \\ &= \frac{q}{2} - \frac{1}{2p} \left(q + \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_q} \chi_1(yx^2) \right) \\ &\quad + \frac{1}{2p} \sum_{b \in \mathbb{F}_p^*} G(\bar{\eta}, \lambda_b^*) \sum_{x \in \mathbb{F}_q} \chi_1(bx^2) \\ &= \frac{q}{2} - \frac{q}{2p} - \frac{1}{2p} \sum_{y \in \mathbb{F}_p^*} \eta(y) G(\eta, \chi_1) \\ &\quad + \frac{1}{2p} G(\bar{\eta}, \lambda_1) \sum_{b \in \mathbb{F}_p^*} \bar{\eta}(-b) \eta(b) G(\eta, \chi_1) \\ &= \frac{q}{2} - \frac{q}{2p} + \frac{1}{2p} G(\bar{\eta}, \lambda_1) G(\eta, \chi_1) \sum_{b \in \mathbb{F}_p^*} \bar{\eta}(-b) \bar{\eta}(b) \\ &= \frac{p^n - p^{n-1} + (-1)^{(p-1)(n+3)/4}(p-1)p^{(n-1)/2}}{2}, \end{aligned}$$

where the last equality follows from Lemma II.3. Thus, the flock size of $\mathfrak{C}$ is

$$K = \frac{p^n - p^{n-1} + (-1)^{(p-1)(n+3)/4}(p-1)p^{(n-1)/2}}{2}.$$

According to Theorem III.1, $\mathfrak{C}$ is a QCSS with parameters $(p^n, K, p^n - 1, \vartheta_{max})$, where

$$K = \frac{p^n - p^{n-1} + (-1)^{(p-1)(n+3)/4}(p-1)p^{(n-1)/2}}{2},$$

and

$$\vartheta_{max} = \frac{p^n + p^{n-1} - (-1)^{(p-1)(n+3)/4}(p-1)p^{(n-1)/2}}{2}.$$

It remains to show that $\mathfrak{C}$ is asymptotically optimal with respect to the lower bound in (1). Observe that the corresponding lower bound is

$$\vartheta_{opt} = K \sqrt{\frac{(p^n - 1)^2(p^n + p^{n-1} - s)}{(p^{2n} - p^n - 1)(p^n - p^{n-1} + s)}},$$

For some given prime $2 < p < 50$ and $n = 3$, Table IV provides some explicit values of the parameters of the QCSSs defined by Theorem III.4 and the corresponding numerical data of the lower bound bound in (1) for comparison. It is indicated that the QCSSs defined by Theorem III.4 are asymptotically optimal.

Table IV: Parameters of the $(p^3, \frac{p^3 - p^2 + (-1)^{(p-1)/2} p(p-1)}{2}, p^3 - 1, \frac{p^3 + p^2 + p(p-1)}{2})$ -QCSS of Theorem III.4

p	M	K	N	ϑ_{max}	ϑ_{opt}	$\frac{\vartheta_{max}}{\vartheta_{opt}}$
3	27	6	26	21.0000	11.0230	1.90511
5	125	60	124	85.0000	62.2017	1.36652
7	343	126	342	217.000	165.114	1.31425
11	1331	550	1330	781.000	655.154	1.19209
13	2197	1092	2196	1261.00	1098.23	1.14821
17	4913	2448	4912	2737.00	2456.23	1.11431
19	6859	3078	6858	3781.00	3411.19	1.10841
23	12167	5566	12166	6601.00	6061.20	1.08906
29	24389	12180	24388	13021.0	12194.2	1.06780
31	29791	13950	29790	15841.0	14865.2	1.06564
37	50653	25308	50652	26677.0	25326.2	1.05334
41	68921	34440	68920	36121.0	34460.2	1.04819
43	79507	37926	79506	41581.0	39711.2	1.04708
47	103823	49726	103822	54097.0	51865.2	1.04303

Remark 2. From Theorems III.2, III.3 and III.4, we see that the cardinalities of the employed sets E are $\frac{q-o(q)}{2}$, where $o(q) > 0$ and $\lim_{q \rightarrow +\infty} \frac{o(q)}{q} = 0$. Along this line, if one chooses any subset of $\mathbb{F}_q$ with the cardinality $\frac{q-o(q)}{2}$ or $\frac{q+o(q)}{2}$, then an infinite family of asymptotically optimal periodic QCSSs with parameters $(q, \frac{q-o(q)}{2}, q-1, \frac{q-o(q)}{2})$ or $(q, \frac{q+o(q)}{2}, q-1, \frac{q+o(q)}{2})$ is proposed by Theorem III.1. Consequently, Theorem III.1 can produce many infinite families of asymptotically optimal periodic QCSSs with flexible parameters.

IV. CONCLUDING REMARKS

In this paper, we proposed a general construction of periodic QCSSs by additive characters over finite fields. The periodic QCSSs produced by this general construction have small alphabet sizes and larger set sizes. It is indicated that the periodic tolerance and flock size are determined by the employed subset of $\mathbb{F}_q$. By constructing three suitable subsets of $\mathbb{F}_q^*$, we presented three new constructions of asymptotically optimal periodic QCSSs with new parameters and small alphabet sizes. We hope that more asymptotically optimal periodic QCSSs with small alphabet sizes can be generated by our general construction and this is also the focus and direction in our future work.

For practical MC-CDMA communications with high power transmission efficiency, the column sequence peak-to-mean envelope power ratio (PMEPR) of each quasi-complementary matrix should be as low as possible [15]. It can be easily seen that the maximum PMEPR of the QCSSs with parameters $(9, 3, 8, 6)$ presented in Example 2 is equal to 3. In fact, not all the QCSSs constructed by Theorem III.1 have the maximum PMEPR of K and the value of PMEPR is related to the selection of the set E . An interesting open problem is how

to determine the column sequence PMEPR of the proposed QCSS in Theorem III.1.

ACKNOWLEDGEMENT

We are grateful to the anonymous referees and the associate editor, Prof. Kai-Uwe Schmidt, for useful comments and suggestions that improved the presentation and quality of this paper.

REFERENCES

- [1] H. H. Chen, J. F. Yeh, and N. Suehiro, "A multicarrier CDMA architecture based on orthogonal complementary codes for new generations of wideband wireless communications," IEEE Commun. Mag., vol. 39, no. 10, pp. 126-135, Oct. 2001.
- [2] H. H. Chen, The Next Generation CDMA Technologies, 1st ed. New York, NY, USA: Wiley, Jul. 2007.
- [3] H. H. Chen, S. W. Chu, and M. Guizani, "On next generation CDMA technologies: The real approach for perfect orthogonal code generation," IEEE Trans. Veh. Technol., vol. 57, no. 5, pp. 2822-2833, Sep. 2008.
- [4] P. Fan, W. Yuan, and Y. Tu, "Z-complementary binary sequences," IEEE Signal Process. Lett., vol. 14, no. 8, pp. 401-404, Aug. 2007.
- [5] Z. Heng, C. Ding and Q. Yue, "New constructions of asymptotically optimal codebooks with multiplicative characters," IEEE Trans. Inf. Theory, vol. 63, no. 10, pp. 6179-6187, 2017.
- [6] Y. Li, T. Yan, and C. Lv, "Construction of a near-optimal quasicomplementary sequence set from almost difference set," Cryptogr. Commun., 2018. DOI: 10.1007/s12095-018- 0330-5.
- [7] Y. Li, T. Liu, and C. Xu, "Constructions of asymptotically optimal quasicomplementary sequence sets," IEEE Commun. Lett., vol. 22, no. 8, pp. 1516-1519, Aug. 2018.
- [8] Y. Li, L. Tian, T. Liu, and C. Xu, "Two constructions of asymptotically optimal quasi-complementary sequence sets" IEEE Trans. Commun., vol. 67, no. 3, pp. 1910-1924, 2019.
- [9] Y. Li, L. Tian, T. Liu, and C. Xu, "Constructions of quasi-complementary sequence sets associated with characters," IEEE Trans. Inf. Theory, vol. 65, no. 7, pp. 4597-4608, 2019.
- [10] Z. Liu, U. Parampalli, Y. L. Guan, and S. Boztas, "Constructions of optimal and near-optimal quasicomplementary sequence sets from Singer difference sets", IEEE Wire. Commun. Lett., vol. 2, no. 5, pp. 487-490, Oct. 2013.
- [11] Z. Liu, Y. L. Guan, and W. H. Mow, "A tighter correlation lower bound for quasi-complementary sequence sets," IEEE Trans. Inf. Theory, vol. 60, no. 1, pp. 388-396, Jan. 2014.
- [12] Z. Liu, Y. L. Guan, and W. H. Mow, "Asymptotically locally optimal weight vector design for a tighter correlation lower bound of quasicomplementary sequence sets," IEEE Trans. Inf. Theory, vol. 65, no. 12, pp. 3107-3119, Jun. 2017.

- [13] Z. Liu, Y. L. Guan, B. C. Ng, and H. H. Chen, "Correlation and set size bounds of complementary sequences with low correlation zones," *IEEE Trans. Commun.*, vol. 59, no. 12, pp. 3285-3289, Dec. 2011.
- [14] Z. Liu, Y. L. Guan, and H. H. Chen, "Fractional-delay-resilient receiver design for interference-free MC-CDMA communications based on complete complementary codes," *IEEE Trans. Wireless Commun.*, vol. 14, no. 3, pp. 1226-1236, Mar. 2015.
- [15] Z. Liu, Y. L. Guan and U. Parampalli, "New complete complementary codes for the peak-to-mean power control in MC-CDMA," *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 1105-1113, Mar. 2014.
- [16] J. Li, A. Huang, M. Guizani, and H. H. Chen, "Inter-group complementary codes for interference-resistant CDMA wireless communications," *IEEE Trans. Wireless Commun.*, vol. 7, no. 1, pp. 166-174, Jan. 2008.
- [17] R. Lidl and H. Niederreiter, *Finite fields*. Cambridge university press, 1997.
- [18] G. Luo and X. Cao, "Two constructions of asymptotically optimal codebooks via the hyper Eisenstein sum," *IEEE Trans. Inf. Theory*, vol. 64, no. 10, pp. 6498-6505, Oct. 2018.
- [19] G. Luo and X. Cao, "A construction of linear codes and strongly regular graphs from q -polynomials," *Discrete Mathematics.*, vol. 340, pp. 2262-2274, 2017.
- [20] R. E. A. C. Paley, On orthogonal matrices, *J. Math. Phys.*, vol. 12, pp. 311-320, 1933.
- [21] A. Samad, A. R. Adhikary, S. Majhi, "Receiver design for quasiasynchronous MC-CDMA by using QCSS code," in *Proc., Intl. Conf. Commun. Signal Process.*, Apr. 2016, pp. 1159-1163.
- [22] Z. Wang and G. Gong, "New sequences design from Weil representation with low two-dimensional correlation in both time and phase shifts," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4600-4611, July 2011.
- [23] Z. Zhou, T. Hellesteth, and U. Parampalli, "A family of polyphase sequences with asymptotically optimal correlation," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 2896-2900, Apr. 2018.

PLACE
PHOTO
HERE

Xiwan Cao received the Ph.D. degree in Mathematics from Peking University, Beijing, China, in 2004. Currently, he is a professor in Mathematics at Nanjing University of Aeronautics and Astronautics. His research interests include combinatorics, coding theory, commutative algebra and information theory.

PLACE
PHOTO
HERE

Minjia Shi Minjia Shi received the B.S. degree in mathematics from Anqing Normal University, China, in 2004, the M.S. degree in mathematics from the Hefei University of Technology, China, in 2007, and the Ph.D. degree from the Institute of Computer Network Systems, Hefei University of Technology, China, in 2010. From August 2012 to August 2013, he was a Visiting Researcher with the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. From July 2016 to August 2016, he was a Visiting Researcher with Telecom Paris Tech, Paris, France. He has been teaching with the School of Mathematical Sciences, Anhui University, China, since 2007, where he has been a Master's Supervisor and an Associate Professor since April 2012, and a Professor since 2017. He has been a Ph.D. Supervisor, since 2014. He is the author of over 100 journal articles and two books. His research interests include algebraic coding theory and cryptography.

Tor Hellesteth (M'89-SM'96-F'97) received the Cand. Real. and Dr. Philos. degrees in mathematics from the University of Bergen, Bergen, Norway, in 1971 and 1979, respectively.

From 1973-1980, he was a Research Assistant at the Department of Mathematics, University of Bergen. From 1981-1984, he was at the Chief Head quarters of Defense in Norway. Since 1984, he has been a Professor in the Department of Informatics, University of Bergen. During the academic years 1977-1978 and 1992-1993, he was on sabbatical leave at the University of Southern California, Los Angeles, and during 1979-1980, he was a Research Fellow at the Eindhoven University of Technology, Eindhoven, the Netherlands. His research interests include coding theory and cryptology. Prof. Hellesteth served as an Associate Editor for Coding Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY during the period 1991-1993 and 2012-2014. He was Program Chairman for Eurocrypt 1993 and for the Information Theory Workshop in 1997 in Longyearbyen, Norway. He was a Program Co-Chairman for **SE**quences and **T**heir **A**pplications (SETA) in 1998, 2001, 2004, 2006, 2012, 2018 and 2020. He was also a Program Co-Chairman for the IEEE Information Theory Workshop in Solstrand, Norway in 2007. During 2007-2009 he served on the Board of Governors for the IEEE Information Theory Society. In 1997 he was elected an IEEE Fellow for his contributions to coding theory and cryptography. In 2004 he was elected as a member of Det Norske Videnskaps-Akademi.

PLACE
PHOTO
HERE

Gaojun Luo received the Ph.D. degree in Mathematics from Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2019. He is currently a Research Fellow with Nanyang Technological University. His research interests include sequences, quantum information theory and coding theory.