

# New Correlation Bound and Construction of Quasi-Complementary Sequence Sets

Palash Sarkar, Chunlei Li, Sudhan Majhi, and Zilong Liu

**Abstract**—Quasi-complementary sequence sets (QCSSs) have attracted sustained research interests for simultaneously supporting more active users in multi-carrier code-division multiple-access (MC-CDMA) systems compared to complete complementary codes (CCCs). In this paper, we investigate a novel class of QCSSs composed of multiple CCCs. We derive a new aperiodic correlation lower bound for this type of QCSSs, which is tighter than the existing bounds for QCSSs. We then present a systematic construction of such QCSSs with a small alphabet size and low maximum correlation magnitude, and also show that the constructed aperiodic QCSSs can meet the newly derived bound asymptotically.

**Index Terms**—Multi-carrier code-division multiple-access (MC-CDMA), aperiodic correlation, complete complementary code (CCC), quasi-complementary sequence set (QCSS), multivariate function.

## I. INTRODUCTION

As a generalization of the Golay complementary pair [1], the complementary sequence set introduced by Tseng and Liu [2] consists of  $M \geq 2$  constituent sequences of length  $L$  having zero aperiodic auto-correlation sum for all nonzero time shifts. A complementary sequence set is usually arranged as an  $M \times L$  matrix (known as a complementary matrix or complementary code). A set of  $K$  complementary codes with the same order  $(M, L)$  is called a mutually orthogonal complementary sequence set (MOCSS) if any two distinct complementary codes have zero aperiodic cross-correlation sums for all time shifts [3]. A MOCSS has its size  $K \leq M$  and it is known as a complete complementary code (CCC) when the equality is reached. Due to the ideal auto- and cross-correlation properties, CCCs have a salient feature for supporting interference-free multi-carrier code-division multiple-access (MC-CDMA) communication where users are assigned with different complementary codes from a CCC [4]–[6].

Palash Sarkar and Chunlei Li are with the Department of Informatics, Selmer Center, University of Bergen, Norway, e-mail: palash.sarkar@uib.no; chunlei.li@uib.no.

Sudhan Majhi is with the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore, India, e-mail: smajhi@iisc.ac.in.

Zilong Liu is with the School of Computer Science and Electronic Engineering, University of Essex, UK, e-mail: zilong.liu@essex.ac.uk.

To support more users in MC-CDMA systems, the notion of low-correlation zone complementary sequence set (CSS), which refers to a set of complementary codes or codes having low maximum correlation magnitudes within a time-shift zone around the origin, was proposed [7]; in particular, when the maximum correlation magnitude within the zone is zero, it reduces to a zero-correlation zone CSS [8]–[10]. By extending the low correlation zone to all the non-trivial time-shifts, quasi-complementary sequence sets (QCSSs) with uniformly low maximum correlation magnitude have been investigated in [11]. A QCSS-based MC-CDMA system is expected to accommodate larger amount of asynchronous time-offsets, whilst supporting more users [12], [13].

### A. Existing Works on the Constructions and the Correlation Bounds of QCSSs

In this subsection, we recall some basics and known results on QCSSs. Let  $q$  be a positive integer and  $\mathcal{A}_q = \{\xi_q^i \mid 0 \leq i < q\}$ , where  $\xi_q = \exp(2\pi\sqrt{-1}/q)$  is a  $q$ -th primitive root of unity. We denote by  $\mathcal{A}_q^{M \times L}$  the set of all  $M \times L$  matrices over  $\mathcal{A}_q$ . A subset of  $\mathcal{A}_q^{M \times L}$  is termed a  $(K, M, L, \theta)$ -QCSS over  $\mathcal{A}_q$  if it consists of  $K$  matrices in  $\mathcal{A}_q^{M \times L}$  and its maximum magnitude of aperiodic correlation sums equals a positive value  $\theta$ . The multipath interference and multiuser interference in QCSS-based MC-CDMA system are closely related to the maximum correlation sum magnitude  $\theta$ , which is desired to be small. In the literature, several researchers have studied the lower bound on  $\theta$ . Welch in [14] first gave the following lower bound:

$$\theta \geq ML \sqrt{\frac{\frac{K}{M} - 1}{K(2L - 1) - 1}}. \quad (1)$$

In 2014, Liu, Guan and Mow [15] extended the idea of Levenshtein bound [16] for  $M \geq 2$  and provided a tighter correlation lower bound for the case of  $K \geq 3M$  and  $L \geq 2$ :

$$\theta \geq \sqrt{ML \left(1 - 2\sqrt{\frac{M}{3K}}\right)}. \quad (2)$$

With respect to a lower bound, the optimality of a QCSS can be evaluated in terms of the optimality factor  $\rho$ , which

is defined as the ratio of its maximum correlation magnitude  $\theta$  and the lower bound [11]. A  $(K, M, L, \theta)$ -QCSS is said to be optimal if  $\rho = 1$ , near-optimal if  $1 < \rho \leq 2$ , and asymptotically optimal if  $\rho$  tends to 1 for sufficiently large  $L$ , with respect to a lower bound, which is usually taken as the best known one.

For periodic QCSSs, the first known optimal and near-optimal QCSSs were proposed in [11] with the aid of Singer difference sets. Several other constructions on periodic QCSSs using various algebraic tools, such as difference sets and characters over finite fields, can be found in [17]–[20]. Aperiodic QCSSs with asymptotically optimal correlation properties have been developed with the help of various tools, such as permutation functions and Florentine rectangles [21]–[23]. The QCSSs in [22] and [23] appear as a collection of CCCs with low inter-set cross-correlation properties. In practice, this type of QCSSs can be useful in a multi-cell (or multi-cluster) mobile network where each cell is assigned with a distinctive CCC for interference-free MC-CDMA communication; at the same time, each cell also receives multiuser interference from other neighbouring cells [24], [25]. In this setting, the low inter-set cross-correlation property may permit minimum inter-cell interference, whilst achieving zero intra-cell interference due to the ideal correlation properties of CCCs. Besides low correlation, it is also desirable to design QCSSs over an alphabet of small size for the ease of practical implementations [20].

### B. Motivations and Contributions

Motivated by the promising applications of QCSSs in MC-CDMA systems, in this paper we are interested in investigating aperiodic QCSSs that are composed of multiple CCCs. Fundamentally, we aim to understand the theoretical trade-offs between different parameters of this type of QCSSs. Furthermore, we target at developing systematic constructions with both desirable correlation properties and flexible parameters.

Our first contribution in this paper is the derivation of a new lower bound on the maximum correlation magnitude of the new type of QCSSs. The new bound is obtained by a revisit to the generalized Levenshtein bound for QCSSs in [15] with extra consideration on a special feature of such QCSSs. Several forms of this new lower bound are derived by setting proper weighting vectors in the bounding function. As listed in Table I, they are shown to be tighter than the lower bound in [15]. Here it is worth noting that the bound in [15] was proposed for generic QCSSs and that new bounds in Table I should be used to evaluate aperiodic QCSSs composed of multiple CCCs. It is to be noted that the QCSSs reported in

Table I: Aperiodic correlation lower bounds for  $(K, M, L, \theta)$ -QCSSs composed of  $(M, L)$ -CCCs

$N = K/M$	Derived correlation lower bound	Derivation	Constraints
$N = 2$	$\theta^2 \geq \frac{ML^2}{2L-1}$	Corollary 1	$L, M \geq 2$
$N = 3$	$\theta^2 \geq \frac{ML^2}{2L-1}$	Corollary 1	$3 \leq L \leq 25, M \geq 2$
	$\theta^2 \geq ML \left(1 - \frac{L^2(2\pi^2+4N-16)-N\pi^2}{16L^2(N-1)}\right)$	Corollary 2	$L > 25, M \geq 2$
	$\theta^2 \geq \frac{ML}{3}$	[15]	$L, M \geq 2$
$N = 4$	$\theta^2 \geq ML \left(1 - \frac{L^2(2\pi^2+4N-16)-N\pi^2}{16L^2(N-1)}\right)$	Corollary 2	$L \geq 5, M \geq 2$
	$\theta^2 \geq ML \left(1 - \frac{L-1}{2L-1}\right)$	Corollary 2	$L = 4, M \geq 2$
	$\theta^2 \geq ML \left(1 - \frac{1}{\sqrt{3}}\right)$	[15]	$L, M \geq 2$
$N > 4$	$\theta^2 \geq ML \left(1 - \frac{\pi\sqrt{N(2L^2-N)}-4L}{4(N-1)L}\right)$	Corollary 2	$L \geq 5, M \geq 2$
	$\theta^2 \geq ML \left(1 - \frac{2}{\sqrt{3N}}\right)$	[15]	$L, M \geq 2$

[22] and [23] satisfy our proposed aperiodic correlation lower bound.

In the construction of QCSSs, multivariate functions have turned to be an effective tool to generate sequences with flexible parameters. Multivariate functions were studied in [26] to design CCCs with flexible parameters and then soon followed by [27] to construct Z-complementary sequences and by [28] to construct Golay complementary array set. Our second contribution in this paper is a systematic construction framework of aperiodic QCSSs using multivariate functions from a graphical perspective. We consider the multivariate functions from  $\mathbb{Z}_p^m$  to  $\mathbb{Z}_q$ , where  $p$  is an arbitrary prime divisor of  $q$ . This type of multivariate functions are referred to as  $q$ -ary functions in this paper for ease of presentation. With a graphical approach, we utilize  $q$ -ary functions in  $m$  variables to construct a  $(p^{n+1}(p-1), p^{n+1}, p^m, p^m)$ -QCSS over  $\mathcal{A}_q$ , where  $1 \leq n < m$ . The key requirement on the employed  $q$ -ary function  $f$  is that the graph of each restriction of  $f$  on certain  $n$  variables yields a Hamiltonian path with edges having identical weights of  $q/p$ . We show that such  $q$ -ary functions give rise to  $p-1$  distinct  $(p^{n+1}, p^m)$ -CCCs, and a QCSS composed of these CCCs has maximum correlation magnitude  $p^m$ . Notice that the alphabet size  $q$  of proposed QCSSs can be as small as  $p$ , which is different from the known QCSSs as listed in Table II, for which the alphabet size is required to be at least the sequence length. To the best of our knowledge, it is the first time in the literature that a construction of aperiodic QCSSs can maintain a small alphabet size irrespective of the sequence length and set size. Finally, it is shown that the proposed QCSSs can asymptotically meet the newly derived aperiodic correlation lower bound.

The structure of this paper is outlined as follows: In Section II, we introduce the essential mathematical tools utilized in this work. Section III derives the proposed new tighter correlation lower bounds for QCSSs comprised of multiple CCCs. In Section IV, we present our contributions related to

the construction of QCSSs that can meet the correlation lower bound introduced in Section III. Lastly, Section V concludes this work.

## II. PRELIMINARIES

We first define some notations which will be used throughout the paper:

- $\mathbb{Z}_t = \mathbb{Z}/t\mathbb{Z}$  is the set of all integers modulo  $t$
- $q$  is a positive integer and  $p$  is an arbitrary prime divisor of  $q$
- $\xi_q = \exp(2\pi\sqrt{-1}/q)$  is a primitive  $q$ -th root of unity
- $\mathcal{A}_q = \{\xi_q^i : 0 \leq i < q\}$  and  $\mathcal{A}_q^{M \times L}$  is the set of matrices over  $\mathcal{A}_q$
- $\mathbf{0}_L$  denotes the zero vector of length  $L$
- lower-case letters in bold, e.g.,  $\mathbf{a}$ ,  $\mathbf{b}$ , denote sequences of certain length
- upper-case letters in bold, e.g.,  $\mathbf{C}$ ,  $\mathbf{X}$ ,  $\mathbf{Y}$ , denote matrices or codes over  $\mathcal{A}_q$
- $T^u(\mathbf{a}) = (a_{L-u}, \dots, a_{L-1}, a_0, \dots, a_{L-u-1})$  for a sequence  $\mathbf{a} = (a_0, a_1, \dots, a_{L-1})$
- $|a|$ ,  $a^*$  denote the magnitude and conjugate of a complex number  $a$ , respectively
- $\langle \mathbf{a}, \mathbf{b} \rangle = a_0 b_0^* + a_1 b_1^* + \dots + a_{L-1} b_{L-1}^*$  denotes the inner product between two complex-valued sequences  $\mathbf{a} = (a_0, a_1, \dots, a_{L-1})$  and  $\mathbf{b} = (b_0, b_1, \dots, b_{L-1})$
- $\mathbf{a} \cdot \mathbf{b}$  denotes the inner product for two real-valued sequences  $\mathbf{a}$  and  $\mathbf{b}$
- $\lceil a \rceil$  denotes the integer closest to a real number  $a$
- $[a, b]$  denotes a closed interval consisting of real numbers  $x$  satisfying  $a \leq x \leq b$
- $[a : b] = [a, \dots, b]$  for integers  $a \leq b$
- $\emptyset$  denotes the empty set
- $|S|$  denotes the size of a set  $S$

### A. Aperiodic Auto- and Cross-Correlation

For any two complex-valued sequences  $\mathbf{a} = (a_0, a_1, \dots, a_{L-1})$  and  $\mathbf{b} = (b_0, b_1, \dots, b_{L-1})$  of length  $L$ , we define the aperiodic cross-correlation function (ACCF) at time-shift  $\tau$ , where  $0 \leq |\tau| < L$  as

$$\Theta(\mathbf{a}, \mathbf{b})(\tau) = \begin{cases} \sum_{\alpha=0}^{L-\tau-1} a_\alpha b_{\alpha+\tau}^*, & 0 \leq \tau < L, \\ \sum_{\alpha=0}^{L+\tau-1} a_{\alpha-\tau} b_\alpha^*, & -L < \tau < 0. \end{cases} \quad (3)$$

For  $\mathbf{a} = \mathbf{b}$ , the ACCF defined in (3) reduces to the aperiodic auto-correlation function (AACF) of  $\mathbf{a}$ , which will be denoted as  $\Theta(\mathbf{a})(\tau)$  for short.

Let  $\mathcal{C} = \{\mathbf{C}_1, \mathbf{C}_2, \dots, \mathbf{C}_K\}$  be a collection of  $K$  codes, each containing  $M$  sequences of length  $L$ . By arranging each code as a two-dimensional matrix, we write  $\mathbf{C}_k$  as

$$\mathbf{C}_k = \begin{bmatrix} \mathbf{c}_k^1 \\ \mathbf{c}_k^2 \\ \vdots \\ \mathbf{c}_k^M \end{bmatrix}_{M \times L},$$

where  $k = 1, \dots, K$ . The ACCF (sum) between  $\mathbf{C}_{k_1}$  and  $\mathbf{C}_{k_2}$  for  $1 \leq k_1, k_2 \leq K$  is defined as

$$\Theta(\mathbf{C}_{k_1}, \mathbf{C}_{k_2})(\tau) = \sum_{j=1}^M \Theta(\mathbf{c}_{k_1}^j, \mathbf{c}_{k_2}^j)(\tau). \quad (4)$$

For  $k_1 = k_2 = k$ , the ACCF in (4) reduces to the AACF of  $\mathbf{C}_k$  and we denote it by  $\Theta(\mathbf{C}_k)(\tau)$ . Define

$$\begin{aligned} \theta_A &= \max\{|\Theta(\mathbf{C}_k)(\tau)| : k = 1, \dots, K, 0 < |\tau| < L\}, \\ \theta_C &= \max\{|\Theta(\mathbf{C}_{k_1}, \mathbf{C}_{k_2})(\tau)| : 1 \leq k_1 \neq k_2 \leq K, \\ & \quad 0 \leq |\tau| < L\}. \end{aligned}$$

The maximum correlation magnitude of  $\mathcal{C}$  is given by  $\theta = \max\{\theta_A, \theta_C\}$ . This collection of codes is called an aperiodic QCSS, denoted by  $(K, M, L, \theta)$ -QCSS. In particular, when  $\theta = 0$  and  $K = M$ ,  $\mathcal{C}$  is said to be a CCC, denoted by an  $(M, L)$ -CCC.

In order to investigate the lower bound on  $\theta$  for QCSSs, we recall an interesting function from [15, Eq. (17)] below. For two  $(K, M, L, \theta)$ -QCSSs  $\mathcal{X}, \mathcal{Y} \subset \mathcal{A}_q^{M \times L}$ , define the following function:

$$\begin{aligned} F(\mathcal{X}, \mathcal{Y}) &= \frac{1}{|\mathcal{X}||\mathcal{Y}|} \times \\ & \sum_{\mathbf{X} \in \mathcal{X}} \sum_{\mathbf{Y} \in \mathcal{Y}} \sum_{u=0}^{2L-2} \sum_{v=0}^{2L-2} |\langle T^u(\mathbf{X}, \mathbf{0}_{L-1}), T^v(\mathbf{Y}, \mathbf{0}_{L-1}) \rangle|^2 w_u w_v, \end{aligned} \quad (5)$$

with

$$\begin{aligned} & \langle T^u(\mathbf{X}, \mathbf{0}_{L-1}), T^v(\mathbf{Y}, \mathbf{0}_{L-1}) \rangle \\ &= \sum_{j=1}^M \langle T^u(\mathbf{X}^j, \mathbf{0}_{L-1}), T^v(\mathbf{Y}^j, \mathbf{0}_{L-1}) \rangle, \end{aligned} \quad (6)$$

where  $T$  represents the right cyclic shift operator,  $(\mathbf{X}^j, \mathbf{0}_{L-1}), (\mathbf{Y}^j, \mathbf{0}_{L-1})$  denote the concatenation of the  $j$ th row of  $\mathbf{X}$ ,  $\mathbf{Y}$  and  $\mathbf{0}_{L-1}$ , respectively, and  $\mathbf{w} = (w_0, w_1, \dots, w_{2L-2})$  is a weight vector, satisfying

$$\sum_{j=0}^{2L-2} w_j = 1 \text{ and } w_j \geq 0 \text{ for } 0 \leq j \leq 2L-2.$$

In the case of  $\mathcal{X} = \mathcal{Y} = \mathcal{C}$ , a lower bound on  $F(\mathcal{C}, \mathcal{C})$  was derived in [15]. We represent the lower bound in the

Table II: The parameters of the existing and proposed aperiodic QCSSs

Ref.	$K$	$M$	$L$	$\theta$	Alphabet	Constraints
Th. 1 [21]	$u(u+1)$	$u$	$u$	$u$	$\mathbb{Z}_u$	$u$ is power of prime
Th. 2 [21]	$u^2$	$u$	$u-1$	$u$	$\mathbb{Z}_u$	$u$ is power of prime, $u \geq 5$
[22]	$N(t_0-1)$	$N$	$N$	$N$	$\mathbb{Z}_N$	$N (\geq 5)$ is odd positive integer with $t_0$ as its smallest prime factor
[23]	$N \times F(N)$	$N$	$N$	$N$	$\mathbb{Z}_N$	$N (\geq 2)$ is any integer, $F(N)$ is the maximum number of rows for which $F(N) \times N$ Florentine rectangle exists
Proposed	$p^{n+1}(p-1)$	$p^{n+1}$	$p^m$	$p^m$	$\mathbb{Z}_q$	$p$ is a prime number, $m$ is any positive integer, $n (\leq m-1)$ is any non-negative integer, $q$ is a positive multiple of $p$

following lemma which will be used in Section III to obtain new correlation lower bound for  $\theta$ :

**Lemma 1** ([15]). *Let  $\mathcal{C}$  be a  $(K, M, L, \theta)$ -QCSS. Then*

$$F(\mathcal{C}, \mathcal{C}) \geq \sum_{u,v=0}^{2L-2} M(L - \tau_{u,v,L}) w_u w_v, \quad (7)$$

where

$$0 \leq \tau_{u,v,L} = \min\{|v-u|, 2L-1-|v-u|\} \leq L-1.$$

In the following, we present some basics on  $q$ -ary functions and its relation with graphs and sequences. We also discuss some basic and necessary properties of sequences.

### B. Sequences associated with $q$ -ary Functions

Let  $q$  be a positive integer and  $p$  is a prime divisor of  $q$ . For example, let  $q = 12 = 2^2 \cdot 3$ , in this case  $p$  can be either 2 or 3. For a  $q$ -ary function  $f : \mathbb{Z}_p^m \rightarrow \mathbb{Z}_q$ , it defines a  $\mathbb{Z}_q$ -valued sequence  $\mathbf{f} = (f_0, f_1, \dots, f_{p^m-1})$ , where the coordinate  $f_i = f(i_0, i_1, \dots, i_{m-1})$  for  $0 \leq i < p^m$  with  $i = \sum_{j=0}^{m-1} i_j p^{m-j-1}$  and the arithmetic operations on variables in the function  $f$  are taken modulo  $q$ . In the sequel we shall identify an integer  $i$  with  $0 \leq i < p^m$  as its  $p$ -ary vector representation  $(i_0, i_1, \dots, i_{m-1})$  when there is no ambiguity. We define the complex-valued sequence associated with  $f$ , denoted by  $\psi_q(f)$ , as

$$\psi_q(f) = (\xi_q^{f_0}, \xi_q^{f_1}, \dots, \xi_q^{f_{p^m-1}}).$$

When there is no ambiguity in the context, we will write  $\psi_q(f)$  as  $\psi(f)$  for simplicity. For  $\mathbf{x} = (x_0, x_1, \dots, x_{m-1}) \in \mathbb{Z}_p^m$  and a subset  $J = \{j_0, j_1, \dots, j_{n-1}\} \subset \mathbb{Z}_m$ , we define  $\mathbf{x}_J = (x_{j_0}, x_{j_1}, \dots, x_{j_{n-1}})$  as the restriction of the vector  $\mathbf{x}$  on  $J$ . For  $\mathbf{c} = (c_0, c_1, \dots, c_{n-1}) \in \mathbb{Z}_p^n$  and  $\mathbf{x}_J = \mathbf{c}$ , we define the

complex-valued sequence corresponding to the restricted  $q$ -ary function  $f|_{\mathbf{x}_J=\mathbf{c}}$  as follows:

$$\psi(f|_{\mathbf{x}_J=\mathbf{c}}) = (a_0, a_1, \dots, a_{p^m-1}) \text{ with} \\ a_i = \begin{cases} \xi_q^{f_i}, & i_J = \mathbf{c}, \\ 0, & \text{otherwise.} \end{cases} \quad (8)$$

For any two functions  $f, g : \mathbb{Z}_p^m \rightarrow \mathbb{Z}_q$ , below we define a set of ordered pairs  $(\gamma, \delta)$  to calculate the ACCF between two  $q$ -ary restricted functions,  $\psi(f|_{\mathbf{x}_J=\mathbf{c}_1})$  and  $\psi(g|_{\mathbf{x}_J=\mathbf{c}_2})$ , where  $\mathbf{c}_i \in \mathbb{Z}_p^n$  for  $i = 1, 2$ , at a time-shift  $0 \leq \tau < p^m$  as follows:

$$\mathbf{B}_\tau(\mathbf{c}_1, \mathbf{c}_2) = \{(\gamma, \delta) : \delta = \gamma + \tau, 0 \leq \gamma \leq p^m - \tau - 1, \\ \gamma_J = \mathbf{c}_1, \delta_J = \mathbf{c}_2\} \quad (9)$$

where  $\gamma_J, \delta_J$  correspond to the restrictions of the vector representations of  $\gamma, \delta$ , respectively. Following (8), the complex-valued sequences  $\psi(f|_{\mathbf{x}_J=\mathbf{c}_1})$  and  $\psi(g|_{\mathbf{x}_J=\mathbf{c}_2})$  can be expressed as follows:

$$\psi(f|_{\mathbf{x}_J=\mathbf{c}_1}) = (a_0, a_1, \dots, a_{p^m-1}) \text{ with} \\ a_\gamma = \begin{cases} \xi_q^{f_\gamma}, & \gamma_J = \mathbf{c}_1, \\ 0, & \text{otherwise,} \end{cases} \\ \psi(g|_{\mathbf{x}_J=\mathbf{c}_2}) = (b_0, b_1, \dots, b_{p^m-1}) \text{ with} \\ b_\delta = \begin{cases} \xi_q^{g_\delta}, & \delta_J = \mathbf{c}_2, \\ 0, & \text{otherwise.} \end{cases} \quad (10)$$

From (3), (9) and (10), the ACCF can be expressed as

$$\Theta(\psi(f|_{\mathbf{x}_J=\mathbf{c}_1}), \psi(g|_{\mathbf{x}_J=\mathbf{c}_2}))(\tau) = \sum_{\gamma=0}^{p^m-\tau-1} a_\gamma b_\delta^* \\ = \sum_{(\gamma, \delta) \in \mathbf{B}_\tau(\mathbf{c}_1, \mathbf{c}_2)} \xi_q^{f_\gamma - g_\delta}. \quad (11)$$

When  $\mathbf{c}_1 = \mathbf{c}_2 = \mathbf{c}$ , we denote the notation  $\mathbf{B}_\tau(\mathbf{c}_1, \mathbf{c}_2)$  in (9) by  $\mathbf{A}_\tau(\mathbf{c})$  which can be expressed as follows:

$$\mathbf{A}_\tau(\mathbf{c}) = \{(\gamma, \delta) : 0 \leq \gamma \leq p^m - \tau - 1, \delta = \gamma + \tau, \gamma_J = \delta_J = \mathbf{c}\}. \quad (12)$$

From (3), (10) and (12), the ACCF between  $\psi(f|_{\mathbf{x}_J=\mathbf{c}})$  and  $\psi(g|_{\mathbf{x}_J=\mathbf{c}})$  can be expressed as

$$\Theta(\psi(f|_{\mathbf{x}_J=\mathbf{c}}), \psi(g|_{\mathbf{x}_J=\mathbf{c}}))(\tau) = \sum_{(\gamma, \delta) \in \mathbf{A}_\tau(\mathbf{c})} \xi_q^{f_\gamma - g_\delta}. \quad (13)$$

When  $f = g$ , the ACCF in (13) reduces to the AACF of  $\psi(f|_{\mathbf{x}_J=\mathbf{c}})$ .

The following example illustrates the sequences associated with a  $q$ -ary function and the calculation of ACCF between sequences associated with restricted  $q$ -ary functions.

**Example 1.** Assume  $p = 3$ ,  $m = 3$ , and  $q = 3$ . Let us consider  $f : \mathbb{Z}_3^3 \rightarrow \mathbb{Z}_3$  as follows:

$$f(x_0, x_1, x_2) = x_0x_2 + 2x_2x_1 + 2x_1^2 + x_2 + 1.$$

According to the above definitions, the associated sequences  $f$ ,  $\psi(f)$  and restricted sequences  $\psi(f|_{\mathbf{x}_J=\mathbf{c}})$  w.r.t  $J = \{0, 2\}$  and  $\mathbf{c} \in \{(0, 2), (1, 2), (2, 2)\}$  can be given in the Table III, where the blanks for the last three rows  $\psi(f|_{\mathbf{x}_J=\mathbf{c}})$  indicate that the corresponding coordinates take values of 0. For  $\mathbf{c}_1 = (0, 2)$ ,  $\mathbf{c}_2 = (1, 2)$ , and  $\mathbf{c} = (0, 2)$ , from (9) and (12),

$$\mathbf{B}_\tau(\mathbf{c}_1, \mathbf{c}_2) = \emptyset, \quad \forall \tau \neq 3, 6, 9, 12, 15,$$

and

$$\mathbf{A}_\tau(\mathbf{c}) = \emptyset, \quad \forall \tau \neq 0, 3, 6.$$

Therefore,

$$\Theta(\psi(f|_{\mathbf{x}_J=\mathbf{c}_1}), \psi(f|_{\mathbf{x}_J=\mathbf{c}_2}))(\tau) = 0, \quad \forall \tau \neq 3, 6, 9, 12, 15,$$

and

$$\Theta(\psi(f|_{\mathbf{x}_J=\mathbf{c}}))(\tau) = 0, \quad \forall \tau \neq 0, 3, 6.$$

When  $\tau \in \{3, 6, 9, 12, 15\}$ , for example  $\tau = 3$ , from the row  $\psi(f|_{\mathbf{x}_J=(0,2)})$  in Table III we see  $\gamma_J = \mathbf{c}_1 = (0, 2)$  can hold only for  $\gamma \in \{2, 5, 8\}$ ; furthermore, since  $\tau = 3$  we see that  $\delta = \gamma + \tau$  with  $\delta_J = \mathbf{c}_2 = (1, 2)$  can only hold for  $\delta = 11$ , as indicated by the row  $\psi(f|_{\mathbf{x}_J=(1,2)})$ . To summarize, we list  $\mathbf{A}_\tau(\mathbf{c})$  for  $\tau = 0, 3, 6$ , and  $\mathbf{B}_\tau(\mathbf{c}_1, \mathbf{c}_2)$  for  $\tau = 3, 6, 9, 12, 15$  in Table IV, where  $\mathbf{A}_\tau, \mathbf{B}_\tau$  are used for simplicity. From the Table IV, we can express  $\Theta(\psi(f|_{\mathbf{x}_J=\mathbf{c}_1}), \psi(f|_{\mathbf{x}_J=\mathbf{c}_2}))(\tau)$  and  $\Theta(\psi(f|_{\mathbf{x}_J=\mathbf{c}}))(\tau)$  for  $\tau = 3$  as follows:  $\Theta(\psi(f|_{\mathbf{x}_J=\mathbf{c}_1}), \psi(f|_{\mathbf{x}_J=\mathbf{c}_2}))(3) = \sum_{(\gamma, \delta) \in \mathbf{B}_3(\mathbf{c}_1, \mathbf{c}_2)} \xi_3^{f_\gamma - f_\delta} = \xi_3^{f_8 - f_{11}} = \xi_3^{1-2} = \xi_3^{-1}$ , and  $\Theta(\psi(f|_{\mathbf{x}_J=\mathbf{c}}))(3) = \sum_{(\gamma, \delta) \in \mathbf{A}_3(\mathbf{c})} \xi_3^{f_\gamma - f_\delta} = \xi_3^{f_2 - f_5} + \xi_3^{f_5 - f_8} = \xi_3^{0-0} + \xi_3^{0-1} = 1 + \xi_3^{-1}$ . For other values of  $\tau$ ,

we can calculate the ACCFs similarly by following (11), (13) and the Table IV.

We can observe that there are  $p^{m-n}$  nonzero components in  $\psi(f|_{\mathbf{x}_J=\mathbf{c}})$  for a choice of  $\mathbf{c}$  in  $\mathbb{Z}_p^n$ . From (8) (and as illustrated in the Table III), it is clear that the nonzero positions in  $\psi(f|_{\mathbf{x}_J=\mathbf{c}_1})$  and  $\psi(f|_{\mathbf{x}_J=\mathbf{c}_2})$  for two distinct  $\mathbf{c}_1$  and  $\mathbf{c}_2$  in  $\mathbb{Z}_p^n$  are always distinct. Therefore,  $\psi(f)$  can be expressed as

$$\psi(f) = \sum_{\mathbf{c} \in \mathbb{Z}_p^n} \psi(f|_{\mathbf{x}_J=\mathbf{c}}). \quad (14)$$

With this relation, one can express the ACCF between two sequences  $\psi(f)$  and  $\psi(g)$  in terms of their corresponding restricted sequences.

**Lemma 2.** Let  $f$  and  $g$  be two  $q$ -ary functions in  $m$  variables. The ACCF between  $\psi(f)$  and  $\psi(g)$  can be expressed as

$$\Theta(\psi(f), \psi(g))(\tau) = \sum_{\mathbf{c}_1, \mathbf{c}_2 \in \mathbb{Z}_p^n} \Theta(\psi(f|_{\mathbf{x}_J=\mathbf{c}_1}), \psi(g|_{\mathbf{x}_J=\mathbf{c}_2}))(\tau).$$

*Proof:* Following the relation in (14), we have

$$\begin{aligned} & \Theta(\psi(f), \psi(g))(\tau) \\ &= \Theta \left( \sum_{\mathbf{c}_1 \in \mathbb{Z}_p^n} \psi(f|_{\mathbf{x}_J=\mathbf{c}_1}), \sum_{\mathbf{c}_2 \in \mathbb{Z}_p^n} \psi(g|_{\mathbf{x}_J=\mathbf{c}_2}) \right) (\tau) \\ &= \sum_{\mathbf{c}_1 \in \mathbb{Z}_p^n} \Theta \left( \psi(f|_{\mathbf{x}_J=\mathbf{c}_1}), \sum_{\mathbf{c}_2 \in \mathbb{Z}_p^n} \psi(g|_{\mathbf{x}_J=\mathbf{c}_2}) \right) (\tau) \\ &= \sum_{\mathbf{c}_1, \mathbf{c}_2 \in \mathbb{Z}_p^n} \Theta(\psi(f|_{\mathbf{x}_J=\mathbf{c}_1}), \psi(g|_{\mathbf{x}_J=\mathbf{c}_2}))(\tau). \end{aligned}$$

### C. Quadratic Functions and Graphs

A quadratic  $q$ -ary function from  $\mathbb{Z}_p^m$  to  $\mathbb{Z}_q$  can be expressed as

$$f(x_0, x_1, \dots, x_{m-1}) = \sum_{0 \leq i, j < m} q_{i,j} x_i x_j + \sum_{0 \leq j < m} c_j x_j + c,$$

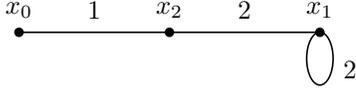
where  $q_{i,j}, c_j, c \in \mathbb{Z}_q$ . For a quadratic  $q$ -ary function  $f$ , we define its graph  $G(f)$  as a graph, in which there are  $m$  vertices labeled as  $x_i$ , where there is an edge between vertices  $x_i$  and  $x_j$  if  $q_{i,j} \neq 0$ . A Hamiltonian path in a graph is the path that visits each vertex exactly once. A graph contains only one vertex with no edges is also known as a Hamiltonian path [29]. For instance, Figure 1 represents the graph of  $f(x_0, x_1, x_2) = x_0x_2 + 2x_2x_1 + 2x_1^2 + x_2 + 1$  in Example 1.

### III. TIGHTER LOWER BOUNDS ON THE MAXIMUM CORRELATION MAGNITUDE OF QCSSS

In this section, we will further investigate the lower bound on the maximum correlation magnitude for  $(K, M, L, \theta)$ -QCSSs that are composed of multiple CCCs.

Table III: Sequences corresponding to the ternary function  $x_0x_2 + 2x_2x_1 + 2x_1^2 + x_2 + 1$ 

$i$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
$i_0i_1i_2$	000	001	002	010	011	012	020	021	022	100	101	102	110	111	112	120	121	122	200	201	202	210	211	212	220	221	222
$\mathbf{f}$	1	2	0	0	0	0	0	2	1	1	0	2	0	1	2	0	0	0	1	1	1	0	2	1	0	1	2
$\psi(f)$	$\xi_3^1$	$\xi_3^2$	$\xi_3^0$	$\xi_3^0$	$\xi_3^0$	$\xi_3^0$	$\xi_3^0$	$\xi_3^2$	$\xi_3^1$	$\xi_3^1$	$\xi_3^0$	$\xi_3^2$	$\xi_3^0$	$\xi_3^1$	$\xi_3^2$	$\xi_3^0$	$\xi_3^0$	$\xi_3^0$	$\xi_3^1$	$\xi_3^1$	$\xi_3^1$	$\xi_3^0$	$\xi_3^2$	$\xi_3^1$	$\xi_3^0$	$\xi_3^1$	$\xi_3^2$
$\psi(f _{\mathbf{x}_J=(0,2)})$			$\xi_3^0$			$\xi_3^0$			$\xi_3^1$																		
$\psi(f _{\mathbf{x}_J=(1,2)})$												$\xi_3^2$			$\xi_3^2$		$\xi_3^0$										
$\psi(f _{\mathbf{x}_J=(2,2)})$																					$\xi_3^1$			$\xi_3^1$			$\xi_3^2$

Figure 1: Graph of the function  $x_0x_2 + 2x_2x_1 + 2x_1^2 + x_2 + 1$ 

For the weight vector  $\mathbf{w}$  in (5), we define a quadratic form

$$Q(\mathbf{w}, a) = a \sum_{u=0}^{2L-2} w_u^2 + \sum_{u,v=0}^{2L-2} \tau_{u,v,L} w_u w_v, \quad (15)$$

where  $a$  is a real number. Below we present the first main theorem of this paper.

**Theorem 1.** *Let  $N \geq 2$  and  $\mathcal{C}$  be a collection of  $N$  different  $(M, L)$ -CCCs. Then the maximum correlation magnitude  $\theta$  of  $\mathcal{C}$  satisfies*

$$\theta^2 \geq \frac{M \left( L - Q \left( \mathbf{w}, \frac{ML^2}{K} \right) \right)}{1 - \frac{M}{K}},$$

where  $K = NM$ .

*Proof:* Assume  $\mathcal{C} = \cup_{i=1}^N \mathcal{C}_i$ , where  $\mathcal{C}_i$  is an  $(M, L)$ -CCC.

Table IV:  $\mathbf{A}_\tau(\mathbf{c})$  for  $\mathbf{c} = (0, 2)$ , and  $\mathbf{B}_\tau(\mathbf{c}_1, \mathbf{c}_2)$  for  $\mathbf{c}_2 = (1, 2)$ 

$\mathbf{B}_3$	$\{(8, 11)\}$	$\mathbf{A}_0$	$\{(2, 2), (5, 5), (8, 8)\}$
$\mathbf{B}_6$	$\{(5, 11), (8, 14)\}$		
$\mathbf{B}_9$	$\{(2, 11), (5, 14), (8, 17)\}$	$\mathbf{A}_3$	$\{(2, 5), (5, 8)\}$
$\mathbf{B}_{12}$	$\{(2, 14), (5, 17)\}$		
$\mathbf{B}_{15}$	$\{(2, 17)\}$	$\mathbf{A}_6$	$\{(2, 8)\}$

Substituting  $\mathcal{D} = \mathcal{C}$  in (5), we have

$$\begin{aligned} & |\mathcal{C}|^2 F(\mathcal{C}, \mathcal{C}) \\ &= \sum_{\mathbf{X} \in \mathcal{C}} \sum_{\mathbf{Y} \in \mathcal{C}} \sum_{u=0}^{2L-2} \sum_{v=0}^{2L-2} |\langle T^u(\mathbf{X}, \mathbf{0}_{L-1}), T^v(\mathbf{Y}, \mathbf{0}_{L-1}) \rangle|^2 w_u w_v \\ &= \sum_{i=1}^N \sum_{\mathbf{X}, \mathbf{Y} \in \mathcal{C}_i} \sum_{u,v=0}^{2L-2} |\langle T^u(\mathbf{X}, \mathbf{0}_{L-1}), T^v(\mathbf{Y}, \mathbf{0}_{L-1}) \rangle|^2 w_u w_v \\ &\quad + \sum_{i,j=1}^N \sum_{\substack{\mathbf{X} \in \mathcal{C}_i \\ i \neq j}} \sum_{\mathbf{Y} \in \mathcal{C}_j} \sum_{u,v=0}^{2L-2} |\langle T^u(\mathbf{X}, \mathbf{0}_{L-1}), T^v(\mathbf{Y}, \mathbf{0}_{L-1}) \rangle|^2 w_u w_v \\ &= S_1 + S_2, \end{aligned} \quad (16)$$

where

$$S_1 = \sum_{i=1}^N \sum_{\mathbf{X}, \mathbf{Y} \in \mathcal{C}_i} \sum_{u,v=0}^{2L-2} |\langle T^u(\mathbf{X}, \mathbf{0}_{L-1}), T^v(\mathbf{Y}, \mathbf{0}_{L-1}) \rangle|^2 w_u w_v,$$

and

$$S_2 = \sum_{i,j=1}^N \sum_{\substack{\mathbf{X} \in \mathcal{C}_i \\ i \neq j}} \sum_{\mathbf{Y} \in \mathcal{C}_j} \sum_{u,v=0}^{2L-2} |\langle T^u(\mathbf{X}, \mathbf{0}_{L-1}), T^v(\mathbf{Y}, \mathbf{0}_{L-1}) \rangle|^2 w_u w_v.$$

As  $\mathcal{C}_i$  is an  $(M, L)$ -CCC, for  $\mathbf{X}, \mathbf{Y} \in \mathcal{C}_i$  and  $v \leq u$ ,

$$\begin{aligned} & \langle T^u(\mathbf{X}, \mathbf{0}_{L-1}), T^v(\mathbf{Y}, \mathbf{0}_{L-1}) \rangle \\ &= \Theta(\mathbf{X}, \mathbf{Y})(\tau_{u,v,L}) \\ &= \begin{cases} ML, & \mathbf{X} = \mathbf{Y}, \tau_{u,v,L} = 0, \\ 0, & \mathbf{X} = \mathbf{Y}, 1 \leq \tau_{u,v,L} < L, \\ 0, & \mathbf{X} \neq \mathbf{Y}, 0 \leq \tau_{u,v,L} < L, \end{cases} \end{aligned} \quad (17)$$

and for  $v > u$ ,

$$\begin{aligned} & \langle T^u(\mathbf{X}, \mathbf{0}_{L-1}), T^v(\mathbf{Y}, \mathbf{0}_{L-1}) \rangle \\ &= \Theta(\mathbf{X}, \mathbf{Y})(-\tau_{u,v,L}) \\ &= \begin{cases} 0, & \mathbf{X} = \mathbf{Y}, 1 \leq \tau_{u,v,L} < L, \\ 0, & \mathbf{X} \neq \mathbf{Y}, 0 < \tau_{u,v,L} < L. \end{cases} \end{aligned} \quad (18)$$

Using (17) and (18) in  $S_1$ , we have

$$\begin{aligned}
S_1 &= \sum_{i=1}^N \sum_{\mathbf{X}, \mathbf{Y} \in \mathcal{C}_i} \sum_{u, v=0}^{2L-2} \left| \langle T^u(\mathbf{X}, \mathbf{0}_{L-1}), \right. \\
&\quad \left. T^v(\mathbf{Y}, \mathbf{0}_{L-1}) \rangle \right|^2 w_u w_v \\
&= \sum_{i=1}^N \sum_{\substack{\mathbf{X}, \mathbf{Y} \in \mathcal{C}_i \\ \mathbf{X}=\mathbf{Y}}} \sum_{u, v=0}^{2L-2} \left| \langle T^u(\mathbf{X}, \mathbf{0}_{L-1}), \right. \\
&\quad \left. T^v(\mathbf{Y}, \mathbf{0}_{L-1}) \rangle \right|^2 w_u w_v \\
&+ \sum_{i=1}^N \sum_{\substack{\mathbf{X}, \mathbf{Y} \in \mathcal{C}_i \\ \mathbf{X} \neq \mathbf{Y}}} \sum_{u \neq v}^{2L-2} \left| \langle T^u(\mathbf{X}, \mathbf{0}_{L-1}), \right. \\
&\quad \left. T^v(\mathbf{Y}, \mathbf{0}_{L-1}) \rangle \right|^2 w_u w_v \\
&+ \sum_{i=1}^N \sum_{\substack{\mathbf{X}, \mathbf{Y} \in \mathcal{C}_i \\ \mathbf{X} \neq \mathbf{Y}}} \sum_{u, v=0}^{2L-2} \left| \langle T^u(\mathbf{X}, \mathbf{0}_{L-1}), \right. \\
&\quad \left. T^v(\mathbf{Y}, \mathbf{0}_{L-1}) \rangle \right|^2 w_u w_v \\
&= \sum_{i=1}^N \sum_{\mathbf{X} \in \mathcal{C}_i} \sum_{u=0}^{2L-2} \Theta^2(\mathbf{X})(0) w_u^2 + 0 + 0 \\
&= KM^2 L^2 \sum_{u=0}^{2L-2} w_u^2,
\end{aligned} \tag{19}$$

where  $K = MN$ . Now,

$$\begin{aligned}
S_2 &= \sum_{i, j=1}^N \sum_{\mathbf{X} \in \mathcal{C}_i} \sum_{\substack{\mathbf{Y} \in \mathcal{C}_j \\ i \neq j}} \sum_{u, v=0}^{2L-2} \left| \langle T^u(\mathbf{X}, \mathbf{0}_{L-1}), \right. \\
&\quad \left. T^v(\mathbf{Y}, \mathbf{0}_{L-1}) \rangle \right|^2 w_u w_v \\
&\leq \theta^2 \sum_{i, j=1}^N \sum_{\substack{\mathbf{X} \in \mathcal{C}_i \\ i \neq j}} \sum_{\mathbf{Y} \in \mathcal{C}_j} \sum_{u, v=0}^{2L-2} w_u w_v \\
&= \theta^2 K(K - M).
\end{aligned} \tag{20}$$

Combining (16), (19), and (20) gives

$$F(\mathcal{C}, \mathcal{C}) = \frac{S_1 + S_2}{K^2} \leq \frac{M^2 L^2}{K} \sum_{u=0}^{2L-2} w_u^2 + \theta^2 \left(1 - \frac{M}{K}\right). \tag{21}$$

From Lemma 1 and (21) it follows that

$$\begin{aligned}
&\frac{M^2 L^2}{K} \sum_{u=0}^{2L-2} w_u^2 + \theta^2 \left(1 - \frac{M}{K}\right) \\
&\geq \sum_{u, v=0}^{2L-2} M(L - \tau_{u, v, L}) w_u w_v \\
&= ML - M \sum_{u, v=0}^{2L-2} \tau_{u, v, L} w_u w_v.
\end{aligned}$$

Therefore, we have

$$\theta^2 \geq \frac{ML - \frac{M^2 L^2}{K} \sum_{u=0}^{2L-2} w_u^2 - M \sum_{u, v=0}^{2L-2} \tau_{u, v, L} w_u w_v}{1 - \frac{M}{K}}. \tag{22}$$

The desired conclusion directly follows from the definition of  $Q(\mathbf{w}, a)$  in (15).  $\blacksquare$

Theorem 1 shows that the maximum correlation magnitude of  $\mathcal{C} = \cup_{i=1}^N \mathcal{C}_i$  heavily depends on the weight vector  $\mathbf{w}$ . In order to obtain tighter correlation lower bound for  $\theta$ , our task now is to choose suitable weight vectors in (22). We start with the weight vector  $\mathbf{w}$  from step functions.

**Corollary 1.** Suppose the weight vector  $\mathbf{w} = (w_0, w_1, \dots, w_{2L-2})$  is given by

$$w_j = \begin{cases} \frac{1}{t}, & j = 0, 1, \dots, t-1, \\ 0, & j = t, t+1, \dots, 2L-2, \end{cases} \tag{23}$$

where  $0 < t \leq 2L-1$ . Assume that  $L \geq N$ . Then the lower bounds for  $\theta$  are given as follows:

- when  $N = 2, 3$ ,

$$\theta^2 \geq ML \frac{L}{2L-1}, \tag{24}$$

- when  $N \geq 4$ ,

$$\theta^2 \geq ML \left(1 - \frac{2\sqrt{3L^2 N - N^2 - 3L}}{3L(N-1)}\right). \tag{25}$$

*Proof:* As the full proof is lengthy, it is placed in Appendix A. Here we only provide the sketch of the proof. With weight vector  $\mathbf{w}$  given by (23), in the calculation of (22) we need to consider two cases:  $0 < t \leq L$  and  $L+1 \leq t \leq 2L-1$ .

*Case 1:*  $0 < t \leq L$ . In this case,

$$\sum_{u, v=0}^{t-1} \tau_{u, v, L} = \sum_{u=0}^{t-1} \frac{u(u+1)}{2} + \sum_{u=0}^{t-1} \frac{(t-u-1)(t-u)}{2} = \frac{t(t^2-1)}{3}.$$

Substituting the above equality into (22), we obtain

$$\theta^2 \geq \frac{ML}{1 - \frac{M}{K}} \left(1 - \frac{1}{3L} \left(t + \frac{3ML^2 - K}{Kt}\right)\right). \tag{26}$$

We then need to find the value of  $t$  that gives the maximum lower bound. For different choices of  $K/M = N$ , we obtain the following results:

- For  $N = 2, 3$ , the maximum value of the lower bounds in (26) is attained at  $t = L$ , implying

$$\theta^2 \geq \frac{ML}{1 - M/K} \left(\frac{2}{3} - \frac{M}{K} + \frac{1}{3L^2}\right). \tag{27}$$

- For  $N > 3$ , the maximum value of the lower bounds is achieved at  $t = \left\lceil \sqrt{\frac{3L^2}{N} - 1} \right\rceil \in [1, L]$ , and we have the following simplified lower bound:

$$\theta^2 \geq ML \left(1 - \frac{2\sqrt{N(3L^2 - N)} - 3L}{3L(N-1)}\right). \tag{28}$$

*Case 2:*  $L < t \leq 2L-1$ . In this case, we obtain

$$\begin{aligned}
\sum_{u, v=0}^{t-1} \tau_{u, v, L} &= (t+1)(t-L)(L-1) \\
&\quad + (3Lt^2 - t^3 - 3L^2 t + t + 2L^3 - 2L)/3.
\end{aligned} \tag{29}$$

From (22) and (29), we have

$$\theta^2 \geq \frac{M}{3(1-M/K)} \left( t + \frac{a}{t} - \frac{b}{t^2} - 3(L-1) \right), \quad (30)$$

where

$$\begin{aligned} a &= (6L^2 - 6L + 2) - 3ML^2/K, \text{ and} \\ b &= L(L-1)(2L-1). \end{aligned} \quad (31)$$

To find the maximum lower bound, we analyze the function  $f(x) = t + \frac{a}{x} - \frac{b}{x^2}$  over the interval  $[L+1, 2L-1]$ , where we consider both the 1st-order and 2nd-order derivatives. For the different choices of  $N$ , we have the following results:

- when  $N = 2, 3$ , the maximum lower bound is achieved at  $t = 2L - 1$ , implying

$$\theta^2 \geq \frac{ML^2}{2L-1},$$

- when  $N > 3$ , the maximum lower bound is achieved at  $t = L + 1$ , implying

$$\theta^2 \geq ML \left( 1 - \frac{(N+6)L^3 + 3(N-1)L^2 + (2N-3)L - 6N}{3L(L+1)^2(N-1)} \right). \quad (32)$$

Comparing the bounds as derived in Case 1 and Case 2, we reach the desired results. ■

In Remark 1, we compare the correlation lower bounds derived in Corollary 1 with that of bound reported in [15].

**Remark 1.** From [15], the lower-bound on  $\theta$  is given by

$$\theta^2 \geq ML \left( 1 - \frac{2}{\sqrt{3N}} \right), \quad (33)$$

where  $N = K/M \geq 3$ . For  $N = 3$ , it can easily be verified that the derived lower bound in Corollary 1 is tighter than the bound in (33). For  $N > 3$ , we have

$$\frac{\left( \frac{2\sqrt{3L^2N - N^2 - 3L}}{3L(N-1)} \right)}{\frac{2}{\sqrt{3N}}} \leq \frac{\sqrt{N} - \sqrt{3}}{\sqrt{N} - \frac{1}{\sqrt{N}}} < 1. \quad (34)$$

From (25), (33), and (34), it is clear that our derived lower bound on  $\theta$  in Corollary 1 is tighter than the lower bound in [15].

Although we already have a tighter lower bound on  $\theta$  with respect to the weight vector in (23), another weight vector, termed *positive-cycle-of-a-sine-wave* weight vector in [30], may yield a tighter lower bound. Below, we present another corollary to derive the proposed bound of *Theorem 1* with respect to the positive-cycle-of-a-sine-wave weight vector.

Table V: Value of  $\varphi(x)$  at  $x = 2, 3$ , and 4

$x$	2	3	4
$\varphi(x)$	$1 - \frac{L}{N}$	$1 - \frac{L}{2N} - \frac{1}{2L}$	$1 - \frac{429L}{1250N} - \frac{2071}{2500L}$

**Corollary 2.** The positive-cycle-of-a-sine-wave weight vector is given by

$$w_j = \begin{cases} \tan \frac{\pi}{2t} \sin \frac{\pi j}{t}, & j \in \{0, 1, \dots, t-1\}, \\ 0, & j \in \{t, t+1, 2L-2\}, \end{cases}$$

where  $1 < t \leq L$ . Assume  $L \geq N$ . Then the lower bounds for  $\theta$  are given as follows:

- when  $2 \leq L \leq 4$ ,

$$\theta^2 \geq \frac{ML}{N-1} \left( \frac{N}{4} \left( 3 + \tan^2 \frac{\pi}{2L} \right) - \frac{L^2}{2} \tan^2 \frac{\pi}{2L} \right),$$

- when  $L \geq 5$  and  $N = 2, 3, 4$ ,

$$\theta^2 \geq ML \left( 1 - \frac{L^2(2\pi^2 + 4N - 16) - N\pi^2}{16L^2(N-1)} \right),$$

- when  $L \geq 5$  and  $N \geq 5$ ,

$$\theta^2 \geq ML \left( 1 - \frac{\pi\sqrt{N(2L^2 - N)} - 4L}{4(N-1)L} \right).$$

*Proof:* We have the following results from [30]:

$$\sum_{u=0}^{2L-2} w_u^2 = \frac{t}{2} \tan^2 \frac{\pi}{2t}. \quad (35)$$

For  $2 \leq t \leq L$ ,

$$\sum_{u,v=0}^{t-1} \tau_{u,v,L} w_u w_v = \frac{t}{4} \left( 1 - \tan^2 \frac{\pi}{2t} \right). \quad (36)$$

From (22), (35), and (36), we have

$$\theta^2 \geq \frac{ML \left( 1 - \frac{t}{4L} \left( 1 + \frac{2L^2 - N}{N} \tan^2 \frac{\pi}{2t} \right) \right)}{1 - \frac{1}{N}}. \quad (37)$$

Assume  $\varphi(x) = 1 - \frac{x}{4L} \left( 1 + \frac{2L^2 - N}{N} \tan^2 \frac{\pi}{2x} \right)$ . We shall find the maximum value of  $\varphi(x)$  in  $[2 : L]$ . Note that for  $x \geq 5$ , the function  $\tan^2 \frac{\pi}{2x}$  can be approximated as  $\left( \frac{\pi}{2x} \right)^2$  since their difference is roughly 0.0987 at  $x = 5$  and becomes smaller for as  $x$  increases. In order to find the maximum value of  $\varphi(x)$  in  $[2 : L]$ , we divide the derivation in the following two cases:  $L \leq 4$  and  $L \geq 5$ .

**Case 1** ( $L \leq 4$ ). In this case, we need to determine the maximum value of  $\varphi(x)$  within the interval  $[2 : L]$ . This can be easily determined since  $L \leq 4$  and  $x$  can only take on  $L - 1$  values 2, 3, and  $L$ . Table V lists the values  $\varphi(x)$  for  $x = 2, 3, 4$ , where  $N \leq L$ . It can be easily verified that  $\varphi(2) \leq \varphi(3) \leq \varphi(4)$ , indicating that the function  $\varphi(x)$  at

$[2 : L]$  achieves its maximum value at  $x = L$ . Therefore, we can express the maximum as follows: ■

$$\max_{x \in [2, L]} \varphi(x) = \varphi(L) = \frac{1}{4} \left( 3 + \tan^2 \frac{\pi}{2L} \right) - \frac{L^2}{2N} \tan^2 \frac{\pi}{2L}$$

**Case 2** ( $L \geq 5$ ). In this case, we consider the integer interval  $[2 : L] = [2 : 4] \cup [5 : L]$ , indicating

$$\max_{x \in [2: L]} \varphi(x) = \max \left\{ \max_{x \in [2: 4]} \varphi(x), \max_{x \in [5: L]} \varphi(x) \right\}. \quad (38)$$

For the integer interval  $[2 : 4]$ , since  $\varphi(4) \geq \varphi(3) \geq \varphi(2)$ , we have

$$\max_{x \in [2: 4]} \varphi(x) = \varphi(4) = 1 - \frac{429L}{1250N} - \frac{2071}{2500L}.$$

Next we find maximum of  $\varphi(x)$  over the integer interval  $[5 : L]$ . To this end, we will consider it over the interval  $[5, L]$  instead. As discussed in the beginning, we have  $\tan^2 \frac{\pi}{2x} \approx \frac{\pi^2}{4x^2}$  for  $x \in [5, L]$ , thereby we approximate  $\varphi(x)$  as

$$\varphi(x) = 1 - \frac{1}{4L} \left( x + \frac{\pi^2(2L^2 - N)}{4xN} \right).$$

The derivative function  $\varphi'(x)$  has two zeros  $x_0 = \frac{\pi}{2} \sqrt{\frac{2L^2 - N}{N}}$ , and  $-x_0$ . Note that  $x_0$  lies in  $[5, L]$  if  $L \geq N \geq 5$  and  $x_0 \geq L$  otherwise. When  $L \geq N \geq 5$ ,  $\varphi'(x) > 0$  for  $x \in [5, x_0)$  and  $\varphi'(x) < 0$  for  $x \in [x_0, L)$ , this implies that  $\varphi(x)$  is monotonically increasing over  $[5, x_0]$  and monotonically decreasing over  $[x_0, L)$ . Hence  $f$  attains maximum value at  $x = x_0$ , when  $N \geq 5$ . When  $N \leq 4$ , the function  $f$  is monotonically increasing over  $[5, L]$  and therefore attains maximum value at  $x = L$ . Furthermore, we can easily verify that  $\varphi(L) \geq \varphi(4)$  when  $N \leq 4$  and  $\varphi(x_0) \geq \varphi(4)$  when  $N \geq 5$ . That is to say, in Case 2 the function  $\varphi(x)$  achieves its maximum value at  $x = L$  when  $N \leq 4$  and at  $x = x_0$  when  $N \geq 5$ .

Combining the two cases, we have the following simplified lower bounds for  $2 \leq t \leq L$ :

- when  $2 \leq L \leq 4$ , the lower bound in (37) is given by

$$\theta^2 \geq \frac{ML}{N-1} \left( \frac{N}{4} \left( 3 + \tan^2 \frac{\pi}{2L} \right) - \frac{L^2}{2} \tan^2 \frac{\pi}{2L} \right), \quad (39)$$

- when  $L \geq 5$  and  $N \leq 4$ , the maximum lower bound in (37) is approximately given by

$$\theta^2 \geq ML \left( 1 - \frac{L^2(2\pi^2 + 4N - 16) - N\pi^2}{16L^2(N-1)} \right), \quad (40)$$

- when  $L \geq N \geq 5$ , by properly choosing  $t$  around  $x_0$ , we obtain the maximum lower bound in (37) and it is approximately given by

$$\theta^2 \geq ML \left( 1 - \frac{\pi \sqrt{N(2L^2 - N)} - 4L}{4(N-1)L} \right). \quad (41)$$

**Remark 2.** This remark compares the lower bounds derived in Corollary 1 and Corollary 2. We start with the case of  $L \leq 4$ . In this case we have

- for  $N = 2, 3$  and  $N \leq L$ , the lower bound in (24) is tighter than the lower bound in (39),
- for  $N = L = 4$ , the bound in (39) is tighter than that of the lower bound in (25).

Now we compare the bounds for  $L \geq 5$ . According to the bounds in (24) and (40), it suffices to consider the sign of

$$\frac{L-1}{2L-1} - \frac{L^2(2\pi^2 + 4N - 16) - N\pi^2}{16L^2(N-1)}.$$

A routine calculation indicates that

- for  $N = 2$ , the lower bound in (24) is tighter than that in (40),
- for  $N = 3$ , the lower bound in (24) is tighter than that in (40) for  $5 \leq L \leq 25$ , and for  $L > 25$ , the lower bound in (40) is tighter.
- for  $N = 4$ , the the lower bound in (40) is tighter than that in (25) for  $L \geq 5$ ,
- for  $L \geq N \geq 5$ , the tighter bound is given by (41), which is, according to (25) and (41), determined by

$$\begin{aligned} & \frac{2\sqrt{3L^2N - N^2} - 3L}{3L(N-1)} \cdot \frac{4(N-1)L}{\pi\sqrt{N(2L^2 - N)} - 4L} \\ &= \frac{\sqrt{192L^2N - 64N^2} - 12L}{\sqrt{18\pi^2L^2N - 9\pi^2N^2} - 12L} > 1. \end{aligned}$$

In Appendix D, we discuss correlation lower bound for the positive-cycle-of-a-sine-wave when  $L+1 \leq t \leq 2L-1$ , for which the analysis is lengthy. We also compare the result with Remark 2 based on the asymptotic behaviour of the lower bounds.

Finally we summarize the newly derived tighter lower bounds below.

**Remark 3.** For a  $(K, M, L, \theta)$ -QCSS as a collection of  $N \geq 2$  different  $(M, L)$  CCCs, where the sequence length  $L \geq N$ , the lower bounds on the maximum aperiodic correlation magnitude  $\theta$  are improved as follows:

$$\theta^2 \geq \begin{cases} ML \left( 1 - \frac{L-1}{2L-1} \right), & N = 2 \text{ or } N = 3, \\ & N \leq L \leq 25, \\ ML \left( 1 - \frac{L^2(2\pi^2 + 4N - 16) - N\pi^2}{16L^2(N-1)} \right), & N = 3, L > 25 \\ & \text{or } N = 4, L \geq 5, \\ ML \left( 1 - \frac{L-1.2}{2L-1} \right), & N = L = 4, \\ ML \left( 1 - \frac{\pi \sqrt{N(2L^2 - N)} - 4L}{4(N-1)L} \right), & L \geq N \geq 5, \end{cases}$$

where the bound for  $N = L = 4$  is transformed for a more direct comparison. Furthermore, for sufficiently large  $L$ , the lower bounds may be roughly given as follows:

$$\theta^2 \geq \begin{cases} ML/2, & N = 2, \\ ML(1 - \frac{1}{4(N-1)}), & N = 3, 4, \\ ML(1 - \frac{\pi\sqrt{2N-4}}{4(N-1)}), & N \geq 5. \end{cases}$$

#### IV. CONSTRUCTION OF ASYMPTOTICALLY OPTIMAL QCSSs COMPRISED OF CCCs

In this section, we shall first present a construction of CCCs using  $q$ -ary functions, and then we will show that the collection of those CCCs forms asymptotically optimal QCSSs with respect to the correlation lower bounds derived in the previous section.

We first introduce the  $q$ -ary functions which will be used in our construction. For a subset  $J = \{j_0, \dots, j_{n-1}\} \subset \mathbb{Z}_m$  with  $n \leq m-1$ , consider an  $m$ -variable  $q$ -ary function  $f : \mathbb{Z}_p^m \rightarrow \mathbb{Z}_q$  such that for each  $\mathbf{c} \in \mathbb{Z}_p^n$ , the graph  $G(f|_{\mathbf{x}_J=\mathbf{c}})$  is a Hamiltonian path with edges having identical weight  $q/p$ . For the case of  $m = n+1$ ,  $f|_{\mathbf{x}_J=\mathbf{c}}$  is a linear function of one variable, which forms a simplest Hamiltonian path. For  $m > n+1$ , the function  $f|_{\mathbf{x}_J=\mathbf{c}}$  can be algebraically expressed as

$$f|_{\mathbf{x}_J=\mathbf{c}} = \frac{q}{p} \sum_{\alpha=0}^{m-n-2} x_{l_{\pi(\alpha)}} x_{l_{\pi(\alpha+1)}} + \sum_{\alpha=0}^{m-n-1} c_{l_\alpha} x_{l_\alpha} + c, \quad (42)$$

where  $\{l_0, \dots, l_{m-n-1}\} = \mathbb{Z}_m \setminus \{j_0, \dots, j_{n-1}\}$ ,  $\pi$  is a permutation on  $\mathbb{Z}_{m-n}$ , and  $c_{l_0}, c_{l_1}, \dots, c_{l_{m-n-1}}$ , and  $c \in \mathbb{Z}_q$ .

Let  $k$  be an integer such that  $1 \leq k < p$ . For an integer  $t$  with  $0 \leq t < p^{n+1}$ , denote its vector representation w.r.t base- $p$  as  $(\mathbf{t}, t_n) \in \mathbb{Z}_p^{n+1}$ . Let us define the following set of  $q$ -ary functions:

$$\mathcal{C}_t^k = \left\{ f_{d,t} = f + \frac{kq}{p} (\mathbf{d} \cdot \mathbf{x}_J + d_n x_{l_{\pi(0)}}) + \frac{q}{p} (\mathbf{t} \cdot \mathbf{x}_J + t_n x_{l_{\pi(m-n-1)}}) : 0 \leq d < p^{n+1} \right\}, \quad (43)$$

where  $(\mathbf{d}, d_n) = (d_0, d_1, \dots, d_n) \in \mathbb{Z}_p^{n+1}$  is the vector representation of the integer  $d$ . Then we can define a code as  $\psi(C_t^k) = \{\psi(f_{d,t}) | f_{d,t} \in C_t^k\}$  and thereby a set of codes as follows:

$$\mathcal{C}_k = \{\psi(C_t^k) | 0 \leq t < p^{n+1}\}. \quad (44)$$

The following theorem characterizes the correlation properties of the code sets  $\mathcal{C}_k$ .

**Theorem 2.** *Let  $f$  be a  $q$ -ary function as characterized in (42). Then, the code set  $\mathcal{C}_k$  defined in (44) is a  $(p^{n+1}, p^m)$ -CCC over  $\mathcal{A}_q$  for any integer  $k$  with  $1 \leq k < p$ .*

*Proof:* As the full proof is lengthy, here we only provide a sketch of the proof and the full proof can be found in Appendix B.

According to the definition of  $\mathcal{C}_k$ , we represent each set of  $q$ -ary functions  $C_t^k$  given in (43) as follows:  $C_t^k = \{f_{d,t} : 0 \leq d < p^{n+1}\}$ , where

$$\begin{aligned} f_{d,t} &= f + \frac{q}{p} (kd_n x_{l_{\pi(0)}} + t_n x_{l_{\pi(m-n-1)}}) + \frac{q}{p} (k\mathbf{d} + \mathbf{t}) \cdot \mathbf{x}_J \\ &= f_{d_n, t_n} + \frac{q}{p} (k\mathbf{d} + \mathbf{t}) \cdot \mathbf{x}_J. \end{aligned} \quad (45)$$

Let  $\tau$  be an integer satisfying  $0 \leq |\tau| < p^m$ . The ACCF between two codes  $\psi(C_t^k)$  and  $\psi(C_{t'}^k)$  in  $\mathcal{C}_k$  at the time shift  $\tau$  can be expressed as

$$\begin{aligned} &\Theta(\psi(C_t^k), \psi(C_{t'}^k))(\tau) \\ &= \sum_{d=0}^{p^{n+1}-1} \sum_{\mathbf{c}_1, \mathbf{c}_2 \in \mathbb{Z}_p^n} \Theta(\psi(f_{d,t}|_{\mathbf{x}_J=\mathbf{c}_1}), \psi(f_{d,t'}|_{\mathbf{x}_J=\mathbf{c}_2}))(\tau) \\ &= \mathcal{S}_1 + \mathcal{S}_2, \end{aligned} \quad (46)$$

where

$$\mathcal{S}_1 = \sum_{d=0}^{p^{n+1}-1} \sum_{\mathbf{c}_1=\mathbf{c}_2} \Theta(\psi(f_{d,t}|_{\mathbf{x}_J=\mathbf{c}_1}), \psi(f_{d,t'}|_{\mathbf{x}_J=\mathbf{c}_2}))(\tau),$$

and

$$\mathcal{S}_2 = \sum_{d=0}^{p^{n+1}-1} \sum_{\mathbf{c}_1 \neq \mathbf{c}_2} \Theta(\psi(f_{d,t}|_{\mathbf{x}_J=\mathbf{c}_1}), \psi(f_{d,t'}|_{\mathbf{x}_J=\mathbf{c}_2}))(\tau).$$

A routine calculation shows that  $\mathcal{S}_2 = 0$ . The calculation of  $\mathcal{S}_1$  is more complicated. Assume  $\mathbf{c}_1 = \mathbf{c}_2 = \mathbf{c} \in \mathbb{Z}_p^n$ . Then we have

$$\begin{aligned} \mathcal{S}_1 &= \sum_{d=0}^{p^{n+1}-1} \sum_{\mathbf{c} \in \mathbb{Z}_p^n} \Theta(\psi(f_{d,t}|_{\mathbf{x}_J=\mathbf{c}}), \psi(f_{d,t'}|_{\mathbf{x}_J=\mathbf{c}}))(\tau) \\ &= \sum_{(\mathbf{d}, d_n) \in \mathbb{Z}_p^{n+1}} \sum_{\mathbf{c}} \Theta(\psi(f_{d,t}|_{\mathbf{x}_J=\mathbf{c}}), \psi(f_{d,t'}|_{\mathbf{x}_J=\mathbf{c}}))(\tau) \\ &= p^n \sum_{\mathbf{c}} \xi_p^{(\mathbf{t}-\mathbf{t}') \cdot \mathbf{c}} \mathcal{S}_3, \end{aligned} \quad (47)$$

where

$$\mathcal{S}_3 = \sum_{d_n} \Theta(\psi(f_{d_n, t_n}|_{\mathbf{x}_J=\mathbf{c}}), \psi(f_{d_n, t'_n}|_{\mathbf{x}_J=\mathbf{c}}))(\tau).$$

In Appendix B, we consider the calculation of  $\mathcal{S}_3$  in three cases and obtain

$$\mathcal{S}_3 = \begin{cases} p^{m-n+1}, & \tau = 0, t_n = t'_n, \\ 0, & \tau = 0, t_n \neq t'_n, \\ 0, & \tau \neq 0. \end{cases}$$

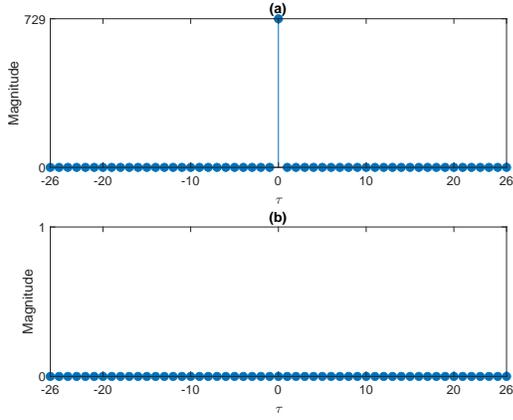


Figure 2: Correlation plot for  $C_k$

The above result, combined with (46), (47) and  $\mathcal{S}_2 = 0$ , implies that

$$\Theta(\psi(C_t^k), \psi(C_{t'}^k))(\tau) = \begin{cases} p^{m+n+1}, & \tau = 0, t = t', \\ 0, & \text{otherwise.} \end{cases}$$

Therefore,  $C_k$  forms a  $(p^{n+1}, p^m)$ -CCC for any choice of  $k$  in  $\{1, 2, \dots, p-1\}$ . ■

The following example illustrates the CCCs constructed in Theorem 2.

**Example 2.** For  $m = 3$ ,  $p = 3$ , and  $q = 6$ , let us consider the following function:

$$f(x_0, x_1, x_2) = x_0x_2 + 2x_2x_1 + x_1x_0 + x_0 + 2x_1 + x_2 + 1.$$

Taking  $J = \{0, 1\}$ , from (43), we construct the following set of 6-ary functions:

$$C_t^k = \{f + 2k(d_0x_0 + d_1x_1 + d_2x_2) + 2(t_0x_0 + t_1x_1 + t_2x_2) : d \in \mathbb{Z}_3^3\}, \quad (45)$$

where  $1 \leq k < 3$ ,  $(t_0, t_1, t_2) \in \mathbb{Z}_3^3$  corresponds to integers  $t = 0, 1, \dots, 26$ , and  $(d_0, d_1, d_2)$  corresponds to integers  $d = 0, 1, \dots, 26$ . Following (44), we obtain  $C_k$ ,  $k = 1, 2$ , as below:

$$C_k = \{\psi(C_t^k) : 0 \leq t < 27\} = \{\psi(C_0^k), \psi(C_1^k), \dots, \psi(C_{26}^k)\}. \quad (46)$$

From (46), it is clear that both  $C_1$  and  $C_2$  contain 27 codes of length 27 over  $\mathcal{A}_6$ . In Table VI, we present the function sets for generating codes in  $C_1$  and  $C_2$ . Besides, in Appendix ??, we list the codes  $\psi(C_0^1)$ ,  $\psi(C_1^1)$ , and  $\psi(C_2^1)$  from  $C_1$  in Table VII, and  $\psi(C_0^2)$ ,  $\psi(C_1^2)$ , and  $\psi(C_2^2)$  from  $C_2$  in Table VIII. In addition, as shown in Figure 2, the AACF and ACCF of the codes in  $C_k$  are ideal. Hence  $C_k$  forms a  $(27, 27)$ -CCC for  $k = 1, 2$ , which is consistent with Theorem 2.

According to Theorem 2, the sets  $C_1, C_2, \dots, C_{p-1}$  are  $(p^{n+1}, p^m)$ -CCCs over  $\mathcal{A}_q$ . In the sequel, we will show that the maximum aperiodic cross-correlation magnitude between two codes from any two distinct CCCs among  $C_1, C_2, \dots, C_{p-1}$  is upper bounded by  $p^m$ . To this end, we need the following proposition.

**Proposition 1.** Let  $g$  and  $h$  be two  $q$ -ary functions from  $\mathbb{Z}_p^m$  to  $\mathbb{Z}_q$ . For any two different integers  $1 \leq k_1, k_2 < p$ , define a set  $\mathcal{S}$  as

$$\mathcal{S} = \{(\mathbf{e}_1, \mathbf{e}_2) : \mathbf{e}_1, \mathbf{e}_2 \in \mathbb{Z}_p^w, k_1\mathbf{e}_1 - k_2\mathbf{e}_2 \equiv \mathbf{0}_w \pmod{p}\}.$$

Then for  $J_1 = \mathbb{Z}_w$  with  $w < m$  and  $\mathbf{x}_{J_1} = (x_0, x_1, \dots, x_{w-1})$ , we have

$$\left| \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \right| \leq p^{m-w}.$$

*Proof:* The full proof is lengthy, so here we only provide important steps of the proof. The details of the full proof can be found in Appendix C.

Let us define a mapping  $\Lambda : \mathcal{S} \rightarrow \mathbb{Z}$  as follows:

$$\Lambda(\mathbf{e}_1, \mathbf{e}_2) = \sum_{t=0}^{w-1} e_{2,t}p^{w-1-t} - \sum_{t=0}^{w-1} e_{1,t}p^{w-1-t}.$$

It can be shown that the above mapping is injective. Define two sets

$$\mathcal{S}' = \{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S} : \Lambda(\mathbf{e}_1, \mathbf{e}_2) \geq 0\} \text{ and}$$

$$\mathcal{S}'' = \{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S} : \Lambda(\mathbf{e}_1, \mathbf{e}_2) \leq 0\}.$$

Clearly they satisfy the following properties:

$$\mathcal{S} = \mathcal{S}' \cup \mathcal{S}'', \text{ and } \mathcal{S}' \cap \mathcal{S}'' = \{(\mathbf{0}_w, \mathbf{0}_w)\},$$

implying  $|\mathcal{S}'| = |\mathcal{S}''| = \frac{p^{w+1}}{2} = E$  since  $|\mathcal{S}| = p^w$ .

Assume that  $(\mathbf{e}_1^i, \mathbf{e}_2^i)$  is an element of  $\mathcal{S}'$  and  $\Lambda(\mathbf{e}_1^i, \mathbf{e}_2^i) = D_i$ , where  $\mathbf{e}_j^i = (e_{j,0}^i, e_{j,1}^i, \dots, e_{j,n-1}^i)$ ,  $i = 1, 2, \dots, E$ , and  $j = 1, 2$ . Since,  $(\mathbf{0}_w, \mathbf{0}_w) \in \mathcal{S}'$  and  $\Lambda$  is an injective mapping, without loss of generality, we can assume that  $0 = D_1 < D_2 < \dots < D_E$ . For  $0 \leq \tau \leq p^m - 1$ , following (9), we have

$$\mathbf{B}_\tau(\mathbf{e}_1^i, \mathbf{e}_2^i) = \{(\gamma, \delta) : \delta = \gamma + \tau, 0 \leq \gamma \leq p^m - \tau - 1, \quad (48)$$

$$\gamma_\alpha = e_{1,\alpha}^i, \delta_\alpha = e_{2,\alpha}^i, 0 \leq \alpha < w\},$$

where  $(\gamma_0, \gamma_1, \dots, \gamma_{m-1})$  and  $(\delta_0, \delta_1, \dots, \delta_{m-1})$  are the base- $p$  vector representations of the non-negative integers  $\gamma$  and  $\delta$ , respectively. Denote  $I_{D_i} = [p^{m-w}(D_i - 1) + 1 : p^{m-w}(D_i + 1) - 1]$ . Then the set  $\mathbf{B}_\tau(\mathbf{e}_1^i, \mathbf{e}_2^i)$  is non-empty if  $\tau$  is taken from  $I_{D_i}$ . In addition, it can be shown that for  $1 \leq i_1 < i_2 \leq E$ ,  $I_{D_{i_1}} \cap I_{D_{i_2}} \neq \emptyset$  iff  $D_{i_2} = D_{i_1} + 1$ .

For a fixed value of  $\tau$  in  $[0 : p^m - 1]$ , we need to consider the following three cases:

Table VI: Sets  $C_t^k$  for the (27, 27)-CCCs  $\mathcal{C}_1$  and  $\mathcal{C}_2$ 

$\mathcal{C}_1$	$\mathcal{C}_2$
$C_0^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) : 0 \leq d < 27\}$	$C_0^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) : 0 \leq d < 27\}$
$C_1^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2x_2 : 0 \leq d < 27\}$	$C_1^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2x_2 : 0 \leq d < 27\}$
$C_2^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 4x_2 : 0 \leq d < 27\}$	$C_2^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 4x_2 : 0 \leq d < 27\}$
$C_3^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2x_1 : 0 \leq d < 27\}$	$C_3^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2x_1 : 0 \leq d < 27\}$
$C_4^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_1 + x_2) : 0 \leq d < 27\}$	$C_4^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_1 + x_2) : 0 \leq d < 27\}$
$C_5^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_0 + 2x_2) : 0 \leq d < 27\}$	$C_5^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_0 + 2x_2) : 0 \leq d < 27\}$
$C_6^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 4x_1 : 0 \leq d < 27\}$	$C_6^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 4x_1 : 0 \leq d < 27\}$
$C_7^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_1 + x_2) : 0 \leq d < 27\}$	$C_7^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_1 + x_2) : 0 \leq d < 27\}$
$C_8^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_1 + 2x_2) : 0 \leq d < 27\}$	$C_8^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_1 + 2x_2) : 0 \leq d < 27\}$
$C_9^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2x_0 : 0 \leq d < 27\}$	$C_9^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2x_0 : 0 \leq d < 27\}$
$C_{10}^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_0 + x_2) : 0 \leq d < 27\}$	$C_{10}^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_0 + x_2) : 0 \leq d < 27\}$
$C_{11}^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_0 + 2x_2) : 0 \leq d < 27\}$	$C_{11}^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_0 + 2x_2) : 0 \leq d < 27\}$
$C_{12}^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_0 + x_1) : 0 \leq d < 27\}$	$C_{12}^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_0 + x_1) : 0 \leq d < 27\}$
$C_{13}^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_0 + x_1 + x_2) : 0 \leq d < 27\}$	$C_{13}^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_0 + x_1 + x_2) : 0 \leq d < 27\}$
$C_{14}^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_0 + x_1 + 2x_2) : 0 \leq d < 27\}$	$C_{14}^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_0 + x_1 + 2x_2) : 0 \leq d < 27\}$
$C_{15}^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_0 + 2x_1) : 0 \leq d < 27\}$	$C_{15}^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_0 + 2x_1) : 0 \leq d < 27\}$
$C_{16}^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_0 + 2x_1 + x_2) : 0 \leq d < 27\}$	$C_{16}^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_0 + 2x_1 + x_2) : 0 \leq d < 27\}$
$C_{17}^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_0 + 2x_1 + 2x_2) : 0 \leq d < 27\}$	$C_{17}^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(x_0 + 2x_1 + 2x_2) : 0 \leq d < 27\}$
$C_{18}^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 4x_0 : 0 \leq d < 27\}$	$C_{18}^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 4x_0 : 0 \leq d < 27\}$
$C_{19}^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_0 + x_2) : 0 \leq d < 27\}$	$C_{19}^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_0 + x_2) : 0 \leq d < 27\}$
$C_{20}^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_0 + 2x_2) : 0 \leq d < 27\}$	$C_{20}^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_0 + 2x_2) : 0 \leq d < 27\}$
$C_{21}^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_0 + x_1) : 0 \leq d < 27\}$	$C_{21}^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_0 + x_1) : 0 \leq d < 27\}$
$C_{22}^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_0 + x_1 + x_2) : 0 \leq d < 27\}$	$C_{22}^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_0 + x_1 + x_2) : 0 \leq d < 27\}$
$C_{23}^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_0 + x_1 + 2x_2) : 0 \leq d < 27\}$	$C_{23}^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_0 + x_1 + 2x_2) : 0 \leq d < 27\}$
$C_{24}^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_0 + 2x_1) : 0 \leq d < 27\}$	$C_{24}^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_0 + 2x_1) : 0 \leq d < 27\}$
$C_{25}^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_0 + 2x_1 + x_2) : 0 \leq d < 27\}$	$C_{25}^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_0 + 2x_1 + x_2) : 0 \leq d < 27\}$
$C_{26}^1 = \{f + 2(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_0 + 2x_1 + 2x_2) : 0 \leq d < 27\}$	$C_{26}^2 = \{f + 4(d_0x_0 + d_1x_1 + d_2x_2) + 2(2x_0 + 2x_1 + 2x_2) : 0 \leq d < 27\}$

Case 1:  $\tau \notin \cup_{i=1}^E I_{D_i}$ . In this case, since  $\tau \geq 0$  and  $\mathbf{B}_\tau(\mathbf{e}_1^i, \mathbf{e}_2^i) = \emptyset$  for all  $i \in [1 : E]$ , we have

$$\sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) = 0.$$

Case 2:  $\tau \in I_{D_i}$  and  $\tau \notin I_{D_j}$  for all  $i \neq j$  in  $[1 : E]$ . In this case, since  $\tau$  does not belong to any  $I_{D_j}$ , we have  $\mathbf{B}_\tau(\mathbf{e}_1^j, \mathbf{e}_2^j) = \emptyset$  for all  $j \in [1 : E] \setminus \{i\}$ . Partition the set  $I_{D_j}$  into two as  $I_{D_j}^{(1)} = \{v \in I_{D_j} : v \leq p^{m-w} D_i\}$  and  $I_{D_j}^{(2)} = \{v \in I_{D_j} : v > p^{m-w} D_i\}$ . Now  $\tau$  can be expressed as follows:

$$\tau = \begin{cases} p^{m-w}(D_i - 1) + \tau_1, & \text{if } \tau \in I_{D_i}^{(1)}, \\ p^{m-w} D_i + \tau_2, & \text{if } \tau \in I_{D_i}^{(2)}, \end{cases}$$

where  $\tau_1 = 1, 2, \dots, p^{m-n}$  and  $\tau_2 = 1, 2, \dots, p^{m-n} - 1$ . Then we have

$$|\mathbf{B}_\tau(\mathbf{e}_1^i, \mathbf{e}_2^i)| = \begin{cases} \tau_1, & \text{if } \tau \in I_{D_i}^{(1)}, \\ p^{m-w} - \tau_2, & \text{if } \tau \in I_{D_i}^{(2)}. \end{cases} \quad (49)$$

We can show that

$$\begin{aligned} & \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \\ &= \sum_{(\gamma, \delta) \in \mathbf{B}_\tau(\mathbf{e}_1^i, \mathbf{e}_2^i)} \xi_q^{g_\gamma - h_\delta}. \end{aligned} \quad (50)$$

From (49) and (50), we have

$$\begin{aligned} & \left| \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \right| \\ & \leq \begin{cases} \tau_1, & \text{if } \tau \in I_{D_i}^{(1)}, \\ p^{m-w} - \tau_2, & \text{if } \tau \in I_{D_i}^{(2)}, \end{cases} \end{aligned}$$

implying

$$\left| \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \right| \leq p^{m-w}.$$

Case 3:  $\tau \in I_{D_i} \cap I_{D_{i+1}}$  for some  $i \in \{1, 2, \dots, E\}$ , where  $D_{i+1} = D_i + 1$ . In this case we have

$$I_{D_i} \cap I_{D_{i+1}} = [p^{m-w} D_i + 1 : p^{m-w}(D_i + 1) - 1].$$

It can be observed that

$$\begin{aligned} & \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \\ &= \sum_{(\gamma, \delta) \in \mathbf{B}_\tau(\mathbf{e}_1^i, \mathbf{e}_2^i)} \xi_q^{g_\gamma - h_\delta} + \sum_{(\gamma, \delta) \in \mathbf{B}_\tau(\mathbf{e}_1^{i+1}, \mathbf{e}_2^{i+1})} \xi_q^{g_\gamma - h_\delta}. \end{aligned}$$

Note that  $\tau$  can be expressed as  $\tau = p^{m-w} D_i + \tau_3 = p^{m-w}(D_{i+1} - 1) + \tau_3$ , where  $\tau_3 = 1, 2, \dots, p^{m-w} - 1$ . There-

Table VII:  $\psi(C_0^1)$ ,  $\psi(C_1^1)$  and  $\psi(C_2^1)$  from (27, 27)-CCC  $\mathcal{C}_1$  over the alphabet  $\mathcal{A}_6$ , where  $\xi_6^i$  is given as  $i$  for simplicity

$\psi(C_0^1)$	$\psi(C_1^1)$	$\psi(C_2^1)$
123303543240531222303105501	141321501204555240321123525	105345525222513204345141543
141321501204555240321123525	105345525222513204345141543	123303543240531222303105501
105345525222513204345141543	123303543240531222303105501	141321501204555240321123525
123525321240153000303321345	141543345204111024321345303	105501303222135042345303321
141543345204111024321345303	105501303222135042345303321	123525321240153000303321345
105501303222135042345303321	123525321240153000303321345	141543345204111024321345303
123141105240315444303543123	141105123204333402321501141	105123141222351420345525105
141105123204333402321501141	105123141222351420345525105	123141105240315444303543123
105123141222351420345525105	123141105240315444303543123	141105123204333402321501141
123303543402153444141543345	141321501420111402105501303	105345525444135420123525321
141321501420111402105501303	105345525444135420123525321	123303543402153444141543345
105345525444135420123525321	123303543402153444141543345	141321501420111402105501303
123525321402315222141105123	141543345420333240105123141	105501303444351204123141105
141543345420333240105123141	105501303444351204123141105	123525321402315222141105123
105501303444351204123141105	123525321402315222141105123	141543345420333240105123141
123141105402531000141321501	141105123420555024105345525	105123141444513042123303543
141105123420555024105345525	105123141444513042123303543	123141105402531000141321501
105123141444513042123303543	123141105402531000141321501	141105123420555024105345525
123303543024315000525321123	141321501042333024543345141	105345525000351042501303105
141321501042333024543345141	105345525000351042501303105	123303543024315000525321123
105345525000351042501303105	123303543024315000525321123	141321501042333024543345141
123525321024531444525543501	141543345042555402543501525	105501303000513420501525543
141543345042555402543501525	105501303000513420501525543	123525321024531444525543501
105501303000513420501525543	123525321024531444525543501	141543345042555402543501525
123141105024153222525105345	141105123042111240543123303	105123141000135204501141321
141105123042111240543123303	105123141000135204501141321	123141105024153222525105345
105123141000135204501141321	123141105024153222525105345	141105123042111240543123303

fore,  $|\mathbf{B}_\tau(\mathbf{e}_1^i, \mathbf{e}_2^i)| = p^{m-w} - \tau_3$  and  $|\mathbf{B}_\tau(\mathbf{e}_1^{i+1}, \mathbf{e}_2^{i+1})| = \tau_3$ . have  $\mathbf{d} \cdot \mathbf{x}_J + d_n x_n = \mathbf{d}_1 \cdot \mathbf{x}_{J_1}$ . Setting Similarly to Case 2, we have

$$\left| \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \right| \leq (p^{m-w} - \tau_3) + \tau_3 = p^{m-w}. \quad (52)$$

$$g = f + \frac{q}{p} (\mathbf{t} \cdot \mathbf{x}_J + t_n x_{l_{\pi(m-n-1)}}),$$

$$h = f + \frac{q}{p} (\mathbf{t}' \cdot \mathbf{x}_J + t'_n x_{l_{\pi(m-n-1)}}).$$

One can express the ACCF sum between two codes  $\psi(C_t^{k_1}) \in \mathcal{C}_{k_1}$  and  $\psi(C_{t'}^{k_2}) \in \mathcal{C}_{k_2}$ , where  $k_1 \neq k_2$ , as

Combining Cases 1, 2, 3 gives

$$\left| \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \right| \leq p^{m-w}, \forall \tau \in [0 : p^m - 1]. \quad (51)$$

The statement for  $\tau \in [-(p^{m-w} - 1) : 0]$  can be similarly shown. ■

**Theorem 3.** Consider  $\mathcal{C}_1, \dots, \mathcal{C}_{p-1}$  given in Theorem 2. Then for  $J = \{0, \dots, n-1\}$  and  $l_{\pi(0)} = n$ , the union  $\cup_{k=1}^{p-1} \mathcal{C}_k$  forms a  $(p^{n+1}(p-1), p^{n+1}, p^m, p^m)$ -QCSS over  $\mathcal{A}_q$ .

*Proof:* Let  $f$  be the function as in (42). Take  $w = n+1$ ,  $J_1 = \{0, 1, \dots, n\} = J \cup \{n\}$  and  $\mathbf{d}_1 = (\mathbf{d}, d_n)$ . Then we

$$\Theta(\psi(C_t^{k_1}), \psi(C_{t'}^{k_2}))(\tau) = \sum_{\mathbf{d}_1} \Theta \left( \psi \left( g + \frac{k_1 q}{p} (\mathbf{d}_1 \cdot \mathbf{x}_{J_1}) \right), \psi \left( h + \frac{k_2 q}{p} (\mathbf{d}_1 \cdot \mathbf{x}_{J_1}) \right) \right) (\tau) = \sum_{\mathbf{d}_1} \sum_{\mathbf{e}_1, \mathbf{e}_2 \in \mathbb{Z}_p^{n+1}} \xi_q^{\frac{k_1 q}{p} \mathbf{d}_1 \mathbf{e}_1 + \frac{k_2 q}{p} \mathbf{d}_1 \mathbf{e}_2} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) = \sum_{\mathbf{d}_1} \sum_{\mathbf{e}_1, \mathbf{e}_2 \in \mathbb{Z}_p^{n+1}} \xi_p^{\mathbf{d}_1 \cdot (k_1 \mathbf{e}_1 - k_2 \mathbf{e}_2)} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \quad (53)$$

Table VIII:  $\psi(C_0^2)$ ,  $\psi(C_1^2)$  and  $\psi(C_2^2)$  from (27, 27)-CCC  $\mathcal{C}_2$  over the alphabet  $\mathcal{A}_6$ , where  $\xi_6^i$  is given as  $i$  for simplicity

$\psi(C_0^2)$	$\psi(C_1^2)$	$\psi(C_2^2)$
123303543240531222303105501	141321501204555240321123525	105345525222513204345141543
105345525222513204345141543	123303543240531222303105501	141321501204555240321123525
141321501204555240321123525	105345525222513204345141543	123303543240531222303105501
123141105240315444303543123	141105123204333402321501141	105123141222351420345525105
105123141222351420345525105	123141105240315444303543123	141105123204333402321501141
141105123204333402321501141	105123141222351420345525105	123141105240315444303543123
123525321240153000303321345	141543345204111024321345303	105501303222135042345303321
105501303222135042345303321	123525321240153000303321345	141543345204111024321345303
141543345204111024321345303	105501303222135042345303321	123525321240153000303321345
123303543024315000525321123	141321501042333024543345141	105345525000351042501303105
105345525000351042501303105	123303543024315000525321123	141321501042333024543345141
141321501042333024543345141	105345525000351042501303105	123303543024315000525321123
123141105024153222525105345	141105123042111240543123303	105123141000135204501141321
105123141000135204501141321	123141105024153222525105345	141105123042111240543123303
141105123042111240543123303	105123141000135204501141321	123141105024153222525105345
123525321024531444525543501	141543345042555402543501525	105501303000513420501525543
105501303000513420501525543	123525321024531444525543501	141543345042555402543501525
141543345042555402543501525	105501303000513420501525543	123525321024531444525543501
123303543402153444141543345	141321501420111402105501303	1053455254441354420123525321
105345525444135420123525321	123303543402153444141543345	141321501420111402105501303
141321501420111402105501303	105345525444135420123525321	123303543402153444141543345
123141105402531000141321501	141105123420555024105345525	105123141444513042123303543
105123141444513042123303543	123141105402531000141321501	141105123420555024105345525
141105123420555024105345525	105123141444513042123303543	123141105402531000141321501
123525321402315222141105123	141543345420333240105123141	105501303444351204123141105
105501303444351204123141105	123525321402315222141105123	141543345420333240105123141
141543345420333240105123141	105501303444351204123141105	123525321402315222141105123

$$= \sum_{\mathbf{e}_1, \mathbf{e}_2 \in \mathbb{Z}_p^{n+1}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \times \sum_{\mathbf{d}_1} \xi_p^{\mathbf{d}_1 \cdot (k_1 \mathbf{e}_1 - k_2 \mathbf{e}_2)}.$$

According to (53), we consider the following cases:

*Case 1:*  $k_1 \mathbf{e}_1 - k_2 \mathbf{e}_2 \not\equiv \mathbf{0}_{n+1} \pmod{p}$ . In this case, we have

$$\sum_{\mathbf{d}_1} \xi_p^{\mathbf{d}_1 \cdot (k_1 \mathbf{e}_1 - k_2 \mathbf{e}_2)} = 0,$$

which implies  $\Theta(\psi(C_t^{k_1}), \psi(C_{t'}^{k_2}))(\tau) = 0$ .

*Case 2:*  $k_1 \mathbf{e}_1 - k_2 \mathbf{e}_2 \equiv \mathbf{0}_{n+1} \pmod{p}$ . In this case we have

$$\sum_{\mathbf{d}_1} \xi_p^{\mathbf{d}_1 \cdot (k_1 \mathbf{e}_1 - k_2 \mathbf{e}_2)} = p^{n+1}.$$

Denote

$$\mathcal{S} = \{(\mathbf{e}_1, \mathbf{e}_2) : \mathbf{e}_1, \mathbf{e}_2 \in \mathbb{Z}^{n+1}, k_1 \mathbf{e}_1 - k_2 \mathbf{e}_2 \equiv \mathbf{0}_{n+1} \pmod{p}\}. \quad (54)$$

Then the result in (53) reduces to the following:

$$\Theta(\psi(C_t^{k_1}), \psi(C_{t'}^{k_2}))(\tau) = p^{n+1} \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau). \quad (55)$$

Applying *Proposition 1* in (55), we obtain

$$\left| \Theta(\psi(C_t^{k_1}), \psi(C_{t'}^{k_2}))(\tau) \right| = p^{n+1} \left| \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \right| \leq p^m.$$

Combining the above cases, it is clear that

$$\left| \Theta(\psi(C_t^{k_1}), \psi(C_{t'}^{k_2}))(\tau) \right| \leq p^m \text{ for } |\tau| < p^m, k_1 \neq k_2. \quad (56)$$

As per Theorem 2, each  $\mathcal{C}_k$  is a  $(p^{n+1}, p^m)$ -CCC set for  $k \in \{1, 2, \dots, p-1\}$ . From (56), it is clear that the maximum magnitude of the ACCFs between the codes from two distinct sets of CCCs  $\mathcal{C}_{k_1}$  and  $\mathcal{C}_{k_2}$  is upper bounded by  $p^m$ . Therefore, the set of codes  $\cup_{k=1}^{p-1} \mathcal{C}_k$  forms a  $(p^{n+1}(p-1), p^{n+1}, p^m, p^m)$ -QCSS over  $\mathcal{A}_q$ . ■

**Remark 4.** As a comparison, Table II lists the existing constructions of aperiodic QCSSs and our proposed construction in this paper. It is clear that in all existing constructions, the alphabets have sizes no less than the length of constituent sequences. Therefore, for any integer  $q$  smaller than  $p^m$  with

$m > 1$ , the known constructions cannot generate the QCSSs as reported in Theorem 3.

The following corollary discusses the optimality of the proposed QCSSs w.r.t the newly derived lower bounds in this paper.

**Corollary 3** (Asymptotic Optimality of the Proposed Construction). *The proposed construction produces  $(p^{n+1}(p-1), p^{n+1}, p^m, p^m)$ -QCSS over  $\mathcal{A}_q$ . We check optimality for  $N > 4$ , with respect to our newly derived tighter lower bound given in Remark 3. The optimality factor  $\rho$  can be expressed as follows:*

$$\begin{aligned} \rho &= \frac{\theta}{\sqrt{ML \left(1 - \frac{\pi \sqrt{N(2L^2 - N) - 4L}}{4(N-1)L}\right)}} \\ &= \frac{p^{\frac{m-n-1}{2}}}{\sqrt{1 - \frac{\pi \sqrt{\frac{(p-1)}{p^2} \left(2 - \frac{p-1}{p^{2m}}\right) - \frac{4}{p}}}{1 - \frac{2}{p}}}}. \end{aligned} \quad (57)$$

In particular, for  $m = n+1$ , it can be observed from (57) that the optimality factor  $\rho$  achieve the value 1 for a sufficiently large value of  $p$ .

Corollary 3 shows that the proposed QCSSs are asymptotically optimal w.r.t to the lowers bound in Corollaries 1 and 2. As a matter of fact, when the prime  $p$  and  $m$  take small values, the resulting QCSSs are near optimal. With respect to the lowers bound in [15] and those in Remark 3, we denote optimal factors

$$\begin{aligned} \rho_1 &= \frac{\theta}{\sqrt{ML \left(1 - 2\sqrt{\frac{M}{3K}}\right)}} \quad \text{and} \\ \rho_2 &= \begin{cases} \frac{\theta}{\sqrt{\frac{ML^2}{2L-1}}}, & N = 2, \\ \frac{\theta}{ML \left(1 - \frac{L^2(2\pi^2 + 4N - 16) - N\pi^2}{16L^2(N-1)}\right)}, & N = 4, \\ \frac{\theta}{\sqrt{ML \left(1 - \frac{\pi \sqrt{N(2L^2 - N) - 4L}}{4(N-1)L}\right)}}, & N > 4. \end{cases} \end{aligned}$$

Table IX lists the values of optimality factors  $\rho_1$ ,  $\rho_2$ , respectively, for certain parameters  $p$  and  $m$ . For  $p = 3$ , the entries are denoted as “–” as the bound in [15] is valid for  $K \geq 3M$ . Table IX clearly shows that the proposed QCSS tends to optimality faster with respect to the proposed bound. Furthermore, we also have compared  $\rho_1$  and  $\rho_2$  for  $N > 4$ , with respect to the proposed  $(p(p-1), p, p, p)$ -QCSS, where  $13 \leq p < 15000$  in Figure 3. In this figure, the horizontal axis represents sequence lengths in the form of prime numbers ranging from 13 to 14983, while the vertical axis represents the values of  $\rho_1$  and  $\rho_2$ , which range from 1 to 1.5382 (the

Table IX: Optimality factors for the proposed QCSS with respect to the proposed lower bound and the lower bound in [15]

$p$	$m$	$K$	$M$	$N$	$L$	$\theta$	$\rho_1$	$\rho_2$
3	1	6	3	2	3	3	–	1.29
	2	18	9	2	9	9	–	1.37
5	1	20	5	4	5	5	1.54	1.27
	2	100	25	4	25	25	1.54	1.3
7	1	42	7	6	7	7	1.38	1.22
	2	294	49	6	49	49	1.38	1.23
11	1	110	11	10	11	11	1.25	1.17
	2	1210	121	10	121	121	1.25	1.18

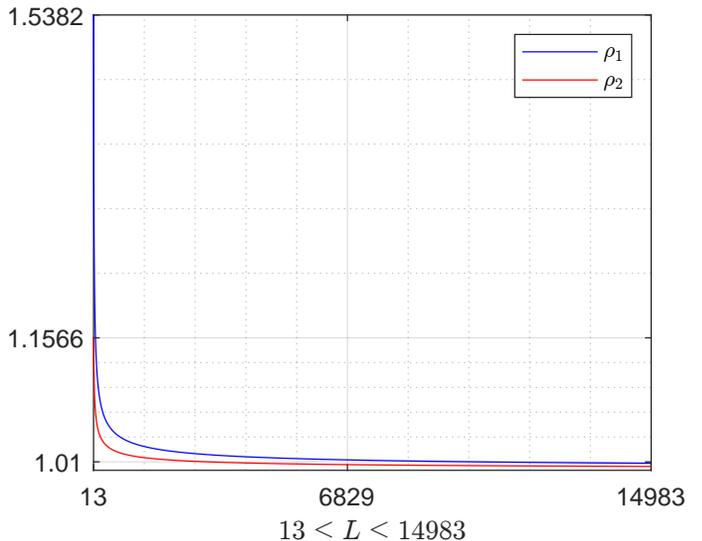


Figure 3: Comparison between the optimality factors  $\rho_1$  and  $\rho_2$  with respect to  $((p-1)p, p, p, p)$ -QCSS for  $13 \leq p < 15000$

value of  $\rho_1$  at  $p = 13$ , where  $\rho_2 = 1.1566$ ). It is evident that  $\rho_2$  tends to converge to 1 faster than  $\rho_1$ .

In the end we provide two examples for the proposed QCSSs.

**Example 3.** Recall from Example 2 that  $m = 3$ ,  $p = 3$ ,  $q = 6$ ,  $J = \{0, 1\}$ ,  $n = 2$ , and the function appears as follows:

$$f(x_0, x_1, x_2) = x_0x_2 + 2x_2x_1 + x_1x_0 + x_0 + 2x_1 + x_2 + 1.$$

In (46), we have derived (27, 27)-CCCs  $\mathcal{C}_1$  and  $\mathcal{C}_2$  from Theorem 2. We present three codes from each of  $\mathcal{C}_1$  and  $\mathcal{C}_2$  in Table VII and Table VIII, respectively, in  $\mathbb{Z}_6$ -valued form.

In this example, we shall consider the maximum ACCF magnitude for codes drawn from  $\mathcal{C}_1$  and  $\mathcal{C}_2$ . As each of  $\mathcal{C}_1$  and  $\mathcal{C}_2$  contains 27 codes, there are 729 possible ACCFs. For clarity, we choose two codes  $\psi(C_0^1) \in \mathcal{C}_1$  and  $\psi(C_1^2) \in \mathcal{C}_2$  and plot their ACCF magnitudes in Figure 4. It can be verified that

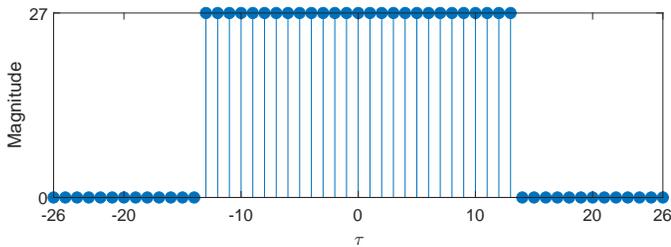


Figure 4: Correlation plot between the codes  $\psi(C_0^1)$  and  $\psi(C_1^2)$

the maximum magnitude among the remaining 728 ACCFs is also given by 27, thus verifying the correlation properties as stated in Theorem 3. Therefore  $C_1 \cup C_2$  forms a  $(54, 27, 27, 27)$ -QCSS over the alphabet  $\mathcal{A}_6$ . As  $N = p - 1 = 2$ , from Remark 3, the optimality factor is  $\rho = \frac{\theta}{\sqrt{\frac{ML^2}{2L-1}}} = 1.40$ . Therefore, the code set  $(54, 27, 27, 27)$ -QCSS forms near-optimal QCSS over  $\mathcal{A}_6$ .

Below we present another example to derive a near-optimal QCSS from Theorem 3.

**Example 4.** Let  $f : \mathbb{Z}_3^2 \rightarrow \mathbb{Z}_3$  be a ternary function given by

$$f(x_0, x_1) = x_0x_1 + x_0^2 + x_1.$$

Taking  $J = \{0\}$ , from (43), we construct the following sets of ternary functions for  $k = 1, 2$ :

$$C_t^k = \{f + k(d_0x_0 + d_1x_1) + (t_0x_0 + t_1x_1) : d_0, d_1 \in \mathbb{Z}_3\},$$

where  $(t_0, t_1) \in \mathbb{Z}_3^2$  corresponds to integers  $t = 0, 1, \dots, 8$ . Table X lists the sequences associated with the functions in  $C_t^k$ .

Numerical results show that the sets  $C_1 = \{\psi(C_t^1) : 0 \leq t < 9\}$ ,  $C_2 = \{\psi(C_t^2) : 0 \leq t < 9\}$  are  $(9, 9)$ -CCCs. It is also confirmed that the maximum magnitude of ACCF between any two codes from  $C_1$  and  $C_2$ , respectively, is upper bounded by 9, indicating that  $C_1 \cup C_2$  forms an  $(18, 9, 9, 9)$ -QCSS over the alphabet  $\mathcal{A}_3$ . As an illustration, Figure 5 (a) and Figure 5 (b) represent the absolute value of AACF and ACCF, respectively, for the CCCs  $C_1$  and  $C_2$ . In Figure 5 (c), we present the absolute value of ACCF between  $\psi(C_0^1)$  and  $\psi(C_0^2)$ . These numerical results are consistent with Theorem 2 and Theorem 3.

In addition, since  $N = 2$ , the optimality factor appears as:  $\rho = \frac{\theta}{\sqrt{\frac{ML^2}{2L-1}}} = 1.37$ . This indicates that the derived  $(18, 9, 9, 9)$ -QCSS  $C_1 \cup C_2$  is near-optimal.

## V. CONCLUSION

In this paper, we have first studied the lower bound on the maximum magnitude of aperiodic auto- and cross-correlation

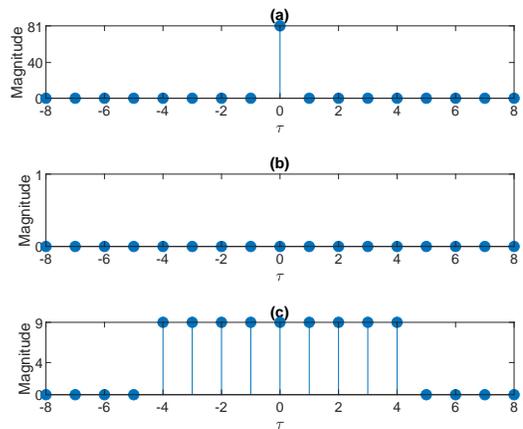


Figure 5: Correlation plot

functions for those QCSSs that appear as the collection of multiple CCCs. By selecting appropriate weight vectors into the bounding function, we have shown that the derived bound is tighter than the bound reported in [15]. Then, we have studied  $q$ -ary functions through a graphical point-of-view to produce aperiodic QCSSs over a small alphabet. The proposed construction generates aperiodic QCSSs over the alphabet  $\mathcal{A}_q$ , where  $q$  is divisible by  $p$ . Unlike the existing aperiodic QCSSs, the proposed construction can maintain a small alphabet size with increasing set size and sequence lengths. It is also to be noted that the obtained QCSSs appears in the form of the collection of multiple sets of CCCs which may guarantee multipath interference free communication in MC-CDMA system as the multipath interference is closely related to the AACFs of the codes assigned to the users. As the sequence length increases, the proposed QCSSs tend to be asymptotically optimal with respect to the derived lower bound.

## APPENDIX A

### PROOF OF COROLLARY 1

Case 1 ( $0 < t \leq L$ ): For  $0 \leq u \leq t - 1$ , we obtain

$$\begin{aligned} \sum_{v=0}^{t-1} \tau_{u,v,L} &= \sum_{v=0}^u (u-v) + \sum_{v=u+1}^{t-1} (v-u) \\ &= \frac{u(u+1)}{2} + \frac{(t-u-1)(t-u)}{2}. \end{aligned}$$

Therefore,

$$\begin{aligned} \sum_{u,v=0}^{t-1} \tau_{u,v,L} &= \sum_{u=0}^{t-1} \frac{u(u+1)}{2} + \sum_{u=0}^{t-1} \frac{(t-u-1)(t-u)}{2} \\ &= \frac{t(t^2-1)}{3}. \end{aligned}$$

Table X: (18, 9, 9, 9)-QCSS over the alphabet  $\mathcal{A}_3$ , where  $\xi_3^i$  is given as  $i$  for simplicity

$\psi(C_0^1)$	$\psi(C_1^1)$	$\psi(C_2^1)$	$\psi(C_3^1)$	$\psi(C_4^1)$	$\psi(C_5^1)$	$\psi(C_6^1)$	$\psi(C_7^1)$	$\psi(C_8^1)$
012102111	021111120	000120102	012210000	021222012	000201021	012021222	021000201	000012210
021111120	000120102	012102111	021222012	000201021	012210000	021000201	000012210	012021222
000120102	012102111	021111120	000201021	012210000	021222012	000012210	012021222	021000201
012210000	021222012	000201021	012021222	021000201	000012210	012102111	021111120	000120102
021222012	000201021	012210000	021000201	000012210	012021222	021111120	000120102	012102111
000201021	012210000	021222012	000012210	012021222	021000201	000120102	012102111	021111120
012021222	021000201	000012210	012102111	021111120	000120102	012210000	021222012	000201021
021000201	000012210	012021222	021111120	000120102	012102111	021222012	000201021	012210000
000012210	012021222	021000201	000120102	012102111	021111120	000201021	012210000	021222012
$\psi(C_0^2)$	$\psi(C_1^2)$	$\psi(C_2^2)$	$\psi(C_3^2)$	$\psi(C_4^2)$	$\psi(C_5^2)$	$\psi(C_6^2)$	$\psi(C_7^2)$	$\psi(C_8^2)$
012102111	021111120	000120102	012210000	021222012	000201021	012021222	021000201	000012210
000120102	012102111	021111120	000201021	012210000	021222012	000012210	012021222	021000201
021111120	000120102	012102111	021222012	000201021	012210000	021000201	000012210	012021222
012021222	021000201	000012210	012102111	021111120	000120102	012210000	021222012	000201021
000012210	012021222	021000201	000120102	012102111	021111120	000201021	012210000	021222012
021000201	000012210	012021222	021111120	000120102	012102111	021222012	000201021	012210000
012210000	021222012	000201021	012021222	021000201	000012210	012102111	021111120	000120102
000201021	012210000	021222012	000012210	012021222	021000201	000120102	012102111	021111120
021222012	000201021	012210000	021000201	000012210	012021222	021111120	000120102	012102111

Substituting  $\sum_{u,v=0}^{t-1} \tau_{u,v,L} = \frac{t(t^2-1)}{3}$  in (22), we have

$$\begin{aligned} \theta^2 &\geq \frac{ML \left(1 - \frac{ML}{Kt} - \frac{(t^2-1)}{3Lt}\right)}{1 - \frac{M}{K}} \\ &= \frac{ML}{1 - \frac{M}{K}} \left(1 - \frac{1}{3L} \left(t + \frac{3ML^2 - K}{Kt}\right)\right). \end{aligned} \quad (58)$$

Define a function  $f(x) = x + \frac{3ML^2 - K}{Kx}$ . We are interested in the minimum value of  $f(x)$  over the interval  $[1, L]$ . Observe that  $f(x)$  is continuous on  $[1, L]$ . Consider its derivative  $f'(x) = 1 - \frac{3ML^2 - K}{Kx^2}$ . It has two zeros  $x_0 = \sqrt{\frac{3ML^2}{K} - 1}$  and  $-x_0$ , and is monotonically increasing over the interval  $[1, L]$ . We now consider the minimum value of  $f(x)$  over the interval  $[1, L]$ .

- 1) When  $N = K/M = 2$ , one has  $x_0 > L$ , which means that  $f'(x) < 0$  over  $[1, L]$ . In this case  $f(x)$  is monotonically decreasing over  $[1, L]$  and achieves the minimum value at  $x = L$ . Then we have

$$f(x) \geq f(L) = 2L - \frac{1}{L} \text{ for } x \in [1, L],$$

which implies

$$\begin{aligned} \theta^2 &\geq \frac{ML}{1 - M/K} \left(\frac{2}{3} - \frac{M}{K} + \frac{1}{3L^2}\right) \\ &= ML \left(\frac{1}{3} + \frac{2}{3L^2}\right). \end{aligned}$$

- 2) When  $N = K/M = 3$ , one has  $x_0 = \sqrt{\frac{3ML^2}{K} - 1} = \sqrt{L^2 - 1} \leq L$ , which is very close to  $L$ . In this case,

$f'(x) < 0$  over the interval  $[1, L]$ , and hence monotonically decreasing. Therefore,  $f(x)$  achieve minimum value at  $x = L$ , and we have the following lower bound:

$$\theta^2 \geq ML \left(\frac{1}{2} + \frac{1}{2L^2}\right).$$

- 3) When  $N = K/M > 3$ , one has  $x_0 = \sqrt{\frac{3ML^2}{K} - 1} < L$ . That is to say,  $f'(x) < 0$  over  $[1, x_0]$  and  $f'(x) > 0$  over  $[x_0, L]$ . This implies that the function  $f(x)$  achieves the minimum value at  $x = x_0$ . Hence we have

$$f(x) \geq f(x_0) = 2\sqrt{\frac{3ML^2}{K} - 1} \text{ for } x \in [1, L].$$

In this case, by properly choosing  $x$  around  $\sqrt{\frac{3L^2}{N} - 1}$ , we have the following simplified lower bound:

$$\theta^2 \geq ML \left(1 - \frac{2\sqrt{N(3L^2 - N)} - 3L}{3L(N - 1)}\right).$$

Case 2 ( $L < t \leq 2L - 1$ ): For  $0 \leq u \leq t - L - 1$ , we obtain

$$\begin{aligned} \sum_{v=0}^{t-1} \tau_{u,v,L} &= \sum_{v=0}^{u-1} (u-v) + \sum_{v=u}^{u+L-1} (v-u) \\ &\quad + \sum_{v=u+L}^{t-1} (2L-1-v+u) \\ &= u(t+1-2L) - L^2 + 2Lt - \frac{t^2+t}{2}. \end{aligned}$$

Hence,

$$\sum_{u=0}^{t-L-1} \sum_{v=0}^{t-1} \tau_{u,v,L} = \frac{(t-L)(t+1)(L-1)}{2}.$$

For  $t - L \leq u \leq L - 1$ , we obtain

$$\begin{aligned} \sum_{v=0}^{t-1} \tau_{u,v,L} &= \sum_{v=0}^u (u-v) + \sum_{v=u+1}^{t-1} (v-u) \\ &= u^2 - (t-1)u + \frac{t^2 - t}{2}. \end{aligned}$$

Hence,

$$\sum_{u=t-L}^{L-1} \sum_{v=0}^{t-1} \tau_{u,v,L} = \frac{3Lt^2 - t^3 - 3L^2t + t + 2L^3 - 2L}{3}.$$

Similarly, we obtain

$$\sum_{u=L}^{t-1} \sum_{v=0}^{t-1} \tau_{u,v,L} = \frac{(t+1)(t-L)(L-1)}{2}.$$

Therefore,

$$\begin{aligned} \sum_{u,v=0}^{t-1} \tau_{u,v,L} &= (t+1)(t-L)(L-1) \\ &+ \frac{3Lt^2 - t^3 - 3L^2t + t + 2L^3 - 2L}{3}. \end{aligned} \quad (59)$$

From (22) and (59), we have

$$\theta^2 \geq \frac{M}{3(1-M/K)} \left( t + \frac{a}{t} - \frac{b}{t^2} - 3(L-1) \right), \quad (60)$$

where

$$\begin{aligned} a &= (6L^2 - 6L + 2) - \frac{3ML^2}{K}, \\ b &= L(L-1)(2L-1). \end{aligned}$$

Similarly we define a function

$$f(x) = x + \frac{a}{x} - \frac{b}{x^2},$$

and will discuss the property of  $f(x)$  on the interval  $[L+1, 2L-1]$ .

We shall consider both the 1st-order and 2nd-order derivatives of  $f(x)$ , which are given by

$$f'(x) = 1 - \frac{a}{x^2} + \frac{2b}{x^3} \quad \text{and} \quad f''(x) = \frac{2a}{x^3} - \frac{6b}{x^4} = \frac{2a}{x^4} \left( x - \frac{3b}{a} \right).$$

The properties of  $f'(x)$  and  $f''(x)$  on the interval  $[L+1, 2L-1]$  will be used to determine the maximum value of  $f(x)$  in  $[L+1, 2L-1]$ .

We start with the property of  $f''(x)$  on  $[L+1, 2L+1]$ . Note that  $f''(x)$  has zero

$$\begin{aligned} x_0 &= \frac{3b}{a} \\ &= \frac{3L(L-1)(2L-1)}{(6L^2 - 6L + 2) - \frac{3ML^2}{K}} \\ &= \frac{6L^3 - 9L^2 + 3L}{(6 - \frac{3}{N})L^2 - 6L + 2} \\ &= L \left( 1 + \frac{(\frac{3}{N}L^2 - 3L + 1)}{(6 - \frac{3}{N})L^2 - 6L + 2} \right). \end{aligned}$$

We need to consider whether  $x_0$  lies in between  $L+1$  and  $2L-1$ . Hence we divide the discussion into three subcases:  $N=2$ ,  $3 \leq N \leq L/3$  and  $N > L/3$ .

1) In the case of  $N=2$ , we have

$$\frac{1}{L} \leq \frac{(\frac{3}{N}L^2 - 3L + 1)}{(6 - \frac{3}{N})L^2 - 6L + 2} < 1.$$

In this case, the root  $x_0 = \frac{3b}{a}$  lies in the interval  $[L+1, 2L-1]$ . This implies  $f''(x) < 0$  for  $x \in [L+1, x_0]$  and  $f''(x) > 0$  for  $x \in (x_0, 2L-1]$ . Consequently, the first order derivative  $f'(x)$  is monotonically decreasing over  $[L+1, x_0]$  and monotonically increasing over  $[x_0, 2L-1]$ . Furthermore, we have

$$\begin{aligned} f'(2L-1) &= \frac{1}{(2L-1)^3} ((2L-1)^3 - a(2L-1) + 2b) \\ &= \frac{\frac{3}{N}L^2 - 1}{(2L-1)^2} \\ &= \frac{\frac{3}{2}L^2 - 1}{(2L-1)^2} > 0 \end{aligned} \quad (61)$$

and

$$\begin{aligned} &f'(L+1) \\ &= \frac{(L+1)^3 - a(L+1) + 2b}{(L+1)^3} \\ &= \frac{(L+1)^3 - ((6L^2 - 6L + 2) - \frac{3}{N}L^2)(L+1)}{(L+1)^3} \\ &+ \frac{2L(L-1)(2L-1)}{(L+1)^3} \\ &= \frac{-(1 - \frac{3}{N})L^3 - L^2(3 - \frac{3}{N}) + 9L - 1}{(L+1)^3} \\ &= \frac{L^3 - 3L^2 + 18L - 2}{2(L+1)^3} > 0. \end{aligned} \quad (62)$$

Since for  $x \in [L+1, 2L-1]$ , the derivative function  $f'(x)$  satisfies  $f'(x) \geq f'(\frac{3b}{a}) = 1 - \frac{a-a^2}{9b^2} + \frac{2a^3}{27b^3} = 1 - \frac{a^3}{27b^2} > 0$  for  $L \geq 2$ . Hence the function  $f(x)$  is monotonically increasing on  $[L+1, 2L-1]$  and it achieves the maximum value at  $x = 2L-1$ . Since

$$\begin{aligned} f(2L-1) &= (2L-1) + \frac{a}{2L-1} - \frac{b}{(2L-1)^2} \\ &= \frac{(9L^2 - 9L + 3) - \frac{3}{N}L^2}{2L-1}. \end{aligned} \quad (63)$$

It follows that (22) becomes

$$\theta^2 \geq \frac{M}{(1-M/K)} \cdot \frac{(1 - \frac{1}{N})L^2}{(2L-1)} = \frac{ML^2}{2L-1}.$$

2) When  $3 \leq N \leq L/3$ , similarly one has

$$\frac{1}{L} < \frac{(\frac{3}{N}L^2 - 3L + 1)}{(6 - \frac{3}{N})L^2 - 6L + 2} < 1,$$

implying that  $f'(x)$  is monotonically decreasing over  $[L+1, x_0]$  and monotonically increasing over  $[x_0, 2L-1]$ . From the calculations in (61) and (62), one has

$$f'(2L-1) = \frac{\frac{3}{N}L^2 - 1}{(2L-1)^2} > 0$$

and

$$f'(L+1) = \frac{-(1 - \frac{3}{N})L^3 - L^2(3 - \frac{3}{N}) + 9L - 1}{(L+1)^3} < 0.$$

This implies the minimum value  $f'(x_0) < 0$ . Then the function  $f'(x)$  has a zero  $x_1$  in the interval  $[x_0, 2L-1]$ . That is to say,  $f'(x) < 0$  for  $x \in [L+1, x_1]$  and  $f'(x) \geq 0$  for  $x \in [x_1, 2L-1]$ . Hence the function  $f(x)$  is monotonically decreasing on  $[L+1, x_1]$  and is monotonically increasing on  $[x_1, 2L-1]$ . Consequently, the maximum value of  $f(x)$  is attained either at  $x = L+1$  or  $x = 2L-1$ .

Note that

$$\begin{aligned} & f(L+1) - f(2L-1) \\ &= (L+1) + \frac{a}{L+1} - \frac{b}{(L+1)^2} \\ & \quad - \left( (2L-1) + \frac{a}{2L-1} - \frac{b}{(2L-1)^2} \right) \\ &= \frac{(L-2)}{(L+1)^2(2L-1)} \left( \frac{N-3}{N}L^3 - \frac{3}{N}L^2 - 4L + 3 \right). \end{aligned}$$

This implies that for  $L \geq 3N$ ,  $f(L+1) < f(2L-1)$  for  $N = 3$ , and  $f(L+1) > f(2L-1)$  for  $N > 3$ . Therefore, for  $N = 3$  one has

$$\theta^2 \geq \frac{M}{(1-M/K)} \cdot \frac{(1 - \frac{1}{N})L^2}{(2L-1)} = \frac{ML^2}{2L-1},$$

and for  $N > 3$ , we have

$$\begin{aligned} \theta^2 &\geq \frac{M}{(1-M/K)} \times \\ & \frac{(2N-3)L^3 + 3(N-1)L^2 + NL + 6N}{3(L+1)^2N} \\ &= ML \left( 1 - \frac{(N+6)L^3 + 3(N-1)L^2 + (2N-3)L - 6N}{3L(L+1)^2(N-1)} \right). \end{aligned} \quad (64)$$

- 3) When  $N > L/3 \geq 3$ , one has  $x_0 = 3b/a < L+1$  for  $L \geq 9$ . In this case  $f''(L+1) > 0$  and  $f''(2L-1) > 0$ , implying that  $f'(x)$  is monotonically increasing over  $[L+1, 2L-1]$ . Similarly, one has  $f'(L+1) < 0$  and  $f'(2L-1) > 0$ . Hence  $f(x)$  achieve the maximum value either at  $L+1$  or  $2L-1$ . Similar to the previous discussion for the case, we know

$f(L+1) > f(2L-1)$  when  $N > L/3 \geq 3$ . Then the lower bound is as given in (64).

In summary, for  $L+1 \leq t \leq 2L-1$ , when  $N = 2, 3$ , the bound is given by

$$\theta^2 \geq \frac{ML^2}{2L-1},$$

and when  $N > 3$ , the bound is given by

$$\theta^2 \geq ML \left( 1 - \frac{(N+6)L^3 + 3(N-1)L^2 + (2N-3)L - 6N}{3L(L+1)^2(N-1)} \right). \quad (65)$$

Comparing the lower bounds in *Case 1* and *Case 2*, we have the following result:

- when  $N = 2, 3$ , the maximum value of the lower bounds is achieved from (60) at  $t = 2L-1$ , namely,

$$\theta^2 \geq \frac{ML^2}{2L-1},$$

- when  $N > 3$ , the maximum value of the lower bounds is achieved from (58) at  $\left\lceil \sqrt{\frac{3L^2}{N} - 1} \right\rceil$ . The lower bound is approximately given by

$$\theta^2 \geq ML \left( 1 - \frac{2\sqrt{3L^2N - N^2} - 3L}{3L(N-1)} \right).$$

## APPENDIX B

### PROOF OF THEOREM 2

According to the definition of  $\mathcal{C}_k$ , we represent each set of  $q$ -ary functions  $C_t^k$  given in (43) as follows:  $C_t^k = \{f_{d,t} : 0 \leq d < p^{n+1}\}$ , where  $f_{d,t} = f_{d_n, t_n} + \frac{q}{p}(k\mathbf{d} + \mathbf{t}) \cdot \mathbf{x}_J$ ,  $f_{d_n, t_n} = f + \frac{q}{p}(kd_n x_{l_{\pi(0)}} + t_n x_{l_{\pi(m-n-1)}})$ , and  $(d_0, d_1, \dots, d_n)$  is the vector representation of  $d$  with respect to base- $p$ . Let  $\tau$  be an integer satisfying  $0 \leq |\tau| < p^m$ . The ACCF between two codes  $\psi(C_t^k)$  and  $\psi(C_{t'}^k)$  in  $\mathcal{C}_k$  at the time shift  $\tau$  can be expressed as

$$\begin{aligned} & \Theta(\psi(C_t^k), \psi(C_{t'}^k))(\tau) \\ &= \sum_{d=0}^{p^{n+1}-1} \Theta(\psi(f_{d,t}), \psi(f_{d,t'}))(\tau) \\ &= \sum_{d=0}^{p^{n+1}-1} \sum_{\mathbf{c}_1, \mathbf{c}_2 \in \mathbb{Z}_p^n} \Theta(\psi(f_{d,t}|_{\mathbf{x}_J=\mathbf{c}_1}), \psi(f_{d,t'}|_{\mathbf{x}_J=\mathbf{c}_2}))(\tau) \\ &= \sum_{d=0}^{p^{n+1}-1} \sum_{\mathbf{c}_1=\mathbf{c}_2} \Theta(\psi(f_{d,t}|_{\mathbf{x}_J=\mathbf{c}_1}), \psi(f_{d,t'}|_{\mathbf{x}_J=\mathbf{c}_2}))(\tau) + \\ & \quad \sum_{d=0}^{p^{n+1}-1} \sum_{\mathbf{c}_1 \neq \mathbf{c}_2} \Theta(\psi(f_{d,t}|_{\mathbf{x}_J=\mathbf{c}_1}), \psi(f_{d,t'}|_{\mathbf{x}_J=\mathbf{c}_2}))(\tau) \\ &= \mathcal{S}_1 + \mathcal{S}_2, \end{aligned} \quad (66)$$

where

$$\mathcal{S}_1 = \sum_{d=0}^{p^{n+1}-1} \sum_{\mathbf{c}_1=\mathbf{c}_2} \Theta(\psi(f_{d,t}|_{\mathbf{x}_J=\mathbf{c}_1}), \psi(f_{d,t'}|_{\mathbf{x}_J=\mathbf{c}_2}))(\tau),$$

and

$$\mathcal{S}_2 = \sum_{d=0}^{p^{n+1}-1} \sum_{\mathbf{c}_1 \neq \mathbf{c}_2} \Theta(\psi(f_{d,t}|_{\mathbf{x}_J=\mathbf{c}_1}), \psi(f_{d,t'}|_{\mathbf{x}_J=\mathbf{c}_2}))(\tau). \quad (67)$$

Now,

$$\psi(f_{d,t}|_{\mathbf{x}_J=\mathbf{c}_1}) = \xi_p^{k(\mathbf{d} \cdot \mathbf{c}_1)} \xi_p^{\mathbf{t} \cdot \mathbf{c}_1} \psi(f_{d_n, t_n} |_{\mathbf{x}_J=\mathbf{c}_1}), \quad (68)$$

and

$$\psi(f_{d,t'}|_{\mathbf{x}_J=\mathbf{c}_2}) = \xi_p^{k(\mathbf{d} \cdot \mathbf{c}_2)} \xi_p^{\mathbf{t}' \cdot \mathbf{c}_2} \psi(f_{d_n, t'_n} |_{\mathbf{x}_J=\mathbf{c}_2}), \quad (69)$$

where  $\mathbf{t}' = (t'_0, t'_1, \dots, t'_{n-1})$ , and  $(t'_0, t'_1, \dots, t'_{n-1}, t'_n)$  is the vector representation of  $\mathbf{t}'$  with respect to base- $p$ . Let us first start with  $\mathcal{S}_2$  in (67),

$$\begin{aligned} \mathcal{S}_2 &= \sum_{d=0}^{p^{n+1}-1} \sum_{\mathbf{c}_1 \neq \mathbf{c}_2} \Theta(\psi(f_{d,t}|_{\mathbf{x}_J=\mathbf{c}_1}), \psi(f_{d,t'}|_{\mathbf{x}_J=\mathbf{c}_2}))(\tau) \\ &= \sum_{(\mathbf{d}, d_n) \in \mathbb{Z}_p^{n+1}} \sum_{\mathbf{c}_1 \neq \mathbf{c}_2} \xi_p^{k(\mathbf{d} \cdot (\mathbf{c}_1 - \mathbf{c}_2))} \xi_p^{(\mathbf{t} \cdot \mathbf{c}_1 - \mathbf{t}' \cdot \mathbf{c}_2)} \\ &\quad \times \Theta(\psi(f_{d_n, t_n} |_{\mathbf{x}_J=\mathbf{c}_1}), \psi(f_{d_n, t'_n} |_{\mathbf{x}_J=\mathbf{c}_2}))(\tau) \\ &= \sum_{d_n} \sum_{\mathbf{c}_1 \neq \mathbf{c}_2} \xi_p^{(\mathbf{t} \cdot \mathbf{c}_1 - \mathbf{t}' \cdot \mathbf{c}_2)} \Theta(\psi(f_{d_n, t_n} |_{\mathbf{x}_J=\mathbf{c}_1}), \\ &\quad \psi(f_{d_n, t'_n} |_{\mathbf{x}_J=\mathbf{c}_2}))(\tau) \sum_{\mathbf{d}} \xi_p^{k(\mathbf{d} \cdot (\mathbf{c}_1 - \mathbf{c}_2))}. \end{aligned}$$

Since,  $1 \leq k \leq p-1$  and  $\mathbf{c}_1 \neq \mathbf{c}_2$ ,  $\sum_{\mathbf{d}} \xi_p^{k(\mathbf{d} \cdot (\mathbf{c}_1 - \mathbf{c}_2))} = 0$ . Therefore,  $\mathcal{S}_2 = 0$ . Now let us move to  $\mathcal{S}_1$ . Let us assume  $\mathbf{c}_1 = \mathbf{c}_2 = \mathbf{c} \in \mathbb{Z}_p^n$ . Then

$$\begin{aligned} \mathcal{S}_1 &= \sum_{d=0}^{p^{n+1}-1} \sum_{\mathbf{c}_1=\mathbf{c}_2} \Theta(\psi(f_{d,t}|_{\mathbf{x}_J=\mathbf{c}_1}), \psi(f_{d,t'}|_{\mathbf{x}_J=\mathbf{c}_2}))(\tau) \\ &= \sum_{(\mathbf{d}, d_n) \in \mathbb{Z}_p^{n+1}} \sum_{\mathbf{c}} \Theta(\psi(f_{d,t}|_{\mathbf{x}_J=\mathbf{c}_1}), \psi(f_{d,t'}|_{\mathbf{x}_J=\mathbf{c}_2}))(\tau). \end{aligned} \quad (70)$$

From (70), (68), and (69), we have

$$\begin{aligned} \mathcal{S}_1 &= \sum_{(\mathbf{d}, d_n) \in \mathbb{Z}_p^{n+1}} \sum_{\mathbf{c}} \xi_p^{k(\mathbf{d} \cdot (\mathbf{c} - \mathbf{c}))} \xi_p^{(\mathbf{t} - \mathbf{t}') \cdot \mathbf{c}} \\ &\quad \times \Theta(\psi(f_{d_n, t_n} |_{\mathbf{x}_J=\mathbf{c}}), \psi(f_{d_n, t'_n} |_{\mathbf{x}_J=\mathbf{c}}))(\tau) \\ &= p^n \sum_{d_n} \sum_{\mathbf{c}} \xi_p^{(\mathbf{t} - \mathbf{t}') \cdot \mathbf{c}} \Theta(\psi(f_{d_n, t_n} |_{\mathbf{x}_J=\mathbf{c}}), \\ &\quad \psi(f_{d_n, t'_n} |_{\mathbf{x}_J=\mathbf{c}}))(\tau) \\ &= p^n \sum_{\mathbf{c}} \xi_p^{(\mathbf{t} - \mathbf{t}') \cdot \mathbf{c}} \mathcal{S}_3, \end{aligned} \quad (71)$$

where

$$\mathcal{S}_3 = \sum_{d_n} \Theta(\psi(f_{d_n, t_n} |_{\mathbf{x}_J=\mathbf{c}}), \psi(f_{d_n, t'_n} |_{\mathbf{x}_J=\mathbf{c}}))(\tau).$$

Let us recall  $\gamma$  and  $\delta$  and their base- $p$  vector representations  $(\gamma_0, \gamma_1, \dots, \gamma_{m-1})$  and  $(\delta_0, \delta_1, \dots, \delta_{m-1})$ , respectively, and  $\mathbf{A}_\tau(\mathbf{c}) = \{(\gamma, \delta) : 0 \leq \gamma \leq p^m - \tau - 1, \delta = \gamma + \tau, \gamma_{j_\alpha} = c_\alpha, \delta_{j_\alpha} = c_\alpha, \alpha = 0, 1, \dots, n-1\}$  as defined in Section II-B. Based on the definition of complex-valued sequence corresponding to restricted  $q$ -ary function given in Section II-A, the  $\gamma$ th component of  $\psi(f_{d_n, t_n} |_{\mathbf{x}_J=\mathbf{c}})$  is given by  $\xi_q^{(f_{d_n, t_n})_\gamma}$  if  $\gamma_{j_\alpha} = c_\alpha$  for  $\alpha = 0, 1, \dots, n-1$ , else the value is zero, where  $(f_{d_n, t_n})_\gamma = f_{d_n, t_n}(\gamma_0, \gamma_1, \dots, \gamma_{m-1})$ . Similarly, the  $\gamma$ th component of  $\psi(f_{d_n, t'_n} |_{\mathbf{x}_J=\mathbf{c}})$  is given by  $\xi_q^{(f_{d_n, t'_n})_\gamma}$  if  $\gamma_{j_\alpha} = c_\alpha$  for  $\alpha = 0, 1, \dots, n-1$ , else the value is zero, where  $(f_{d_n, t'_n})_i = f_{d_n, t'_n}(\gamma_0, \gamma_1, \dots, \gamma_{m-1})$ . Then  $\mathcal{S}_3$  can be expressed as

$$\begin{aligned} \mathcal{S}_3 &= \sum_{d_n} \Theta(\psi(f_{d_n, t_n} |_{\mathbf{x}_J=\mathbf{c}}), \psi(f_{d_n, t'_n} |_{\mathbf{x}_J=\mathbf{c}}))(\tau) \\ &= \sum_{d_n} \sum_{(\gamma, \delta) \in \mathbf{A}_\tau(\mathbf{c})} \xi_q^{(f_{d_n, t_n})_\gamma - (f_{d_n, t'_n})_\delta}. \end{aligned} \quad (72)$$

*Case 1* ( $\tau \neq 0, \gamma_{l_{\pi(0)}} \neq \delta_{l_{\pi(0)}}$ ): Since,  $0 < k < p$ ,  $\sum_{d_n} \xi_p^{kd_n(\gamma_{l_{\pi(0)}} - \delta_{l_{\pi(0)}})} = 0$ . From (72), we have

$$\begin{aligned} \mathcal{S}_3 &= \sum_{d_n} \sum_{(\gamma, \delta) \in \mathbf{A}_\tau(\mathbf{c})} \xi_q^{(f_\gamma - f_\delta) + \frac{\gamma k d_n}{p} (\gamma_{l_{\pi(0)}} - \delta_{l_{\pi(0)}})} \\ &\quad \times \xi_q^{\frac{q}{p} (t_n \gamma_{l_{\pi(m-n-1)}} - t'_n \delta_{l_{\pi(m-n-1)}})} \\ &= \sum_{d_n} \sum_{(\gamma, \delta) \in \mathbf{A}_\tau(\mathbf{c})} \xi_q^{f_\gamma - f_\delta} \xi_p^{kd_n(\gamma_{l_{\pi(0)}} - \delta_{l_{\pi(0)}})} \\ &\quad \times \xi_p^{(t_n \gamma_{l_{\pi(m-n-1)}} - t'_n \delta_{l_{\pi(m-n-1)}})} \\ &= \sum_{(\gamma, \delta) \in \mathbf{A}_\tau(\mathbf{c})} \xi_q^{f_\gamma - f_\delta} \xi_p^{(t_n \gamma_{l_{\pi(m-n-1)}} - t'_n \delta_{l_{\pi(m-n-1)}})} \\ &\quad \times \sum_{d_n} \xi_p^{kd_n(\gamma_{l_{\pi(0)}} - \delta_{l_{\pi(0)}})} \\ &= 0, \end{aligned}$$

where  $f_\gamma = f(\gamma_0, \gamma_1, \dots, \gamma_{m-1})$  and  $f_\delta = f(\delta_0, \delta_1, \dots, \delta_{m-1})$ .

*Case 2* ( $\tau \neq 0, \gamma_{l_{\pi(0)}} = \delta_{l_{\pi(0)}}$ ): We assume  $u$  is the smallest positive integer for which  $\gamma_{l_{\pi(u)}} \neq \delta_{l_{\pi(u)}}$ . Let us also assume  $\gamma^v$  to be an integer whose base- $p$  vector representation is given by  $(\gamma_0, \gamma_1, \dots, \kappa p + \gamma_{l_{\pi(u-1)}} - v, \dots, \gamma_{m-1})$ , where  $v \in \{1, 2, \dots, p-1\}$ , and  $\kappa = 0$  when  $\gamma_{l_{\pi(u)}} - v \geq 0$  and  $\kappa = 1$  when  $\gamma_{l_{\pi(u)}} - v < 0$ . Similarly, we assume  $\delta^v$  to be an integer whose base- $p$  vector representation is given by  $(\delta_0, \delta_1, \dots, \kappa p + \delta_{l_{\pi(u-1)}} - v, \dots, \delta_{m-1})$ . It is clear that,  $\gamma^v$  and  $\delta^v$  differs from  $\gamma$  and  $\delta$ , respectively, only at  $l_{\pi(u-1)}$ th position. It is also to be noted that, it can easily be drawn an invertible between any two pairs in

$\{(\gamma, \delta), (\gamma^0, \delta^0), \dots, (\gamma^{p-1}, \delta^{p-1})\}$ . Therefore, each of the  $p$  pairs contributes to  $\mathcal{S}_3$ . Now

$$\begin{aligned} & (f_{d_n, t_n})_{\gamma^v} - (f_{d_n, t'_n})_{\delta^v} - ((f_{d_n, t_n})_{\gamma} - (f_{d_n, t'_n})_{\delta}) \\ &= f_{\gamma^v} - f_{\delta^v} - (f_{\gamma} - f_{\delta}) \end{aligned} \quad (73)$$

Since  $\gamma^v$  and  $\gamma$  differs only at the position  $l_{\pi(u-1)}$ , and  $\gamma_{j\alpha} = c_\alpha$  for  $\alpha = 0, 1, \dots, n-1$ ,

$$\begin{aligned} f_{\gamma^v} - f_{\gamma} &= q\kappa(\gamma_{l_{\pi(u-2)}} + \gamma_{l_{\pi(u)}}) + \kappa p g_{l_{\pi(u-1)}} \\ &\quad - v \left( \frac{q}{p} \gamma_{l_{\pi(u-2)}} + \frac{q}{p} \gamma_{l_{\pi(u)}} + g_{l_{\pi(u-1)}} \right). \end{aligned} \quad (74)$$

Similarly,

$$\begin{aligned} f_{\delta^v} - f_{\delta} &= q\kappa(\delta_{l_{\pi(u-2)}} + \delta_{l_{\pi(u)}}) + \kappa p g_{l_{\pi(u-1)}} \\ &\quad - v \left( \frac{q}{p} \delta_{l_{\pi(u-2)}} + \frac{q}{p} \delta_{l_{\pi(u)}} + g_{l_{\pi(u-1)}} \right). \end{aligned} \quad (75)$$

Since  $\gamma_{l_{\pi(\alpha)}} = \delta_{l_{\pi(\alpha)}}$  for  $\alpha = 0, 1, \dots, u-1$ , from (73), (74), and (75), we have

$$\begin{aligned} & (f_{d_n, t_n})_{\gamma^v} - (f_{d_n, t'_n})_{\delta^v} - ((f_{d_n, t_n})_{\gamma} - (f_{d_n, t'_n})_{\delta}) \\ &= f_{\gamma^v} - f_{\delta^v} - (f_{\gamma} - f_{\delta}) \\ &= q\kappa(\gamma_{l_{\pi(u)}} - \delta_{l_{\pi(u)}}) + \frac{vq}{p}(\delta_{l_{\pi(u)}} - \gamma_{l_{\pi(u)}}). \end{aligned} \quad (76)$$

Since  $\xi_q^{q\kappa(\gamma_{l_{\pi(u)}} - \delta_{l_{\pi(u)}})} = 1$ , from (76), we have

$$\begin{aligned} & \sum_{v=1}^{p-1} \xi_q^{(f_{d_n, t_n})_{\gamma^v} - (f_{d_n, t'_n})_{\delta^v} - ((f_{d_n, t_n})_{\gamma} - (f_{d_n, t'_n})_{\delta})} \\ &= \sum_{v=1}^{p-1} \xi_q^{q\kappa(\gamma_{l_{\pi(u)}} - \delta_{l_{\pi(u)}})} \xi_p^{v(\delta_{l_{\pi(u)}} - \gamma_{l_{\pi(u)}})} \\ &= \sum_{v=1}^{p-1} \xi_p^{v(\delta_{l_{\pi(u)}} - \gamma_{l_{\pi(u)}})} \\ &= -1. \end{aligned}$$

Therefore,

$$\xi_q^{(f_{d_n, t_n})_{\gamma} - (f_{d_n, t'_n})_{\delta}} + \sum_{v=1}^{p-1} \xi_q^{(f_{d_n, t_n})_{\gamma^v} - (f_{d_n, t'_n})_{\delta^v}} = 0.$$

*Case 3* ( $\tau = 0$ ): Since  $\tau = 0$ ,  $\gamma = \delta$ , from (72), we have

$$\begin{aligned} \mathcal{S}_3 &= \sum_{d_n} \Theta(\psi(f_{d_n, t_n} |_{\mathbf{x}_J = \mathbf{c}}), \psi(f_{d_n, t'_n} |_{\mathbf{x}_J = \mathbf{c}}))(\tau) \\ &= \sum_{d_n} \sum_{(\gamma, \gamma) \in \mathbf{A}_\tau(\mathbf{c})} \xi_q^{(f_{d_n, t_n})_{\gamma} - (f_{d_n, t'_n})_{\delta}} \\ &= \sum_{(\gamma, \gamma) \in \mathbf{A}_\tau(\mathbf{c})} \xi_q^{f_{\gamma} - f_{\delta}} \xi_p^{t_n \gamma_{l_{\pi(m-n-1)}} - t'_n \delta_{l_{\pi(m-n-1)}}} \\ &\quad \times \sum_{d_n} \xi_p^{k d_n (\gamma_{l_{\pi(0)}} - \delta_{l_{\pi(0)}})} \\ &= p \sum_{(\gamma, \gamma) \in \mathbf{A}_\tau(\mathbf{c})} \xi_p^{t_n \gamma_{l_{\pi(m-n-1)}} - t'_n \delta_{l_{\pi(m-n-1)}}} \\ &= p \sum_{(\gamma, \gamma) \in \mathbf{A}_\tau(\mathbf{c})} \xi_p^{(t_n - t'_n) \gamma_{l_{\pi(m-n-1)}}} \\ &= p p^{m-n-1} \sum_{\gamma_{l_{\pi(m-n-1)}} = 0}^{p-1} \xi_p^{(t_n - t'_n) \gamma_{l_{\pi(m-n-1)}}} \\ &= \begin{cases} p^{m-n+1}, & t_n = t'_n, \\ 0, & t_n \neq t'_n. \end{cases} \end{aligned}$$

Combining all the above cases in (71), we have

$$\begin{aligned} \mathcal{S}_1 &= \begin{cases} p^{m-n+1} p^n \sum_{\mathbf{c}} \xi_p^{(\mathbf{t} - \mathbf{t}') \cdot \mathbf{c}}, & \tau = 0, t_n = t'_n, \\ 0, & \text{otherwise,} \end{cases} \\ &= \begin{cases} p^{m+n+1}, & \tau = 0, \mathbf{t} = \mathbf{t}', t_n = t'_n, \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \quad (77)$$

From (66) and (77), we have

$$\begin{aligned} & \Theta(\psi(C_t^k), \psi(C_{t'}^k))(\tau) \\ &= \begin{cases} p^{m+n+1}, & \tau = 0, \mathbf{t} = \mathbf{t}', t_n = t'_n, \\ 0, & \text{otherwise,} \end{cases} \\ &= \begin{cases} p^{m+n+1}, & \tau = 0, t = t', \\ 0, & 0 < |\tau| < p^m, t = t', \\ 0, & 0 \leq |\tau| < p^m, t \neq t'. \end{cases} \end{aligned}$$

Therefore,  $C_k$  forms  $(p^{n+1}, p^m)$ -CCC for any choice of  $k$  in  $\{1, 2, \dots, p-1\}$ .

## APPENDIX C

### PROOF OF PROPOSITION 1

For any element  $(\mathbf{e}_1, \mathbf{e}_2)$  in  $\mathcal{S}$ , we have

$$\begin{aligned} k_1 \mathbf{e}_1 - k_2 \mathbf{e}_2 &\equiv \mathbf{0}_w \pmod{p} \\ \Rightarrow \mathbf{e}_2 &\equiv \begin{pmatrix} k_1 \\ k_2 \end{pmatrix} \mathbf{e}_1 \pmod{p}, \end{aligned}$$

where  $\frac{1}{k_2}$  represents the multiplicative inverse of  $k_2$  with respect to modulo  $p$  operation. Therefore,  $|\mathcal{S}| = p^w$ . Let us define a mapping  $\Lambda : \mathcal{S} \rightarrow \mathbb{Z}$  as follows:

$$\begin{aligned} \Lambda(\mathbf{e}_1, \mathbf{e}_2) &= (\mathbf{e}_2 - \mathbf{e}_1) \cdot (p^{w-1}, p^{w-2}, \dots, 1) \\ &= \sum_{t=0}^{w-1} e_{2,t} p^{w-1-t} - \sum_{t=0}^{w-1} e_{1,t} p^{w-1-t}. \end{aligned} \quad (78)$$

For any two  $(\mathbf{e}_1, \mathbf{e}_2)$  and  $(\mathbf{e}'_1, \mathbf{e}'_2)$  in  $\mathcal{S}$ , we have  $k_1 \mathbf{e}_1 - k_2 \mathbf{e}_2 \equiv \mathbf{0}_w \pmod{p}$  and  $k_1 \mathbf{e}'_1 - k_2 \mathbf{e}'_2 \equiv \mathbf{0}_w \pmod{p}$ , where  $\mathbf{e}_1 = (e_{1,0}, e_{1,1}, \dots, e_{1,w-1})$ ,  $\mathbf{e}_2 = (e_{2,0}, e_{2,1}, \dots, e_{2,w-1})$ ,  $\mathbf{e}'_1 = (e'_{1,0}, e'_{1,1}, \dots, e'_{1,w-1})$ , and  $\mathbf{e}'_2 = (e'_{2,0}, e'_{2,1}, \dots, e'_{2,w-1})$ . Therefore,

$$\begin{aligned} \mathbf{e}_2 - \mathbf{e}_1 &\equiv \left( \frac{k_1 - k_2}{k_2} \right) \mathbf{e}_1 \pmod{p}, \\ \text{and} & \\ \mathbf{e}'_2 - \mathbf{e}'_1 &\equiv \left( \frac{k_1 - k_2}{k_2} \right) \mathbf{e}'_1 \pmod{p}. \end{aligned} \quad (79)$$

From (79), it can be observed that  $\Lambda$  is an injective mapping. Since,  $0 < k_1 \neq k_2 < p$ , and  $k_1 \mathbf{e}_1 - k_2 \mathbf{e}_2 \equiv \mathbf{0}_w \pmod{p}$ ,

$$\Lambda(\mathbf{e}_1, \mathbf{e}_2) = 0 \text{ iff } \mathbf{e}_1 = \mathbf{e}_2 = \mathbf{0}_w.$$

Now let us define two vectors  $\bar{\mathbf{e}}_1$  and  $\bar{\mathbf{e}}_2$  whose components are defined as follows:

$$\bar{e}_{i,\alpha} = \begin{cases} p - e_{i,\alpha}, & \text{if } e_{i,\alpha} \neq 0, \\ 0, & \text{otherwise,} \end{cases} \quad (80)$$

where  $i = 1, 2$ , and  $\alpha = 0, 1, \dots, w-1$ . From (78) and (80), it is clear that  $\Lambda(\mathbf{e}_1, \mathbf{e}_2) = -\Lambda(\bar{\mathbf{e}}_1, \bar{\mathbf{e}}_2)$ . From the mapping, define two sets  $\mathcal{S}' = \{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S} : \Lambda(\mathbf{e}_1, \mathbf{e}_2) \geq 0\}$  and  $\mathcal{S}'' = \{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S} : \Lambda(\mathbf{e}_1, \mathbf{e}_2) \leq 0\}$ . Then the set  $\mathcal{S}$  can be expressed as  $\mathcal{S} = \mathcal{S}' \cup \mathcal{S}''$ , where  $\mathcal{S}' \cap \mathcal{S}'' = \{\mathbf{0}_w\}$ . From (80), we have  $|\mathcal{S}'| = |\mathcal{S}''| = \frac{p^w + 1}{2} = E$ . We assume that  $(\mathbf{e}'_1, \mathbf{e}'_2)$  is an element of  $\mathcal{S}'$  and  $\Lambda(\mathbf{e}'_1, \mathbf{e}'_2) = D_i$ , where  $\mathbf{e}'_j = (e'_{j,0}, e'_{j,1}, \dots, e'_{j,w-1})$ ,  $i = 1, 2, \dots, E$ , and  $j = 1, 2$ . Since,  $(\mathbf{0}_w, \mathbf{0}_w) \in \mathcal{S}'$  and  $\Lambda$  is an injective mapping, without loss of generality, let us assume that  $0 = D_1 < D_2 < \dots < D_E$ .

For  $0 \leq \tau \leq p^m - 1$ , following (9), we have  $\mathbf{B}_\tau(\mathbf{e}'_1, \mathbf{e}'_2) = \{(\gamma, \delta) : \delta = \gamma + \tau, 0 \leq \gamma \leq p^m - \tau - 1, \gamma_\alpha = e'_{1,\alpha}, \delta_\alpha = e'_{2,\alpha}, \alpha = 0, 1, \dots, w-1\}$ , where  $(\gamma_0, \gamma_1, \dots, \gamma_{m-1})$  and  $(\delta_0, \delta_1, \dots, \delta_{m-1})$  are the base- $p$  vector representations of the

non-negative integers  $\gamma$  and  $\delta$ , respectively. Now,

$$\begin{aligned} \tau &= \delta - \gamma \\ &= \sum_{\alpha=0}^{m-1} (\delta_\alpha - \gamma_\alpha) p^{m-\alpha-1} \\ &= \sum_{\alpha=0}^{w-1} (e'_{2,\alpha} - e'_{1,\alpha}) p^{m-\alpha-1} + \sum_{\alpha=w}^{m-1} (\delta_\alpha - \gamma_\alpha) p^{m-\alpha-1} \\ &= p^{m-w} (\mathbf{e}'_2 - \mathbf{e}'_1) \cdot (p^{w-1}, p^{w-2}, \dots, 1) \\ &\quad + \sum_{\alpha=w}^{m-1} (\delta_\alpha - \gamma_\alpha) p^{m-\alpha-1} \\ &= p^{m-w} D_i + \sum_{\alpha=w}^{m-1} (\delta_\alpha - \gamma_\alpha) p^{m-\alpha-1}. \end{aligned}$$

The set  $\mathbf{B}_\tau(\mathbf{e}'_1, \mathbf{e}'_2)$  is non-empty if  $p^{m-w} D_i + \sum_{\alpha=w}^{m-1} ((p-1) - 0) p^{m-\alpha-1} \geq \tau \geq p^{m-w} D_i + \sum_{\alpha=w}^{m-1} (0 - (p-1)) p^{m-\alpha-1}$ , or  $\tau \in [p^{m-w}(D_i - 1) + 1 : p^{m-w}(D_i + 1) - 1] = I_{D_i}$ , say. Hence,

$$\mathbf{B}_\tau(\mathbf{e}'_1, \mathbf{e}'_2) \neq \emptyset \text{ iff } \tau \in I_{D_i}. \quad (81)$$

Let us assume that  $(\mathbf{e}'_1, \mathbf{e}'_2)$  and  $(\mathbf{e}'_1, \mathbf{e}'_2)$  are two distinct elements in  $\mathcal{S}'$  with  $D_{i_1} < D_{i_2}$ . Now

$$\begin{aligned} &I_{D_{i_1}} \cap I_{D_{i_2}} \\ &= \begin{cases} [p^{m-w} D_{i_1} + 1, p^{m-w}(D_{i_1} + 1) - 1], & \text{if } D_{i_2} = D_{i_1} + 1, \\ \emptyset, & \text{if } D_{i_2} > D_{i_1} + 1. \end{cases} \end{aligned} \quad (82)$$

From (82), it is clear that

$$I_{D_{i_1}} \cap I_{D_{i_2}} \neq \emptyset \text{ iff } D_{i_2} = D_{i_1} + 1.$$

Therefore, for a fixed value of  $\tau$  in  $[0, p^m - 1]$ , we need to consider the following three cases: *Case 1:* In this case, we consider  $\tau \notin \cup_{i=1}^E I_{D_i}$ . From (81), we have  $\mathbf{B}_\tau(\mathbf{e}'_1, \mathbf{e}'_2) = \emptyset \forall i \in [1 : E]$ . Since,  $\tau \geq 0$  and  $\mathbf{B}_\tau(\mathbf{e}'_1, \mathbf{e}'_2) = \emptyset \forall i \in [1 : E]$ ,

$$\begin{aligned} &\sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \\ &= \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}'} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \\ &= \sum_{i=1}^E \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}'_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}'_2}))(\tau) \\ &= \sum_{i=1}^E \sum_{(\gamma, \delta) \in \mathbf{B}_\tau(\mathbf{e}'_1, \mathbf{e}'_2)} \xi_q^{g\gamma - h\delta} \\ &= 0. \end{aligned}$$

Therefore,  $\left| \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \right| = 0$  when  $\tau \notin \cup_{i=1}^E I_{D_i}$ .

*Case 2:* In this case, we consider  $\tau \in I_{D_i}$  and  $\tau \notin I_{D_j} \forall i \neq j \in [1 : E]$ . Since  $\tau \notin \cup_{j=1, j \neq i}^E I_{D_j}$ ,

$\mathbf{B}_\tau(\mathbf{e}_1^j, \mathbf{e}_2^j) = \emptyset$  for all  $j \in \{1, 2, \dots, E\} \setminus \{i\}$ . Now  $I_{D_i}$  can be expressed as  $I_{D_i} = ([p^{m-w}(D_i - 1) + 1 : p^{m-w}D_i] \cup ([p^{m-w}D_i : p^{m-w}(D_i + 1) - 1])$ . Now  $\tau$  can be expressed as follows:

$$\tau = \begin{cases} p^{m-w}(D_i - 1) + \tau_1, & \text{if } \tau \in [p^{m-w}(D_i - 1) + 1 : p^{m-w}D_i], \\ p^{m-w}D_i + \tau_2, & \text{if } \tau \in (p^{m-w}D_i : p^{m-w}(D_i + 1) - 1], \end{cases}$$

where  $\tau_1 \in [1 : p^{m-n}]$  and  $\tau_2 \in [1 : p^{m-n} - 1]$ . Also,

$$|\mathbf{B}_\tau(\mathbf{e}_1^i, \mathbf{e}_2^i)| = \begin{cases} \tau_1, & \text{if } \tau \in [p^{m-w}(D_i - 1) + 1 : p^{m-w}D_i], \\ p^{m-w} - \tau_2, & \text{if } \tau \in (p^{m-w}D_i : p^{m-w}(D_i + 1) - 1]. \end{cases} \quad (83)$$

Now,

$$\begin{aligned} & \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \\ &= \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}'} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \\ &= \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1^i}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2^i}))(\tau) \\ & \quad + \sum_{\substack{j=1 \\ j \neq i}}^E \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1^j}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2^j}))(\tau) \\ &= \sum_{(\gamma, \delta) \in \mathbf{B}_\tau(\mathbf{e}_1^i, \mathbf{e}_2^i)} \xi_q^{g_\gamma - h_\delta} + \sum_{\substack{j=1 \\ j \neq i}}^E \sum_{(\gamma, \delta) \in \mathbf{B}_\tau(\mathbf{e}_1^j, \mathbf{e}_2^j)} \xi_q^{g_\gamma - h_\delta} \\ &= \sum_{(\gamma, \delta) \in \mathbf{B}_\tau(\mathbf{e}_1^i, \mathbf{e}_2^i)} \xi_q^{g_\gamma - h_\delta}. \end{aligned} \quad (84)$$

From (83) and (84), we have

$$\begin{aligned} & \left| \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \right| \\ &= \left| \sum_{(\gamma, \delta) \in \mathbf{B}_\tau(\mathbf{e}_1^i, \mathbf{e}_2^i)} \xi_q^{g_\gamma - h_\delta} \right| \\ &\leq \begin{cases} \tau_1, & \text{if } \tau \in [p^{m-w}(D_i - 1) + 1 : p^{m-w}D_i], \\ p^{m-w} - \tau_2, & \text{if } \tau \in (p^{m-w}D_i : p^{m-w}(D_i + 1) - 1]. \end{cases} \end{aligned} \quad (85)$$

Since  $\tau_1 \in [1 : p^{m-w}]$  and  $\tau_2 \in [1 : p^{m-w} - 1]$ , from (85), we have

$$\left| \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \right| \leq p^{m-w}.$$

*Case 3:* In this case, we consider  $\tau \in I_{D_i} \cap I_{D_{i+1}}$  for some  $i \in [1 : E]$ , where  $D_{i+1} = D_i + 1$ . From (82), we have

$$(I_{D_i} \cap I_{D_{i+1}}) = [p^{m-w}D_i + 1 : p^{m-w}(D_i + 1) - 1]. \quad (86)$$

Also,  $\mathbf{B}_\tau(\mathbf{e}_1^i, \mathbf{e}_2^i) = \emptyset \forall i \in [1 : E] \setminus \{i, i + 1\}$ . Therefore,

$$\begin{aligned} & \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \\ &= \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}'} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \\ &= \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1^i}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2^i}))(\tau) \\ & \quad + \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1^{i+1}}, \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2^{i+1}}))(\tau) \\ & \quad + \sum_{\substack{j=1 \\ j \neq i, i+1}}^E \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1^j}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2^j}))(\tau) \\ &= \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1^i}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2^i}))(\tau) \\ & \quad + \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1^{i+1}}, \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2^{i+1}}))(\tau) \\ &= \sum_{(\gamma, \delta) \in \mathbf{B}_\tau(\mathbf{e}_1^i, \mathbf{e}_2^i)} \xi_q^{g_\gamma - h_\delta} + \sum_{(\gamma, \delta) \in \mathbf{B}_\tau(\mathbf{e}_1^{i+1}, \mathbf{e}_2^{i+1})} \xi_q^{g_\gamma - h_\delta}. \end{aligned} \quad (87)$$

From (86),  $\tau \in [p^{m-w}D_i + 1, p^{m-w}(D_i + 1) - 1] = [p^{m-w}(D_{i+1} - 1) + 1, p^{m-w}(D_{i+1}) - 1]$ , then  $\tau$  can be expressed as  $\tau = p^{m-w}D_i + \tau_3 = p^{m-w}(D_{i+1} - 1) + \tau_3$ , where  $\tau_3 \in [1 : p^{m-w} - 1]$ . Therefore,  $|\mathbf{B}_\tau(\mathbf{e}_1^i, \mathbf{e}_2^i)| = p^{m-w} - \tau_3$  and  $|\mathbf{B}_\tau(\mathbf{e}_1^{i+1}, \mathbf{e}_2^{i+1})| = \tau_3$ . From (87), we have

$$\begin{aligned} & \left| \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \right| \\ &= \left| \sum_{(\gamma, \delta) \in \mathbf{B}_\tau(\mathbf{e}_1^i, \mathbf{e}_2^i)} \xi_q^{g_\gamma - h_\delta} + \sum_{(\gamma, \delta) \in \mathbf{B}_\tau(\mathbf{e}_1^{i+1}, \mathbf{e}_2^{i+1})} \xi_q^{g_\gamma - h_\delta} \right| \\ &\leq \left| \sum_{(\gamma, \delta) \in \mathbf{B}_\tau(\mathbf{e}_1^i, \mathbf{e}_2^i)} \xi_q^{g_\gamma - h_\delta} \right| + \left| \sum_{(\gamma, \delta) \in \mathbf{B}_\tau(\mathbf{e}_1^{i+1}, \mathbf{e}_2^{i+1})} \xi_q^{g_\gamma - h_\delta} \right| \\ &\leq p^{m-w} - \tau_3 + \tau_3 = p^{m-w}. \end{aligned}$$

Therefore,

$$\left| \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \right| \leq p^{m-w}.$$

Combining all the above cases, it is clear that

$$\left| \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \right| \leq p^{m-w} \forall \tau \in [0 : p^m - 1].$$

Similarly, it can be shown that

$$\left| \sum_{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{S}} \Theta(\psi(g|_{\mathbf{x}_{J_1}=\mathbf{e}_1}), \psi(h|_{\mathbf{x}_{J_1}=\mathbf{e}_2}))(\tau) \right| \leq p^{m-w} \forall \tau \in [-(p^{m-w} - 1) : 0]. \quad (88)$$

## APPENDIX D

CORRELATION LOWER BOUND WITH RESPECT TO THE POSITIVE-CYCLE-OF-A-SINE-WAVE WEIGHT VECTOR WHEN  $t \in [L + 1 : 2L - 1]$ 

For  $L + 1 \leq t \leq 2L - 1$ , we have the following results from [30]:

$$\begin{aligned} & \sum_{u,v=0}^{t-1} \tau_{u,v,L} w_u w_v \\ &= -\frac{3t-4L+2}{4} - \frac{t}{4} \tan^2 \frac{\pi}{2t} + \frac{t-L-1}{2} \cos \frac{L\pi}{t} \quad (89) \\ & \quad + \left( \frac{2t-2L+1}{4} \tan \frac{\pi}{2t} + \frac{3}{4 \tan \frac{\pi}{2t}} \right) \sin \frac{L\pi}{t}. \end{aligned}$$

To simplify the derivation, in (35) and (89), we consider the following approximations:

$$\sum_{u=0}^{2L-2} w_u^2 = \frac{t}{2} \tan^2 \frac{\pi}{2t} \approx \frac{\pi^2}{8t},$$

where  $t$  is sufficiently large,

$$\begin{aligned} \sin \frac{L\pi}{t} &\approx \frac{1.3L\pi}{t} - \frac{0.4L^2\pi^2}{t^2}, \\ \cos \frac{L\pi}{t} &\approx 1.3 \left( \frac{\pi}{2} - \frac{L\pi}{t} \right) - 0.4 \left( \frac{\pi}{2} - \frac{L\pi}{t} \right)^2. \end{aligned}$$

With the above approximations, it follows from (22), (35), and (89) that

$$\theta^2 \geq \frac{MN}{80(N-1)} \left( a_0 t + \frac{a_1}{t} + \frac{a_2}{t^2} + \frac{a_3}{t^3} + a_4 \right), \quad (90)$$

where  $a_0 = 4\pi^2 - 26\pi + 60$ ,  $a_1 = 5\pi^2 - \frac{10L^2\pi^2}{N} - 10L\pi^2 - 4L^2\pi + 32L^2\pi^2 - 52L\pi$ ,  $a_2 = 10L^2\pi^2 + 8L^2\pi^3 - 16L^3\pi^2 - 13L\pi^2$ ,  $a_3 = 4L^2\pi^3 - 8L^3\pi^3$ , and  $a_4 = 40 - 156L + 26\pi - 4\pi^2 - 20L\pi^2 + 78L\pi$ . It is challenging to get the maximum value of this lower bound. As an alternation, we provide a numerical comparisons between the above lower bound with the other lower bounds finalized in Remark 2. In Figure 6 (a), (b), (c), and (d), the lower bound in (90) is denoted as  $\theta_1$ , which is compared with the lower bounds  $\theta_2$  in (24) for  $N = 2$  and  $3 \leq L \leq 1000$ ,  $\theta_3$  in (40) for  $N = 3$ ,  $1000 \geq L \geq 26$ , and for  $N = 4$ ,  $5 \leq L \leq 1000$ , and the lower bound  $\theta_4$  in (41) for  $N = 5$  and  $5 \leq L \leq 1000$ .

## REFERENCES

- [1] M. J. E. Golay, "Complementary series," *IRE Trans. Inf. Theory*, vol. 7, no. 2, pp. 82–87, Apr. 1961.
- [2] C.-C. Tseng and C. Liu, "Complementary sets of sequences," *IEEE Trans. Inf. Theory*, vol. 18, no. 5, pp. 644–652, Sep. 1972.
- [3] A. Rathinakumar and A. K. Chaturvedi, "Complete mutually orthogonal Golay complementary sets from Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 1339–1346, Mar. 2008.
- [4] H.-H. Chen, *The Next Generation CDMA Technologies*. Wiley, 2007.
- [5] 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.

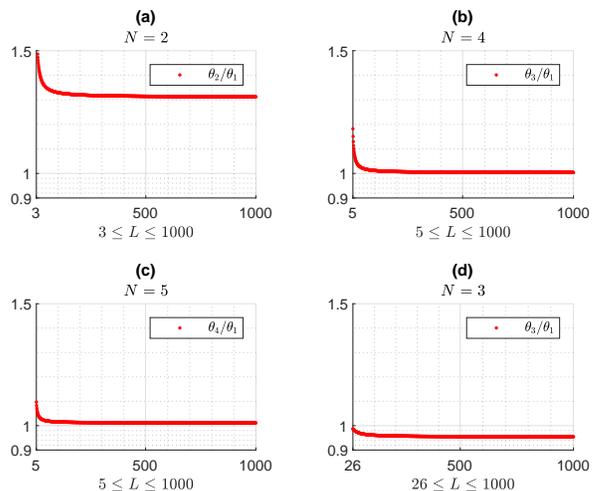


Figure 6: Comparison of the lower bound  $\theta_1$  with the lower bounds  $\theta_2$ ,  $\theta_3$ , and  $\theta_4$

- [6] N. Suehiro and M. Hatori, "N-shift cross-orthogonal sequences," *IEEE Trans. Inf. Theory*, vol. 34, no. 1, pp. 143–146, Jan. 1988.
- [7] Z. L. Liu, Y. L. Guan, B. C. Ng, and H.-H. Chen, "Correlation and set size bounds of complementary sequences with low correlation zone," *IEEE Trans. Commun.*, vol. 59, no. 12, pp. 3285–3289, Dec. 2011.
- [8] P. Sarkar, S. Majhi, H. Vettikalladi, and A. S. Mahajumi, "A direct construction of inter-group complementary code set," *IEEE Access*, vol. 6, pp. 42047–42056, Aug. 2018.
- [9] P. Sarkar, S. Majhi, and Z. Liu, "Optimal Z-complementary code set from generalized Reed-Muller codes," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 1783–1796, Mar. 2019.
- [10] P. Sarkar, S. Majhi, and Z. Liu, "Pseudo-Boolean functions for optimal z-complementary code sets with flexible lengths," *IEEE Signal Process. Lett.*, vol. 28, pp. 1350–1354, July 2021.
- [11] Z. Liu, U. Parampalli, Y. L. Guan, and S. Boztas, "Constructions of optimal and near-optimal quasi-complementary sequence sets from Singer difference sets," *IEEE Wireless Commun. Lett.*, vol. 2, no. 5, pp. 487–490, Oct. 2013.
- [12] A. Samad and S. Majhi, "A near-optimal and low-complex joint multiuser detection for QCSS-MC-CDMA system," *IEEE Systems Journal*, vol. 15, no. 2, pp. 1594–1603, June 2021.
- [13] 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.
- [14] L. Welch, "Lower bounds on the maximum cross correlation of signals (corresp.)," *IEEE Trans. Inf. Theory*, vol. 20, no. 3, pp. 397–399, May 1974.
- [15] 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.
- [16] V. Levenshtein, "New lower bounds on aperiodic crosscorrelation of binary codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 284–288, Jan. 1999.
- [17] Y. Li, T. Liu, and C. Xu, "Constructions of asymptotically optimal quasi-complementary sequence sets," *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1516–1519, Aug. 2018.
- [18] 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, Mar. 2019.
- [19] —, "Constructions of quasi-complementary sequence sets associated

- with characters,” *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4597–4608, July 2019.
- [20] G. Luo, X. Cao, M. Shi, and T. Hellesteth, “Three new constructions of asymptotically optimal periodic quasi-complementary sequence sets with small alphabet sizes,” *IEEE Trans. Inf. Theory*, vol. 67, no. 8, pp. 5168–5177, Aug. 2021.
- [21] Y. Li, L. Tian, and C. Xu, “Constructions of asymptotically optimal aperiodic quasi-complementary sequence sets,” *IEEE Trans. Commun.*, vol. 67, no. 11, pp. 7499–7511, Nov. 2019.
- [22] Z. Zhou, F. Liu, A. R. Adhikary, and P. Fan, “A generalized construction of multiple complete complementary codes and asymptotically optimal aperiodic quasi-complementary sequence sets,” *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3564–3571, June 2020.
- [23] A. R. Adhikary, Y. Feng, Z. Zhou, and P. Fan, “Asymptotically optimal and near-optimal aperiodic quasi-complementary sequence sets based on florentine rectangles,” *IEEE Trans. Commun.*, vol. 70, no. 3, pp. 1475–1485, Mar. 2022.
- [24] Q. Zeng, Z. Liu, and G. Gradoni, “Optimal quasi-orthogonal FH sequences with adaptive array receiver for massive connectivity in asynchronous multi-cluster networks,” *IEEE Trans. Wireless Commun.*, vol. 21, no. 8, pp. 5730–5743, Aug. 2022.
- [25] X. Tang and W. H. Mow, “Design of spreading codes for quasi-synchronous CDMA with intercell interference,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 1, pp. 84–93, Jan. 2006.
- [26] P. Sarkar, Z. Liu, and S. Majhi, “A direct construction of complete complementary codes with arbitrary lengths,” 2021. [Online]. Available: <https://arxiv.org/abs/2102.10517>
- [27] R. Kumar, P. Sarkar, P. K. Srivastava, and S. Majhi, “A direct construction of asymptotically optimal type-II zcp for every possible even length,” *IEEE Signal Process. Lett.*, vol. 28, pp. 1799–1802, Aug. 2021.
- [28] T. Liu, X. Men, Y. Li, and X. Chen, “Constructions of 2-D Golay complementary array sets for MIMO omnidirectional transmission,” *IEEE Commun. Lett.*, vol. 26, no. 7, pp. 1459–1463, July 2022.
- [29] K. G. Paterson, “Generalized Reed-Muller codes and power control in OFDM modulation,” *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 104–120, Jan. 2000.
- [30] Z. Liu, U. Parampalli, Y. L. Guan, and S. Boztaş, “A new weight vector for a tighter Levenshtein bound on aperiodic correlation,” *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1356–1366, Feb. 2014.