Optimal Z-complementary Code Set From Generalized Reed-Muller Codes

Palash Sarkar, Sudhan Majhi, and Zilong Liu

Abstract

Z-complementary code set (ZCCS), an extension of perfect complementary codes (CCs), refers to a set of two-dimensional matrices having zero correlation zone properties. ZCCS can be used in various multi-channel systems to support, for example, quasi-synchronous interference-free multicarrier code-division multiple access communication and optimal channel estimation in multiple-input multiple-output systems. Traditional constructions of ZCCS heavily rely on a series of sequence operations which may not be feasible for rapid hardware generation particularly for long ZCCSs. In this paper, we propose a direct construction of ZCCS using second-order Reed-Muller codes with efficient graphical representation. Our proposed construction, valid for any number of isolated vertices present in the graph, is capable of generating optimal ZCCS meeting the set size upper bound.

Index Terms

Complementary code (CC), code division multiple access (CDMA), generalized Boolean function (GBF), multiple-input multiple-output (MIMO), Reed-Muller (RM) codes, Z-complementary code set (ZCCS), zero correlation zone (ZCZ)

This work was supported in part by the Visvesvaraya Young Faculty Research Fellowship, Ministry of Electronics and Information Technology, Government of India, being implemented by the Digital India Corporation and Early Career Young Scientists by the Science and Engineering Research Board under the Department of Science and Technology, Government of India. The work of Z. Liu was supported in part by National Natural Science Foundation of China (Grant No. 61750110527), Research Fund for International Young Scientists.

Palash Sarkar is with Department of Mathematics and Sudhan Majhi is with the Department of Electrical Engineering, Indian Institute of Technology Patna, India, e-mail: palash.pma15@iitp.ac.in; smajhi@iitp.ac.in.

Zilong Liu is with Institute for Communication Systems, 5G Innovation Centre, University of Surrey, UK, e-mail: zilong.liu@surrey.ac.uk.

I. INTRODUCTION

Code-division multiple-access (CDMA) technology is an important multiuser communication scheme where spreading sequences play a fundamental role in determining the system performance. Traditional spreading sequences, such as Walsh-Hadamard sequences, pseudo-random sequences (e.g., Gold sequences, Kasami sequences, optimal $\mathbb{Z}_4$ sequences), constant amplitude zero auto-correlation (CAZAC) sequences, generally exhibit nonzero cross-correlation properties over asynchronous transmission channels. Because of this, their corresponding CDMA systems may suffer from severe "near-far effect" whereby the desired signals could be overwhelmed by multiple-access interference (MAI). In legacy CDMA systems (e.g., 3G), tedious power control is applied to suppress the near-far effect. In this paper, we are focused on Z-complementary code set (ZCCS) which is capable of supporting interference-free multicarrier CDMA (MC-CDMA) in quasi-synchronous channels (without the need of power control) [1].

In [2], M. J. E. Golay proposed a pair of sequences, known as Golay complementary pair (GCP), with the property that the sum of their aperiodic auto-correlation function (AACF) is zero everywhere except at the zero-shift position. Either sequence in a GCP is called a Golay sequence. In [3], Tseng and Liu extended the idea of GCP to complementary code (CC) each consisting of two or more constituent sequences with the same AACF property. Davis and Jedwab proposed a direct construction of GCP from generalized Boolean function (GBF) to reduce the peak-to-mean envelope power ratio (PMEPR) of orthogonal frequency division multiplexing (OFDM) system [4]–[6]. As a generalization of the Davis-Jedwab construction, Paterson proposed a construction of CC in [7] by associating each CC with a graph[1]. In [7, Th. 24], it is found that after applying deletion operation to several vertices of certain graphs, if the resulting graph consists of a path and one isolated vertex, then the code corresponding to the graph is a CC. Paterson's idea was further extended by Rathinakumar and Chaturvedi [9] for mutually orthogonal Golay complementary sets (MOGCS) which are also called complete complementary codes (CCCs) in this paper. Formally, CCC refers to a collection of CCs where each CC is a two-dimensional matrix (called a complementary matrix) and any two distinct CCs have zero aperiodic cross-correlation sums. The Rathinakumar-Chaturvedi construction, however, gives little information on the code generation when some isolated vertices are present (after deletion operation) in the

[1]Although Paterson's construction is limited to second-order generalized Reed-Muller (RM) codes, generalization to higher-order ones can be found in [8].

associated graph. Recently, a new class of CCC has been introduced in [10] for multi-carrier code division multiple access (MC-CDMA) with column sequence PMEPR of at most 2. This is achieved by properly designing CCs (complementary matrices) such that every column sequence of a complementary matrix is a Golay sequence. The application of CCC has been extended to interference-free MC-CDMA communication by designing a fractional-delay resilient receiver [11].

A drawback of CCC is that the set size is limited by the number of row sequences in each complementary matrix [10]–[13]. This problem can be fixed by ZCCS whose aperiodic auto- and cross-correlation functions display zero correlation zone (ZCZ) properties and whose set size is several times of that of CCC [14]. The ZCZ properties of ZCCS allow MAI mitigation provided that all the received multiuser signals are roughly synchronous within the ZCZ width [15]. In the literature, binary ZCCSs were first introduced by Fan *et al.* [16] and later were extended to generalized pairwise ZCCSs by Feng *et al.* [17] for power efficient quadrature carrier modems. There are another type set of codes, introduced in [18], [19], known as inter-group complementary code set which can be derived as special case of ZCCS. In addition to their applications in MC-CDMA [18], ZCCS have also been employed as optimal training sequences in multiple-input multiple-output (MIMO) communications [20], [21].

In this paper, we propose a direct construction of optimal ZCCS from second-order cosets of the q-ary generalization of the first-order RM codes through a graphical representation. Specifically, we first construct a set of 2^{k+p} codes, each containing 2^{k+1} constituent sequences of length 2^m. These codes are characterized by a graph (consisting of m vertices in total) with the property that deleting k vertices and their associated edges, the entire graph reduces to a path over $m-k-p$ vertices (where all the relevant edges have identical weight of $q/2$) and p isolated vertices. Then, we construct another set of codes by reversing and taking conjugate of the first set of codes. It is interesting to note that the cross-correlation between any two codes from different sets is zero everywhere and the union of these two sets gives a ZCCS of size 2^{k+p+1}. Our proposed construction is flexible in that the ZCZ width and set size of the proposed ZCCS can be varied by freely changing the number of isolated vertices (i.e., p) in the graph. It is shown that the CCC in [9] is a special case of our proposed construction when the number of isolated vertices is set to zero, i.e., $p=0$. It is noted that our proposed construction generates ZCCS directly based on GBF and does not rely on any recursive sequence operations. Hence, the proposed construction is suitable for rapid hardware generation particularly for long ZCCSs.

An efficient hardware generator (based on logic AND gates, selectors, and adders) for 16-QAM almost-complementary sequences can be found in [22, Example 1]. We also point out that the CCC in [10], similar to [9], are characterized by a graph which after deleting some vertices and their associated edges, constitutes one path but with no isolated vertex. This is a major difference with our proposed construction for ZCCS in graph representation.

The remainder of the paper is organized as follows. In Section II, some useful notations and definitions are given. In Section III, a construction of ZCCS is presented and its optimal condition is derived. Later, the proposed ZCCS construction is illustrated by an example. Finally, concluding remarks are drawn in Section IV.

II. Preliminary

A. Definitions of Correlations and Sequences

Let $\mathbf{a} = (a_0, a_1, \cdots, a_{L-1})$ and $\mathbf{b} = (b_0, b_1, \cdots, b_{L-1})$ be two complex-valued sequences of equal length L. For an integer τ, define

$$C(\mathbf{a}, \mathbf{b})(\tau) = \begin{cases} \sum_{i=0}^{L-1-\tau} a_{i+\tau} b_i^*, & 0 \le \tau < L, \\ \sum_{l=0}^{L+\tau-1} a_i b_{i-\tau}^*, & -L < \tau < 0, \\ 0, & \text{otherwise}, \end{cases} \tag{1}$$

and $A(\mathbf{b})(\tau) = C(\mathbf{b}, \mathbf{b})(\tau)$. These functions are called aperiodic CCF (ACCF) between $\mathbf{a}$ and $\mathbf{b}$ and the AACF of $\mathbf{b}$, respectively. Let $\mathbf{C} = \{C_0, C_1, \cdots, C_{K-1}\}$ be a set of K matrices (codes), each having order $M \times L$ as follows.

$$C_\mu = \begin{bmatrix} \mathbf{a}_0^\mu \\ \mathbf{a}_1^\mu \\ \vdots \\ \mathbf{a}_{M-1}^\mu \end{bmatrix}_{M \times L}, \tag{2}$$

where $\mathbf{a}_\nu^\mu$ $(0 \le \nu \le M-1, 0 \le \mu \le K-1)$ is the ν-th row sequence or ν-th constituent sequence of C_μ. Let C_{μ_1}, $C_{\mu_2} \in \mathbf{C}$ $(0 \le \mu_1, \mu_2 \le K-1)$ be any two matrices in $\mathbf{C}$. The ACCF of C_{μ_1} and C_{μ_2} is defined by

$$C(C_{\mu_1}, C_{\mu_2})(\tau) = \sum_{\nu=0}^{M-1} C(\mathbf{a}_\nu^{\mu_1}, \mathbf{a}_\nu^{\mu_2})(\tau). \tag{3}$$

Definition 1: Code set **C** is said to be a set of CCC if $K = M$ and

$$C(C_{\mu_1}, C_{\mu_2})(\tau) = \begin{cases} LK, & \tau = 0, \mu_1 = \mu_2; \\ 0, & 0 < |\tau| < L, \mu_1 = \mu_2; \\ 0, & |\tau| < L, \mu_1 \neq \mu_2. \end{cases} \tag{4}$$

In the above definition, each code C_μ $(0 \leq \mu \leq K-1)$, is said to be a CC. When $M = 2$, C_μ reduces to a GCP and either sequence of the pair is called a Golay sequence.

Definition 2: Code set **C** is called a ZCCS denoted by (K, Z)-ZCCS$_M^L$ if

$$C(C_{\mu_1}, C_{\mu_2})(\tau) = \begin{cases} LM, & \tau = 0, \mu_1 = \mu_2, \\ 0, & 0 < |\tau| < Z, \mu_1 = \mu_2, \\ 0, & |\tau| < Z, \mu_1 \neq \mu_2, \end{cases} \tag{5}$$

where Z is called ZCZ width.

B. Generalized Boolean Functions

Let f be a function of m variables $x_0, x_1, \cdots, x_{m-1}$ over $\mathbb{Z}_q$. A monomial of degree k is defined as the product of any k distinct variables among $x_0, x_1 \cdots x_{m-1}$. There are 2^m distinct monomials over m variables listed below:

$$1, x_0, x_1, \cdots, x_{m-1}, x_0x_1, x_0x_2, \cdots, x_{m-2}x_{m-1}, \cdots, x_0x_1 \cdots x_{m-1}. \tag{6}$$

A function f is said to be a GBF if it can uniquely be expressed as a linear combination of these 2^m monomials, where the coefficient of each monomial is drawn from $\mathbb{Z}_q$. Corresponding to each GBF f, we define a complex valued sequence $\psi(f)$ of length 2^m by defining $\psi(f) = (\omega^{f_0}, \omega^{f_1}, \cdots, \omega^{f_{2^m-1}})$, where $f_i = f(i_0, i_1, \cdots, i_{m-1})$, $\omega = \exp(2\pi\sqrt{-1}/q)$ (q is a positive integer no less than 2) and $(i_0, i_1, \cdots, i_{m-1})$ is the binary vector representation of integer i $(i = \sum_{j=0}^{m-1} i_j 2^j)$. We denote by $\bar{x} = 1 - x$ the binary complement of $x \in \{0, 1\}$. For any given GBF f in m variables, we denote the function $f(1-x_0, 1-x_1, \cdots, 1-x_{m-1})$ or $f(\bar{x}_0, \bar{x}_1, \cdots, \bar{x}_{m-1})$ by $\tilde{f}$. For a complex-valued sequence **a**, let $\tilde{\mathbf{a}}$ denote the sequence obtained by reversing **a** and $\mathbf{a}^*$ its complex conjugate.

C. Some Families of Codes

A linear code over $\mathbb{Z}_q$ of length L is closed under linear combinations of sequences (called codewords). Corresponding to any such code ζ there is a generator matrix G. Linear combinations of the rows of G generate the code. For any fixed sequence $\mathbf{a}$ of length L, $\mathbf{a}+\zeta$ denotes a coset of ζ and $\mathbf{a}$ is said to be a coset representative of ζ. $\mathrm{RM}_q(r,m)$ is said to be the rth order RM code whose codewords are $\mathbb{Z}_q$-valued sequences identified with GBFs of degree at most r in $x_0, x_1, \cdots, x_{m-1}$. The rows of generator matrix G for $\mathrm{RM}_q(r,m)$ are $\mathbb{Z}_q$-valued sequences corresponding to distinct monomials of degree at most r over the variables $x_0, x_1, \cdots, x_{m-1}$. The reader is referred to [7] for more details.

Example 1: Consider $\mathrm{RM}_2(2,3)$, generated by vectors corresponding to the monomials of degree at most 2 in variables x_0, x_1 and x_2. The generator matrix G of $\mathrm{RM}_2(2,3)$ is given as follows.

$$\begin{bmatrix} 11111111 \\ 01010101 \\ 00110011 \\ 00001111 \\ 00010001 \\ 00000101 \\ 00000011 \end{bmatrix} \quad \begin{matrix} 1 \\ x_0 \\ x_1 \\ x_2 \\ x_0x_1 \\ x_0x_2 \\ x_1x_2 \end{matrix}$$

D. Quadratic Forms and Graphs of GBFs

In this subsection, we introduce some lemmas and notations which will be used for our proposed constructions in the next section.

Definition 3: Let f be a GBF of m variables $x_0, x_1, \cdots, x_{m-1}$ over $\mathbb{Z}_q$. Consider a list of k $(0 \leq k < m)$ indices $0 \leq j_0 < j_1 < \cdots j_k < m$ and write $\mathbf{x} = (x_{j_0}, x_{j_1}, \cdots, x_{j_{k-1}})$. Also, consider $\mathbf{c} = (c_0, c_1, \cdots, c_{k-1})$ which is a fixed binary sequence. Define $\psi(f|_{\mathbf{x}=\mathbf{c}})$ as a complex-valued sequence with $\omega^{f(i_0,i_1,\cdots,i_{m-1})}$ as ith component if $i_{j_\alpha} = c_\alpha$ for each $0 \leq \alpha < k$ and equal to zero otherwise, where ω is a (complex-valued) qth root of unity. For $k = 0$, $\psi(f|_{\mathbf{x}=\mathbf{c}})$ reduces to the sequence $\psi(f)$ which has been defined in Subsection II-B.

Let Q be the quadratic form of f. Then, the GBF f can be expressed as [9]

$$f = Q + \sum_{i=0}^{m-1} g_i x_i + g', \tag{7}$$

where $g', g_i \in \mathbb{Z}_q$ are arbitrary.

For a quadratic GBF f, let $G(f)$ denote the graph of f which is obtained by joining the vertices x_i and x_j by an edge if there is a term $q_{i,j}x_ix_j$ $(0 \leq i < j \leq m-1)$ in the GBF f with $q_{i,j} \neq 0$ $(q_{i,j} \in \mathbb{Z}_q)$. Consider the function $f|_{x_j=c}$, obtained by substituting $x_j = c$ in f. It follows that the graph of $f|_{x_j=c}$ is equal to the graph obtained by deleting vertex j from $G(f)$. Similarly the graph of $f|_{\mathbf{x}=\mathbf{c}}$ is obtained by deleting vertices $x_{j_0}, x_{j_1}, \cdots, x_{j_{k-1}}$ from $G(f)$. The final graph is independent of the choice of $\mathbf{c}$. That is, for any $\mathbf{c}$, the quadratic part of the function $f|_{\mathbf{x}=\mathbf{c}}$ is completely described by the graph which is obtained from $G(f)$ by deleting vertices $x_{j_0}, x_{j_1}, \cdots, x_{j_{k-1}}$. Note that the quadratic forms in the functions f and $\tilde{f}$ are the same and therefore, they have the same associated graph.

Example 2: Let f be a GBF of 3 variables over $\mathbb{Z}_2$, as follows

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

Let $\mathbf{x} = (x_0, x_2)$ and $\mathbf{c} = (0, 1)$. Then, the complex-valued vector corresponding to $f|_{x=c}$ can be written as follows.

$$\psi(f|_{\mathbf{x}=\mathbf{c}}) = (0, 0, 0, 0, -, 0, -, 0).$$

E. Truncated Restricted Vectors

Let $\psi(f) = (F_0, F_1, \cdots, F_{L-1})$ be a complex-valued vector of length L and $\psi(f|_{\mathbf{x}=\mathbf{c}})$ be a restriction of it. Also, let $i_{\mathbf{c}}$ and $\bar{i_{\mathbf{c}}}$ be the first and last nonzero entries in the restricted vector $\psi(f|_{\mathbf{x}=\mathbf{c}})$, we have

$$\psi(f|_{\mathbf{x}=\mathbf{c}}) = (0, \cdots, 0, F_{i_{\mathbf{c}}}, F_{i_{\mathbf{c}}+1}, \cdots, F_{\bar{i_{\mathbf{c}}}-1}, F_{\bar{i_{\mathbf{c}}}}, 0, \cdots, 0),$$

where the entries F_i for $i_{\mathbf{c}} < i < \bar{i_{\mathbf{c}}}$, may not necessarily be nonzero. Then, the truncated vector is obtained by truncating the leading and trailing zeros of the restricted vector which is denoted as follows.

$$[\psi(f|_{\mathbf{x}=\mathbf{c}})] = (F_{i_{\mathbf{c}}}, F_{i_{\mathbf{c}}+1}, \cdots, F_{\bar{i_{\mathbf{c}}}-1}, F_{\bar{i_{\mathbf{c}}}}). \tag{8}$$

Lemma 1: [7] Let f, g be GBFs of m variables. Consider $0 \leq j_0 < j_1 < \cdots < j_{k-1} < m$, which is a list of k indices and $\mathbf{c} = (c_0c_1 \cdots c_{k-1})$ and $\mathbf{d} = (d_0d_1 \cdots d_{k-1})$ are two binary

vectors. Write $\mathbf{x} = (x_{j_0} x_{j_1} \cdots x_{j_{k-1}})$ and consider $0 \le i_0 < i_1 < \cdots < i_{l-1} < m$, which is a set of indices which has no intersection with $\{j_0, j_1, \cdots, j_{k-1}\}$. Let $\mathbf{y} = (x_{i_0} x_{i_1} \cdots x_{i_{l-1}})$, then

$$\begin{aligned} &C\left(\psi(f|_{\mathbf{x}=\mathbf{c}}), \psi(g|_{\mathbf{x}=\mathbf{d}})\right)(\tau) \\ &\quad = \sum_{\mathbf{c}_1, \mathbf{c}_2} C\left(\psi(f|_{\mathbf{xy}=\mathbf{cc}_1}), \psi(g|_{\mathbf{xy}=\mathbf{dc}_2})\right)(\tau). \end{aligned} \tag{9}$$

Lemma 2: ([23, Lemma. 1.20]) Let f, g be GBFs of m variables and $\psi(f|_{\mathbf{x}=\mathbf{c}_1})$, $\psi(g|_{\mathbf{x}=\mathbf{c}_2})$ be the corresponding vectors restricting variables $\mathbf{x}$ to $\mathbf{c}_1$ and $\mathbf{c}_2$ for f and g, respectively. Consider $i_{\mathbf{c}_j}$ which is the index of the first nonzero entry in the vector $\psi(.|_{\mathbf{x}=\mathbf{c}_j})$, $j = 1$ or 2, and n_x the length of nonzero pattern. Then, the cross-correlation of the restricted vectors is given by a shifted cross-correlation of the truncated vectors as follows.

$C\left(\psi(f|_{\mathbf{x}=\mathbf{c}_1}), \psi(g|_{\mathbf{x}=\mathbf{c}_2})\right)(\tau)$

$$= \begin{cases} C\left([\psi(f|_{\mathbf{x}=\mathbf{c}_1})], [\psi(g|_{\mathbf{x}=\mathbf{c}_2})]\right)(\tau - (i_{\mathbf{c}_1} - i_{\mathbf{c}_2})), \\ \quad \text{if } (i_{\mathbf{c}_1} - i_{\mathbf{c}_2}) - (n_{\mathbf{x}} - 1) \le \tau \le (i_{\mathbf{c}_1} - i_{\mathbf{c}_2}) + (n_{\mathbf{x}} - 1); \\ 0, \ \text{otherwise.} \end{cases} \tag{10}$$

In particular, when $f = g$ and $\mathbf{c}_1 = \mathbf{c}_2 = \mathbf{c}$,

$$\begin{aligned} &A\left(\psi(f|_{\mathbf{x}=\mathbf{c}})\right)(\tau) \\ &\quad = \begin{cases} A([\psi(f|_{\mathbf{x}=\mathbf{c}})])(\tau), & -(n_{\mathbf{x}} - 1) \le \tau \le (n_{\mathbf{x}} - 1), \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

Lemma 2 will be used in the proof of *Lemma* 5.

Example 3: Let f and g be GBFs of 4 variables over $\mathbb{Z}_2$, as follows.

$$f(x_0, x_1, x_2, x_3) = x_0 x_1 + x_2 x_3 + x_0,$$

$$g(x_0, x_1, x_2, x_3) = x_0 x_2 + x_1 x_3.$$

Let $\mathbf{x} = x_0 x_2$, $\mathbf{c}_1 = (0, 1)$ and $\mathbf{c}_2 = (1, 0)$. Then, the restricted vectors of f and g at $\mathbf{x} = \mathbf{c}_1$ and $\mathbf{x} = \mathbf{c}_2$ are

$$\psi(f|_{\mathbf{x}=\mathbf{c}_1}) = (0, 0, 0, 0, +, 0, +, 0, 0, 0, 0, 0, -, 0, -, 0),$$

$$\psi(g|_{\mathbf{x}=\mathbf{c}_2}) = (0, +, 0, +, 0, 0, 0, 0, 0, +, 0, -, 0, 0, 0, 0).$$

The length of the nonzero pattern $n_{\mathbf{x}} = \bar{i_{\mathbf{c}_j}} - i_{\mathbf{c}_j} + 1$, where $i_{\mathbf{c}_j}$ and $\bar{i_{\mathbf{c}_j}}$ are the indices of the first and last nonzero entries in the vector $\psi(f|_{\mathbf{x}=\mathbf{c}_j})$ $(j = 1, 2)$. Therefore $i_{\mathbf{c}_1} = 4$, $i_{\mathbf{c}_2} = 1$ and $n_{\mathbf{x}} = 11$. Now, we have

$$\begin{aligned}&(C\ (\psi(f|_{\mathbf{x}=\mathbf{c}_1}), \psi(g|_{\mathbf{x}=\mathbf{c}_2}))(\tau))_{\tau=-15}^{15}\\ &\quad = (0^8, -1, 0^3, 1, 0^3, 2, 0, 2, 0^5, -1, 0, -2, 0, -1, 0^2),\end{aligned} \tag{11}$$

where 0^m denotes m consecutive zeros.

Therefore

$$\begin{aligned}&C\left(\psi(f|_{\mathbf{x}=\mathbf{c}_1}), \psi(g|_{\mathbf{x}=\mathbf{c}_2})\right)(\tau)\\ &= \begin{cases} C([\psi(f|_{\mathbf{x}=\mathbf{c}_1})], [\psi(g|_{\mathbf{x}=\mathbf{c}_2})])(\tau+3), & -7 \le \tau \le 13,\\ 0, & \text{otherwise.}\end{cases}\end{aligned} \tag{12}$$

Lemma 3: (Construction of CCC [9])

Let f be a GBF of m variables and $\tilde{f}$ be its reversal. Suppose $G(f)$ contains a set of k distinct vertices labeled $j_0, j_1, \cdots, j_{k-1}$ with the property that deleting those k vertices and all their edges results in a path with $q/2$ being the weight of every edge of the path. Let $(t_0, t_1, \cdots, t_{k-1})$ be the binary representation of the integer t. Define the complementary code C_t to be

$$\left\{ f + \frac{q}{2}\left(\sum_{\alpha=0}^{k-1} d_\alpha x_{j_\alpha} + \sum_{\alpha=0}^{k-1} t_\alpha x_{j_\alpha} + d x_\gamma\right) : d, d_\alpha \in \{0,1\}\right\}, \tag{13}$$

and the counterpart CC $\bar{C}_{2^k+t}$ to be

$$\left\{ \tilde{f} + \frac{q}{2}\left(\sum_{\alpha=0}^{k-1} d_\alpha \bar{x}_{j_\alpha} + \sum_{\alpha=0}^{k-1} t_\alpha \bar{x}_{j_\alpha} + \bar{d} x_\gamma\right) : d, d_\alpha \in \{0,1\}\right\}, \tag{14}$$

where γ be the label of either end vertex in the path. Then

$$\{\psi(C_t) : 0 \le t < 2^k\} \cup \{\psi^*(\bar{C}_{2^k+t}) : 0 \le t < 2^k\} \tag{15}$$

generate a set of CCC, where $\psi^*(\cdot)$ denotes the complex conjugate of $\psi(\cdot)$.

Lemma 3 will be used in *Theorem* 2 to show that the construction of CCC in [9] is a special case of our construction.

Lemma 4: ([14]) For any ZCCS with the parameters K, M, L and Z, the theoretical bound is given by

$$K \le M\lfloor L/Z \rfloor, \tag{16}$$

where Z is the ZCZ width, K is the number of Z-complementary codes, M is the number of constituent sequences in a Z-complementary code and L is the length of each constituent sequence. We call a ZCCS optimal if the equality in (16) is achieved.

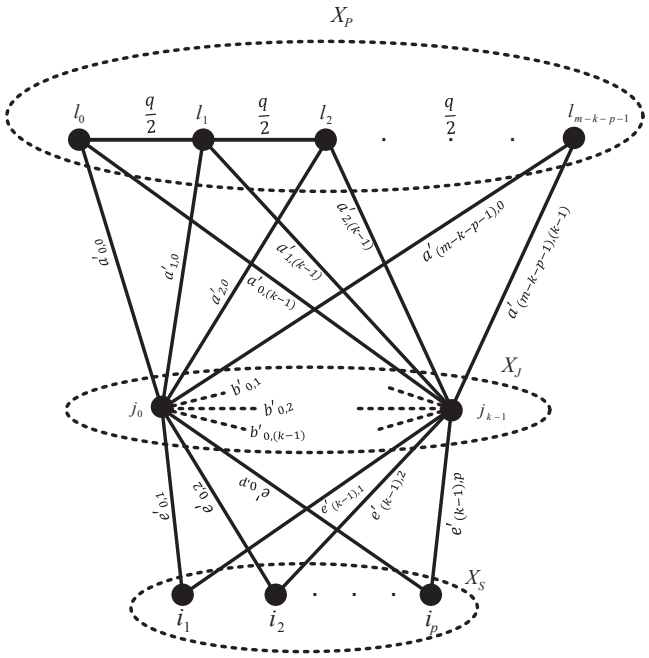

Fig. 1: The graph of the quadratic form Q.

III. Proposed Construction of Z-complementary code Set

In this section, we present a direct construction of ZCCS over $\mathbb{Z}_q$ using a generic graph as shown in Fig. 1. Specifically, Fig. 1 contains m vertices denoted by set $X_I = \{x_0, x_1, \cdots, x_{m-1}\}$. These m vertices are divided into three disjoint sets: $X_P = \{x_{l_0}, x_{l_1}, \cdots, x_{l_{m-k-p-1}}\}$ represents the vertices of a path whose edges have identical weight of $q/2$, $X_J = \{x_{j_0}, x_{j_1}, \cdots, x_{j_{k-1}}\}$, and $X_S = \{x_{i_1}, x_{i_2}, \cdots, x_{i_p}\}$. $a'_{i,\alpha}$'s denote the weights of the edges between vertices from X_P and X_J, $e'_{\alpha,\beta}$'s denote the weights of the edges between vertices from X_J and X_S, and b'_{α_1,α_2}'s denote the weights of edges between any two vertices from X_J. From the graph, it is clear that after deleting all the vertices from the set X_J, the resulting graph contains a path of vertices in the set X_P and p isolated vertices of the set X_S. The quadratic part of the GBF corresponding to the above graph can be expressed as follows.

$$\begin{aligned} Q =& \frac{q}{2} \sum_{i=0}^{m-k-p-2} x_{l_i} x_{l_{i+1}} + \sum_{i=0}^{m-k-p-1} \sum_{\alpha=0}^{k-1} a'_{i,\alpha} x_{l_i} x_{j_\alpha} \\ &+ \sum_{\alpha=0}^{k-1} \sum_{\beta=1}^{p} e'_{\alpha,\beta} x_{j_\alpha} x_{i_\beta} + \sum_{0 \le \alpha_1 < \alpha_2 < k} b'_{\alpha_1,\alpha_2} x_{j_{\alpha_1}} x_{j_{\alpha_2}}, \end{aligned} \tag{17}$$

where $a'_{i,\alpha}$, b'_{α_1,α_2} and $e'_{\alpha,\beta} \in \mathbb{Z}_q$. We also need to define the following vectors which will be used throughout in our construction:

- $\mathbf{x} = (x_{j_0}, x_{j_1}, \cdots, x_{j_{k-1}}) \in \mathbb{Z}_2^k$,
  $\mathbf{x}' = (x_{i_1}, x_{i_1}, \cdots, x_{i_p}) \in \mathbb{Z}_2^p$.
- $\mathbf{c} = (c_0, c_1, \cdots, c_{k-1})$, $\mathbf{c}_i = (c_{i,0}, c_{i,1}, \cdots, c_{i,k-1}) \in \mathbb{Z}_2^k$.
- $\mathbf{c}' = (c'_1, c'_2, \cdots, c'_p)$, $\mathbf{c}'' = (c''_1, c''_1, \cdots, c''_p)$
  and $\mathbf{c}'_j = (c'_{j,1}, c'_{j,2}, \cdots, c'_{j,p}) \in \mathbb{Z}_2^p$.
- $\mathbf{d}' = (d'_1, d'_2, \cdots, d'_p)$, $\mathbf{d}'' = (d''_1, d''_2, \cdots, d''_p) \in \mathbb{Z}_2^p$.
- $\Gamma = (g_{i_1}, g_{i_2}, \cdots, g_{i_p}) \in \mathbb{Z}_q^p$.

For ease of presentation, whenever the context is clear, we sometimes use $C(f, g)(\tau)$ to denote $C(\psi(f), \psi(g))(\tau)$ for any two GBFs f and g. Similar changes will be applied to restricted Boolean functions also.

Furthermore, we need to define the following sets before presenting *Theorem* 1. Let

$$T_{\mathbf{c}'_1-\mathbf{c}'_2} = (\mathbf{c}'_1 - \mathbf{c}'_2) \cdot (2^{i_1}, 2^{i_2}, \cdots, 2^{i_p}), \tag{18}$$

and

$$R_{\tau_i} = \{(\mathbf{c}'_1, \mathbf{c}'_2) : T_{\mathbf{c}'_1-\mathbf{c}'_2} = \tau_i, \mathbf{c}'_1 \neq \mathbf{c}'_2, \mathbf{c}'_1, \mathbf{c}'_2 \in \mathbb{Z}_2^p\}. \tag{19}$$

Here $T_{\mathbf{c}'_1-\mathbf{c}'_2}$ represents nonzero time-shift for a binary pair of vectors $(\mathbf{c}'_1, \mathbf{c}'_2)$. R_{τ_i} is a set which contains all pairs $(\mathbf{c}'_1, \mathbf{c}'_2)$ such that $T_{\mathbf{c}'_1-\mathbf{c}'_2} = \tau_i$. From (18) and (19), it is observed that the number of such distinct τ_i is at most $3^p - 1$.

Example 4: Let $p = 2$, $i_1 = 2$ and $i_2 = 3$. Then, we have $T_{\mathbf{c}'_1-\mathbf{c}'_2} = (\mathbf{c}'_1 - \mathbf{c}'_2) \cdot (2^2, 2^3)$ whose values are taken from the set $\{\pm 4, \pm 8, \pm 12\}$ depending on $\mathbf{c}'_1, \mathbf{c}'_2$. $R_{\tau_i} = \{(\mathbf{c}'_1, \mathbf{c}'_2) : T_{\mathbf{c}'_1-\mathbf{c}'_2} = \tau_i, \mathbf{c}'_1 \neq \mathbf{c}'_2, \mathbf{c}'_1, \mathbf{c}'_2 \in \mathbb{Z}_2^2\}$ for $\tau_i = 4, -4, 8, -8, 12, -12$ are given below.

$$R_4 = \{((0,1),(1,0)), ((1,1),(0,1)), ((1,0),(0,0))\},$$

$$R_{-4} = \{((0,0),(1,0)), ((0,1),(1,1)), ((1,0),(0,1))\},$$

$$R_8 = \{((0,1),(0,0)), ((1,1),(1,0))\},$$

$$R_{-8} = \{((0,0),(0,1)), ((1,0),(1,1))\},$$

$$R_{12} = \{((1,1),(0,0))\},$$

$$R_{-12} = \{((0,0),(1,1))\}.$$

A. Construction of Z-complementary Code Set

In the above context, we are ready to present a construction of ZCCS over $\mathbb{Z}_q$. Let f be a GBF with m variables and Q be the quadratic part of f. For $0 \leq t \leq 2^{k+p}-1$, define the order set S_t, as follows.

$$\left\{ Q + \sum_{i=0}^{m-1} g_i x_i + g' + \frac{q}{2} \left(\sum_{\alpha=0}^{k-1} d_\alpha x_{j_\alpha} + \sum_{\alpha=0}^{k-1} b_\alpha x_{j_\alpha} + \sum_{\alpha=1}^{p} d'_\alpha x_{i_\alpha} + d x_\gamma \right) : d, d_\alpha \in \mathbb{Z}_2 \right\}, \tag{20}$$

where $t = \sum_{\alpha=0}^{k-1} b_\alpha 2^\alpha + \sum_{\alpha=k}^{k+p-1} d'_{\alpha-k+1} 2^\alpha$.

Let $\mathbf{d} = (d_0, d_1, \cdots, d_{k-1})$, $\mathbf{b} = (b_0, b_1, \cdots b_{k-1})$, $\mathbf{b'} = (b'_0, b'_1, \cdots, b'_{k-1})$ $(b_i, b'_i, d_i \in \{0,1\}$, $i = 0, 1, \cdots, k-1)$ be binary vectors and $\mathbf{bd'} = (b_0, b_1, \cdots, b_{k-1}, d'_1, d'_2, \cdots, d'_p)$, $\mathbf{b'd''} = (b'_0, b'_1, \cdots, b'_{k-1}, d''_1, d''_2, \cdots, d''_p)$ are binary representations of t, t' $(0 \leq t, t' \leq 2^{k+p}-1)$ respectively, where $t' = \sum_{\alpha=0}^{k-1} b'_\alpha 2^\alpha + \sum_{\alpha=k}^{k+p-1} d''_{\alpha-k+1} 2^\alpha$. In (20), $g_0, g_1, \cdots, g_{m-1}$ are the coefficients of $x_0, x_1, \cdots, x_{m-1}$. In the beginning of this Section, we have defined $\Gamma = (g_{i_1}, g_{i_2}, \cdots, g_{i_p})$ $(p < m)$, where $i_1, i_2, \cdots, i_p$ all are distinct and belong to the set $\{0, 1, \cdots, m-1\}$. In another words, we can say that $g_{i_1}, g_{i_2}, \cdots, g_{i_p}$ are the coefficients of $x_{i_1}, x_{i_2}, \cdots, x_{i_p}$. Therefore, the term $\sum_{i=0}^{m-1} g_i x_i$ presented in (20), can be expressed as

$$\begin{aligned} \sum_{i=0}^{m-1} g_i x_i &= \sum_{i \in \{0,1,\cdots,m-1\} \setminus \{i_1, i_2, \cdots, i_p\}} g_i x_i + (g_{i_1} x_{i_1} + g_{i_2} x_{i_2} \\ &\qquad + \cdots + g_{i_p} x_{i_p}) \\ &= \sum_{i \in \{0,1,\cdots,m-1\} \setminus \{i_1, i_2, \cdots, i_p\}} g_i x_i + \mathbf{x'} \cdot \Gamma, \end{aligned} \tag{21}$$

where $\mathbf{x'} \cdot \Gamma = g_{i_1} x_{i_1} + g_{i_2} x_{i_2} + \cdots + g_{i_p} x_{i_p}$.

Theorem 1: Suppose $G(f)$ satisfies the property that deleting k vertices specified in X_J and all their associated edges results in a path and p isolates vertices in X_S. Let γ be the label of either end vertex in the path. Then for any choice of $g', g_i \in \mathbb{Z}_q$, the auto-correlation function of the code $\psi(S_t)$ and the cross-correlation function between two codes $\psi(S_t)$ and $\psi(S_{t'})$ are as follows.

1) For $\mathbf{b}' = \mathbf{b}, \mathbf{d}' = \mathbf{d}''$

$$A(\psi(S_t))(\tau) = \begin{cases} 2^{m+k+1}, & \tau = 0, \\ 2^{m-p+1} \sum\limits_{(\mathbf{c}',\mathbf{c}'')\in R_\tau} (-1)^{\mathbf{d}'\cdot(\mathbf{c}'+\mathbf{c}'')} \omega^{(\mathbf{c}'-\mathbf{c}'')\cdot\Gamma} & \\ \qquad \times \sum_{\mathbf{c}} \omega^{g_{\mathbf{c}\mathbf{c}'}-g_{\mathbf{c}\mathbf{c}''}}, & \tau = \tau_i, i = 1, 2, \cdots, r, \\ 0, & \text{otherwise.} \end{cases} \tag{22}$$

2)

$$C(\psi(S_t), \psi(S_{t'}))(\tau) = \begin{cases} 2^{m-p+1} \sum\limits_{(\mathbf{c}',\mathbf{c}'')\in R_\tau} (-1)^{\mathbf{d}'\cdot\mathbf{c}'+\mathbf{d}''\cdot\mathbf{c}''} \omega^{(\mathbf{c}'-\mathbf{c}'')\cdot\Gamma} & \\ \times \left(\sum\limits_{\mathbf{c}} \omega^{g_{\mathbf{c}\mathbf{c}'}-g_{\mathbf{c}\mathbf{c}''}} (-1)^{(\mathbf{b}+\mathbf{b}')\cdot\mathbf{c}} \right), \tau = \tau_i, i = 1, 2, \cdots, r, & \\ 0, & \text{otherwise,} \end{cases} \tag{23}$$

where $0 \le r \le 3^p - 1$, $g_{\mathbf{c}\mathbf{c}'} = \sum_{\alpha=0}^{k-1} \sum_{\beta=1}^{p} e'_{\alpha,\beta} c_\alpha c'_\beta$ and $g_{\mathbf{c}\mathbf{c}''} = \sum_{\alpha=0}^{k-1} \sum_{\beta=1}^{p} e'_{\alpha,\beta} c_\alpha c''_\beta$.

Proof: See Appendix A. ■

Corollary 1: In the context of *Theorem* 1, consider $m-p, m-p+1, \cdots, m-1$, as the labels of p isolated vertices. Then $\{\psi(S_t) : 0 \le t \le 2^{k+p} - 1\}$ is a $(2^{k+p}, 2^{m-p})$-ZCCS$_{2^{k+1}}^{2^m}$.

Proof: Let $s = \min\{|\tau_i| : i = 1, 2, \cdots, r\}$, where
$\tau_i = (\mathbf{c}'_1 - \mathbf{c}'_2) \cdot (2^{m-p}, 2^{m-p+1}, \cdots, 2^{m-1})$.
To find s, we start with

$$\begin{aligned} |\tau_i| &= \left|(\mathbf{c}'_1 - \mathbf{c}'_2) \cdot (2^{m-p}, 2^{m-p+1}, \cdots, 2^{m-1})\right| \\ &= \left| \sum_{j=1}^{p} (c'_{1,j} - c'_{2,j}) 2^{m-p+j-1} \right| \\ &= 2^{m-p} \Big| \{(c'_{1,1} - c'_{2,1}) + (c'_{1,2} - c'_{2,2})2 + \cdots \\ &\qquad + (c'_{1,p} - c'_{2,p}) 2^{p-1}\} \Big| \\ &\ge 2^{m-p}, \quad \text{for} \quad \mathbf{c}_1 \ne \mathbf{c}_2. \end{aligned} \tag{24}$$

Therefore, $|\tau_i| \ge 2^{m-p}$ $\forall i = 1, 2, \cdots, r$, where the equality is met if $c'_{1,j} = c'_{2,j}$ for all j, except for $j = 1$. Hence,

$$s = \min\{|\tau_i| : i = 1, 2, \cdots, r\} = 2^{m-p}. \tag{25}$$

From *Theorem* 1 and (25), it is asserted that for any t, t' $(0 \leq t, t' \leq 2^{k+p}-1)$

$$C(\psi(S_t), \psi(S_{t'}))(\tau) = \begin{cases} 0, & 0 < |\tau| < 2^{m-p}, t = t', \\ 0, & |\tau| \leq 2^{m-p}, t \neq t'. \end{cases} \tag{26}$$

Therefore the set $\{\psi(S_t) : 0 \leq t \leq 2^{k+p}-1\}$ is a $(2^{k+p}, 2^{m-p})$-ZCCS$_{2^{k+1}}^{2^m}$. ■

For each $0 \leq t \leq 2^{k+p}-1$, define the order set $\bar{S}_t$ as follows.

$$\left\{ \tilde{f} + \frac{q}{2}\left(\sum_{\alpha=0}^{k-1} d_\alpha \bar{x}_{j_\alpha} + \sum_{\alpha=0}^{k-1} b_\alpha \bar{x}_{j_\alpha} + \sum_{\alpha=0}^{p-1} d'_\alpha \bar{x}_{i_\alpha} + \bar{d}x_\gamma \right) : d, d_\alpha \in \{0,1\} \right\}. \tag{27}$$

Corollary 2: In the context of Theorem 1, consider $m-p, m-p+1, \cdots, m-1$, as the labels of p isolated vertices. Then $\{\psi(\bar{S}_t) : 0 \leq t \leq 2^{k+p}-1\}$ is a $(2^{k+p}, 2^{m-p})$-ZCCS$_{2^{k+1}}^{2^m}$.

The proof of *Corollary* 2 follows directly from the proofs of *Theorem* 1 and *Corollary* 1.

Theorem 2: Consider $\{\psi(S_t)\}$ and $\{\psi(\bar{S}_t)\}$ in *Corollary* 1 and *Corollary* 2, respectively. Then,

$$\{\psi(S_t) : 0 \leq t \leq 2^{k+p}-1\} \cup \{\psi^*(\bar{S}_t) : 0 \leq t \leq 2^{k+p}-1\},$$

form $(2^{k+p+1}, 2^{m-p})$-ZCCS$_{2^{k+1}}^{2^m}$.

Proof: See Appendix B. ■

It is noted that our proposed ZCCS is optimal with respect to the theoretical bound in *Lemma* 4. Also, when $p = 0$, our proposed construction in *Theorem* 2 reduces to that in [9, Th. 3.6].

Remark 1: From *Theorem* 2 and Fig. 1, it is observed that at least

$$\frac{(m-p)!}{2(k!)}(q-1)^{k(m-k-p)} q^{kp+\frac{k(k-1)}{2}+m+1}$$

distinct optimal ZCCSs can be constructed from our proposed construction.

Proof: See Appendix C. ■

B. EXAMPLE

In this subsection, we provide an example to illustrate our proposed ZCCS construction.

Example 5: Let f be a GBF of 5 variables over $\mathbb{Z}_4$, where the associated graph $G(f)$ is given in Fig. 2. Note that $G(f)$ is a graph of five vertices satisfying the property that deleting x_0, the entire graph reduces to a path consisting of vertices labeled $2, 3, 1$ and an isolated vertex labeled 4. This graph leads to an optimal ZCCS as follows. Let

$$Q = 2(x_2x_3 + x_3x_1 + x_0x_2 + x_0x_3 + x_0x_1 + x_0x_4),$$

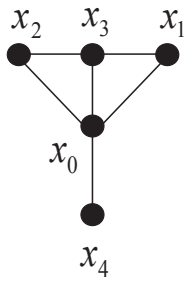

Fig. 2: The graph of the quadratic Boolean function $x_2x_3 + x_3x_1 + x_0x_2 + x_0x_3 + x_0x_1 + x_0x_4$.

TABLE I: Optimal ZCCS over the alphabet $\mathbb{Z}_4$.

$(8, 16)$-ZCCS$_4^{32}$	
C_0	C_1
01320330031223320330013201102130	03300132011021300132033003122332
03300132011021300132033003122332	01320330031223320330013201102130
01100312033023100312011001322112	03120110013221120110031203302310
03120110013221120110031203302310	01100312033023100312011001322112
C_2	C_3
01320330031223322112231023320312	03300132011021302310211221300110
03300132011021302310211221300110	01320330031223322112231023320312
01100312033023102130233223100330	03120110013221122332213021120132
03120110013221122332213021120132	01100312033023102130233223100330
C_4	C_5
01100312211201322130233201322112	21302332013221120110031221120132
21302332013221120110031221120132	01100312211201322130233201322112
01320330213001102112231001102130	21122310011021300132033021300110
21122310011021300132033021300110	01320330213001102112231001102130
C_6	C_7
23322130033023102130233201322112	03120110231003300110031221120132
03120110231003300110031221120132	23322130033023102130233201322112
23102112031223322112231001102130	03300132233203120132033021300110
03300132233203120132033021300110	23102112031223322112231001102130

and

$$f(x_0, x_1, x_2, x_3, x_4) = Q + x_0 + 3x_1.$$

Also, let

$$S_t = \{f + 2(d_0x_0 + b_0x_0 + d_0'x_4 + dx_1) : d, d_0 \in \mathbb{Z}_2\}, 0 \le t \le 3, \tag{28}$$

and

$$\bar{S}_t = \left\{\tilde{f} + 2(d_0\bar{x}_0 + b_0\bar{x}_0 + d_0'\bar{x}_4 + \bar{d}x_1) : d, d_0 \in \mathbb{Z}_2\right\}, 0 \le t \le 3, \tag{29}$$

where $t = b_0 2^0 + d_0' 2^1$ $(b_0, d_0' \in \mathbb{Z}_2)$. Consider $C_t = \psi(S_t)$ and $C_{2^2+t} = \psi^*(\bar{S}_t)$, given in Table I. The correlation properties of the ZCCS in Table I are illustrated in Fig. 3. Specifically, Fig. 3-a presents the absolute value of AACF sum of each code C_x from $\{C_0, C_1, \cdots, C_7\}$, Fig. 3-b

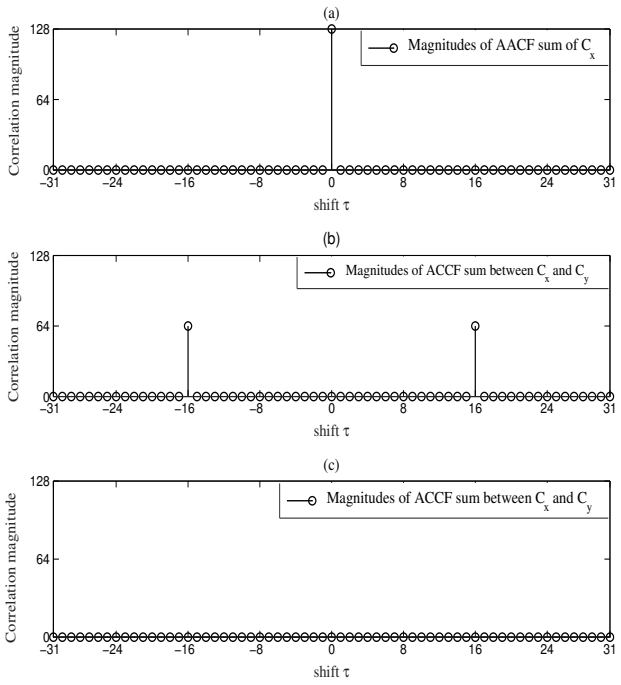

Fig. 3: Correlation plots of $(8, 16)$-ZCCS$_4^{32}$ in Table I.

shows absolute value of ACCF sum between any two distinct codes C_x and C_y ($x = b_0 2^0 + d_0' 2^1$, $y = b_0' 2^0 + d_0'' 2^1$ or, $x = 2^2 + b_0 2^0 + d_0' 2^1$, $y = 2^2 + b_0' 2^0 + d_0'' 2^1$) from $\{C_0, C_1, C_2, C_3\}$ (or from $\{C_4, C_5, C_6, C_7\}$) with the condition $b_0 \neq b_0'$. Fig. 3-c presents the absolute value of ACCF sum between any two distinct codes C_x and C_y with the following senarios:

1) The codes are drawn from $\{C_0, C_1, C_2, C_3\}$ (or from $\{C_4, C_5, C_6, C_7\}$) with the condition $b_0 = b_0'$.
2) One code is drawn from $\{C_0, C_1, C_2, C_3\}$ and the other code from $\{C_4, C_5, C_6, C_7\}$.

It is seen that the ZCZ width is 16. Hence, the ZCCS satisfies the equality of (16) as $K = 8$, $M = 4$, $Z = 16$ and $N = 32$ and therefore, the ZCCS in Table I is optimal.

IV. CONCLUSION

In this paper, we have proposed a direct construction of ZCCS using graphical representation of second-order RM codes. The proposed construction valids for any number of isolated vertices present in the graph, is capable of generating optimal ZCCS with respect to the set size upper bound in *Lemma* 4. It is noted that the construction of CCCs in [9] is a special case of our work

work when the number of isolated vertices is set to zero. Flexible ZCZ width and set size can be obtained by varying the number of isolated vertices.

APPENDIX A
PROOF OF *Theorem* 1

Before proving the *Theorem* 1, we present *Lemma* 5 and *Lemma* 6 where *Lemma* 5 will be used in the proof of *Theorem* 1 and *Lemma* 6 will be used in the proof of both *Theorem* 1 and *Theorem* 2.

Lemma 5: Let f and f' be two GBFs of m variables $x_0, x_1, \cdots, x_{m-1}$ $(m \geq 2)$, such that for some k $(0 \leq k \leq m-p-2,\ p \geq 0)$, $f|_{\mathbf{x}=\mathbf{c}}$ and $f'|_{\mathbf{x}=\mathbf{c}}$ are given by

$$f|_{\mathbf{x}=\mathbf{c}} = P + L + g_{i_1}x_{i_1} + g_{i_2}x_{i_2} + \cdots + g_{i_p}x_{i_p} + g',$$
$$f'|_{\mathbf{x}=\mathbf{c}} = f|_{\mathbf{x}=\mathbf{c}} + \frac{q}{2}x_\gamma,$$

where

$$P = \frac{q}{2}\sum_{\alpha=0}^{m-k-p-2} x_{l_\alpha}x_{l_{\alpha+1}},$$
$$L = \sum_{\alpha=0}^{m-k-p-1} g_{l_\alpha}x_{l_\alpha},$$

$g_{l_\alpha}, g' \in \mathbb{Z}_q$, $\alpha = 0, 1, \cdots, m-k-p-1$ and γ is the label of either end vertex of the path $G(P)$. Then for fixed $\mathbf{c}$ and $\mathbf{d}' \neq \mathbf{d}''$, we have

$$C\left(f|_{\mathbf{xx}'=\mathbf{cd}'}, f|_{\mathbf{xx}'=\mathbf{cd}''}\right)(\tau) + C\left(f'|_{\mathbf{xx}'=\mathbf{cd}'}, f'|_{\mathbf{xx}'=\mathbf{cd}''}\right)(\tau)$$
$$= \begin{cases} \omega^{(d'_1-d''_1)g_{i_1}} + \cdots + (d'_p - d''_p)g_{i_p}2^{m-(k+p)+1}, \\ \qquad\qquad \tau = (d'_1 - d''_1)2^{i_1} + \cdots + (d'_p - d''_p)2^{i_p}, \\ 0, \qquad\qquad \text{otherwise.} \end{cases} \tag{30}$$

Proof: Using *Lemma* 2, in terms of the truncated vectors, the sum of cross-correlations of the hypothesis becomes

$$C\left([f|_{\mathbf{xx}'=\mathbf{cd}'}], [f|_{\mathbf{xx}'=\mathbf{cd}''}]\right)(\tau - (u_1 - u_2))$$
$$+C\left([f'|_{\mathbf{xx}'=\mathbf{cd}'}], [f'|_{\mathbf{xx}'=\mathbf{cd}''}]\right)(\tau - (u_1 - u_2)),$$
$$(u_1 - u_2) - (n_x - 1) \leq \tau \leq (u_1 - u_2) + (n_x - 1),$$

where u_1 is the index of the first nonzero entry in the vector $\psi((.)|_{\mathbf{xx}'=\mathbf{cd}'})$ and u_2 that in $\psi((.)|_{\mathbf{xx}'=\mathbf{cd}''})$. For τ outside of this range, each cross-correlation is zero by the *Lemma* 2, so the

sum is zero too. For convenience write $\tau' = \tau - (u_1 - u_2)$ and thus we consider the sum as follows.

$$\begin{aligned} &C\left([f|_{\mathbf{xx'=cd'}}], [f|_{\mathbf{xx'=cd''}}]\right)(\tau') \\ &+C\left([f'|_{\mathbf{xx'=cd'}}], [f'|_{\mathbf{xx'=cd''}}]\right)(\tau'), -(n_x-1) \leq \tau' \leq (n_x-1). \end{aligned} \tag{31}$$

Next we note that

$$f|_{\mathbf{xx'=cd'}} = f|_{\mathbf{xx'=cd''}} + (d_1' - d_1'')g_{i_1} + \cdots + (d_p' - d_p'')g_{i_p}, \tag{32}$$

which means that the nonzero values in the vector $\psi(f|_{\mathbf{xx'=cd'}})$ are $\omega^{(d_1'-d_1'')g_{i_1}+\cdots+(d_p'-d_p'')g_{i_p}}$ times those in the vector $\psi(f|_{\mathbf{xx'=cd''}})$, only shifted relative to each other. For truncated vectors we have

$$[\psi(f|_{\mathbf{xx'=cd'}})] = \omega^{(d_1'-d_1'')g_{i_1}+\cdots+(d_p'-d_p'')g_{i_p}}[\psi(f|_{\mathbf{xx'=cd''}})]. \tag{33}$$

Substituting (33) and its equivalent expression for $\psi(f'|_{\mathbf{xx'=cd'}})$ into (31), we have for all τ',

$$\begin{aligned} &C([f|_{\mathbf{xx'=cd'}}], [f|_{\mathbf{xx'=cd''}}])(\tau') \\ &\qquad + C([f'|_{\mathbf{xx'=cd'}}], [f'|_{\mathbf{xx'=cd''}}])(\tau') \\ &= C(\omega^{(d_1'-d_1'')g_{i_1}+\cdots+(d_p'-d_p'')g_{i_p}}[f|_{\mathbf{xx'=cd''}}], [f|_{\mathbf{xx'=cd''}}])(\tau') \\ &+ C(\omega^{(d_1'-d_1'')g_{i_1}+\cdots+(d_p'-d_p'')g_{i_p}}[f'|_{\mathbf{xx'=cd''}}], [f'|_{\mathbf{xx'=cd''}}])(\tau') \\ &= \omega^{(d_1'-d_1'')g_{i_1}+\cdots+(d_p'-d_p'')g_{i_p}}\left(C([f|_{\mathbf{xx'=cd''}}], [f|_{\mathbf{xx'=cd''}}])(\tau')\right. \\ &\qquad \left. +C([f'|_{\mathbf{xx'=cd''}}], [f'|_{\mathbf{xx'=cd''}}])(\tau')\right) \\ &= \omega^{(d_1'-d_1'')g_{i_1}+\cdots+(d_p'-d_p'')g_{i_p}}\left(A([f|_{\mathbf{xx'=cd''}}])(\tau')\right. \\ &\qquad \left. +A([f'|_{\mathbf{xx'=cd''}}])(\tau')\right). \end{aligned} \tag{34}$$

Note that the truncated vectors $[\psi(f|_{\mathbf{xx'=cd''}})]$ and $[\psi(f'|_{\mathbf{xx'=cd''}})]$ form a GCP. Therefore

$$\begin{aligned} &A([f|_{\mathbf{xx'=cd''}}])(\tau') + A([f'|_{\mathbf{xx'=cd''}}])(\tau') \\ &\qquad = \begin{cases} 2^{m-(k+p)+1}, & \tau' = 0, \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{35}$$

Substituting the value of auto-correlation sum into (34), we have

$$\begin{aligned} &C([f|_{\mathbf{xx'=cd'}}], [f|_{\mathbf{xx'=cd''}}])(\tau') \\ &\qquad + C([f'|_{\mathbf{xx'=cd'}}], [f'|_{\mathbf{xx'=cd''}}])(\tau') \\ &= \begin{cases} \omega^{(d_1'-d_1'')g_{i_1}+\cdots+(d_p'-d_p'')g_{i_p}}2^{m-(k+p)+1}, & \tau' = 0, \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{36}$$

The above cross-correlation sum is only nonzero at $\tau' = 0$ i.e., when $\tau = u_1 - u_2$, where u_2 and u_1 are determined by $\mathbf{x}, \mathbf{x}', \mathbf{c}, \mathbf{d}'$ and $\mathbf{d}''$, as follows.

$$u_1 = \sum_{\alpha=0}^{k-1} c_\alpha 2^{j_\alpha} + d'_1 2^{i_1} + \cdots + d'_p 2^{i_p},$$
$$u_2 = \sum_{\alpha=0}^{k-1} c_\alpha 2^{j_\alpha} + d''_1 2^{i_1} + \cdots + d''_p 2^{i_p},$$

where $c = (c_0, c_1, \cdots, c_{k-1})$. Hence $u_1 - u_2 = (d'_1 - d''_1)2^{i_1} + \cdots + (d'_p - d''_p)2^{i_p}$. Therefore the cross-correlation sum is nonzero only at $\tau = (d'_1 - d''_1)2^{i_1} + \cdots + (d'_p - d''_p)2^{i_p}$, where the value is $\omega^{(d'_1 - d''_1)g_{i_1} + \cdots + (d'_p - d''_p)g_{i_p}} 2^{m-(k+p)+1}$, and thus *Lemma* 5 is proved. ■

To illustrate *Lemma 5*, let us recall R_{τ_i} which is defined in (19). Consider the GBFs f and f' of 5 variables over $\mathbb{Z}_4$, as follows

$$\begin{aligned} f(x_0, x_1, x_2, x_3, x_4) &= 2(x_2x_3 + x_3x_1 + x_0x_3 + x_0x_1 \\ &\quad + x_0x_2 + x_0x_4), \\ f'(x_0, x_1, x_2, x_3, x_4) &= 2(x_2x_3 + x_3x_1 + x_0x_3 + x_0x_1 \\ &\quad + x_0x_2 + x_0x_4 + x_1). \end{aligned} \tag{37}$$

Both $G(f|_{x_0=c})$ and $G(f'|_{x_0=c})$ $(c \in \mathbb{Z}_2)$ contain a path with x_1 as one of the end vertices and x_4 as isolated vertex. Therefore $p = 1$ and $i_1 = 4$. Hence the possible nonzero time-shifts are $\tau_0 = (1-0) \cdot 2^4 = 16$, $\tau_1 = (0-1) \cdot 2^4 = -16$, and the corresponding set of vectors are $R_{16} = \{(1, 0)\}$, $R_{-16} = \{(0, 1)\}$, respectively. By using *Lemma* 5, we show below that R_{τ_i}'s are

useful in the calculation of cross-correlation sum.

$$\begin{aligned}
&\sum_{c'\neq c''}[C(f|_{x_0x_4=cc'}, f|_{x_0x_4=cc''}) \\
&\qquad +C(f'|_{x_0x_4=cc'}, f'|_{x_0x_4=cc''})] \\
&=\sum_{(c',c'')\in R_{16}}[C(f|_{x_0x_4=cc'}, f|_{x_0x_4=cc''}) \\
&\qquad +C(f'|_{x_0x_4=cc'}, f'|_{x_0x_4=cc''})] \\
&\quad+\sum_{(c',c'')\in R_{-16}}[C(f|_{x_0x_4=cc'}, f|_{x_0x_4=cc''}) \\
&\qquad +C(f'|_{x_0x_4=cc'}, f'|_{x_0x_4=cc''})] \\
&=C(f|_{x_0x_4=c1}, f|_{x_0x_4=c0})+C(f'|_{x_0x_4=c1}, f'|_{x_0x_4=c0}) \\
&\quad+C(f|_{x_0x_4=c0}, f|_{x_0x_4=c1})+C(f'|_{x_0x_4=c0}, f'|_{x_0x_4=c1}) \\
&=\begin{cases}16, & \tau=\pm 16,\\ 0, & \text{otherwise.}\end{cases}
\end{aligned}$$

Lemma 6: [9] Let $\mathbf{d}, \mathbf{c}_1, \mathbf{c}_2 \in \{0,1\}^k$. If $\mathbf{c}_1 \neq \mathbf{c}_2$, $\sum_{\mathbf{d}}(-1)^{\mathbf{d}\cdot(\mathbf{c}_1+\mathbf{c}_2)}=0$.

In the sequel, we provide the proof of *Theorem* 1.

Proof: Let $f = Q + \sum_{i=0}^{m-1} g_i x_i + g'$ and the cross-correlation between $\psi(S_t)$, $\psi(S_{t'})$ can be written as

$$\begin{aligned}
&C(\psi(S_t),\psi(S_{t'}))(\tau)\\
&=\sum_{\mathbf{d}d} C\left(f+\frac{q}{2}\left((\mathbf{d}+\mathbf{b})\cdot\mathbf{x}+\mathbf{d}'\cdot\mathbf{x}'+dx_\gamma\right),\right.\\
&\qquad\left. f+\frac{q}{2}\left((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x}+\mathbf{d}''\cdot\mathbf{x}'+dx_\gamma\right)\right)(\tau)\\
&=S_1+S_2,
\end{aligned}$$

where

$$\begin{aligned}
S_1=\sum_{\mathbf{d}d}\sum_{\mathbf{c}_1\neq\mathbf{c}_2} C\left(f+\frac{q}{2}\left((\mathbf{d}+\mathbf{b})\cdot\mathbf{x}+\mathbf{d}'\cdot\mathbf{x}'+dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}_1},\right.\\
\left. f+\frac{q}{2}\left((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x}+\mathbf{d}''\cdot\mathbf{x}'+dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}_2}\right)(\tau),
\end{aligned} \tag{38}$$

and

$$\begin{aligned}
S_2=\sum_{\mathbf{d}d}\sum_{\mathbf{c}} C\left(f+\frac{q}{2}\left((\mathbf{d}+\mathbf{b})\cdot\mathbf{x}+\mathbf{d}'\cdot\mathbf{x}'+dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}},\right.\\
\left. f+\frac{q}{2}\left((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x}+\mathbf{d}''\cdot\mathbf{x}'+dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}}\right)(\tau).
\end{aligned} \tag{39}$$

To find S_1, we start with

$$\begin{aligned}
&\sum_{\mathbf{d}} C\left(f+\frac{q}{2}\left((\mathbf{d}+\mathbf{b})\cdot\mathbf{x}+\mathbf{d}'\cdot\mathbf{x}'+dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}_1},\right.\\
&\qquad\left. f+\frac{q}{2}\left((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x}+\mathbf{d}''\cdot\mathbf{x}'+dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}_2}\right)(\tau)\\
&=(-1)^{\mathbf{b}\cdot\mathbf{c}_1+\mathbf{b}'\cdot\mathbf{c}_2}C\left(f+\frac{q}{2}\left(\mathbf{d}'\cdot\mathbf{x}'+dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}_1},\right.\\
&\qquad\left. f+\frac{q}{2}\left(\mathbf{d}''\cdot\mathbf{x}'+dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}_2}\right)(\tau)\sum_{\mathbf{d}}(-1)^{\mathbf{d}\cdot(\mathbf{c}_1+\mathbf{c}_2)}.
\end{aligned}\tag{40}$$

By *Lemma* 6 we have $\sum_{\mathbf{d}}(-1)^{\mathbf{d}\cdot(\mathbf{c}_1+\mathbf{c}_2)}=0$ for $\mathbf{c}_1\neq\mathbf{c}_2$, therefore S_1 vanishes for all values of τ. Similarly, to simplify S_2 we start with

$$\begin{aligned}
&\sum_{\mathbf{d}} C\left(f+\frac{q}{2}\left((\mathbf{d}+\mathbf{b})\cdot\mathbf{x}+\mathbf{d}'\cdot\mathbf{x}'+dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}},\right.\\
&\qquad\left. f+\frac{q}{2}\left((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x}+\mathbf{d}''\cdot\mathbf{x}'+dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}}\right)(\tau)\\
&=(-1)^{\mathbf{b}\cdot\mathbf{c}+\mathbf{b}'\cdot\mathbf{c}}C\left(f+\frac{q}{2}\left(\mathbf{d}'\cdot\mathbf{x}'+dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}},\right.\\
&\qquad\left. f+\frac{q}{2}\left(\mathbf{d}''\cdot\mathbf{x}'+dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}}\right)(\tau)\sum_{\mathbf{d}}(-1)^{\mathbf{d}\cdot(\mathbf{c}+\mathbf{c})}\\
&=(-1)^{\mathbf{b}\cdot\mathbf{c}+\mathbf{b}'\cdot\mathbf{c}}2^kC\left(f+\frac{q}{2}\left(\mathbf{d}'\cdot\mathbf{x}'+dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}},\right.\\
&\qquad\left. f+\frac{q}{2}\left(\mathbf{d}''\cdot\mathbf{x}'+dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}}\right)(\tau)\\
&=(-1)^{\mathbf{b}\cdot\mathbf{c}+\mathbf{b}'\cdot\mathbf{c}}2^k\sum_{\mathbf{c}'\mathbf{c}''}C\left(f+\frac{q}{2}\left(\mathbf{d}'\cdot\mathbf{x}'+dx_\gamma\right)|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'},\right.\\
&\qquad\left. f+\frac{q}{2}\left(\mathbf{d}''\cdot\mathbf{x}'+dx_\gamma\right)|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}''}\right)(\tau)\\
&=(-1)^{\mathbf{b}\cdot\mathbf{c}+\mathbf{b}'\cdot\mathbf{c}}2^k\sum_{\mathbf{c}'\mathbf{c}''}(-1)^{\mathbf{d}'\cdot\mathbf{c}'+\mathbf{d}''\cdot\mathbf{c}''}C\left(f+\frac{q}{2}dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'},\right.\\
&\qquad\left. f+\frac{q}{2}dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}''}\right)(\tau)\\
&=(-1)^{\mathbf{b}\cdot\mathbf{c}+\mathbf{b}'\cdot\mathbf{c}}2^k\left(\sum_{\mathbf{c}'=\mathbf{c}''}(-1)^{\mathbf{d}'\cdot\mathbf{c}'+\mathbf{d}''\cdot\mathbf{c}''}\,C\left(f+\frac{q}{2}dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'},\right.\right.\\
&\qquad\left.\left. f+\frac{q}{2}dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}''}\right)(\tau)\right.\\
&\quad\left.+\sum_{\mathbf{c}'\neq\mathbf{c}''}(-1)^{\mathbf{d}'\cdot\mathbf{c}'+\mathbf{d}''\cdot\mathbf{c}''}\,C\left(f+\frac{q}{2}dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'},\right.\right.\\
&\qquad\left.\left. f+\frac{q}{2}dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}''}\right)(\tau)\right)\\
&=(-1)^{\mathbf{b}\cdot\mathbf{c}+\mathbf{b}'\cdot\mathbf{c}}2^k\left(\sum_{\mathbf{c}'=\mathbf{c}''}(-1)^{(\mathbf{d}'+\mathbf{d}'')\cdot\mathbf{c}'}A\left(f+\frac{q}{2}dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'}\right)(\tau)\right.\\
&\quad\left.+\sum_{\mathbf{c}'\neq\mathbf{c}''}(-1)^{\mathbf{d}'\cdot\mathbf{c}'+\mathbf{d}''\cdot\mathbf{c}''}\,C\left(f+\frac{q}{2}dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'},\right.\right.\\
&\qquad\left.\left. f+\frac{q}{2}dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}''}\right)(\tau)\right)\\
&=(-1)^{\mathbf{b}\cdot\mathbf{c}+\mathbf{b}'\cdot\mathbf{c}}2^k(L_1+L_2),
\end{aligned}\tag{41}$$

where

$$L_1=\sum_{\mathbf{c}'=\mathbf{c}''}(-1)^{(\mathbf{d}'+\mathbf{d}'')\cdot\mathbf{c}'}A\left(f+\frac{q}{2}dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'}\right)(\tau),\tag{42}$$

and

$$L_2 = \sum_{\mathbf{c}' \neq \mathbf{c}''} (-1)^{\mathbf{d}'\cdot\mathbf{c}'+\mathbf{d}''\cdot\mathbf{c}''} C\left(f + \frac{q}{2} dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'}, \right. \\ \left. f + \frac{q}{2} dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}''}\right)(\tau). \tag{43}$$

Since $G(f|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'})$ is a path over $m-k-p$ (p is the number of isolated vertices) vertices,

$$\sum_d A\left(f + \frac{q}{2} dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'}\right)(\tau) = \begin{cases} 2^{m-(k+p)+1}, & \tau = 0, \\ 0, & \text{otherwise.} \end{cases} \tag{44}$$

Now from (42) and (44) we have

$$\sum_d L_1 = \begin{cases} 2^{m-(k+p)+1} \sum_{\mathbf{c}'=\mathbf{c}''} (-1)^{(\mathbf{d}'+\mathbf{d}'')\cdot\mathbf{c}'}, & \tau = 0, \\ 0, & \text{otherwise.} \end{cases} \tag{45}$$

Therefore,

$$\sum_d L_1 = \begin{cases} 2^{m-k+1}, & \tau = 0, \mathbf{d}' = \mathbf{d}'', \\ 0, & \tau = 0, \mathbf{d}' \neq \mathbf{d}'', \\ 0, & \text{otherwise.} \end{cases} \tag{46}$$

To find simplified value of L_2, we start with

$$\{(\mathbf{c}', \mathbf{c}'') : \mathbf{c}', \mathbf{c}'' \in \mathbb{Z}_q \quad \text{and} \quad \mathbf{c}' \neq \mathbf{c}''\} = \cup_{i=1}^r R_{\tau_i}.$$

Therefore

$$\begin{aligned} L_2 &= \sum_{\mathbf{c}' \neq \mathbf{c}''} (-1)^{\mathbf{d}'\cdot\mathbf{c}'+\mathbf{d}''\cdot\mathbf{c}''} C\left(f + \frac{q}{2} dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'}, \right. \\ &\qquad \left. f + \frac{q}{2} dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}''}\right)(\tau) \\ &= \sum_{(\mathbf{c}',\mathbf{c}'') \in \cup_{i=1}^r R_{\tau_i}} (-1)^{\mathbf{d}'\cdot\mathbf{c}'+\mathbf{d}''\cdot\mathbf{c}''} C\left(f + \frac{q}{2} dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'}, \right. \\ &\qquad \left. f + \frac{q}{2} dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}''}\right)(\tau) \\ &= \sum_{i=1}^r \sum_{(\mathbf{c}',\mathbf{c}'') \in R_{\tau_i}} (-1)^{\mathbf{d}'\cdot\mathbf{c}'+\mathbf{d}''\cdot\mathbf{c}''} C\left(f + \frac{q}{2} dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'}, \right. \\ &\qquad \left. f + \frac{q}{2} dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}''}\right)(\tau). \end{aligned} \tag{47}$$

Since the vertices $x_{i_1}, x_{i_2}, \cdots x_{i_p}$ are isolated by the deletion operations, in the function f the only quadratic terms involving variables x_{i_β}'s are those with the variables of the deleted vertices. Thus the only quadratic terms in x_{i_β}'s in f can be expressed as follows.

$$\sum_{\alpha=0}^{k-1}\sum_{\beta=1}^{p} e'_{\alpha,\beta}x_{j_\alpha}x_{i_\beta}, \tag{48}$$

where $e'_{\alpha,\beta}$ are the weights of the edges between the deleted vertices and the isolated vertices. Now the term $\left(f+\frac{q}{2}dx_\gamma\right)|_{\mathbf{xx'=cc'}}$ can be written as

$$\begin{aligned}
&\left(f+\frac{q}{2}dx_\gamma\right)|_{\mathbf{xx'=cc'}}\\
&=\left(f'+\sum_{\alpha=0}^{k-1}\left(\sum_{\beta=1}^{p}e'_{\alpha,\beta}x_{j_\alpha}x_{i_\beta}\right)+\frac{q}{2}dx_\gamma\right)|_{\mathbf{xx'=cc'}}\\
&=\left(f'+\sum_{\alpha=0}^{k-1}\left(\sum_{\beta=1}^{p}e'_{\alpha,\beta}c_\alpha c'_\beta\right)+\frac{q}{2}dx_\gamma\right)|_{\mathbf{xx'=cc'}}\\
&=\omega^{g_{\mathbf{cc'}}}\left(f'+\frac{q}{2}dx_\gamma\right)|_{\mathbf{xx'=cc'}}(\text{where } g_{\mathbf{cc'}}\triangleq\sum_{\alpha=0}^{k-1}\sum_{\beta=1}^{p}e'_{\alpha,\beta}c_\alpha c'_\beta).
\end{aligned}$$

Similarly

$$\begin{aligned}
&\left(f+\frac{q}{2}dx_\gamma\right)|_{\mathbf{xx''=cc''}}\\
&=\omega^{g_{\mathbf{cc''}}}\left(f'+\frac{q}{2}dx_\gamma\right)|_{\mathbf{xx''=cc''}}(\text{where } g_{\mathbf{cc''}}\triangleq\sum_{\alpha=0}^{k-1}\sum_{\beta=1}^{p}e'_{\alpha,\beta}c_\alpha c''_\beta).
\end{aligned} \tag{49}$$

Therefore, the term $C\left(f+\frac{q}{2}dx_\gamma|_{\mathbf{xx'=cc'}}, f+\frac{q}{2}dx_\gamma|_{\mathbf{xx'=cc''}}\right)(\tau)$ can be simplified to

$$\begin{aligned}
&C\left(f+\frac{q}{2}dx_\gamma|_{\mathbf{xx'=cc'}}, f+\frac{q}{2}dx_\gamma|_{\mathbf{xx'=cc''}}\right)(\tau)\\
&=\omega^{g_{\mathbf{cc'}}-g_{\mathbf{cc''}}}C\left(f'+\frac{q}{2}dx_\gamma|_{\mathbf{xx'=cc'}}, f'+\frac{q}{2}dx_\gamma|_{\mathbf{xx'=cc''}}\right)(\tau).
\end{aligned} \tag{50}$$

By *Lemma* 5, we have

$$\begin{aligned}
&\sum_d C\left(f'+\frac{q}{2}dx_\gamma|_{\mathbf{xx'=cc'}}, f'+\frac{q}{2}dx_\gamma|_{\mathbf{xx'=cc''}}\right)(\tau)\\
&=\begin{cases}
2^{m-(k+p)+1}\omega^{(c'_1-c''_1)g_{i_1}+\cdots+(c'_p-c''_p)g_{i_p}},\\
\qquad\qquad \tau=(c'_1-c''_1)2^{i_1}+\cdots+(c'_p-c''_p)2^{i_p},\\
0, \qquad\qquad \text{otherwise.}
\end{cases}\\
&=\begin{cases}
2^{m-(k+p)+1}\omega^{(\mathbf{c'}-\mathbf{c''})\cdot\Gamma}, \quad \tau=T_{(\mathbf{c'}-\mathbf{c''})},\\
0, \qquad\qquad\qquad \text{otherwise.}
\end{cases}
\end{aligned} \tag{51}$$

Now from (47) and (51) we have,

$$\begin{aligned}
&\sum_d L_2 \\
&= \sum_{i=1}^{r} \sum_{(\mathbf{c}',\mathbf{c}'')\in R_{\tau_i}} (-1)^{\mathbf{d}'\cdot\mathbf{c}'+\mathbf{d}''\cdot\mathbf{c}''} \sum_d C\left(f+\frac{q}{2}dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}'},\right. \\
&\qquad\qquad \left. f+\frac{q}{2}dx_\gamma|_{\mathbf{x}\mathbf{x}'=\mathbf{c}\mathbf{c}''}\right)(\tau) \\
&= \begin{cases} 2^{m-(k+p)+1} \\ \times \sum_{(\mathbf{c}',\mathbf{c}'')\in R_\tau} \omega^{g_{\mathbf{c}\mathbf{c}'}-g_{\mathbf{c}\mathbf{c}''}}(-1)^{\mathbf{d}'\cdot\mathbf{c}'+\mathbf{d}''\cdot\mathbf{c}''}\omega^{(\mathbf{c}'-\mathbf{c}'')\cdot\Gamma}, \\ \qquad\qquad \tau=\tau_i, i=1,2,\cdots,r, \\ 0, \qquad\qquad \text{otherwise.} \end{cases}
\end{aligned} \tag{52}$$

For $\mathbf{d}'=\mathbf{d}''$, from (46) and (52) we have

$$\begin{aligned}
&\sum_d (L_1+L_2) \\
&= \begin{cases} 2^{m-k+1}, \qquad\qquad \tau=0, \\ 2^{m-(k+p)+1} \\ \times \sum_{(\mathbf{c}',\mathbf{c}'')\in R_\tau} \omega^{g_{\mathbf{c}\mathbf{c}'}-g_{\mathbf{c}\mathbf{c}''}}(-1)^{\mathbf{d}'\cdot(\mathbf{c}'+\mathbf{c}'')}\omega^{(\mathbf{c}'-\mathbf{c}'')\cdot\Gamma}, \\ \qquad\qquad \tau=\tau_i, i=1,2,\cdots,r, \\ 0, \qquad\qquad \text{otherwise.} \end{cases}
\end{aligned} \tag{53}$$

If $\mathbf{d}'\neq\mathbf{d}''$, from (46) and (52) we have

$$\begin{aligned}
&\sum_d (L_1+L_2) \\
&= \begin{cases} 2^{m-(k+p)+1} \\ \times \sum_{(\mathbf{c}',\mathbf{c}'')\in R_\tau} \omega^{g_{\mathbf{c}\mathbf{c}'}-g_{\mathbf{c}\mathbf{c}''}}(-1)^{\mathbf{d}'\cdot\mathbf{c}'+\mathbf{d}''\cdot\mathbf{c}''}\omega^{(\mathbf{c}'-\mathbf{c}'')\cdot\Gamma}, \\ \qquad\qquad \tau=\tau_i, i=1,2,\cdots,r, \\ 0, \qquad\qquad \text{otherwise.} \end{cases}
\end{aligned} \tag{54}$$

For $\mathbf{d}' = \mathbf{d}''$, from (41), (53) we have

$$\begin{aligned}
&\sum_{\mathbf{d},d} C\left(f + \frac{q}{2}\left((\mathbf{d+b})\cdot\mathbf{x} + \mathbf{d}'\cdot\mathbf{x}' + dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}},\right.\\
&\qquad\left. f + \frac{q}{2}\left((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x} + \mathbf{d}''\cdot\mathbf{x}' + dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}}\right)(\tau)\\
&= (-1)^{\mathbf{b}\cdot\mathbf{c}+\mathbf{b}'\cdot\mathbf{c}} 2^k \sum_d (L_1 + L_2)\\
&= \begin{cases}
2^{m+1}(-1)^{\mathbf{b}\cdot\mathbf{c}+\mathbf{b}'\cdot\mathbf{c}}, & \tau = 0,\\
2^{m-p+1}(-1)^{\mathbf{b}\cdot\mathbf{c}+\mathbf{b}'\cdot\mathbf{c}} & \\
\times \sum\limits_{(\mathbf{c}',\mathbf{c}'')\in R_\tau} \omega^{g_{\mathbf{cc}'}-g_{\mathbf{cc}''}}(-1)^{\mathbf{d}'\cdot(\mathbf{c}'+\mathbf{c}'')}\omega^{(\mathbf{c}'-\mathbf{c}'')\cdot\Gamma}, & \\
\qquad\qquad \tau = \tau_i, i = 1, 2, \cdots, r, & \\
0, & \text{otherwise.}
\end{cases}
\end{aligned} \tag{55}$$

For $\mathbf{d}' \neq \mathbf{d}''$, from (41) and (52) we have

$$\begin{aligned}
&\sum_{\mathbf{d},d} C\left(f + \frac{q}{2}\left((\mathbf{d+b})\cdot\mathbf{x} + \mathbf{d}'\cdot\mathbf{x}' + dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}},\right.\\
&\qquad\left. f + \frac{q}{2}\left((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x} + \mathbf{d}''\cdot\mathbf{x}' + dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}}\right)(\tau)\\
&= (-1)^{\mathbf{b}\cdot\mathbf{c}+\mathbf{b}'\cdot\mathbf{c}} 2^k \sum_d (L_1 + L_2)\\
&= \begin{cases}
2^{m-p+1}(-1)^{\mathbf{b}\cdot\mathbf{c}+\mathbf{b}'\cdot\mathbf{c}} & \\
\times \sum\limits_{(\mathbf{c}',\mathbf{c}'')\in R_\tau} \omega^{g_{\mathbf{cc}'}-g_{\mathbf{cc}''}}(-1)^{\mathbf{d}'\cdot\mathbf{c}'+\mathbf{d}''\cdot\mathbf{c}''}\omega^{(\mathbf{c}'-\mathbf{c}'')\cdot\Gamma}, & \\
\qquad\qquad \tau = \tau_i, i = 1, 2, \cdots, r, & \\
0, & \text{otherwise.}
\end{cases}
\end{aligned} \tag{56}$$

For $\mathbf{d}' = \mathbf{d}''$, $\mathbf{b} = \mathbf{b}'$, from (38), (55) and using *Lemma* 5 we have

$$\begin{aligned} S_2 &= \sum_{\mathbf{d}d} \sum_{\mathbf{c}} C \Big(f + \frac{q}{2} \left((\mathbf{d+b}) \cdot \mathbf{x} + \mathbf{d}' \cdot \mathbf{x}' + dx_\gamma \right) |_{\mathbf{x}=\mathbf{c}}, \\ &\qquad\qquad f + \frac{q}{2} \left((\mathbf{d} + \mathbf{b}') \cdot \mathbf{x} + \mathbf{d}'' \cdot \mathbf{x}' + dx_\gamma \right) |_{\mathbf{x}=\mathbf{c}} \Big) (\tau) \\ &= \begin{cases} 2^{m+1} \sum_{\mathbf{c}} (-1)^{\mathbf{b}\cdot\mathbf{c} + \mathbf{b}'\cdot\mathbf{c}}, & \tau = 0, \\ 2^{m-p+1} \sum_{(\mathbf{c}', \mathbf{c}'') \in R_\tau} (-1)^{\mathbf{d}'\cdot(\mathbf{c}'+\mathbf{c}'')} \omega^{(\mathbf{c}'-\mathbf{c}'')\cdot\Gamma} \\ \times \sum_{\mathbf{c}} \omega^{g_{\mathbf{c}\mathbf{c}'} - g_{\mathbf{c}\mathbf{c}''}} (-1)^{\mathbf{b}\cdot\mathbf{c} + \mathbf{b}'\cdot\mathbf{c}}, & \tau = \tau_i, i = 1, 2, \cdots, r, \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{57}$$

$$= \begin{cases} 2^{m+k+1}, & \tau = 0, \\ 2^{m-p+1} \sum_{(\mathbf{c}', \mathbf{c}'') \in R_\tau} (-1)^{\mathbf{d}'\cdot(\mathbf{c}'+\mathbf{c}'')} \omega^{(\mathbf{c}'-\mathbf{c}'')\cdot\Gamma} \\ \times \sum_{\mathbf{c}} \omega^{g_{\mathbf{c}\mathbf{c}'} - g_{\mathbf{c}\mathbf{c}''}}, & \tau = \tau_i, i = 1, 2, \cdots, r, \\ 0, & \text{otherwise.} \end{cases}$$

For $\mathbf{d}' \neq \mathbf{d}''$, $\mathbf{b} = \mathbf{b}'$, from (38), (56) and using *Lemma* 5 we have

$$\begin{aligned} S_2 &= \sum_{\mathbf{d}d} \sum_{\mathbf{c}} C \Big(f + \frac{q}{2} \left((\mathbf{d+b}) \cdot \mathbf{x} + \mathbf{d}' \cdot \mathbf{x}' + dx_\gamma \right) |_{\mathbf{x}=\mathbf{c}}, \\ &\qquad\qquad f + \frac{q}{2} \left((\mathbf{d} + \mathbf{b}') \cdot \mathbf{x} + \mathbf{d}'' \cdot \mathbf{x}' + dx_\gamma \right) |_{\mathbf{x}=\mathbf{c}} \Big) (\tau) \\ &= \begin{cases} 2^{m-p+1} \sum_{(\mathbf{c}', \mathbf{c}'') \in R_\tau} (-1)^{\mathbf{d}'\cdot\mathbf{c}' + \mathbf{d}''\cdot\mathbf{c}''} \omega^{(\mathbf{c}'-\mathbf{c}'')\cdot\Gamma} \\ \times \sum_{\mathbf{c}} \omega^{g_{\mathbf{c}\mathbf{c}'} - g_{\mathbf{c}\mathbf{c}''}} (-1)^{\mathbf{b}\cdot\mathbf{c} + \mathbf{b}'\cdot\mathbf{c}}, & \tau = \tau_i, i = 1, 2, \cdots, r, \\ 0, & \text{otherwise.} \end{cases} \\ &= \begin{cases} 2^{m-p+1} \sum_{(\mathbf{c}', \mathbf{c}'') \in R_\tau} (-1)^{\mathbf{d}'\cdot\mathbf{c}' + \mathbf{d}''\cdot\mathbf{c}''} \omega^{(\mathbf{c}'-\mathbf{c}'')\cdot\Gamma} \\ \times \sum_{\mathbf{c}} \omega^{g_{\mathbf{c}\mathbf{c}'} - g_{\mathbf{c}\mathbf{c}''}}, & \tau = \tau_i, i = 1, 2, \cdots, r, \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{58}$$

For $\mathbf{d}' = \mathbf{d}''$, $\mathbf{b} \neq \mathbf{b}'$, from (57) and *Lemma* 5 we have

$$\begin{aligned} S_2 &= \sum_{\mathbf{d}d} \sum_{\mathbf{c}} C\left(f + \frac{q}{2}\left((\mathbf{d+b})\cdot\mathbf{x} + \mathbf{d}'\cdot\mathbf{x}' + dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}},\right. \\ &\qquad \left. f + \frac{q}{2}\left((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x} + \mathbf{d}''\cdot\mathbf{x}' + dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}}\right)(\tau) \\ &= \begin{cases} 2^{m+1}\sum_{\mathbf{c}}(-1)^{\mathbf{b}\cdot\mathbf{c}+\mathbf{b}'\cdot\mathbf{c}}, & \tau = 0, \\ 2^{m-p+1}\sum_{(\mathbf{c}',\mathbf{c}'')\in R_\tau}(-1)^{\mathbf{d}'\cdot(\mathbf{c}'+\mathbf{c}'')}\omega^{(\mathbf{c}'-\mathbf{c}'')\cdot\Gamma} \\ \sum_{\mathbf{c}}\omega^{g_{\mathbf{c}\mathbf{c}'}-g_{\mathbf{c}\mathbf{c}''}}(-1)^{\mathbf{b}\cdot\mathbf{c}+\mathbf{b}'\cdot\mathbf{c}}, \tau = \tau_i, i = 1,2,\cdots,r, \\ 0, \qquad \text{otherwise.} \end{cases} \\ &= \begin{cases} 2^{m-p+1}\sum_{(\mathbf{c}',\mathbf{c}'')\in R_\tau}(-1)^{\mathbf{d}'\cdot(\mathbf{c}'+\mathbf{c}'')}\omega^{(\mathbf{c}'-\mathbf{c}'')\cdot\Gamma} \\ \times\sum_{\mathbf{c}}\omega^{g_{\mathbf{c}\mathbf{c}'}-g_{\mathbf{c}\mathbf{c}''}}(-1)^{\mathbf{b}\cdot\mathbf{c}+\mathbf{b}'\cdot\mathbf{c}}, \ \tau=\tau_i, i=1,2,\cdots,r, \\ 0, \qquad \text{otherwise.} \end{cases} \end{aligned} \tag{59}$$

For $\mathbf{d}' \neq \mathbf{d}''$, $\mathbf{b} \neq \mathbf{b}'$, from (58) and using *Lemma* 5 we have

$$\begin{aligned} S_2 &= \sum_{\mathbf{d}d} \sum_{\mathbf{c}} C\left(f + \frac{q}{2}\left((\mathbf{d+b})\cdot\mathbf{x} + \mathbf{d}'\cdot\mathbf{x}' + dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}},\right. \\ &\qquad \left. f + \frac{q}{2}\left((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x} + \mathbf{d}''\cdot\mathbf{x}' + dx_\gamma\right)|_{\mathbf{x}=\mathbf{c}}\right)(\tau) \\ &= \begin{cases} 2^{m-p+1}\sum_{(\mathbf{c}',\mathbf{c}'')\in R_\tau}(-1)^{\mathbf{d}'\cdot\mathbf{c}'+\mathbf{d}''\cdot\mathbf{c}''}\omega^{(\mathbf{c}'-\mathbf{c}'')\cdot\Gamma} \\ \times\sum_{\mathbf{c}}\omega^{g_{\mathbf{c}\mathbf{c}'}-g_{\mathbf{c}\mathbf{c}''}}(-1)^{\mathbf{b}\cdot\mathbf{c}+\mathbf{b}'\cdot\mathbf{c}}, \tau = \tau_i, i = 1,2,\cdots,r, \\ 0, \qquad \text{otherwise.} \end{cases} \end{aligned} \tag{60}$$

The result in (57) proves the hypothesis 1 given in (22).

(58), (59) and (60) prove the hypothesis 2 given in (23).

■

APPENDIX B

PROOF OF *Theorem* 2

Proof: Let $t' = \sum_{\alpha=0}^{k-1} b'_\alpha 2^\alpha + \sum_{\alpha=k}^{k+p-1} d'_\alpha 2^\alpha$ and $t'' = \sum_{\alpha=0}^{k-1} b''_\alpha 2^\alpha + \sum_{\alpha=k}^{k+p-1} d''_\alpha 2^\alpha$ $(b'_\alpha, b''_\alpha, d'_\alpha, d''_\alpha \in \mathbb{Z}_2$ and $0 \leq t', t'' \leq 2^{k+p} - 1)$. Since the labels of the isolated vertices are $m-p, m-p+$

$1, \cdots, m-1$, we consider $\mathbf{x}' = (x_{m-p}, x_{m-p+1}, \cdots, x_{m-1})$ and $\Gamma = (g_{m-p}, g_{m-p+1}, \cdots, g_{m-1})$. To prove *Theorem* 2, we only need to show

$$C(\psi(S'_t), \psi^*(\bar{S}_{t''})) = 0, \quad |\tau| \leq 2^{m-p}.$$

Let us start with

$$\begin{aligned}
&C(\psi(S_{t'}), \psi^*(\bar{S}_{t''}))(\tau) \\
&= \sum_{\mathbf{d}} C\left(f + \frac{q}{2}\left((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x} + \mathbf{d}'\cdot\mathbf{x}' + x_\gamma\right),\right. \\
&\qquad\qquad \left.\tilde{f}^* + \frac{q}{2}\left((\mathbf{d}+\mathbf{b}'')\cdot\bar{\mathbf{x}} + \mathbf{d}''\cdot\bar{\mathbf{x}'}\right)\right)(\tau) \\
&+ \sum_{\mathbf{d}} C\left(f + \frac{q}{2}\left((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x} + \mathbf{d}'\cdot\mathbf{x}'\right),\right. \\
&\qquad\qquad \left.\tilde{f}^* + \frac{q}{2}\left((\mathbf{d}+\mathbf{b}'')\cdot\bar{\mathbf{x}} + \mathbf{d}''\cdot\bar{\mathbf{x}'} + x_\gamma\right)\right)(\tau) \\
&= K_1 + K_2,
\end{aligned} \tag{61}$$

where

$$\begin{aligned}
K_1 = \sum_{\mathbf{d}} C\left(f + \frac{q}{2}\left((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x} + \mathbf{d}'\cdot\mathbf{x}' + x_\gamma\right),\right. \\
\left.\tilde{f}^* + \frac{q}{2}\left((\mathbf{d}+\mathbf{b}'')\cdot\bar{\mathbf{x}} + \mathbf{d}''\cdot\bar{\mathbf{x}'}\right)\right)(\tau),
\end{aligned} \tag{62}$$

and

$$\begin{aligned}
K_2 = \sum_{\mathbf{d}} C\left(f + \frac{q}{2}\left((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x} + \mathbf{d}'\cdot\mathbf{x}'\right),\right. \\
\left.\tilde{f}^* + \frac{q}{2}\left((\mathbf{d}+\mathbf{b}'')\cdot\bar{\mathbf{x}} + \mathbf{d}''\cdot\bar{\mathbf{x}'} + x_\gamma\right)\right)(\tau).
\end{aligned} \tag{63}$$

The cross-correlation term at RHS of (62) can be further reduced to

$$\begin{aligned}
&C\left(f + \frac{q}{2}\left((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x} + \mathbf{d}'\cdot\mathbf{x}' + x_\gamma\right),\right. \\
&\qquad\qquad \left.\tilde{f}^* + \frac{q}{2}\left((\mathbf{d}+\mathbf{b}'')\cdot\bar{\mathbf{x}} + \mathbf{d}''\cdot\bar{\mathbf{x}'}\right)\right)(\tau) \\
&= \sum_{\mathbf{c}_1,\mathbf{c}_2} C\left(f + \frac{q}{2}\left((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x} + \mathbf{d}'\cdot\mathbf{x}' + x_\gamma\right)|_{\mathbf{x}=\mathbf{c}_1},\right. \\
&\qquad\qquad \left.\tilde{f}^* + \frac{q}{2}\left((\mathbf{d}+\mathbf{b}'')\cdot\bar{\mathbf{x}} + \mathbf{d}''\cdot\bar{\mathbf{x}'}\right)|_{\mathbf{x}=\mathbf{c}_2}\right)(\tau) \\
&= \sum_{\mathbf{c}_1,\mathbf{c}_2} (-1)^{(\mathbf{b}'\cdot\mathbf{c}_1)+(\mathbf{b}''\cdot\bar{\mathbf{c}_2})}(-1)^{\mathbf{d}\cdot(\mathbf{c}_1+\bar{\mathbf{c}}_2)} \\
&\qquad \times \left(C\left(f + \frac{q}{2}\left(\mathbf{d}'\cdot\mathbf{x}' + x_\gamma\right)|_{\mathbf{x}=\mathbf{c}_1},\right.\right. \\
&\qquad\qquad \left.\left.\tilde{f}^* + \frac{q}{2}\mathbf{d}''\cdot\bar{\mathbf{x}'}|_{\mathbf{x}=\mathbf{c}_2}\right)(\tau)\right).
\end{aligned}$$

Therefore (62) is simplified to

$$\begin{aligned}
K_1 &= \sum_{\mathbf{d}} C\left(f + \frac{q}{2}\left((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x} + \mathbf{d}'\cdot\mathbf{x}' + x_\gamma\right),\right. \\
&\qquad\qquad \left.\tilde{f}^* + \frac{q}{2}\left((\mathbf{d}+\mathbf{b}'')\cdot\bar{\mathbf{x}} + \mathbf{d}''\cdot\bar{\mathbf{x}}'\right)\right)(\tau) \\
&= \sum_{\mathbf{d}}\sum_{\mathbf{c}_1,\mathbf{c}_2}(-1)^{(\mathbf{b}'\cdot\mathbf{c}_1)+(\mathbf{b}''\cdot\bar{\mathbf{c}_2})}(-1)^{\mathbf{d}\cdot(\mathbf{c}_1+\bar{\mathbf{c}}_2)} \\
&\qquad \times\left(C\left(f + \frac{q}{2}\left(\mathbf{d}'\cdot\mathbf{x}' + x_\gamma\right)|_{\mathbf{x}=\mathbf{c}_1},\right.\right. \\
&\qquad\qquad \left.\left.\tilde{f}^* + \frac{q}{2}\mathbf{d}''\cdot\bar{\mathbf{x}}'|_{\mathbf{x}=\mathbf{c}_2}\right)(\tau)\right) \\
&= \sum_{\mathbf{c}_1,\mathbf{c}_2}(-1)^{(\mathbf{b}'\cdot\mathbf{c}_1)+(\mathbf{b}''\cdot\bar{\mathbf{c}_2})}C\left(f+\frac{q}{2}\left(\mathbf{d}'\cdot\mathbf{x}'+x_\gamma\right)|_{\mathbf{x}=\mathbf{c}_1},\right. \\
&\qquad\qquad \left.\tilde{f}^* + \frac{q}{2}\mathbf{d}''\cdot\bar{\mathbf{x}}'|_{\mathbf{x}=\mathbf{c}_2}\right)(\tau)\sum_{\mathbf{d}}(-1)^{\mathbf{d}\cdot(\mathbf{c}_1+\bar{\mathbf{c}}_2)}.
\end{aligned} \tag{64}$$

By applying *Lemma* 6, the above can be express as

$$\begin{aligned}
K_1 = &\sum_{\substack{\mathbf{c}_1,\mathbf{c}_2\\ \mathbf{c}_1-\mathbf{c}_2=\mathbf{1}}} 2^k(-1)^{(\mathbf{b}'\cdot\mathbf{c}_1)+(\mathbf{b}''\cdot\bar{\mathbf{c}_2})} \\
&\qquad \times\left(C\left(f + \frac{q}{2}\left(\mathbf{d}'\cdot\mathbf{x}' + x_\gamma\right)|_{\mathbf{x}=\mathbf{c}_1},\right.\right. \\
&\qquad\qquad \left.\left.\tilde{f}^* + \frac{q}{2}\mathbf{d}''\cdot\bar{\mathbf{x}}'|_{\mathbf{x}=\mathbf{c}_2}\right)(\tau)\right).
\end{aligned} \tag{65}$$

The cross-correlation term in (65) can be simplified to

$$\begin{aligned}
&C\left(f + \frac{q}{2}\left(\mathbf{d}'\cdot\mathbf{x}' + x_\gamma\right)|_{\mathbf{x}=\mathbf{c}_1}, \tilde{f}^* + \frac{q}{2}\mathbf{d}''\cdot\bar{\mathbf{x}}'|_{\mathbf{x}=\mathbf{c}_2}\right)(\tau) \\
&= \sum_{i=0}^{1}\sum_{j=0}^{1} C\left(f + \frac{q}{2}\left(\mathbf{d}'\cdot\mathbf{x}' + x_\gamma\right)|_{\mathbf{x}x_\gamma=\mathbf{c}_1 i},\right. \\
&\qquad\qquad \left.\tilde{f}^* + \frac{q}{2}\mathbf{d}''\cdot\bar{\mathbf{x}}'|_{\mathbf{x}x_\gamma=\mathbf{c}_2 j}\right)(\tau) \\
&= \sum_{i=0}^{1}\sum_{j=0}^{1}(-1)^i C\left(f + \frac{q}{2}\mathbf{d}'\cdot\mathbf{x}'|_{\mathbf{x}x_\gamma=\mathbf{c}_1 i},\right. \\
&\qquad\qquad \left.\tilde{f}^* + \frac{q}{2}\mathbf{d}''\cdot\bar{\mathbf{x}}'|_{\mathbf{x}x_\gamma=\mathbf{c}_2 j}\right)(\tau).
\end{aligned} \tag{66}$$

Therefore the final expression of (62) can be expressed as

$$\begin{aligned} K_1 = & \sum_{\substack{\mathbf{c}_1,\mathbf{c}_2 \\ \mathbf{c}_1-\mathbf{c}_2=\mathbf{1}}} 2^k(-1)^{(\mathbf{b}'\cdot\mathbf{c}_1)+(\mathbf{b}''\cdot\bar{\mathbf{c}_2})} C\left(f+\frac{q}{2}\left(\mathbf{d}'\cdot\mathbf{x}'+x_\gamma\right)|_{\mathbf{x}=\mathbf{c}_1},\right. \\ & \qquad\qquad \left.\tilde{f}^* + \frac{q}{2}\mathbf{d}''\cdot\bar{\mathbf{x}}'|_{\mathbf{x}=\mathbf{c}_2}\right)(\tau) \\ = & \sum_{\substack{\mathbf{c}_1,\mathbf{c}_2 \\ \mathbf{c}_1-\mathbf{c}_2=\mathbf{1}}} 2^k(-1)^{(\mathbf{b}'\cdot\mathbf{c}_1)+(\mathbf{b}''\cdot\bar{\mathbf{c}_2})} \left\{\sum_{i=0}^{1}\sum_{j=0}^{1}(-1)^i\right. \\ & \qquad \times\left(C\left(f+\frac{q}{2}\mathbf{d}'\cdot\mathbf{x}'|_{\mathbf{x}x_\gamma=\mathbf{c}_1 i},\right.\right. \\ & \qquad\qquad \left.\left.\left.\tilde{f}^* + \frac{q}{2}\mathbf{d}''\cdot\bar{\mathbf{x}}'|_{\mathbf{x}x_\gamma=\mathbf{c}_2 j}\right)(\tau)\right)\right\}. \end{aligned} \tag{67}$$

Similarly, (63) can be simplified to

$$\begin{aligned} K_2 = & \sum_{\substack{\mathbf{c}_1,\mathbf{c}_2 \\ \mathbf{c}_1-\mathbf{c}_2=\mathbf{1}}} 2^k(-1)^{(\mathbf{b}'\cdot\mathbf{c}_1)+(\mathbf{b}''\cdot\bar{\mathbf{c}_2})} C\left(f+\frac{q}{2}\mathbf{d}'\cdot\mathbf{x}'|_{\mathbf{x}=\mathbf{c}_1},\right. \\ & \qquad\qquad \left.\tilde{f}^* + \frac{q}{2}\left(\mathbf{d}''\cdot\bar{\mathbf{x}}'+x_\gamma\right)|_{\mathbf{x}=\mathbf{c}_2}\right)(\tau) \\ = & \sum_{\substack{\mathbf{c}_1,\mathbf{c}_2 \\ \mathbf{c}_1-\mathbf{c}_2=\mathbf{1}}} 2^k(-1)^{(\mathbf{b}'\cdot\mathbf{c}_1)+(\mathbf{b}''\cdot\bar{\mathbf{c}_2})} \left\{\sum_{i=0}^{1}\sum_{j=0}^{1}(-1)^j\right. \\ & \qquad \times\left(C\left(f+\frac{q}{2}\mathbf{d}'\cdot\mathbf{x}'|_{\mathbf{x}x_\gamma=\mathbf{c}_1 i},\right.\right. \\ & \qquad\qquad \left.\left.\left.\tilde{f}^* + \frac{q}{2}\mathbf{d}''\cdot\bar{\mathbf{x}}'|_{\mathbf{x}x_\gamma=\mathbf{c}_2 j}\right)(\tau)\right)\right\}. \end{aligned} \tag{68}$$

Therefore, (61) can be expressed as

$$
\begin{aligned}
&C(\psi(S_{t'}),\psi^*(\bar{S}_{t''}))(\tau)\\
&=K_1+K_2\\
&=\sum_{\substack{\mathbf{c}_1,\mathbf{c}_2\\ \mathbf{c}_1-\mathbf{c}_2=\mathbf{1}}} 2^{k+1}(-1)^{(\mathbf{b}'\cdot\mathbf{c}_1)+(\mathbf{b}''\cdot\bar{\mathbf{c}_2})}\Big\{C\left(f+\frac{q}{2}\mathbf{d}'\cdot\mathbf{x}'|_{\mathbf{x}x_\gamma=\mathbf{c}_1 0},\right.\\
&\qquad\qquad\left.\tilde{f}^*+\frac{q}{2}\mathbf{d}''\cdot\bar{\mathbf{x}}'|_{\mathbf{x}x_\gamma=\mathbf{c}_2 0}\right)(\tau)\\
&\quad -C\left(f+\frac{q}{2}\mathbf{d}'\cdot\mathbf{x}'|_{\mathbf{x}x_\gamma=\mathbf{c}_1 1},\tilde{f}^*+\frac{q}{2}\mathbf{d}''\cdot\bar{\mathbf{x}}'|_{\mathbf{x}x_\gamma=\mathbf{c}_2 1}\right)(\tau)\Big\}\\
&=\sum_{\mathbf{c}} 2^{k+1}(-1)^{(\mathbf{b}'\cdot\mathbf{c}_1)+(\mathbf{b}''\cdot\bar{\mathbf{c}_2})}\Big\{C\left(f+\frac{q}{2}\mathbf{d}'\cdot\mathbf{x}'|_{\mathbf{x}x_\gamma=\mathbf{c}0},\right.\\
&\qquad\qquad\left.\tilde{f}^*+\frac{q}{2}\mathbf{d}''\cdot\bar{\mathbf{x}}'|_{\mathbf{x}x_\gamma=\mathbf{c}+\mathbf{1}0}\right)(\tau)\\
&\quad -C\left(f+\frac{q}{2}\mathbf{d}'\cdot\mathbf{x}'|_{\mathbf{x}x_\gamma=\mathbf{c}1},\tilde{f}^*+\frac{q}{2}\mathbf{d}''\cdot\bar{\mathbf{x}}'|_{\mathbf{x}x_\gamma=\mathbf{c}+\mathbf{1}1}\right)(\tau)\Big\}\\
&=\sum_{\mathbf{c}} 2^{k+1}(-1)^{(\mathbf{b}'\cdot\mathbf{c}_1)+(\mathbf{b}''\cdot\bar{\mathbf{c}_2})}\\
&\qquad\times\Bigg\{\sum_{\mathbf{c}'_1,\mathbf{c}'_2}\Big(C\left(f+\frac{q}{2}\mathbf{d}'\cdot\mathbf{x}'|_{\mathbf{x}x_\gamma\mathbf{x}'=\mathbf{c}0\mathbf{c}'_1},\right.\\
&\qquad\qquad\left.\tilde{f}^*+\frac{q}{2}\mathbf{d}''\cdot\bar{\mathbf{x}}'|_{\mathbf{x}x_\gamma\mathbf{x}'=\mathbf{c}+\mathbf{1}0\mathbf{c}'_2}\right)(\tau)\\
&\quad -C\left(f+\frac{q}{2}\mathbf{d}'\cdot\mathbf{x}'|_{\mathbf{x}x_\gamma\mathbf{x}'=\mathbf{c}1\mathbf{c}'_1},\right.\\
&\qquad\qquad\left.\tilde{f}^*+\frac{q}{2}\mathbf{d}''\cdot\bar{\mathbf{x}}'|_{\mathbf{x}x_\gamma\mathbf{x}'=\mathbf{c}+\mathbf{1}1\mathbf{c}'_2}\right)(\tau)\Big)\Bigg\}\\
&=\sum_{\mathbf{c}} 2^{k+1}(-1)^{(\mathbf{b}'\cdot\mathbf{c}_1)+(\mathbf{b}''\cdot\bar{\mathbf{c}_2})}\Bigg\{\sum_{\mathbf{c}'_1,\mathbf{c}'_2}(-1)^{(\mathbf{d}'\cdot\mathbf{c}'_1)+(\mathbf{d}''\cdot\bar{\mathbf{c}}''_2)}\\
&\qquad\times\left(C\left(f|_{\mathbf{x}x_\gamma\mathbf{x}'=\mathbf{c}0\mathbf{c}'_1},\tilde{f}^*|_{\mathbf{x}x_\gamma\mathbf{x}'=\mathbf{c}+\mathbf{1}0\mathbf{c}'_2}\right)(\tau)\right.\\
&\qquad\qquad\left.-C\left(f|_{\mathbf{x}x_\gamma\mathbf{x}'=\mathbf{c}1\mathbf{c}'_1},\tilde{f}^*|_{\mathbf{x}x_\gamma\mathbf{x}'=\mathbf{c}+\mathbf{1}1\mathbf{c}'_2}\right)(\tau)\right)\Bigg\}.
\end{aligned}
$$

Since $G(f|_{\mathbf{x}=\mathbf{c}})$ contains a path over $m-k-p$ vertices and p isolated vertices, the Boolean function $f|_{\mathbf{x}=\mathbf{c}}$ can be expressed as

$$
\begin{aligned}
f|_{\mathbf{x}=\mathbf{c}}=&\frac{q}{2}\sum_{\alpha=0}^{m-k-p-2}x_{l_\alpha}x_{l_{\alpha+1}}+\sum_{\alpha=0}^{m-k-p-1}g_{l_\alpha}x_{l_\alpha}\\
&+\sum_{j=1}^{p}g_{m-p-1+j}x_{m-p-1+j}+g'.
\end{aligned}
$$

Let h_1 denotes the function obtained from f by substituting $\mathbf{x}=\mathbf{c}$, $\mathbf{x}'=\mathbf{c}'_1$ and $x_\gamma=1$ for some binary vectors $\mathbf{c}$ and $\mathbf{c}'_1$ and let h_2 be the corresponding function when $\mathbf{x}=\mathbf{c}$, $\mathbf{x}'=\mathbf{c}'_1$ and $x_\gamma=0$. Further we assume that $\gamma=l_{m-k-p-1}$ without loss of generality. Then the function h_1 and h_2 can be expressed as

$$\begin{aligned}
h_1 =&\frac{q}{2}\sum_{\alpha=0}^{m-k-p-3} x_{l_\alpha}x_{l_{\alpha+1}}+\sum_{\alpha=0}^{m-k-p-2} g_{l_\alpha}x_{l_\alpha}+\Gamma\cdot\mathbf{c}'_1\\
&+\frac{q}{2}x_{l_{m-k-p-2}}+g_{l_{m-k-p-1}}+g',\\
h_2 =&\frac{q}{2}\sum_{\alpha=0}^{m-k-p-3} x_{l_\alpha}x_{l_{\alpha+1}}+\sum_{\alpha=0}^{m-k-p-2} g_{l_\alpha}x_{l_\alpha}+\Gamma\cdot\mathbf{c}'_1+g'.
\end{aligned}$$

Similarly, the nonzero components of the complex vectors $\mathbf{a}=\psi(f|_{\mathbf{x}x_\gamma\mathbf{x}'=\mathbf{c}1\mathbf{c}'_1})$ and $\mathbf{b}=\psi(f|_{\mathbf{x}x_\gamma\mathbf{x}'=\mathbf{c}0\mathbf{c}'_1})$ are given by the functions h_1 and h_2 respectively. Let $\mathbf{c}$ and $\mathbf{d}$ be two complex vectors whose nonzero components are obtained from the functions $h_1-\Gamma\cdot\mathbf{c}'_1$ and $h_2-\Gamma\cdot\mathbf{c}'_1$. Therefore, $\mathbf{a}=\omega^{\Gamma\cdot\mathbf{c}'_1}\mathbf{c}$ and $\mathbf{b}=\omega^{\Gamma\cdot\mathbf{c}'_1}\mathbf{d}$.

Similarly, the nonzero components of the vectors $\mathbf{a}_1=\psi^*(\tilde{f}|_{\mathbf{x}x_\gamma\mathbf{x}'=\mathbf{c}+\mathbf{1}0\mathbf{c}'_2})$ and $\mathbf{b}_1=\psi^*(\tilde{f}|_{\mathbf{x}x_\gamma\mathbf{x}'=\mathbf{c}+\mathbf{1}1\mathbf{c}'_2})$ are obtained by the functions

$$\begin{aligned}
h_3 =&\frac{q}{2}\sum_{\alpha=0}^{m-k-p-3}(1-x_{l_\alpha})(1-x_{l_{\alpha+1}})+\sum_{\alpha=0}^{m-k-p-2} g_{l_\alpha}(1-x_{l_\alpha})\\
&+\Gamma\cdot\bar{\mathbf{c}}'_2+\frac{q}{2}(1-x_{l_{m-k-p-2}})+g_{l_{m-k-p-1}}+g'\\
=&\tilde{h}_1-\Gamma\cdot(\bar{\mathbf{c}}'_1)+\Gamma\cdot\bar{\mathbf{c}}'_2,\\
h_4 =&\frac{q}{2}\sum_{\alpha=0}^{m-k-p-3}(1-x_{l_\alpha})(1-x_{l_{\alpha+1}})+\sum_{\alpha=0}^{m-k-p-2} g_{l_\alpha}(1-x_{l_\alpha})\\
&+\Gamma\cdot\bar{\mathbf{c}}'_2+g'\\
=&\tilde{h}_2-\Gamma\cdot(\bar{\mathbf{c}}'_1)+\Gamma\cdot\bar{\mathbf{c}}'_2.
\end{aligned}$$

Therefore $\mathbf{a}_1=\omega^{\Gamma\cdot\bar{c}'_2}\tilde{\mathbf{c}}^*$ and $\mathbf{b}_1=\omega^{\Gamma\cdot\bar{c}'_2}\tilde{\mathbf{d}}^*$.

Now, the difference of cross-correlation terms of (69) can be simplified to

$$\begin{aligned}
&C\left(f|_{\mathbf{x}x_\gamma\mathbf{x}'=\mathbf{c}0\mathbf{c}'_1},\tilde{f}^*|_{\mathbf{x}x_\gamma\mathbf{x}'=\mathbf{c}+\mathbf{1}0\mathbf{c}'_2}\right)(\tau)\\
&\qquad\qquad -C\left(f|_{\mathbf{x}x_\gamma\mathbf{x}'=\mathbf{c}1\mathbf{c}'_1},\tilde{f}^*|_{\mathbf{x}x_\gamma\mathbf{x}'=\mathbf{c}+\mathbf{1}1\mathbf{c}'_2}\right)(\tau)\\
=&C(\mathbf{b},\mathbf{a}_1)(\tau)-C(\mathbf{a},\mathbf{b}_1)(\tau)\\
=&\omega^{\Gamma\cdot\mathbf{c}'_1}\bar{\omega}^{\Gamma\cdot\bar{c}'_2}\left(C(\mathbf{d},\tilde{\mathbf{c}}^*)(\tau)-C(\mathbf{c},\tilde{\mathbf{d}}^*)(\tau)\right).
\end{aligned}\tag{69}$$

For any two complex sequences $\mathbf{c}$ and $\mathbf{d}$, recall the identity

$$C(\mathbf{c}, \tilde{\mathbf{d}}^*)(\tau) = C(\tilde{\mathbf{d}}, \mathbf{c}^*)(-\tau) = C(\mathbf{d}, \tilde{\mathbf{c}}^*)(\tau).$$

Therefore, substituting (69) in (69) and using the above identity we have $K_1 + K_2 = 0$, thus completing the proof.

■

APPENDIX C
PROOF OF *Remark 1*

Proof: In Fig. 1, if we fix the set $X_S = \{x_{i_1}, x_{i_2}, \cdots, x_{i_p}\}$ in $\{x_{m-p}, x_{m-p+1}, \cdots, x_{m-1}\}$, then a GBF corresponding to Fig. 1 produces an optimal ZCCS. Our task is to find out the number of such distinct GBFs. After fixing $X_S = \{x_{m-p}, x_{m-p+1}, \cdots, x_{m-1}\}$, the set $X_J = \{x_{j_0}, x_{j_1}, \cdots, x_{j_{k-1}}\}$ can be chosen in $\binom{m-p}{k}$ ways. For each choice of X_J, the set X_P can be chosen in only one way. The quadratic form Q given in (17), can be expressed as $Q = Q_1 + Q_2 + Q_3 + Q_4$ where

$$\begin{aligned} Q_1 &= \frac{q}{2} \sum_{i=0}^{m-k-p-2} x_{l_i} x_{l_{i+1}}, \\ Q_2 &= \sum_{i=0}^{m-k-p-1} \sum_{\alpha=0}^{k-1} a'_{i,\alpha} x_{l_i} x_{j_\alpha}, \\ Q_3 &= \sum_{\alpha=0}^{k-1} \sum_{\beta=1}^{p} e'_{\alpha,\beta} x_{j_\alpha} x_{i_\beta}, \\ Q_4 &= \sum_{0 \le \alpha_1 < \alpha_2 < k} b'_{\alpha_1,\alpha_2} x_{j_{\alpha_1}} x_{j_{\alpha_2}}. \end{aligned} \tag{70}$$

For each choice of $\binom{m-p}{k}$, we get $\frac{(m-k-p)!}{2}$ distinct Q_1, $(q-1)^{k(m-k-p)}$ distinct Q_2, q^{kp} distinct Q_3, and $q^{\frac{k(k-1)}{2}}$ distinct Q_4. Finally, we get at least

$$\frac{(m-p)!}{2(k!)} (q-1)^{k(m-k-p)} q^{kp + \frac{k(k-1)}{2}} \tag{71}$$

distinct quadratic forms. Corresponding to each quadratic form Q, we get q^{m+1} distinct GBFs. Therefore there exist at least $\frac{(m-p)!}{2(k!)} (q-1)^{k(m-k-p)} q^{kp + \frac{k(k-1)}{2} + m + 1}$ distinct GBFs corresponding to which we get the same number of distinct optimal ZCCSs. In the above enumeration, we have taken $a'_{i,\alpha} \in \mathbb{Z}_q \setminus \{\frac{q}{2}\}$, otherwise sometimes we can get some ZCCSs more than once. ■

REFERENCES

[1] H.-H. Chen, *The Next Generation CDMA Technologies*. Wiley, 2007.

[2] M. Golay, "Complementary series," *IRE Trans. Inf. Theory*, vol. 7, no. 2, pp. 82–87, Apr. 1961.

[3] C.-C. Tseng and C. Liu, "Complementary sets of sequences," *IEEE Trans. Inf. Theory*, vol. 18, no. 5, pp. 644–652, Sep. 1972.

[4] J. A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2397–2417, Nov. 1999.

[5] Y. Li, "A construction of general QAM Golay complementary sequences," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5765–5771, Nov. 2010.

[6] Z. Liu, Y. Li, and Y. L. Guan, "New constructions of general QAM Golay complementary sequences," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7684–7692, Nov. 2013.

[7] 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.

[8] K. U. Schmidt, "Complementary sets, generalized Reed-Muller codes, and power control for OFDM," *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 808–814, Feb. 2007.

[9] 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.

[10] Z. Liu, Y. L. Guan, and U. Parampalli, "New complete complementary codes for peak-to-mean power control in multi-carrier CDMA," *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 1105–1113, Mar. 2014.

[11] 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.

[12] S. Das, S. Budišin, S. Majhi, Z. Liu, and Y. L. Guan, "A multiplier-free generator for polyphase complete complementary codes," *IEEE Trans. Signal Process.*, vol. 66, no. 5, pp. 1184–1196, Mar. 2018.

[13] S. Das, S. Majhi, and Z. Liu, "A novel class of complete complementary codes and their applications for apu matrices," *IEEE Signal Process. Lett.*, vol. 25, no. 9, pp. 1300–1304, Sept. 2018.

[14] Z. 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.

[15] Z. Liu, Y. L. Guan, and U. Parampalli, "A new construction of zero correlation zone sequences from generalized Reed-Muller codes," in *2014 IEEE Information Theory Workshop*, Nov. 2014, pp. 591–595.

[16] P. Fan, W. Yuan, and Y. Tu, "Z-complementary binary sequences," *IEEE Signal Process. Lett.*, vol. 14, no. 8, pp. 509–512, Aug. 2007.

[17] L. Feng, P. Fan, X. Tang, and K. K. Loo, "Generalized pairwise Z-complementary codes," *IEEE Signal Process. Lett.*, vol. 15, pp. 377–380, 2008.

[18] J. Li, A. Huang, M. Guizani, and H.-H. Chen, "Inter group complementary codes for interference resistant CDMA wireless communications," *IEEE Trans. Wireless Commun.*, vol. 7, no. 1, pp. 166–174, Jan. 2008.

[19] P. Sarkar, S. Majhi, H. Vettikalladi, and A. S. Mahajumi, "A direct construction of inter-group complementary code set," *IEEE Access*, pp. 1–1, 2018.

[20] W. Yuan, Y. Tu, and P. Fan, "Optimal training sequences for cyclic-prefix-based single-carrier multi-antenna systems with space-time block-coding," *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4047–4050, Nov. 2008.

[21] H. M. Wang, X. Q. Gao, B. Jiang, X. H. You, and W. Hong, "Efficient MIMO channel estimation using complementary sequences," *IET Commun.*, vol. 1, no. 5, pp. 962–969, Oct. 2007.

[22] Z. Liu and Y. L. Guan, "16-QAM almost-complementary sequences with low PMEPR," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 668–679, Feb. 2016.

[23] T. E. Stinchcombe, "Aperiodic correlations of length 2^m sequences, complementarity, and power control for OFDM," Ph.D. dissertation, University of London, Apr. 2000.