A New Construction of Zero Correlation Zone Sequences from Generalized Reed-Muller Codes

Zilong Liu, Yong Liang Guan
School of Electrical and Electronic Engineering
Nanyang Technological University
Singapore
Email: {zilongliu,eylguan}@ntu.edu.sg

Udaya Parampalli
Department of Computing and Information Systems
University of Melbourne
VIC 3010, Australia
Email: udaya@unimelb.edu.au

***Abstract*—In this paper, we present a direct construction of zero-correlation zone (ZCZ) sequence sets (each associated with a graph) from the second order cosets of the first-order generalized Reed-Muller codes. This settles an open problem introduced by Rathinakumar and Chaturvedi in their 2008 paper.**

I. Introduction

Zero-correlation zone (ZCZ) sequences were proposed in the late 1990s, aiming to eliminate the "near-far effect" and to achieve interference-free performance [1] in asynchronous code-division multiple access (CDMA) communication systems. By definition, ZCZ sequences possess zero auto- and cross- correlations over a region around the in-phase timing position. Hence, ZCZ sequence sets are used in a quasi-synchronous CDMA system, where received signals are approximately synchronized with transmitted signals [2].

The past decade has witnessed significant developments in the area of ZCZ sequence constructions [3]−[6]. In the literature, an interesting research direction has been to construct ZCZ sequences through a sequence transform of mutually orthogonal complementary codes (MOCCs). MOCCs can be represented as a set of two-dimensional matrices with zero aperiodic auto- and cross- correlation sums. For more details on perfect- and quasi- complementary codes, readers are referred to [7]−[16].

In [17], by constructing complete complementary codes (CCC) based on generalized Reed-Muller codes, Rathinakumar and Chaturvedi postulated that there may also exist direct constructions of ZCZ sequences using generalized Reed-Muller codes: "*We believe that the direct construction of Golay complementary sets ... can be used to algebraically construct such ZCZ sets. One possible approach is to associate a graph with a ZCZ sequence set and relate the IFW*[1] *property of the ZCZ sequences to that graph.*" This is referred to as the Rathinakumar-Chaturvedi open problem in this paper. Solving this open problem will uncover deeper inherent connections between ZCZ sequences, CCC, and Reed-Muller codes, which may be useful in finding new ZCZ sequence constructions. In addition, it will simplify the sequence generation and facilitate the sequence enumeration, owing to the Reed-Muller code properties.

[1]i.e., interference free window.

Recently, Gong, Huo and Yang found that certain Golay sequences constructed from generalized Reed-Muller codes feature the zero autocorrelation zone (ZACZ) property [18]. In particular, they raised an open problem similar to that in [17]: how can CDMA spreading sequences be constructed from Golay sequences with the ZACZ property? A possible solution is to construct CDMA spreading sequences with zero auto- and cross- correlation zone properties from generalized Reed-Muller codes.

In this paper, we settle the Rathinakumar-Chaturvedi open problem by constructing ZCZ sequence sets from the second order cosets of the first-order generalized Reed-Muller codes. Interestingly, each of the proposed ZCZ sequence sets is associated with a two-layer graph where the ZCZ width is equal to the power of the vertex number in the upper layer of its graph.

II. Preliminaries

Given two length-N complex-valued sequences $\mathbf{a} = [a_0, a_1, \cdots, a_{N-1}]$ and $\mathbf{b} = [b_0, b_1, \cdots, b_{N-1}]$, their aperiodic correlation function at time-shift τ is defined as

$$\rho(\mathbf{a},\mathbf{b})(\tau) = \sum_{t=0}^{N-1-\tau} a_t b^*_{t+\tau}, \quad 0 \leq \tau \leq N-1. \qquad (1)$$

When $\mathbf{a} \neq \mathbf{b}$, $\rho(\mathbf{a},\mathbf{b})(\tau)$ is called the aperiodic cross-correlation function (ACCF); Otherwise, it is called aperiodic auto-correlation function (AACF). For simplicity, the AACF of $\mathbf{a}$ will be sometimes written as $\rho(\mathbf{a})(\tau)$.

In addition, the periodic cross- (or auto-) correlation function between $\mathbf{a}$ and $\mathbf{b}$ is defined as

$$\theta(\mathbf{a},\mathbf{b})(\tau) = \rho(\mathbf{a},\mathbf{b})(\tau) + \rho^*(\mathbf{b},\mathbf{a})(N-\tau). \qquad (2)$$

A. ZCZ sequences

Let $\mathcal{A} = \{\mathbf{a}_0, \mathbf{a}_1, \cdots, \mathbf{a}_{K-1}\}$ be a set of K sequences, each of length L, i.e.,

$$\mathbf{a}_i = \left[a^i_0, a^i_1, \cdots, a^i_n, \cdots, a^i_{L-1}\right], \ 0 \leq i \leq K-1. \qquad (3)$$

Definition 1: $\mathcal{A}$ is said to be a (K, L, Z)-ZCZ sequence set if and only if it satisfies the following two conditions:

1) $\theta(\mathbf{a}_i)(\tau) = 0$ holds for any $0 \leq i \leq K-1$ and $1 \leq |\tau| \leq Z$;

2) $\theta(\mathbf{a}_i, \mathbf{a}_j)(\tau) = 0$ holds for any $i \neq j$ and $0 \leq |\tau| \leq Z$.

B. Complete Complementary Codes (CCC)

Let $\mathcal{C} = \{C_0, C_1, \cdots, C_{K-1}\}$ be a set of K matrices, each of order $M \times N$, i.e.,

$$C_\mu = \begin{bmatrix} \mathbf{c}_0^\mu \\ \mathbf{c}_1^\mu \\ \vdots \\ \mathbf{c}_{M-1}^\mu \end{bmatrix}_{M\times N}, \ 0 \leq \mu \leq K-1. \tag{4}$$

The aperiodic cross-correlation function between C_μ and C_ν (where $0 \leq \mu, \nu \leq K-1$), which is in the form of "aperiodic correlation sum", is defined as

$$\rho(C_\mu, C_\nu)(\tau) = \sum_{m=0}^{M-1} \rho(\mathbf{c}_m^\mu, \mathbf{c}_m^\nu)(\tau). \tag{5}$$

Definition 2: $\mathcal{C}$ is said to be a (K, M, N)-mutually orthogonal complementary code set (MOCCS) if $\rho(C_\mu, C_\nu)(\tau) = 0$ for any $\mu \neq \nu$, and $\mu = \nu, \tau \neq 0$. It is known that $K \leq M$ [13]. When $K = M$, $\mathcal{C}$ is said to be a set of CCC.

C. Generalized Reed-Muller Codes for CCC Constructions

The following notations will be used throughout this paper.

- $\mathbb{Z}_q = \{0, 1, \cdots, q-1\}$;
- $\xi = \exp(2\pi\sqrt{-1}/q)$, the qth root of unity;
- Denote by $[i_0, i_1, \cdots, i_{n-1}]_2$ the binary representation of the integer $i = \sum_{\alpha=0}^{n-1} i_\alpha 2^\alpha$, where the most significant bit (MSB) is represented by i_{n-1}. For simplicity, we write $i = [i_0, i_1, \cdots, i_{n-1}]_2$.
- Denote by $\overline{x} = 1 - x$ the binary complement of $x \in \{0, 1\}$.

Definition 3: For $\mathbf{x} = [x_0, x_1, \cdots, x_{n-1}] \in \{0,1\}^n$, the q-ary generalized Boolean function (GBF) $f(x_0, x_1, \cdots, x_{n-1})$ is defined as a mapping $f : \{0,1\}^n \to \mathbb{Z}_q$. The algebraic normal form of f can be written as a sum of monomials, i.e.,

$$f(x_0, x_1, \cdots, x_{n-1}) = \sum_{0\leq i \leq 2^n-1} c_i \prod_{\alpha=0}^{n-1} x_\alpha^{i_\alpha}, \quad c_i \in \mathbb{Z}_q. \tag{6}$$

If $r = \max\{\sum i_\alpha : c_i \sum i_\alpha \neq 0\}$, we say that the algebraic degree of f is r, i.e., $\deg(f) = r$. For $f_i = f(i_0, i_1, \cdots, i_{n-1})$, define the $\mathbb{Z}_q$-valued vector $\boldsymbol{f}$ and the complex-valued vector $\psi(f)$ (both of which are associated with f)

$$\begin{aligned} \boldsymbol{f} &= [f_0, f_1, \cdots, f_{2^n-1}], \\ \psi(f) &= \left[\xi^{f_0}, \xi^{f_1}, \cdots, \xi^{f_{2^n-1}}\right] \end{aligned} \tag{7}$$

respectively.

Definition 4: Denote by $\text{RM}_q(r, n)$ the rth order $\mathbb{Z}_q$-valued generalized Reed-Muller code (which is a linear code over $\mathbb{Z}_q$) whose generator matrix is formed by the binary vectors associated with all monomials of algebraic degree at most r in $x_0, x_1, \cdots, x_{n-1}$.

For instance, the following matrix

$$\begin{array}{cc} \begin{bmatrix} 11111111 \\ 01010101 \\ 00110011 \\ 00001111 \\ 00010001 \\ 00000101 \\ 00000011 \end{bmatrix} & \begin{array}{c} 1 \\ x_0 \\ x_1 \\ x_2 \\ x_0x_1 \\ x_0x_2 \\ x_1x_2 \end{array} \end{array}$$

is the generator matrix for $\text{RM}_4(2, 3)$ over $\mathbb{Z}_4$.

Definition 5: $\tilde{f} = f(\bar{x}_0, \bar{x}_1, \cdots, \bar{x}_{n-1})$ is called the reversal of f because

$$\psi\left(\tilde{f}\right) = \left[\xi^{f_{2^n-1}}, \xi^{f_{2^n-2}}, \cdots, \xi^{f_0}\right].$$

Definition 6: Let $J = \{j_0, j_1, \cdots, j_{k-1}\} \subset \{0, 1, \cdots, n-1\}$ and $\mathbf{x}_J = [x_{j_0}, x_{j_1}, \cdots, x_{j_{k-1}}]$. $f|_{\mathbf{x}_J=\mathbf{d}}$ is called a restriction of f over constant $\mathbf{d} \in \{0,1\}^k$. Specifically, $\psi(f|_{\mathbf{x}_J=\mathbf{d}})$ is a sequence of length 2^n with the elements coincide with that of $\psi(f)$ at the positions i where $i_{j_\alpha} = d_\alpha$ for each $0 \leq \alpha < k$, and equal to zero otherwise.

Next, we show existing constructions of complementary codes based on the second order cosets of $\text{RM}_q(1, m)$.

Lemma 1: (Construction of complementary codes [19])
Let $\deg(f) = 2$. Denote by $Q : \{0,1\}^n \to \mathbb{Z}_q$ the quadratic part of f, where

$$Q = \sum_{0\leq u<v\leq n-1} q_{uv} x_u x_v, \quad q_{uv} \in \mathbb{Z}_q. \tag{8}$$

Furthermore, denote by $G(Q)$ the graph of Q which is formed by joining vertices u and v by an edge if it has a non-zero weight of q_{uv} for any $0 \leq u < v \leq n-1$. Also, let $I = \{i_0, i_1, \cdots, i_{n-k-1}\} \subset \{0, 1, \cdots, n-1\} \setminus J$, where J is defined in *Definition 6*. Suppose that deleting the vertex set J from $G(Q)$ results in a Hamiltonian path, i.e.,

$$f|_{\mathbf{x}_J=\mathbf{d}} = \frac{q}{2} \sum_{\alpha=0}^{n-k-2} x_{i_{\pi(\alpha)}} x_{i_{\pi(\alpha+1)}} + \sum_{\alpha=0}^{n-k-1} l_\alpha x_{i_\alpha} + l, \tag{9}$$

where $l_\alpha, l \in \mathbb{Z}_q$, and π is a permutation of $(0, 1, \cdots, n-k-1)$. Then

$$\left\{ f + \frac{q}{2}\left(\sum_{\alpha=0}^{k-1} y_\alpha x_{j_\alpha} + y_k x_a\right) : y_k, y_\alpha \in \mathbb{Z}_2 \right\} \tag{10}$$

generate a complementary matrix of order $2^{k+1} \times 2^n$ over $\mathbb{Z}_q$, where $a = i_{\pi(0)}$ or $i_{\pi(n-k-1)}$.

The following CCC construction is an extension of the construction in *Lemma 1*:

Lemma 2: (Construction of CCC [17])
Consider the q-ary GBF f in *Lemma 1*, and its reversal $\tilde{f}$. Let $t = [t_0, t_1, \cdots, t_{k-1}]_2$. Define complementary codes C_t

and C_{2^k+t} as

$$\left\{f+\frac{q}{2}\left(\sum_{\alpha=0}^{k-1} y_\alpha x_{j_\alpha}+y_k x_a+\sum_{\gamma=0}^{k-1} t_\gamma x_{j_\gamma}\right): y_k, y_\alpha \in \mathbb{Z}_2\right\}, \tag{11}$$

and

$$\left\{\tilde{f}+\frac{q}{2}\left(\sum_{\alpha=0}^{k-1} y_\alpha \bar{x}_{j_\alpha}+\bar{y}_k x_a+\sum_{\gamma=0}^{k-1} t_\gamma \bar{x}_{j_\gamma}\right): y_k, y_\alpha \in \mathbb{Z}_2\right\}, \tag{12}$$

respectively. Then

$$\left\{\psi\left(C_t\right): 0 \leq t \leq 2^k-1\right\} \cup\left\{\psi^*\left(C_{2^k+t}\right): 0 \leq t \leq 2^k-1\right\}, \tag{13}$$

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

III. Proposed ZCZ Construction from Generalized Reed-Muller Codes

First, we need the following lemma.

Lemma 3: Let $q = 2$. For $k+2$ binary variables in $x_0, x_1, \cdots, x_k, x_{k+1}$, consider the following Boolean function

$$h=\sum_{\alpha=1}^{k+1} c_\alpha x_\alpha x_0+\sum_{1 \leq \mu<\nu \leq k} d_{\mu \nu} x_\mu x_\nu+\sum_{\beta=0}^{k+1} e_\beta x_\beta+e^{\prime}, \tag{14}$$

where $c_{k+1}=1, c_\alpha \in \mathbb{Z}_2$ for $1 \leq \alpha \leq k$, $d_{\mu\nu}, e_\beta, e' \in \mathbb{Z}_2$. Denote by $\boldsymbol{h}$ the resultant binary vector over $\mathbb{Z}_2^{k+2}$, i.e.,

$$\boldsymbol{h}=[h_0, h_1, \cdots, h_{2^{k+2}-1}]. \tag{15}$$

For $0 \leq \tau \leq 2^{k+1}-1$, we have

$$(-1)^{h_\tau+h_{\tau+1}}+(-1)^{h_{\tau+2^{k+1}}+h_{\tau+1+2^{k+1}}}=0, \tag{16}$$

where the additions in the subscripts are performed modulo 2^{k+2}.

Proof: The proof of (16) follows if we can show

$$h_\tau+h_{\tau+1}+h_{\tau+2^{k+1}}+h_{\tau+1+2^{k+1}} \equiv 1 \pmod 2, \tag{17}$$

for $0 \leq \tau \leq 2^{k+1}-1$. For $0 \leq \tau \leq 2^{k+1}-2$, denote by

$$\begin{aligned} \tau &=[\tau_0, \tau_1, \cdots, \tau_k, 0]_2, \\ \tau+1 &=[\tau_0', \tau_1', \cdots, \tau_k', 0]_2. \end{aligned} \tag{18}$$

Clearly,

$$\begin{aligned} \tau+2^{k+1} &=[\tau_0, \tau_1, \cdots, \tau_k, 1]_2, \\ \tau+1+2^{k+1} &=[\tau_0', \tau_1', \cdots, \tau_k', 1]_2. \end{aligned} \tag{19}$$

By (14), (18) and (19), we have

$$\left\{\begin{aligned} h_\tau =& \sum_{\alpha=1}^{k+1} c_\alpha \tau_\alpha \tau_0+\sum_{1 \leq \mu<\nu \leq k} d_{\mu \nu} \tau_\mu \tau_\nu \\ &+\sum_{\beta=0}^{k+1} e_\beta \tau_\beta+e', \\ h_{\tau+2^{k+1}} =& h_\tau+\tau_0+e_{k+1} \end{aligned}\right. \tag{20}$$

and

$$\left\{\begin{aligned} h_{\tau'} =& \sum_{\alpha=1}^{k+1} c_\alpha \tau_\alpha' \tau_0'+\sum_{1 \leq \mu<\nu \leq k} d_{\mu \nu} \tau_\mu' \tau_\nu' \\ &+\sum_{\beta=0}^{k+1} e_\beta \tau_\beta'+e', \\ h_{\tau'+2^{k+1}} =& h_{\tau'}+\tau_0'+e_{k+1} \end{aligned}\right. \tag{21}$$

Therefore,

$$\begin{aligned} & h_\tau+h_{\tau+1}+h_{\tau+2^{k+1}}+h_{\tau+1+2^{k+1}} \\ =& \underbrace{h_\tau+h_{\tau+2^{k+1}}}+\underbrace{h_{\tau+1}+h_{\tau+1+2^{k+1}}} \\ \equiv& \tau_0+\tau_0' \\ \equiv& 1 \pmod 2, \end{aligned}$$

which is (17), thus completing the proof. ■

Example 1: Let $k=2$. The following Boolean function

$$h=x_3 x_0+x_0 x_2+x_2 x_1+x_3+x_0+1 \tag{22}$$

results in

$$\boldsymbol{h}=[\underbrace{1,0,1,0,1,1,0,0}_{\text{length}=8}, \underbrace{0,0,0,0,0,1,1,0}_{\text{length}=8}]$$

which satisfies (16). In particular, if $h=x_3x_0$, one gets

$$\boldsymbol{h}=[\underbrace{0,0,0,0,0,0,0,0}_{\text{length}=8}, \underbrace{0,1,0,1,0,1,0,1}_{\text{length}=8}]$$

which also satisfies (16).

Theorem 1: Consider a set of CCC generated by *Lemma 2*, i.e., $\mathcal{C}=\{C_0, C_1, \cdots, C_{2^{k+1}-1}\}$, where

$$C_\mu=\begin{bmatrix} \mathbf{c}_0^\mu \\ \mathbf{c}_1^\mu \\ \vdots \\ \mathbf{c}_{2^{k+1}-1}^\mu \end{bmatrix}_{2^{k+1} \times 2^n}, \quad 0 \leq \mu \leq 2^{k+1}-1. \tag{23}$$

Based on $\boldsymbol{h}$ in (15), define two matrices $\mathcal{H}^0$ and $\mathcal{H}^1$ in (24) and (25), respectively. Then, the rows of matrix

$$\mathcal{H}=[\mathcal{H}^0, \mathcal{H}^1]$$

form a

$$(K=2^{k+1}, L=2^{n+k+2}, Z=2^n)$$

ZCZ sequence set.

Proof: Denote by $\mathcal{H}_i$ the ith row vector of $\mathcal{H}$. For $0 \leq \tau \leq 2^n$, the periodic cross-correlation function between $\mathcal{H}_i$ and $\mathcal{H}_j$ is shown in (26).

Next, by (16), (26) and the zero aperiodic sum property of $\mathcal{C}$, we have

$$\begin{aligned} & \theta(\mathcal{H}_i, \mathcal{H}_j)(\tau) \\ =& 2 \cdot \sum_{m=0}^{2^{k+1}-1} \rho(\mathbf{c}_m^i, \mathbf{c}_m^j)(\tau) \\ =& 2\rho(C_i, C_j)(\tau) \\ =& \begin{cases} 2^{k+n+2}, & \text{if } i=j \text{ and } \tau=0; \\ 0, & \text{otherwise} \end{cases} \end{aligned} \tag{27}$$

$$\mathcal{H}^0=\begin{bmatrix} \mathbf{c}_0^0(-1)^{h_0}, & \mathbf{c}_1^0(-1)^{h_1}, & \cdots, & \mathbf{c}_{2^{k+1}}^0(-1)^{h_{2^{k+1}-1}} \\ \mathbf{c}_0^1(-1)^{h_0}, & \mathbf{c}_1^1(-1)^{h_1}, & \cdots, & \mathbf{c}_{2^{k+1}}^1(-1)^{h_{2^{k+1}-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{c}_0^{2^{k+1}-1}(-1)^{h_0}, & \mathbf{c}_1^{2^{k+1}-1}(-1)^{h_1}, & \cdots, & \mathbf{c}_{2^{k+1}}^{2^{k+1}-1}(-1)^{h_{2^{k+1}-1}} \end{bmatrix}. \tag{24}$$

$$\mathcal{H}^1=\begin{bmatrix} \mathbf{c}_0^0(-1)^{h_{2^{k+1}}}, & \mathbf{c}_1^0(-1)^{h_{2^{k+1}+1}}, & \cdots, & \mathbf{c}_{2^{k+1}}^0(-1)^{h_{2^{k+2}-1}} \\ \mathbf{c}_0^1(-1)^{h_{2^{k+1}}}, & \mathbf{c}_1^1(-1)^{h_{2^{k+1}+1}}, & \cdots, & \mathbf{c}_{2^{k+1}}^1(-1)^{h_{2^{k+2}-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{c}_0^{2^{k+1}-1}(-1)^{h_{2^{k+1}}}, & \mathbf{c}_1^{2^{k+1}-1}(-1)^{h_{2^{k+1}+1}}, & \cdots, & \mathbf{c}_{2^{k+1}}^{2^{k+1}-1}(-1)^{h_{2^{k+2}-1}} \end{bmatrix}. \tag{25}$$

$$\begin{aligned} &\theta(\mathcal{H}_i,\mathcal{H}_j)(\tau) \\ =&2\cdot\sum_{m=0}^{2^{k+1}-1}\rho(\mathbf{c}_m^i,\mathbf{c}_m^j)(\tau)+\left[\underbrace{(-1)^{h_{2^{k+1}-1}+h_{2^{k+1}}}+(-1)^{h_{2^{k+2}-1}+h_0}}\right]\rho^*(\mathbf{c}_0^j,\mathbf{c}_{2^{k+1}-1}^i)(L-\tau) \\ &+\sum_{m=0}^{2^{k+1}-2}\left[\underbrace{(-1)^{h_m+h_{m+1}}+(-1)^{h_{m+2^{k+1}}+h_{m+1+2^{k+1}}}}\right]\rho^*(\mathbf{c}_{m+1}^j,\mathbf{c}_m^i)(L-\tau). \end{aligned} \tag{26}$$

Thus, the proof of *Theorem 1* follows. ■

Remark 1: The proposed ZCZ construction in *Theorem 1* is a generalization of that in [3], where

$$\boldsymbol{h}=[\underbrace{0,0,\cdots,0,0}_{\text{length}=2^{k+1}},\underbrace{0,1,,\cdots,0,1}_{\text{length}=2^{k+1}}]$$

(which is generated by $h=x_0x_{k+1}$) is used, as indicated by the latter case of *Example 1*.

Based on *Lemma 2*, *Lemma 3* and *Theorem 1*, we are now ready to present the proposed ZCZ construction based on generalized Reed-Muller codes. For completeness, some definitions will be given again.

Theorem 2: For $n+k+2$ binary variables $x_0,x_1,\cdots,$ x_{n+k+1}, define a GBF $f(x_0,x_1,\cdots,x_{n-1})$ which satisfies the condition in *Lemma 1*, i.e., deleting the vertex set $J=\{j_0,j_1,\cdots,j_{k-1}\}$ from the graph of f results in a Hamiltonian path characterized by $\frac{q}{2}\sum_{\alpha=0}^{n-k-2}x_{i_{\pi(\alpha)}}x_{i_{\pi(\alpha+1)}}$ over $I=\{i_0,i_1,\cdots,i_{n-k-1}\}$, where π is a permutation of $(0,1,\cdots,n-k-1)$, $I\cup J=\{0,1,\cdots,n-1\}$ and $I\cap J=\emptyset$. Also, define another GBF $h(x_n,x_{n+1},\cdots,x_{n+k+1})$ as

$$\begin{aligned} h=&\frac{q}{2}\sum_{\alpha=1}^{k+1}c_\alpha x_{\alpha+n}x_n+\frac{q}{2}\sum_{1\le\mu<\nu\le k}d_{\mu\nu}x_{\mu+n}x_{\nu+n} \\ &+\frac{q}{2}\sum_{\beta=0}^{k+1}e_\beta x_{\beta+n}, \end{aligned} \tag{28}$$

where $c_{k+1}=1,c_\alpha\in\mathbb{Z}_2$ for $1\le\alpha\le k$, $d_{\mu\nu},e_\beta,\in\mathbb{Z}_2$. Let ϖ be a permutation of $(0,1,\cdots,k)$, and $t=[t_0,t_1,\cdots,t_{k-1}]_2$. Also, let a be either end-vertex of the Hamiltonian path, i.e., $a=i_{\pi(0)}$ or $i_{\pi(n-k-1)}$. Generate two sequence sets $\{\mathbf{z}_t:0\le t\le 2^k-1\}$ and $\{\mathbf{z}_{t+2^k}:0\le t\le 2^k-1\}$ by

$$\left\{f+h+\frac{q}{2}\left(\sum_{\alpha=0}^{k-1}x_{n+\varpi(\alpha)}x_{j_\alpha}+x_{n+\varpi(k)}x_a+\sum_{\gamma=0}^{k-1}t_\gamma x_{j_\gamma}\right)\right\} \tag{29}$$

and

$$\left\{\tilde{f}+h+\frac{q}{2}\left(\sum_{\alpha=0}^{k-1}x_{n+\varpi(\alpha)}\bar{x}_{j_\alpha}+\bar{x}_{n+\varpi(k)}x_a+\sum_{\gamma=0}^{k-1}t_\gamma \bar{x}_{j_\gamma}\right)\right\} \tag{30}$$

respectively. Then,

$$\{\psi(\mathbf{z}_t)\}\cup\{\psi^*(\mathbf{z}_{t+2^k})\},\quad\text{where } 0\le t\le 2^k-1 \tag{31}$$

form a $(K=2^{k+1},L=2^{n+k+2},Z=2^n)$-ZCZ sequence set.

Proof: The proof of this theorem can be obtained by applying *Lemma 2* and *Theorem 1*. It is however omitted due to the space limitation. ■

Example 2: Let $q=4,k=1,n=3$, $J=\{0\}$ and $I=\{1,2\}$. Also, let

$$\begin{aligned} f&=2x_1x_2+3x_0x_2+x_0x_1+3x_1+x_2+1, \\ h&=2x_3x_5+2x_3x_4+2x_3+2x_5+3. \end{aligned}$$

Clearly,

$$\begin{aligned} \tilde{f}&=f(1-x_0,1-x_1,1-x_2) \\ &=2x_1x_2+3x_0x_2+x_0x_1+2x_1+2x_2+3. \end{aligned}$$

Generate two sequence sets $\{\mathbf{z}_t:t\in\mathbb{Z}_2\}$ and $\{\mathbf{z}_{t+2}:t\in\mathbb{Z}_2\}$ by

$$\left\{f+h+2(x_0x_3+x_1x_4)+2tx_0\right\}$$

and

$$\left\{\tilde{f}+h+2(\bar{x}_0x_6+x_1\bar{x}_4)+2t\bar{x}_0\right\}$$

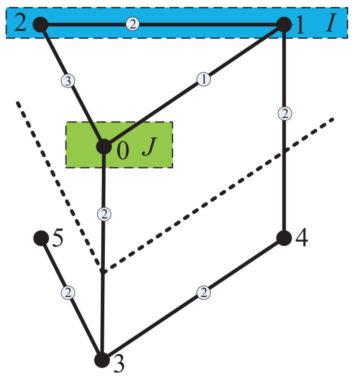

Fig. 1. Graph representation of $f + h + 2(x_0x_3 + x_1x_4)$

respectively. A graph representation of $f+h+2(x_0x_3+x_1x_4)$ is given in Fig. 1, with every edge's weight is shown in a small circle. It is seen that this graph features a two-layer structure where the upper layer and lower layer (separated by the dashed lines) are specified by vertex sets $\{0, 1, 2\}$ and $\{3, 4, 5\}$, respectively. Also, deleting the vertex set $J = \{0\}$, its upper layer graph reduces to a Hamiltonian path (characterized by $2x_1x_2$) over $I = \{1, 2\}$. For $\{\mathbf{z}_0, \mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3\}$ shown in (32), we by *Theorem 2* assert that

$$\left\{\xi^{\mathbf{z}_0}, \xi^{\mathbf{z}_1}\right\} \cup \left\{\xi^{-\mathbf{z}_2}, \xi^{-\mathbf{z}_3}\right\}$$

form a $(K = 4, L = 64, Z = 8)$-ZCZ sequence set, where $\xi = \sqrt{-1}$. Interestingly, the ZCZ width is equal to the power of vertex number in the upper layer of the graph in Fig. 1.

$$\begin{aligned}
\mathbf{z}_0 =&[00301022201030020012100002101202\\
&\quad 22123200201030022230322202101202],\\
\mathbf{z}_1 =&[023212202221232000210120200121000\\
&\quad 20103002221232002032302000121000],\\
\mathbf{z}_2 =&[222303222021012022201030002212320\\
&\quad 00012100202101200023212202212320],\\
\mathbf{z}_3 =&[02032302000121000221232022010300\\
&\quad 20210120000121002003010222010300].
\end{aligned} \tag{32}$$

IV. Conclusions

In this paper, we have settled the Rathinakumar-Chaturvedi open problem positively by presenting a new construction of ZCZ sequences from generalized Reed-Muller codes. As shown in *Example 2*, every proposed ZCZ sequence set is associated with a two-layer graph (see Fig. 1), where the ZCZ width is equal to the power of vertex number (i.e., 2^n) in the upper layer graph. Our proposed construction also extends and generalizes the ZCZ construction in [3], thus yielding many new ZCZ sequences which have not been discovered before, as shown in *Remark 1*.

V. Acknowledgement

The work of Zilong Liu and Yong Liang Guan is supported by the Advanced Communications Research Program DSOCL06271, a research grant from the Defense Research and Technology Office (DRTech), Ministry of Defence, Singapore. The work of U. Parampalli is supported in part by the University of Melbournes Communications Sensing and Coding (CSC) Research Network, supported by IRRTF and the Innovative Disciplines Intelligence Base 111 Project No.111-2-14, of MoE, China.

References

[1] P. Fan, N. Suehiro, N. Kuroyanagi, and X. Deng, "A class of binary sequences with zero correlation zone," *IEE Electron. lett.*, vol. 35, pp. 777-779, May 1999.

[2] N. Suehiro, "A signal design without co-channel interference for approximately synchronized CDMA system," *IEEE J. Sel. Areas Commun.*, vol. SAC-12, pp. 837-841, June 1994.

[3] X. Deng and P. Fan, "Spreading sequence sets with zero correlation zone," *IEE Electron. lett.*, vol. 36, pp. 993-994, 2000.

[4] H. Torii, M. Nakamura, and N. Suehiro, "A new class of zero-correlation zone sequences," *IEEE Trans. Inf. Theory*, vol. 50, pp. 559-565, Mar. 2004.

[5] A. Rathinakumar and A. K. Chaturvedi, "A new framework for constructing mutually orthogonal complementary sets and ZCZ sequences," *IEEE Trans. Inf. Theory*, vol. 52, pp. 3817-3826, Aug. 2006.

[6] X. Tang, P. Fan, and J. Lindner, "Multiple binary ZCZ sequence sets with good cross-correlation property based on complementary sequence sets," *IEEE Trans. Inf. Theory*, vol. 56, pp. 4038-4045, Aug. 2010.

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

[8] C. Tseng and C. Liu, "Complementary sets of sequences," *IEEE Trans. Inf. Theory,* vol. IT-18, no. 5, pp. 644-665, Sept. 1972.

[9] 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.

[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. 1105-113, Mar. 2014.

[11] Z. Liu, Y. L. Guan, B. C. Ng, and H. H. Chen, "Correlation and set size bounds of complementary sequences with low correlation zones," *IEEE Trans. Commun.*, vol. 59, no. 12, pp. 3285-3289, Dec. 2011.

[12] Z. Liu, Y. L. Guan, and W. H. Mow, "Improved lower bound for quasi-complementary sequence sets," in *Proc. 2011 IEEE Int. Symposium on Information Theory (ISIT'2011)*, St. Petersburg, Russia, Aug. 2011, pp. 489-493.

[13] 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.

[14] Z. Liu, U. Parampalli, Y. L. Guan and S. Boztaş, "Constructions of optimal and near-optimal quasi-complementary sequence sets from Singer difference sets," *IEEE Wireless Commun. Letters*, vol. 2, no. 5, pp. 487-490, Oct. 2013.

[15] Z. Liu, U. Parampalli and Y. L. Guan, "On even-period binary Z-complementary pairs with large ZCZs", *IEEE Signal Process. Lett.*, vol. 21, no. 3, pp. 284-287, Mar. 2014.

[16] Z. Liu, U. Parampalli and Y. L. Guan, "Optimal odd-length Z-complementary pairs", *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5768-5781, Sept. 2014.

[17] 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.

[18] G. Gong, F. Huo and Y. Yang, "Large zero autocorrelation zones of Golay sequences and their applications," *IEEE Trans. Commun.*, vol. 61, no. 9, pp. 3967-3979, Sept. 2013.

[19] 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.