two cases we get infinite classes of DPM. The most important result is the construction of DPM from ternary vectors of lengths at least 13 to permutations of the same length. Using the DPMs (or the DIMs) and known ternary codes, we get new larger permutation arrays in many cases; a couple of examples are gives as illustrations.

REFERENCES

[1] A. E. Brouwer, H. O. Hämäläinen, P. R. J. Östergård, and N. J. A. Sloane, "Bounds on mixed binary/ternary codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 140–161, Jan. 1998.

[2] J.-C. Chang, "Distance-increasing mappings from binary vectors to permutations," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 359–363, Jan. 2005.

[3] J.-C. Chang, "New algorithms of distance-increasing mappings from binary vectors to permutations by swaps," *Designs, Codes Cryptogr.*, vol. 39, pp. 335–345, Jan. 2006.

[4] J.-C. Chang, "Distance-increasing mappings from binary vectors to permutations that increase Hamming distances by at least two," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1683–1689, Apr. 2006.

[5] J.-C. Chang, R.-J. Chen, T. Kløve, and S.-C. Tsai, "Distance-preserving mappings from binary vectors to permutations," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 1054–1059, Apr. 2003.

[6] H. C. Ferreira and A. J. H. Vinck, "Inference cancellation with permutation trellis arrays," in *Proc. IEEE Veh. Technol. Conf.*, 2000, pp. 2401–2407.

[7] H. C. Ferreira, A. J. H. Vinck, T. G. Swart, and I. de Beer, "Permutation trellis codes," *IEEE Trans. Commun.*, vol. 53, no. 11, pp. 1782–1789, Nov. 2005.

[8] H. C. Ferreira, D. Wright, and A. L. Nel, "Hamming distance-preserving mappings and trellis codes with constrained binary symbols," *IEEE Trans. Inf. Theory*, vol. 35, no. 5, pp. 1098–1103, Sep. 1989.

[9] Y.-Y. Huang, S.-C. Tsai, and H.-L. Wu, "On the construction of permutation arrays via mappings from binary vectors to permutations," *Designs, Codes Cryptogr.*, vol. 40, pp. 139–155, 2006.

[10] K. Lee, "New distance-preserving maps of odd length," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2539–2543, Oct. 2004.

[11] K. Lee, "Cyclic constructions of distance-preserving maps," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4292–4396, Dec. 2005.

[12] K. Lee, "Distance-increasing maps of all length by simple mapping algorithms," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3344–3348, Jul. 2006.

[13] J.-S. Lin, J.-C. Chang, and R.-J. Chen, "New simple constructions of distance-increasing mappings from binary vectors to permutations," *Inf. Process. Lett.*, vol. 100, no. 2, pp. 83–89, Oct. 2006.

[14] J.-S. Lin, J.-C. Chang, R.-J. Chen, and T. Kløve, Distance-Preserving Mappings from Ternary Vectors to Permutations arXiv, 0704.1358v1 [cs.DM].

[15] T.-T. Lin, S.-C. Tsai, and H.-L. Wu, "Distance-preserving mappings from ternary vectors to permutations," *Manuscript*, 2007.

[16] V. S. Pless and W. C. Huffman, Eds., *Handbook of Coding Theory*. Amsterdam, The Netherlands: Elsevier, 1998.

[17] T. G. Swart and H. C. Ferreira, "A generalized upper bound and a multilevel construction for distance-preserving mappings," *IEEE Trans. Inf. Theory*, vol. 52, no. 8, pp. 3685–3695, Aug. 2006.

Complete Mutually Orthogonal Golay Complementary Sets From Reed–Muller Codes

Appuswamy Rathinakumar, *Student Member, IEEE*, and Ajit Kumar Chaturvedi, *Senior Member, IEEE*

***Abstract*—Recently Golay complementary sets were shown to exist in the subsets of second-order cosets of a q-ary generalization of the first-order Reed–Muller (RM) code. We show that mutually orthogonal Golay complementary sets can also be directly constructed from second-order cosets of a q-ary generalization of the first-order *RM* code. This identification can be used to construct zero correlation zone (ZCZ) sequences directly and it also enables the construction of ZCZ sequences with special subsets.**

***Index Terms*—Complementary sets, generalized Boolean function, mutually orthogonal Golay complementary sets, Reed–Muller (RM) codes, zero correlation zone (ZCZ) sequences.**

I. INTRODUCTION

Zero correlation zone (ZCZ) sequences are a generalization of orthogonal sequences. Their superior correlation properties can be utilized to improve the spectral efficiency of an approximately synchronized[1] CDMA system over a similar system that uses conventional orthogonal sequences [3]. Further, CDMA systems employing ZCZ sequences have been shown to be performing as well as OFDM systems in fast time-varying multipath channels at a considerably lower computational complexity [14]. Recently, ZCZ sequences have found applications in ternary direct sequence Ultra Wideband (TS-UWB) systems [13]. It has been shown that the TS-UWB (also known as multicode UWB) systems employing appropriate ZCZ sequences can support different data rate requirements at a constant bit error rate performance level [13]. They are also applicable in broadband satellite IP networks, where sequence sets with small autocorrelation and cross correlation within a detection aperture are needed [15], [16].

Mutually orthogonal Golay Complementary Sets (MOGCS) are an integral part in the construction of ZCZ sequences. Traditionally, ZCZ sequences have been constructed by iterative methods starting from a pair of MOGCS. In [3], several constructions of ZCZ sequences starting from any set of MOGCS were given. Many recursive constructions of MOGCS are known [9],[2] [3], [6], [7], [5], [3]. In [1] and [2], a long standing problem of directly constructing Golay Complementary Sets (GCS) [6] was solved by constructing GCS from Reed–Muller (RM) codes. Specifically, GCS were shown to be subsets in second-order cosets of a q-ary generalization $\mathrm{RM}_q(1, m)$ of the first-order RM code. Size of the set was shown to be directly related to a graph associated with the coset leader.

Manuscript received July 28, 2004; revised November 29, 2007.

A. Rathinakumar was with the Department of Electrical Engineering, Indian Institute of Technology, Kanpur, UP 208016, India. He is now with the Department of Electrical and Computer Engineering, University of California, San Diego, La Jolla, CA 92093 USA (e-mail: rathnam@ucsd.edu).

A. K. Chaturvedi is with the Department of Electrical Engineering, Indian Institute of Technology, Kanpur, UP 208016, India (e-mail: akc@iitk.ac.in).

Communicated by K. G. Paterson, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2007.915980

[1]A DS CDMA system is said to be approximately synchronized if the modulated sequences are synchronized up to a small fraction of the sequence length.

[2]The concept of zero correlation sequences first appears in [9] as semiperfect sequences.

We consider the problem of direct construction of complete mutually orthogonal GCS (MOGCS)[3] from RM codes and show that they can also be constructed from second-order cosets of the same q-ary generalization of the first-order RM code. Our approach is to establish a framework in which MOGCS can be identified to be in the second-order cosets of the q-ary generalization of RM codes given in [2]. The importance of such an identification is that it enables one to relate different sets of ZCZ sequences by the corresponding MOGCS used in their construction. Our work is motivated in part by the observation that given the number of sequences in a ZCZ set and its interference free window (IFW) length, the sequence set can be constructed as a union of a large number of ZCZ sets containing fewer sequences of the given length. In turn, the correlation properties of the smaller sets can be designed better than that of the larger set which helps improve the spectral efficiency further [3]. Indeed, such a construction of orthogonal sets combining two ZCZ sets each having unity IFW length was shown in [4], [3]. Directly constructing MOGCS from RM codes and characterizing the MOGCS that form ZCZ sequences with given parameters is a promising direction toward construction of such ZCZ sequences.

Beginning with the GCS identified in [2], we identify a set of permutations of the GCS which generate mutually orthogonal Golay complementary sets. It is shown that there are 2^k such permutations on a complementary set containing 2^{k+1} sequences. We then construct another complementary set with the same associated graph as the original set. The same set of permutations identified earlier are applied on this set to generate further 2^k mutually orthogonal Golay complementary sets. We then conclude our main result by establishing that these two sets are mutually orthogonal. We emphasize that not every permutation of a given GCS will produce an orthogonal complementary set and identifying the permutations that do so is an important contribution of this work.

The rest of the correspondence is organized as follows: Section II provides the necessary background and establishes basic notations. Section III collects all our main results. After identifying a number of permutations of a complementary set to generate MOGCS, generating complete MOGCS is discussed. Some of the applications of the direct construction are pointed out in Section IV. We conclude the correspondence in Section V.

II. Background and Notation

A. Correlation Parameters

The aperiodic cross-correlation $\mathbf{C}(\mathbf{a},\mathbf{b})(\tau)$ between two length L complex-valued sequences $\mathbf{a}$ and $\mathbf{b}$ is defined as

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

and

$$\mathbf{A}(\mathbf{a})(\tau)=\mathbf{C}(\mathbf{a},\mathbf{a})(\tau)$$

denotes the *aperiodic autocorrelation* of the sequence $\mathbf{a}$.

We also define the correlation functions for $\mathbb{Z}_q$-valued vectors. This is done by defining $\omega = e^{2\pi i/q}$ and associating with each vector $\mathbf{a}=[a_0a_1\cdots a_{n-1}]$, where $a_i\in\mathbb{Z}_q$, a complex-valued vector $\mathbf{a}'=[a'_0a'_1\cdots a'_{n-1}]$, in which $a'_i=\omega^{a_i}$. If $\mathbf{a}$ and $\mathbf{b}$ are $\mathbb{Z}_q$-valued vectors, then we define the function $\mathbf{C}(\mathbf{a},\mathbf{b})(\cdot)$ to be the cross-correlation function of the associated complex-valued vectors $\mathbf{a}'$ and $\mathbf{b}'$.

[3]A collection of MOGCS is said to be *complete* if the collection contains the maximum number of complementary sets, which is known to be equal to the size of the complementary sets [5].

The periodic crosscorrelation between the sequences $\mathbf{a}$ and $\mathbf{b}$ is defined as

$$\phi_{\mathbf{ab}}(\tau)=\mathbf{C}(\mathbf{a},\mathbf{b})(\tau)+\mathbf{C}(\mathbf{b},\mathbf{a})^*(L-\tau).$$

Definition 2.1: A set of M, length L vectors $\{\mathbf{a}^i\}_{i=1}^M$ is said to be a Golay complementary set (GCS) if

$$\sum_{i=1}^{M}\mathbf{A}(\mathbf{a}^i,\mathbf{a}^i)(\tau)=0 \qquad \forall\,\tau\ne 0. \tag{2}$$

Notice that a Golay complementary set is an ordered set of sequences.

Definition 2.2: Two Golay complementary sets $\{\mathbf{a}_m^i\}_{i=1}^M$ and $\{\mathbf{a}_n^i\}_{i=1}^M$ are said to be *mutually orthogonal* if

$$\sum_{i=1}^{M}\mathbf{C}(\mathbf{a}_m^i,\mathbf{a}_n^i)(\tau)=0 \qquad \forall\,\tau.$$

Definition 2.3: The number of Golay complementary sets that are pairwise mutually orthogonal is at most equal to the number of sequences in a Golay complementary set. Such a collection of maximum possible number of orthogonal Golay complementary sets is said to be *complete*.

Definition 2.4: Let $\{\mathbf{b}_n\}_{n=1}^M$ be a set of M sequences, each of length L. The zero periodic autocorrelation zone T_{ACZ} and the zero periodic crosscorrelation zone T_{CCZ} of this sequence set are defined to be [12]

$$\begin{aligned}T_{\mathrm{ACZ}}&=\max\{T\mid \phi_{\mathbf{b}_n\mathbf{b}_n}(\tau)=0,\forall n,\mid\tau\mid\le T,\tau\ne 0\}\\ T_{\mathrm{CCZ}}&=\max\{T\mid \phi_{\mathbf{b}_m\mathbf{b}_n}(\tau)=0,\forall m\ne n,\mid\tau\mid\le T\}\end{aligned}$$

where, $\phi_{\mathbf{b}_m\mathbf{b}_n}(\tau)$ denotes the periodic crosscorrelation between the sequences $\mathbf{b}_m$ and $\mathbf{b}_n$.

Definition 2.5: The Interference Free Window (IFW) of the sequence set $\{\mathbf{b}_n\}_{n=1}^M$, denoted by T, is defined to be the minimum of the zero autocorrelation zone and the zero crosscorrelation zone values, i.e.

$$T=\min\{T_{\mathrm{ACZ}},T_{\mathrm{CCZ}}\}.$$

The set $\{\mathbf{b}_n\}_{n=1}^M$ with IFW of T is said to constitute a Zero Correlation Zone (ZCZ) sequence set of M sequences of length L and is denoted by ZCZ-(L,M,T).

Two distinct sets of sequences $\{\mathbf{b}_m^1\}_{m=1}^M$ and $\{\mathbf{b}_n^2\}_{n=1}^M$ are said to be mutually orthogonal, if

$$\phi_{\mathbf{b}_m^1\mathbf{b}_n^2}(0)=0 \quad \forall\ m \text{ and } n.$$

B. Constructing ZCZ Sequences From MOGCS

Here we briefly outline constructing ZCZ sequences from MOGCS for motivating the study of MOGCS although we do not need these constructions in this paper. Let $\mathcal{A}$ be a $M\times MN$ matrix whose rows form a collection of MOGCS. Each complementary set has M sequences of length N and the ith row of $\mathcal{A}$ constitutes the ith complementary set, such a matrix said to be a MOGCS matrix. Let it be partitioned as $\mathcal{A}=\begin{bmatrix}\mathcal{A}_1 & \mathcal{A}_2 & \cdots\mathcal{A}_M\end{bmatrix}$, where each $\mathcal{A}_i$ is an $M\times N$ matrix. We will denote the ith row of $\mathcal{A}$ by $\mathbf{a}_i$, the ith row of $\mathcal{A}_j$ by $\mathbf{a}_i^j$ and the (i,j)th scalar entry of $\mathcal{A}$ by $a_{i,j}$. Let $\mathcal{H}$ be a $P \times KQ$ matrix with complex valued entries having the same magnitude. For convenience, we will assume that this magnitude is 1. We define the matrix operation "$\varnothing_K$" as

$$\mathcal{A}\varnothing_K\mathcal{H} = \begin{bmatrix} \mathcal{C}(h_{11},\ldots,h_{1K}) & \cdots & \mathcal{C}(h_{1(QK-K+1)},\ldots,h_{1(QK)}) \\ \mathcal{C}(h_{21},\ldots,h_{2K}) & \cdots & \mathcal{C}(h_{2(QK-K+1)},\ldots,h_{2(QK)}) \\ \cdots & \ddots & \cdots \\ \mathcal{C}(h_{P1},\ldots,h_{PK}) & \cdots & \mathcal{C}(h_{P(QK-K+1)},\ldots,h_{P(QK)}) \end{bmatrix} \quad (3)$$

(viewed as a $PM \times KQMN$ scalar matrix) where

$$\mathcal{C}(h_{ij},h_{i(j+1)},\ldots,h_{i(j+K)}) = \Big[(h_{ij}\mathcal{A}_1,h_{i(j+1)}\mathcal{A}_1,\ldots,h_{i(j+K)}\mathcal{A}_1)\cdots (h_{ij}\mathcal{A}_M,h_{i(j+1)}\mathcal{A}_M,\ldots,h_{i(j+K)}\mathcal{A}_M)\Big]_{M\times KMN}$$

with $(h_{ij}\mathcal{A}_1,h_{i(j+1)}\mathcal{A}_1,\ldots,h_{i(j+K)}\mathcal{A}_1)$ denoting a sequence of length KN.

Let each element of a column vector be cyclically moved one row up, upon pre-multiplication by S, a shift operator. We will denote the conjugate transpose of the matrix $\mathcal{H}$ by $\mathcal{H}^*$. Consider the binary vectors $d_{11} = (1,0,1,0,\ldots,1,0)$ and $d_{21} = (1,1,0,1,1,0,\ldots,1,1,0)$. In general, d_{ij} is constructed by a repeated pattern of i ones and j zeros. Define matrices $\mathbf{D}_{ij} = \mathrm{diag}(d_{ij})$ and $\overline{\mathbf{D}}_{ij} = \mathrm{diag}(\overline{d}_{ij})$, where $\overline{d}_{ij}$ is the binary complement of d_{ij}.

Then, the following lemma is an example construction of ZCZ sequences from MOGCS sets [3].

Lemma 2.6: If $\mathcal{A}$ is a MOGCS matrix, then the rows of the matrix $\mathcal{B} = \mathcal{A}\varnothing_2\mathcal{H}$ form a ZCZ-$(2MNQ, MP, N)$ if $\mathcal{H}$ satisfies the following:

1) $\mathcal{H}\mathcal{H}^* = (MN)\mathbf{I}$ where $\mathbf{I}$ is the identity matrix;
2) $\mathcal{H}\mathbf{D}_{11}\mathbf{S}\mathcal{H}^* = 0 = \mathcal{H}\mathbf{D}_{11}\mathbf{S}^*\mathcal{H}^*$.

Similar constructions have been established in [3] for $K \geq 2$. Notations in the following two subsections are adopted from [2]. We restate them here for completeness.

C. Generalized Reed–Muller Codes

For $q \geq 2$, we define a length L linear code over $\mathbb{Z}_q$ to be a set of $\mathbb{Z}_q$-valued vectors (called codewords) of length L that is closed under the operation of addition over the commutative group $\mathbb{Z}_q$. A set of codewords constitute a code $\mathcal{C}$. By a *coset* of $\mathcal{C}$, we mean a set of the form $\mathbf{a} + \mathcal{C}$ where $\mathbf{a}$ is some fixed vector over $\mathbb{Z}_q$. The vector $\mathbf{a}$ is called a *coset representative* for the coset $\mathbf{a} + \mathcal{C}$.

Definition 2.7: A map $f : \{0,1\}^m \to \mathbb{Z}_q$ of $\{0,1\}$-valued variables $x_0, x_1, \ldots, x_{m-1}$ is called a generalized Boolean function.

Every such function can be written in algebraic normal form as a sum of monomials of the form $x_{j_0}x_{j_1}\cdots x_{j_{r-1}}$ (in which $j_0, j_1, \ldots, j_{r-1}$ are distinct). With each generalized Boolean function f we identify a length 2^m, $\mathbb{Z}_q$-valued vector $\mathbf{f} = [f_0 f_1 \cdots f_{2^m-1}]$ in which

$$f_i = f(x_0, x_1, \ldots, x_{m-1})$$

where $[x_0 x_1 \cdots x_{m-1}]$ is the binary expansion of the integer i. A complex-valued vector $\mathbf{f}'$ is associated with every $\mathbf{f}$, where $f_i' = \omega^{f_i}$ and ω is a complex qth root of unity. When it is clear from the context, we will just use f to refer to all three.

Definition 2.8: For $q \geq 2$ and $0 \leq r \leq m$, $\mathrm{RM}_q(r,m)$ is defined to be the linear code over $\mathbb{Z}_q$ that is generated by the $\mathbb{Z}_q$-valued vectors corresponding to the monomials of degree at most r in $x_0, x_1, \ldots, x_{m-1}$.

The rows of a generator matrix for the rth order generalized Reed–Muller code $\mathrm{RM}_q(r,m)$ over $\mathbb{Z}_q$ can be represented by the collection of all monomials of degree at most r in $x_0, x_1, \ldots, x_{m-1}$.

Let $f : \{0,1\}^m \to \mathbb{Z}_q$ be a generalized Boolean function in variables $x_0, x_1, \ldots, x_{m-1}$. Let $0 \leq j_0 < j_1 < \cdots < j_{k-1} < m$ be a list of k indices and write $\mathbf{x} = [x_{j_0}x_{j_1}\cdots x_{j_{k-1}}]$. Let $\mathbf{c} = [c_0 c_1 \cdots c_{k-1}]$ be a binary word of length k. Then we define the vector $f|_{\mathbf{x}=\mathbf{c}}$ to be the complex-valued vector with component $i = \sum_{j=0}^{m-1} i_j 2^j$ equal to $\omega^{f(i_0,i_1,\ldots,i_{m-1})}$ if $i_{j_\alpha} = c_\alpha$ for each $0 \leq \alpha < k$, and equal to 0, otherwise. Here ω is a complex qth root of unity. In the case where $\mathbf{x}$ and $\mathbf{c}$ are of length zero, we define $f|_{\mathbf{x}=\mathbf{c}}$ to be the complex-valued vector associated with f.

The following simple consequences can be easily obtained from the definitions. For any $\mathbf{x}$ defined as above

$$\mathbf{f}' = \sum_{\mathbf{c}} f|_{\mathbf{x}=\mathbf{c}}$$

and the Boolean function associated with the complex vector $f|_{\mathbf{x}=\mathbf{c}}$ can be written as

$$f \cdot \prod_{\alpha:c_\alpha=1} x_{j_\alpha} \prod_{\alpha:c_\alpha=0} (1 - x_{j_\alpha}).$$

For completeness, we repeat the following lemma from [2].

Lemma 2.9: Let $f, g : \{0,1\}^m \to \mathbb{Z}_q$ be generalized Boolean functions in variables $x_0, x_1, \ldots, x_{m-1}$. Let $0 \leq j_0 < j_1 < \cdots < j_{k-1} < m$ be a list of k indices and let $\mathbf{c} = [c_0 c_1 \cdots c_{k-1}]$ and $\mathbf{d} = [d_0 d_1 \cdots d_{k-1}]$ be binary-valued vectors. Write $\mathbf{x} = [x_{j_0}x_{j_1}\cdots x_{j_{k-1}}]$ and suppose $0 \leq i_1 < i_2 < \cdots < i_{l-1} < m$ is a set of indices not in $\{j_0, j_1, \ldots, j_{k-1}\}$. Denote $\mathbf{y} = [x_{i_0}x_{i_1}\cdots x_{i_{l-1}}]$, then

$$\mathbf{C}(f|_{\mathbf{x}=\mathbf{c}}, g|_{\mathbf{x}=\mathbf{d}})(\tau) = \sum_{\mathbf{c}_1,\mathbf{c}_2} \mathbf{C}(f|_{\mathbf{xy}=\mathbf{cc}_1}, g|_{\mathbf{xy}=\mathbf{dc}_2})(\tau). \quad (4)$$

D. Quadratic Forms and Graphs

Let $Q : \{0,1\}^m \to \mathbb{Z}_q$ be the generalized Boolean function defined by

$$Q(x_0, x_1, \ldots, x_{m-1}) = \sum_{0 \leq i < j < m} q_{ij} x_i x_j$$

where $q_{ij} \in \mathbb{Z}_q$, so that Q is a quadratic form in m variables over $\mathbb{Z}_q$. We associate a labeled *graph* $G(Q)$ on m vertices with Q as follows. We label the vertices by $0, 1, \ldots, m-1$ and join vertices i and j by an edge labeled q_{ij} if $q_{ij} \neq 0$. If $f : \{0,1\}^m \to \mathbb{Z}_q$ is a quadratic function (i.e., a generalized Boolean function corresponding to a codeword of $\mathrm{RM}_q(2,m)$), then we define $G(f)$ to be the graph $G(Q)$ where Q is the quadratic part of f. We say that a graph G of the type defined above is a *path* if either

- $m = 1$ (in which case the graph contains a single vertex and no edges), or;
- $m \geq 2$ and G has exactly $m - 1$ edges, all labeled $q/2$ which form a Hamiltonian path in G.

For $m \geq 2$, a path on m vertices corresponds to a quadratic form of the type

$$\frac{q}{2} \cdot \sum_{\alpha=1}^{m-1} x_{\pi(\alpha-1)} x_{\pi(\alpha)} \tag{5}$$

where π is a permutation of $\{0, 1, \ldots, m-1\}$.

Let $Q : \{0,1\}^m \rightarrow \mathbb{Z}_q$ be a quadratic form in m variables $x_0, x_1, \ldots, x_{m-1}$. A quadratic generalized boolean function is of the form [2]:

$$f = Q + \sum_{l=0}^{m-1} g_l x_l + g'$$

where $g', g_l \in \mathbb{Z}_q$ are arbitrary. Consider the function $f|_{x_j = c}$, obtained by substituting $x_j = c$ in f. It follows that the graph of the function $f|_{x_j=c}$ is equal to the graph obtained by deleting vertex j of $G(f)$. By extension, if we have a list of k indices $0 < j_0 < \cdots < j_{k-1} < m$ and write $\mathbf{x} = [x_{j_0} x_{j_1} \cdots x_{j_{k-1}}]$ and $\mathbf{c} = [c_0 c_1 \cdots c_{k-1}]$ then the graph of the function $f|_{\mathbf{x}=\mathbf{c}}$ is obtained by deleting vertices $j_0, j_1, \ldots, j_{k-1}$ of $G(f)$. The final graph is independent of the choice of $\mathbf{c}$. So for any $\mathbf{c}$, the quadratic part of the function $f|_{\mathbf{x}=\mathbf{c}}$ is completely described by the graph obtained from $G(f)$ by deleting some vertices.

III. Mutually Orthogonal Golay Complementary Sets

The following section collects known results on the direct construction of GCS from *RM* codes. We then present one of our main results identifying permutations of a complementary set that generate MOGCS. We conclude this section by constructing complete MOGCS by a form of generalization of the reverse and conjugate method of generating MOGCS introduced in [6] and [5].

A. GCS From Reed–Muller Codes

We repeat [2, Th. 9] to be used later in the proof of our main theorem.

Lemma 3.1: If the function $f|_{\mathbf{x}=\mathbf{c}}$ is a quadratic function and if $G(f|_{\mathbf{x}=\mathbf{c}})$ is a path, then the complex vector $f|_{\mathbf{x}=\mathbf{c}}$ and any vector of the form $(f + (q/2)x_\beta + r)\,|_{\mathbf{x}=\mathbf{c}}$ form a Golay complementary pair.[4] Where $r \in \mathbb{Z}_q$ is arbitrary and β is either the single vertex of $G(f|_{\mathbf{x}=\mathbf{c}})$ when $k = m-1$, or an end vertex of the path in $G(f|_{\mathbf{x}=\mathbf{c}})$ when $0 \leq k < m-1$.

The following result [2, Th. 12] establishes that the codewords of arbitrary second-order cosets of $\mathrm{RM}_q(1,m)$ lie in Golay complementary sets.

Lemma 3.2: Suppose $Q : \{0,1\}^m \rightarrow \mathbb{Z}_q$ is a quadratic form in variables $x_0, x_1, \ldots, x_{m-1}$. Suppose further that $G(Q)$ contains a set of k distinct vertices labeled $j_0, j_1, \ldots, j_{k-1}$ with the property that deleting those k vertices and all their edges results in a path. Let β be the label of either end vertex in this path (or the single vertex of the graph when $k = m-1$). Then for any choice of $g', g_i \in \mathbb{Z}_q$

$$\left\{ Q + \sum_{i=0}^{m-1} g_i x_i + g' + \frac{q}{2}\left(\sum_{\alpha=0}^{k-1} d_\alpha x_{j_\alpha} + d x_\beta\right) : d, d_\alpha \in \{0,1\} \right\} \tag{6}$$

is a Golay complementary set of size 2^{k+1}.

[4]A complementary pair is a complementary set with just two sequences.

B. MOGCS From Reed–Muller Codes

In this section, we prove the main theorem for constructing mutually orthogonal Golay complementary sets. Suppose $Q : \{0,1\}^m \rightarrow \mathbb{Z}_q$ is a quadratic form in variables $x_0, x_1, \ldots, x_{m-1}$. For $0 \leq t < 2^k$, define the ordered set S_t (with the natural order induced by the binary vector $[d d_0 d_1 \cdots d_{k-1}]$) to be

$$\left\{ Q + \sum_{i=0}^{m-1} g_i x_i + g' + \frac{q}{2}\left(\sum_{\alpha=0}^{k-1} d_\alpha x_{j_\alpha} + \sum_{\alpha=0}^{k-1} b_\alpha x_{j_\alpha} + d x_\beta\right) : d, d_\alpha \in \{0,1\} \right\} \tag{7}$$

where $t = \sum_{\alpha=0}^{k-1} b_\alpha 2^\alpha$. The following theorem identifies 2^k mutually orthogonal Golay complementary sets with 2^{k+1} sequences each. We denote the all-one vector of appropriate dimension by $\mathbf{1}$ and the modulo 2 addition is denoted by $\oplus$.

Theorem 3.3: Suppose that $G(Q)$ contains a set of k distinct vertices labeled $j_0, j_1, \ldots, j_{k-1}$ with the property that deleting those k vertices and all their edges results in a path. Let β be the label of either end vertex in this path (or the single vertex of the graph when $k = m-1$). Then for any choice of $g', g_i \in \mathbb{Z}_q$, the set S_t is a Golay complementary set for each $0 \leq t < 2^k$. Further, for $t' \neq t$, $S_{t'}$ and S_t are mutually orthogonal complementary sets.

Proof: For any t, the sequences in the set S_t are obtained by permuting the set of sequences in (6). It follows directly from Lemma 3.2 that S_t is a Golay complementary set for every $0 \leq t < 2^k$. It remains to show that any two distinct such sets are mutually orthogonal. Let $\mathbf{x} = [x_{j_0} x_{j_1} \cdots x_{j_{k-1}}]$, $\mathbf{d} = [d_0 d_1 \cdots d_{k-1}]$ and $\mathbf{b} = [b_0 b_1 \cdots b_{k-1}]$. Let $t = \sum_{\alpha=0}^{k-1} b_\alpha 2^\alpha$, $t' = \sum_{\alpha=0}^{k-1} b'_\alpha 2^\alpha$ and $t \neq t'$. To prove that S_t and $S_{t'}$ are mutually orthogonal, by Lemma 2.9 we write

$$\sum_{\mathbf{d},d} \mathbf{C}\Big(f + \frac{q}{2}\Big((\mathbf{d}+\mathbf{b})\cdot\mathbf{x} + d x_\beta\Big), f + \frac{q}{2}\Big((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x} + d x_\beta\Big)\Big)(l) = L_1 + L_2$$

where

$$L_1 = \sum_{\mathbf{d},d} \sum_{\mathbf{c}_1 \neq \mathbf{c}_2} \mathbf{C}\left(\left(f + \frac{q}{2}\Big((\mathbf{d}+\mathbf{b})\cdot\mathbf{x} + d x_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_1} \left(f + \frac{q}{2}\Big((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x} + d x_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_2}\right)(l) \tag{8}$$

and

$$L_2 = \sum_{\mathbf{d},d} \sum_{\mathbf{c}} \mathbf{C}\left(\left(f + \frac{q}{2}\Big((\mathbf{d}+\mathbf{b})\cdot\mathbf{x} + d x_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}} \left(f + \frac{q}{2}\Big((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x} + d x_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}}\right)(l). \tag{9}$$

Consider the following sum in L_1 for a fixed $d, \mathbf{c}_1$ and $\mathbf{c}_2$

$$\begin{aligned}
&\sum_{\mathbf{d}} \mathbf{C}\left(\left(f+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b})\cdot\mathbf{x}+dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_1}\right.\\
&\qquad\left.\left(f+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x}+dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_2}\right)(l)\\
&=\sum_{\mathbf{d}} \mathbf{C}\left(\left(f+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b})\cdot\mathbf{c}_1+dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_1}\right.\\
&\qquad\left.\left(f+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b}')\cdot\mathbf{c}_2+dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_2}\right)(l) \qquad (10)\\
&=\sum_{\mathbf{d}} (-1)^{\mathbf{d}\cdot(\mathbf{c}_1\oplus\mathbf{c}_2)}\, \mathbf{C}\left(\left(f+\frac{q}{2}\Big(\mathbf{b}\cdot\mathbf{c}_1+dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_1}\right.\\
&\qquad\left.\left(f+\frac{q}{2}\Big(\mathbf{b}'\cdot\mathbf{c}_2+dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_2}\right)(l) \qquad (11)\\
&=\mathbf{C}\left(\left(f+\frac{q}{2}\Big(\mathbf{b}\cdot\mathbf{c}_1+dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_1}\right.\\
&\qquad\left.\left(f+\frac{q}{2}\Big(\mathbf{b}'\cdot\mathbf{c}_2+dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_2}\right)(l)\cdot\sum_{\mathbf{d}}(-1)^{\mathbf{d}\cdot(\mathbf{c}_1\oplus\mathbf{c}_2)}. \qquad (12)
\end{aligned}$$

Since $\mathbf{c}_1 \neq \mathbf{c}_2$ in the term L_1, the function $\mathbf{d}\cdot(\mathbf{c}_1\oplus\mathbf{c}_2)$ takes the values 0 and 1 equally often, thus (12) vanishes for all l.

Now consider the following sum in L_2 for a given $\mathbf{c}$ and $\mathbf{d}$:

$$\begin{aligned}
&\sum_{d} \mathbf{C}\left(\left(f+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b})\cdot\mathbf{x}+dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}}\right.\\
&\qquad\left.\left(f+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b}')\cdot\mathbf{x}+dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}}\right)(l)=\\
&\qquad\sum_{d} \mathbf{C}\left(\left(f+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b})\cdot\mathbf{c}+dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}}\right.\\
&\qquad\left.\left(f+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b}')\cdot\mathbf{c}+dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}}\right)(l). \qquad (13)
\end{aligned}$$

The above sum can be rewritten as

$$\begin{aligned}
&\sum_{d} \mathbf{C}\left(\left(f+\frac{q}{2}\Big((\mathbf{b}+\mathbf{b}')\cdot\mathbf{c}+dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}}\right.\\
&\qquad\left.\left(f+\frac{q}{2}\Big(dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}}\right)(l)=\\
&\qquad(-1)^{(\mathbf{b}\oplus\mathbf{b}')\cdot\mathbf{c}}\cdot\sum_{d} \mathbf{C}\left(\left(f+\frac{q}{2}\Big(dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}}\right.\\
&\qquad\left.\left(f+\frac{q}{2}\Big(dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}}\right)(l). \qquad (14)
\end{aligned}$$

Note that

$$\begin{aligned}
&\sum_{d} \mathbf{C}\left(\left(f+\frac{q}{2}\Big(dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}},\left(f+\frac{q}{2}\Big(dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}}\right)(l)=\\
&\qquad\mathbf{A}\Big(f|_{\mathbf{x}=\mathbf{c}}\Big)(l)+\mathbf{A}\left(\left(f+\frac{q}{2}\Big(x_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}}\right)(l) \qquad (15)
\end{aligned}$$

which is zero for all $l \neq 0$ by Lemma 3.1. For $l = 0$

$$\mathbf{A}\Big(f|_{\mathbf{x}=\mathbf{c}}\Big)(0)=\mathbf{A}\left(\left(f+\frac{q}{2}\Big(x_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}}\right)(0)=2^{m-k} \qquad (16)$$

for all $\mathbf{c} \in \{0,1\}^k$. Substituting this back in (14), we obtain

$$\begin{aligned}
&\sum_{d} \mathbf{C}\left(\left(f+\frac{q}{2}\Big((\mathbf{b}+\mathbf{b}')\cdot\mathbf{c}+dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}}\right.\\
&\qquad\left.\left(f+\frac{q}{2}\Big(dx_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}}\right)(0)=(-1)^{(\mathbf{b}\oplus\mathbf{b}')\cdot\mathbf{c}}\cdot 2^{m-k+1} \qquad (17)
\end{aligned}$$

since we are considering the case $\mathbf{b} \neq \mathbf{b}'$, we have $\mathbf{b}\oplus\mathbf{b}' \neq (0)$, and so the linear functional $(\mathbf{b}\oplus\mathbf{b}')\cdot\mathbf{c}$ (regard as a function of $\mathbf{c}$) is not equal to the zero functional. Hence it is balanced, i.e., takes on the values 0 and 1 equally often as $\mathbf{c}$ varies. Hence the sum

$$\sum_{\mathbf{c}}(-1)^{(\mathbf{b}\oplus\mathbf{b}')\cdot\mathbf{c}}\cdot 2^{m-k+1}=0.$$

□

The codeword represented by the quadratic Q will be in the second-order RM code. In our construction, Q is the coset leader of the second-order coset used to construct MOGCS.

C. Complete Mutually Orthogonal Golay Complementary Sets

In this section, we discuss the construction of complete complementary sets from the RM codes. For any given generalized Boolean function f in m variables $x_0, x_1, \ldots, x_{m-1}$, we denote by $\tilde{f}$, the function $f(1-x_0, 1-x_1, \ldots, 1-x_{m-1})$. Let $\bar{\mathbf{x}}$ denote the vector $\mathbf{1}-\mathbf{x}$. For a complex sequence $\mathbf{a}$, let $\tilde{\mathbf{a}}$ denote the sequence obtained by reversing $\mathbf{a}$ and $\mathbf{a}^*$ its complex conjugate. Note that the quadratic forms in the functions f and $\tilde{f}$ are the same, thus, they have the same associated graph. The following lemma follows directly from the above discussion and Lemma 3.2.

Lemma 3.4: Suppose that there exist a set of k distinct vertices in the graph $G(f)$ such that deleting those k vertices and all their edges results in a path. Let β be the label of either end vertex in this path (or the single vertex of the graph when $k = m-1$). Then for each $0 \le t < 2^k$, the ordered set $\bar{S}_t$ given by

$$\left\{\tilde{f}+\frac{q}{2}\left(\sum_{\alpha=0}^{k-1} d_\alpha \bar{x}_{j_\alpha}+\sum_{\alpha=0}^{k-1} b_\alpha \bar{x}_{j_\alpha}+dx_\beta\right): d, d_\alpha \in \{0,1\}\right\} \qquad (18)$$

is a Golay complementary set of size 2^{k+1}, where $t=\sum_{\alpha=0}^{k-1} b_\alpha 2^\alpha$.

Consider the set $\bar{S}_t$ (with the natural order induced by the binary vector $[\bar{d}d_0d_1\cdots d_{k-1}]$), the following corollary is evident from Theorem 3.3.

Corollary 3.5: The complementary sets $\bar{S}_t$ and $\bar{S}_{t'}$ are mutually orthogonal whenever $t \neq t'$.

The following theorem identifies 2^{k+1} mutually orthogonal complementary sets of size 2^{k+1}. By S_t^*, we denote the ordered set containing the complex conjugate of the corresponding sequences in S_t.

Theorem 3.6: Suppose that the quadratic function f is as in Lemma 3.4, then the 2^{k+1} complementary sets given by

$$\{S_t : 0 \le t < 2^k\} \cup \{\bar{S}_t^* : 0 \le t < 2^k\}$$

form complete mutually orthogonal Golay complementary sets.

Proof: It is enough to show that any complementary set S_{t_1} is mutually orthogonal to any other complementary set $\bar{S}_{t_2}^*$. Let

$$\begin{aligned}\sum_{\mathbf{d}} &\mathbf{C}\left(f+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b})\cdot\mathbf{x}+x_\beta\Big), \tilde{f}^*+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b}')\cdot\bar{\mathbf{x}}\Big)\right)(l)\\ &+\mathbf{C}\left(f+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b})\cdot\mathbf{x}\Big), \tilde{f}^*+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b}')\cdot\bar{\mathbf{x}}+x_\beta\Big)\right)(l)\\ &=L \end{aligned} \tag{19}$$

where

$$\begin{aligned} L=\sum_{\mathbf{d}}\sum_{\mathbf{c}_1,\mathbf{c}_2}&\mathbf{C}\left(\left(f+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b})\cdot\mathbf{x}+x_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_1}\right.\\ &\left.\left(\tilde{f}^*+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b}')\cdot\bar{\mathbf{x}}\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_2}\right)(l)\\ &+\mathbf{C}\left(\left(f+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b})\cdot\mathbf{x}\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_1}\right.\\ &\left.\left(\tilde{f}^*+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b}')\cdot\bar{\mathbf{x}}+x_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_2}\right)(l). \end{aligned} \tag{20}$$

For a given $\mathbf{c}_1$ and $\mathbf{c}_2$, consider the following sum of the first correlation term in (20)

$$\begin{aligned} \sum_{\mathbf{d}}&\mathbf{C}\left(\left(f+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b})\cdot\mathbf{x}+x_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_1}\right.\\ &\left.\left(\tilde{f}^*+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b}')\cdot\bar{\mathbf{x}}\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_2}\right)(l)\\ &=\sum_{\mathbf{d}}\mathbf{C}\left(\left(f+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b})\cdot\mathbf{x}+x_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_1}\right.\\ &\left.\left(\tilde{f}^*+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b}')\cdot(\mathbf{1}-\mathbf{x})\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_2}\right)(l) \end{aligned} \tag{21}$$

$$\begin{aligned} &=\mathbf{C}\left(\left(f+\frac{q}{2}\Big(x_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_1}, \tilde{f}^*|_{\mathbf{x}=\mathbf{c}_2}\right)(l)\\ &\quad\cdot\sum_{\mathbf{d}}\left((-1)^{\mathbf{b}\cdot\mathbf{c}_1\oplus\mathbf{b}'\cdot\mathbf{c}_2}\cdot(-1)^{(\mathbf{d}\oplus\mathbf{b}')\cdot\mathbf{1}}\cdot(-1)^{\mathbf{d}\cdot(\mathbf{c}_1\oplus\mathbf{c}_2)}\right)\\ &=\mathbf{C}\left(\left(f+\frac{q}{2}\Big(x_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_1}, \tilde{f}^*|_{\mathbf{x}=\mathbf{c}_2}\right)(l)\\ &\quad\cdot(-1)^{\mathbf{b}\cdot\mathbf{c}_1\oplus\mathbf{b}'\cdot\mathbf{c}_2\oplus\mathbf{b}'\cdot\mathbf{1}}\cdot\sum_{\mathbf{d}}(-1)^{\mathbf{d}\cdot(\mathbf{c}_1\oplus\mathbf{c}_2\oplus\mathbf{1})}. \end{aligned} \tag{22}$$

The sum in (22) is zero whenever $(\mathbf{c}_1\oplus\mathbf{c}_2)\neq\mathbf{1}$. So when $(\mathbf{c}_1=\mathbf{c}_2)$, the first correlation term in (20) vanishes. Thus, summing (22) over all $\mathbf{c}_1\neq\mathbf{c}_2$, we obtain

$$\begin{aligned} \sum_{\substack{\mathbf{c}_1\neq\mathbf{c}_2\\ \mathbf{c}_1+\mathbf{c}_2=\mathbf{1}}}&\mathbf{C}\left(\left(f+\frac{q}{2}\Big(x_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_1}, \tilde{f}^*|_{\mathbf{x}=\mathbf{c}_2}\right)(l)\\ &\cdot(-1)^{\mathbf{b}\cdot\mathbf{c}_1\oplus\mathbf{b}'\cdot\mathbf{c}_2\oplus\mathbf{b}'\cdot\mathbf{1}}\,2^k\\ &=\sum_{\mathbf{c}}\mathbf{C}\left(\left(f+\frac{q}{2}\Big(x_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}}, \tilde{f}^*|_{\mathbf{x}=(\mathbf{c}\oplus\mathbf{1})}\right)(l)\\ &\cdot(-1)^{\mathbf{b}'\cdot\mathbf{1}}\,2^k\cdot(-1)^{\mathbf{b}\cdot\mathbf{c}\oplus\mathbf{b}'\cdot(\mathbf{1}\oplus\mathbf{c})}\\ &=\sum_{\mathbf{c}}\mathbf{C}\left(\left(f+\frac{q}{2}\Big(x_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}}, \tilde{f}^*|_{\mathbf{x}=(\mathbf{c}\oplus\mathbf{1})}\right)(l)\,2^k\\ &\cdot(-1)^{(\mathbf{b}\oplus\mathbf{b}')\cdot\mathbf{c}}. \end{aligned} \tag{23}$$

The algebra in (21)–(23) applies equally to the second correlation term in (20) as well. It can be verified that

$$\begin{aligned} \sum_{\mathbf{d}}&\mathbf{C}\left(\left(f+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b})\cdot\mathbf{x}\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_1}\right.\\ &\left.\left(\tilde{f}^*+\frac{q}{2}\Big((\mathbf{d}+\mathbf{b}')\cdot\bar{\mathbf{x}}+x_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}_2}\right)(l)\\ &=\sum_{\mathbf{c}}\mathbf{C}\left(f|_{\mathbf{x}=\mathbf{c}}, \left(\tilde{f}^*+\frac{q}{2}\Big(x_\beta\Big)\right)\Big|_{\mathbf{x}=(\mathbf{c}\oplus\mathbf{1})}\right)(l)\\ &\cdot 2^k\cdot(-1)^{(\mathbf{b}\oplus\mathbf{b}')\cdot\mathbf{c}}. \end{aligned} \tag{24}$$

Thus

$$\begin{aligned} L=\sum_{\mathbf{c}}&\left(\mathbf{C}\left(\left(f+\frac{q}{2}\Big(x_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}}, \tilde{f}^*|_{\mathbf{x}=(\mathbf{c}\oplus\mathbf{1})}\right)(l)\right.\\ &\left.+\mathbf{C}\left(f|_{\mathbf{x}=\mathbf{c}}, \left(\tilde{f}^*+\frac{q}{2}\Big(x_\beta\Big)\right)\Big|_{\mathbf{x}=(\mathbf{c}\oplus\mathbf{1})}\right)(l)\right)\cdot 2^k\\ &\cdot(-1)^{(\mathbf{b}\oplus\mathbf{b}')\cdot\mathbf{c}}. \end{aligned} \tag{25}$$

By Lemma 2.9

$$\begin{aligned} &\mathbf{C}\left(\left(f+\frac{q}{2}\Big(x_\beta\Big)\right)\Big|_{\mathbf{x}=\mathbf{c}}, \tilde{f}^*|_{\mathbf{x}=(\mathbf{c}\oplus\mathbf{1})}\right)(l)\\ &=\mathbf{C}\left(\left(f+\frac{q}{2}\Big(x_\beta\Big)\right)\Big|_{\mathbf{x}x_\beta=\mathbf{c}0}, \tilde{f}^*|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})0}\right)(l)\\ &\quad+\mathbf{C}\left(\left(f+\frac{q}{2}\Big(x_\beta\Big)\right)\Big|_{\mathbf{x}x_\beta=\mathbf{c}0}, \tilde{f}^*|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})1}\right)(l)\\ &\quad+\mathbf{C}\left(\left(f+\frac{q}{2}\Big(x_\beta\Big)\right)\Big|_{\mathbf{x}x_\beta=\mathbf{c}1}, \tilde{f}^*|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})0}\right)(l)\\ &\quad+\mathbf{C}\left(\left(f+\frac{q}{2}\Big(x_\beta\Big)\right)\Big|_{\mathbf{x}x_\beta=\mathbf{c}1}, \tilde{f}^*|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})1}\right)(l)\\ &=\mathbf{C}\left(f|_{\mathbf{x}x_\beta=\mathbf{c}0}, \tilde{f}^*|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})0}\right)(l)\\ &\quad+\mathbf{C}\left(f|_{\mathbf{x}x_\beta=\mathbf{c}0}, \tilde{f}^*|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})1}\right)(l)\\ &\quad-\mathbf{C}\left(f|_{\mathbf{x}x_\beta=\mathbf{c}1}, \tilde{f}^*|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})0}\right)(l)\\ &\quad-\mathbf{C}\left(f|_{\mathbf{x}x_\beta=\mathbf{c}1}, \tilde{f}^*|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})1}\right)(l). \end{aligned} \tag{26}$$

Similarly

$$\begin{aligned} &\mathbf{C}\left(f|_{\mathbf{x}=\mathbf{c}}, \left(\tilde{f}^*+\frac{q}{2}\Big(x_\beta\Big)\right)\Big|_{\mathbf{x}=(\mathbf{c}\oplus\mathbf{1})}\right)(l)\\ &=\mathbf{C}\left(f|_{\mathbf{x}x_\beta=\mathbf{c}0}, \tilde{f}^*|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})0}\right)(l)\\ &\quad-\mathbf{C}\left(f|_{\mathbf{x}x_\beta=\mathbf{c}0}, \tilde{f}^*|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})1}\right)(l)\\ &\quad+\mathbf{C}\left(f|_{\mathbf{x}x_\beta=\mathbf{c}1}, \tilde{f}^*|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})0}\right)(l)\\ &\quad-\mathbf{C}\left(f|_{\mathbf{x}x_\beta=\mathbf{c}1}, \tilde{f}^*|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})1}\right)(l). \end{aligned} \tag{27}$$

Substituting (26) and (27) back in (25)

$$L = 2\sum_{\mathbf{c}}\Bigg(\mathbf{C}\Big(f|_{\mathbf{x}x_\beta=\mathbf{c}0}, \tilde{f}^*|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})0}\Big)(l) - \mathbf{C}\Big(f|_{\mathbf{x}x_\beta=\mathbf{c}1}, \tilde{f}^*|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})1}\Big)(l)\Bigg)\cdot 2^k\cdot(-1)^{(\mathbf{b}\oplus\mathbf{b}')\cdot\mathbf{c}}. \quad (28)$$

Since $G(f|_{\mathbf{x}=\mathbf{c}})$ forms a path, the function obtained by substituting $\mathbf{x}=\mathbf{c}$ in f should be of the form

$$f|_{\mathbf{x}=\mathbf{c}} = \frac{q}{2}\sum_{i=1}^{m-k-1} x_{\pi(i-1)}x_{\pi(i)} + \sum_{i=0}^{m-k-1} x_{\pi(i)}g_i + g' \quad (29)$$

for some permutation π, and $g_i, g' \in \mathbb{Z}_q$.

Let h_1 denote the function obtained from f by substituting $\mathbf{x}=\mathbf{c}$ and $x_\beta = 0$ for some binary vector $\mathbf{c}$ and let h_2 be the corresponding function when $\mathbf{x}=\mathbf{c}$ and $x_\beta = 1$. Further let $\beta = \pi(m-k-1)$ without loss of generality. Then

$$h_1 = \frac{q}{2}\sum_{i=1}^{m-k-2} x_{\pi(i-1)}x_{\pi(i)} + \sum_{\substack{i=0:\\ \pi(i)\neq m-k-1}}^{m-k-1} x_{\pi(i)}g_i + g' \quad (30)$$

$$h_2 = h_1 + \frac{q}{2}x_{\pi(m-k-2)} + g_{m-k-1}. \quad (31)$$

The nonzero components of the complex vectors $\mathbf{a} = f|_{\mathbf{x}x_\beta=\mathbf{c}0}$ and $\mathbf{b} = f|_{\mathbf{x}x_\beta=\mathbf{c}1}$ are given by the functions h_1 and h_2 respectively. The nonzero components of the vector $\tilde{f}|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})0}$ are given by the function

$$\begin{aligned} h_3 &= \frac{q}{2}\sum_{i=1}^{m-k-2}(1-x_{\pi(i-1)})(1-x_{\pi(i)}) \\ &\quad + \sum_{\substack{i=0:\\ \pi(i)\neq m-k-1}}^{m-k-1}(1-x_{\pi(i)})g_i + g' + \frac{q}{2}(1-x_{\pi(m-k-2)}) \\ &\quad + g_{m-k-1} \\ &= \tilde{h}_2 \end{aligned} \quad (32)$$

and similarly the function corresponding to the sequence $\tilde{f}|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})1}$ is $\tilde{h}_1$.

Moreover, since the nonzero components in the sequence $\tilde{f}^*|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})0}$ occur when $\mathbf{x}x_\beta = (\mathbf{1}\oplus\mathbf{c})1$, this sequence is exactly, $\tilde{\mathbf{b}}^*$. Also, the sequence represented by the complex vector $\tilde{f}^*|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})1}$ is $\tilde{\mathbf{a}}^*$. For any two complex sequences $\mathbf{a}$ and $\mathbf{b}$, recall the identity

$$\mathbf{C}(\mathbf{a},\tilde{\mathbf{b}}^*)(l) = \mathbf{C}(\tilde{\mathbf{b}},\mathbf{a}^*)(-l) = \mathbf{C}(\mathbf{b},\tilde{\mathbf{a}}^*)(l).$$

Thus

$$\mathbf{C}\Big(f|_{\mathbf{x}x_\beta=\mathbf{c}0}, \tilde{f}^*|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})0}\Big)(l) = \mathbf{C}\Big(f|_{\mathbf{x}x_\beta=\mathbf{c}1}, \tilde{f}^*|_{\mathbf{x}x_\beta=(\mathbf{c}\oplus\mathbf{1})1}\Big)(l)$$

proving that L is zero, thus completing the proof. □

All the sequences in the complementary sets identified by the Theorem 3.6 lie in the same coset whose coset leader is given by the quadratic form Q in the function f. Totally, 2^{k+2} sequences are chosen from this second-order coset of the first-order RM code and ordered to form two mutually orthogonal Golay complementary sets. All other complementary sets are obtained by certain permutations of the sequences in each of these sets.

As noted, Theorem 3.6 is a form of generalization of [6, Th. 11] where construction of a mutually orthogonal Golay complementary set of a given complementary pair was discussed[5] (which can be easily extended to any complementary set with even number of sequences). The construction there involved reversing the sequences and multiplying one of the inverted sequences by -1. For polyphase sequences, it was noted in [5] that an additional conjugation is necessary. Theorem 3.6 is a generalization of this approach in the sense that it constructs 2^k complementary sets which are mutually orthogonal in addition to being orthogonal to the complementary sets constructed in Theorem 3.3. We outline an application of our direct construction in the next section.

IV. ZCZ Sequences and Reed–Muller Codes

The ZCZ sequences can be constructed by certain operations (Kronecker product followed by a length dependent permutation of columns) on the matrices formed by ordering mutually orthogonal Golay complementary sets as its rows. It was shown in [3] that this operation is equivalent to the construction of certain orthogonal complementary sets starting from smaller sets. Since we have associated each of these complementary set to a coset of the RM code, we have a direct relation between a ZCZ sequence and the corresponding coset. In order to directly construct the ZCZ sequences from RM codes, it remains to identify the subset of permutations that were used in Theorem 3.3 that would generate ZCZ sequences.

The concept of orthogonal sets of ZCZ sequences and large ZCZ sets with smaller subsets of larger interference free window than the original set were introduced in [3]. Constructions there involves searching for matrices satisfying a number of conditions and becomes computationally infeasible for large alphabets or large matrix dimensions. We believe that the direct construction of Golay complementary sets in this paper can be used to algebraically construct such ZCZ sets. On possible approach is to associate a graph with a ZCZ sequence set and relate the IFW property of the ZCZ sequences to that graph. Thus, different subsets of the ZCZ set can all be associated with a subgraph of that graph. Further work is needed to conclusively answer these questions.

V. Conclusion

Motivated by the direct construction of Golay complementary sets, we have presented a direct construction of complete mutually orthogonal Golay complementary sets from second-order cosets of a q-ary generalization of the first-order RM codes. The motivation behind the construction is to be able to construct ZCZ sequence sets with smaller subsets having superior correlation properties than the complete set.

References

[1] 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. 9, pp. 2397–2417, Nov. 1999.

[2] 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.

[5]Mutually orthogonal Golay complementary pairs were referred to as mates in their work.

[3] A. Rathinakumar and A. K. Chaturvedi, "Some new ZCZ sequences and mutually orthogonal complementary sets," *IEEE Trans. Inf. Theory*, vol. 52, no. 8, pp. 3817–3826, Aug. 2006.
[4] A. Rathinakumar and A. K. Chaturvedi, "Mutually orthogonal sets of ZCZ sequences," *Electron. Lett.*, vol. 40, pp. 1133–1134, Sep. 2004.
[5] R. L. Frank, "Polyphase complementary codes," *IEEE Trans. Inf. Theory*, vol. IT-26, no. 6, pp. 641–647, Nov. 1980.
[6] C. C. Tseng and C. L. Liu, "Complementary sets of sequences," *IEEE Trans. Inf. Theory*, vol. 18, no. 5, pp. 644–652, Sep. 1972.
[7] R. Sivaswamy, "Multiphase complementary codes," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 5, pp. 546–552, Sep. 1978.
[8] H. Torii, M. Nakamura, and N. Suehiro, "A new class of zero-correlation zone sequences," *IEEE Trans. Inf. Theory*, vol. 50, no. 3, pp. 559–565, Mar. 2004.
[9] B. M. Popovic, "Class of binary sequences for mobile channel estimation," *IEE Electron. Lett.*, vol. 31, no. 12, pp. 944–945, Jun. 1995.
[10] P. Fan and L. Hao, "Generalized orthogonal sequences and their applications in synchronous CDMA systems," *IEICE Trans. Fund.*, vol. E89-A, no. 11, pp. 2054–2066, Nov. 2000.
[11] X. H. Tang, P. Z. Fan, and S. Matsufuji, "Lower bounds on the maximum correlation of sequence set with low or zero correlation zone," *IEE Electron. Lett.*, vol. 36, no. 13, pp. 551–552, Mar. 2000.
[12] P. Z. Fan, N. Suehiro, and X. Deng, "Class of binary sequences with zero correlation zone," *IEE Electron. Lett.*, vol. 35, no. 10, pp. 777–778, May 1999.
[13] D. Wu, P. Spasojevic, and I. Seskar, "Ternary zero correlation zone sequences for multiple code UWB," in *Proc. 38th Conf. Inf. Sci. Syst. (CISS'04)*, Princeton, NJ, Mar. 2004, pp. 939–943.
[14] J. Weng, T. Le-Ngoc, and Y. Xu, "ZCZ-CDMA and OFDMA using M-QAM for broadband wireless communications," *Wireless Commun. Mobile Comput.*, vol. 4, no. 4, pp. 427–438, 2004.
[15] N. Abramson, "Internet access using VSATs," *IEEE Commun. Mag.*, vol. 38, pp. 60–68, Jul. 2000.
[16] X. Zeng, L. Hu, and Q. Liu, "New sequence sets with zero-correlation zone," *IEEE Trans. Inf. Theory*, submitted for publication.

On the Intersection of $\mathbb{Z}_2\mathbb{Z}_4$-Additive Perfect Codes

Josep Rifà, *Senior Member, IEEE*, Faina Ivanovna Solov'eva, and Mercè Villanueva

***Abstract*—The intersection problem for $\mathbb{Z}_2\mathbb{Z}_4$-additive (extended and nonextended) perfect codes, i.e., which are the possibilities for the number of codewords in the intersection of two $\mathbb{Z}_2\mathbb{Z}_4$-additive codes $\mathcal{C}_1$ and $\mathcal{C}_2$ of the same length, is investigated. Lower and upper bounds for the intersection number are computed and, for any value between these bounds, codes which have this given intersection value are constructed. For all these $\mathbb{Z}_2\mathbb{Z}_4$-additive codes $\mathcal{C}_1$ and $\mathcal{C}_2$, the abelian group structure of the intersection codes $\mathcal{C}_1 \cap \mathcal{C}_2$ is characterized. The parameters of this abelian group structure corresponding to the intersection codes are computed and lower and upper bounds for these parameters are established. Finally, for all possible parameters between these bounds, constructions of codes with these parameters for their intersections are given.**

***Index Terms*—Additive codes, extended perfect codes, intersection, perfect codes.**

I. Introduction and Basic Definitions

Let $\mathbb{F}^n$ be the n-dimensional vector space of all n-tuples over the finite field $\mathbb{F} = \mathbb{Z}_2$. The *Hamming distance* $d(v, s)$ between two vectors $v, s \in \mathbb{F}^n$ is the number of coordinates in which v and s differ.

A *binary code* C of length n is a nonempty subset of $\mathbb{F}^n$. The elements of a code are called *codewords*. The *minimum distance* d of a code C is the minimum value of $d(a, b)$, where $a, b \in C$ and $a \neq b$. The *error correcting capability* of a code C is the value $e = \lfloor \frac{d-1}{2} \rfloor$ and C is called an e*-error correcting code*. Two binary codes C_1 and C_2 of length n are *isomorphic* if there exists a coordinate permutation π such that $C_2 = \{\pi(c) \mid c \in C_1\}$. They are *equivalent* if there exists a vector $a \in \mathbb{F}^n$ and a coordinate permutation π such that $C_2 = \{a + \pi(c) \mid c \in C_1\}$.

A binary *perfect 1-error correcting code* (briefly in this correspondence, *binary perfect code*) C of length n is a subset of $\mathbb{F}^n$, with minimum distance $d = 3$, such that all the vectors in $\mathbb{F}^n$ are within distance one from a codeword. For any $t > 1$ there exists exactly one binary linear perfect code of length $2^t - 1$, up to equivalence, which is the well-known *Hamming code*. An *extended code* of the code C is a code resulting from adding an overall parity check digit to each codeword of C.

The intersection problem for binary perfect codes was proposed by Etzion and Vardy in [8]. They presented a complete solution to this problem for binary Hamming codes: for each $t \geq 3$, there exist two Hamming codes H_1 and H_2 of length $n = 2^t - 1$ such that the

Manuscript received December 2, 2006; revised May 28, 2007. This work has been partially supported by the Spanish MEC and the European FEDER Grant MTM2006-03250 and also by the UAB Grant PNL2006-13. Part of this manuscript was produced during a visit by F. I. Solov'eva to the Autonomous University of Barcelona under the Grant VIS2007-16. The material in this correspondence was presented in part at the International Workshop on Coding and Cryptography (WCC'07), Versailles, France, April 2007.

J. Rifà and M. Villanueva are with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain (e-mail: josep.rifa@autonoma.edu; merce.villanueva@autonoma.edu).

F. I. Solov'eva is with the Sobolev Institute of Mathematics and Novosibirsk State University, Novosibirsk, Russia (e-mail: sol@math.nsc.ru).

Communicated by T. Etzion, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2007.915917