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 given as illustrations.

REFERENCES


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 synchronized1 DS 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 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

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

2The 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 \(C(a, b)(\tau)\) between two length \(L\) complex-valued sequences \(a\) and \(b\) is defined as

\[
C(a, b)(\tau) = \begin{cases} 
\sum_{\omega=0}^{L-1} a_{\omega} b_{\omega+\tau}^*, & \text{if } 0 \leq \tau \leq L - 1 \\
0, & \text{if } L < \tau < 0
\end{cases}
\]

and

\[
A(a)(\tau) = C(a, a)(\tau)
\]

denotes the aperiodic autocorrelation of the sequence \(a\).

We also define the correlation functions for \(Z_q\)-valued vectors. This is done by defining \(\omega = e^{2\pi i / q}\) and associating with each vector \(a = [a_0, a_1, \ldots, a_{q-1}]\), where \(a_i \in Z_q\), a complex-valued vector \(a^* = [a_0^*, a_1^*, \ldots, a_{q-1}^*]\).

\(^3\)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].
will denote the $i$th row of $A$ by $a_i$, the $j$th row of $A_j$ by $a'_j$ and the $(i,j)$th scalar entry of $A$ by $a_{ij}$. Let $\mathcal{H}$ be a $P \times K$ matrix with complex valued entries having the same magnitude. For convenience, we will assume that this magnitude is 1. We define the matrix operation "$\mathcal{O}_k$" as
\[
\mathcal{A}\mathcal{O}_k\mathcal{H} = \begin{bmatrix}
\mathcal{C}(h_{11}, \ldots, h_{1K}) & \cdots & \mathcal{C}(h_{1(QK-K+1)}, \ldots, h_{1(QK)}) \\
\mathcal{C}(h_{21}, \ldots, h_{2K}) & \cdots & \mathcal{C}(h_{2(QK-K+1)}, \ldots, h_{2(QK)}) \\
\vdots & \ddots & \vdots \\
\mathcal{C}(h_{P1}, \ldots, h_{PK}) & \cdots & \mathcal{C}(h_{P(QK-K+1)}, \ldots, h_{P(QK)})
\end{bmatrix}_{M \times K \times MN}
\] (viewed as a $PM \times KQM$N scalar matrix) where
\[
\mathcal{C}(h_{ij}, h_{i(j+1)}, \ldots, h_{i(j+K)}) = \left[ (h_{ij}, a_1, h_{i(j+1)}, a_1, \ldots, h_{i(j+K)}, a_1) \cdots (h_{ij}, a_M, h_{i(j+1)}, a_M, \ldots, h_{i(j+K)}, a_M) \right]_{M \times K \times MN}
\]
with $(h_{ij}, a_1, h_{i(j+1)}, a_1, \ldots, h_{i(j+K)}, a_1)$ denoting a sequence of length $K \times N$.

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 $d_{i1} = (1, 0, 1, 0, \ldots, 1, 0)$ and $d_{i2} = (1, 1, 0, 1, 1, 0, \ldots, 1, 0)$. In general, $d_{ij}$ is constructed by a repeated pattern of $i$ ones and $j$ zeros. Define matrices $\overline{D}_{ij} = \text{diag}(d_{ij})$ and $\overline{D}^*_{ij} = \text{diag}(d^*_{ij})$, where $d_{ij}$ is the binary complement of $d_{ij}$.

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

**Lemma 2.6:** If $\mathcal{A}$ is a MOGCS matrix, then the rows of the matrix $\mathcal{B} = \mathcal{A}\mathcal{O}_k\mathcal{H}$ form a $\ZC$-$(2MN, MP, N)$ over $\mathcal{H}$ if $\mathcal{H}$ satisfies the following:
1) $\mathcal{H}\mathcal{H}^* = (MN)I$ where $I$ is the identity matrix;
2) $\mathcal{H}\overline{D}_{i1}\overline{D}^*_{i1} = 0 = \mathcal{H}\overline{D}_{i1}\overline{D}^*_{i2}$. Similar constructions have been established in [3] for $K \geq 2$. Note: 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 $a + \mathcal{C}$ where $a$ is some fixed vector over $\mathbb{Z}_q$. The vector $a$ is called a coset representative for the coset $a + \mathcal{C}$.

**Definition 2.7:** A map $f : \{0, 1\}^m \rightarrow \mathbb{Z}_q$ 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 $x_{i_0}x_{i_1} \cdots x_{i_r}$ (in which $j_0, j_1, \ldots, j_r$ are distinct). With each generalized Boolean function $f$ we identify a length $2^m$, $\mathbb{Z}_q$-valued vector $f = [f_0 f_1 \cdots f_{2^m-1}]$ 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 $f'$ is associated with every $f$, where $f'_i = \omega^i$ and $\omega$ is a complex $q$th 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 $0 \leq r \leq m$, $\RM_q(r, m)$ 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 $r$th order generalized Reed–Muller code $\RM_q(r, m)$ 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 $f : \{0, 1\}^m \rightarrow \mathbb{Z}_q$ be a generalized Boolean function in variables $x_0, x_1, \ldots, x_{m-1}$. Let $0 \leq j_0 < j_1 < \cdots < j_k = m$ be a list of $k$ indices and write $f_{[j_0j_1\cdots j_k]} = [x_{j_0}x_{j_1}\cdots x_{j_k}]$. Let $e = [e_0, \ldots, e_{m-1}]$ be a binary word of length $k$. Then we define the vector $f_{[j_0e]}$ to be the complex-valued vector with component $i = \sum_{j=0}^{m-1} e_j 2^j$ equal to $\omega^{f_{[j_0j_1\cdots j_k]} e}$ if $j_0j_1\cdots j_k \in e$, and equal to 0, otherwise. Here $\omega$ is a complex $q$th root of unity. In the case where $x$ and $e$ are of length zero, we define $f_{[j_0e]}$ to be the complex-valued vector associated with $f$.

The following simple consequences can be easily obtained from the definitions. For any $x$ defined as above
\[
f' = \sum_e f_{[x-e]}^e
\]
and the Boolean function associated with the complex vector $f_{[x-e]}$ can be written as
\[
f = \prod_{x \in e} x_{\alpha} \prod_{x \not\in e} (1 - x_{\alpha}).
\]

**Lemma 2.9:** Let $f, g : \{0, 1\}^m \rightarrow \mathbb{Z}_q$ be generalized Boolean functions in variables $x_0, x_1, \ldots, x_{m-1}$. Let $0 \leq j_0 < j_1 < \cdots < j_k = m$ be a list of $k$ indices and let $e = [e_0, \ldots, e_{m-1}]$ and $d = [d_0, d_1, \ldots, d_{m-1}]$ be binary-valued vectors. Write $x = [x_{j_0}, x_{j_1}, \ldots, x_{j_k}]$ and suppose $0 \leq i_1 < i_2 < \cdots < i_k < m$ is a set of indices not in $\{j_0, j_1, \ldots, j_k\}$. Denote $y = [x_{j_0}, x_{j_1}, \ldots, x_{j_k}, x_{i_1}, \ldots, x_{i_k}]$, then
\[
\mathcal{C}(f_{[x-e]}, g_{[y-e]})(\tau) = \sum_{c_1, c_2} \mathcal{C}(f_{[x-y-e_1]}, g_{[y-x-e_2]})(\tau).
\]

### D. Quadratic Forms and Graphs

Let $Q : \{0, 1\}^m \rightarrow \mathbb{Z}_q$ 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 $f : \{0, 1\}^m \rightarrow \mathbb{Z}_q$ is a quadratic function (i.e., a generalized Boolean function corresponding to a codeword of $\RM_q(2, m)$), 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 $G$. 

---

*IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 54, NO. 3, MARCH 2008 1341*

*Authorized licensed use limited to: INDIAN INSTITUTE OF TECHNOLOGY KANPUR. Downloaded on September 30, 2009 at 03:12 from IEEE Xplore. Restrictions apply.*
For $m \geq 2$, a path on $m$ vertices corresponds to a quadratic form of the type

$$f(x) = Q + \sum_{i=0}^{m-1} g_i x_i + g'$$

where $g', g_i \in \mathbb{Z}_2$ are arbitrary. Consider the function $f(x) = Q + \sum_{i=0}^{m-1} g_i x_i + g'$ 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 $\mathbf{x} = [x_{j_0}, x_{j_1}, \ldots, x_{j_{k-1}}]$ and $\mathbf{c} = [c_{j_0}, c_{j_1}, \ldots, c_{j_{k-1}}]$ then the graph of the function $f|_{x_{j_0} = \cdots = x_{j_{k-1}}}$ 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 $f|_{x_{j_0} = \cdots = x_{j_{k-1}}}$ 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–Müller Codes

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

Lemma 3.1: If the function $f|_{x_{j_0} = \cdots = x_{j_{k-1}}}$ is a quadratic function and if $G(f|_{x_{j_0} = \cdots = x_{j_{k-1}}})$ is a path, then the complex vector $f|_{x_{j_0} = \cdots = x_{j_{k-1}}}$ and any vector of the form $f + (q/2) x_{j_0} + (q/2) x_{j_1} + \cdots + (q/2) x_{j_{k-1}}$ form a Golay complementary pair.4

Where $r \in \mathbb{Z}_2$ is arbitrary and $\beta$ is either the single vertex of $G(f|_{x_{j_0} = \cdots = x_{j_{k-1}}})$ when $k = m - 1$, or an end vertex of the path in $G(f|_{x_{j_0} = \cdots = x_{j_{k-1}}})$ when $0 \leq k < m - 1$.

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

Lemma 3.2: Suppose $Q : \{0, 1\}^m \rightarrow \mathbb{Z}_2$ 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 $0_0, 0_1, \ldots, 0_{k-1}$ with the property that deleting those $k$ vertices and all their edges results in a path. Let $\beta$ 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 $g', g_i \in \mathbb{Z}_2$

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

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

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

B. MOGCS From Reed–Müller Codes

In this section, we prove the main theorem for constructing mutually orthogonal Golay complementary sets. Suppose $Q : \{0, 1\}^m \rightarrow \mathbb{Z}_2$ 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 $[dd_1d_1 \cdots d_{k-1}]$) to be

$$\left\{ \begin{array}{l}
Q + \sum_{i=0}^{m-1} g_i x_i + g' + \frac{q}{2} \left( \sum_{\alpha=0}^{k-1} d_{\alpha} x_{\alpha} + \sum_{\alpha=0}^{k-1} b_{\alpha} x_{\alpha} + dx_{\beta} \right) :
\end{array} \right\}$$

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 $1$ and the mod $2$ addition is denoted by $\oplus$.

Theorem 3.3: Suppose that $G(Q)$ contains a set of $k$ distinct vertices labeled $0_0, 0_1, \ldots, 0_{k-1}$ with the property that deleting those $k$ vertices and all their edges results in a path. Let $\beta$ 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 $g', g_i \in \mathbb{Z}_2$, 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 $\mathbf{x} = [x_0, x_1, \ldots, x_{m-1}], \mathbf{d} = [dd_1 \cdots d_{k-1}]$ and $\mathbf{b} = [b_0b_1 \cdots b_{k-1}]$. 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

$$\sum_{d, \varnothing} C \left( f + \frac{q}{2} \left( \mathbf{d} + \mathbf{b} \right) \cdot \mathbf{x} + dx_{\beta} \right) \cdot f + \frac{q}{2} \left( \mathbf{d} + \mathbf{b}' \right) \cdot \mathbf{x} + dx_{\beta} \right) \right|_{\mathbf{x}=\mathbf{c}}$$

where

$$L_1 = \sum_{d, \varnothing} \sum_{\mathbf{c} \neq \mathbf{c}_1} C \left( f + \frac{q}{2} \left( \mathbf{d} + \mathbf{b} \right) \cdot \mathbf{x} + dx_{\beta} \right) \left|_{\mathbf{x} = \mathbf{c}_1} \right. = L_1 + L_2$$

and

$$L_2 = \sum_{d, \varnothing} \sum_{\mathbf{c} \neq \mathbf{c}_2} C \left( f + \frac{q}{2} \left( \mathbf{d} + \mathbf{b} \right) \cdot \mathbf{x} + dx_{\beta} \right) \left|_{\mathbf{x} = \mathbf{c}_2} \right. \left( l \right)$$


Authorized licensed use limited to: INDIAN INSTITUTE OF TECHNOLOGY KANPUR. Downloaded on September 30, 2009 at 03:12 from IEEE Xplore. Restrictions apply.
Consider the following sum in $L_1$ for a fixed $d, e_1$ and $e_2$

$$
\sum_d C \left( f + \frac{q}{2} \left( (d + b) \cdot x + dx_\beta \right) \right)_{x = e_1} \left( f + \frac{q}{2} \left( (d + b') \cdot x + dx_\beta \right) \right)_{x = e_2}(l)
$$

(10)

$$
= \sum_d C \left( f + \frac{q}{2} \left( (d + b) \cdot e_1 + dx_\beta \right) \right)_{x = e_1} \left( f + \frac{q}{2} \left( (d + b') \cdot e_2 + dx_\beta \right) \right)_{x = e_2}(l)
$$

(11)

$$
= C \left( f + \frac{q}{2} \left( (b \cdot e_1 + dx_\beta) \right) \right)_{x = e_1} \left( f + \frac{q}{2} \left( (b' \cdot e_2 + dx_\beta) \right) \right)_{x = e_2}(l) \sum_d (-1)^d (e_1 \oplus e_2)
$$

(12)

Since $e_1 \neq e_2$ in the term $L_1$, the function $d \cdot (e_1 \oplus e_2)$ 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 $e$ and $d$:

$$
\sum_d C \left( f + \frac{q}{2} \left( (d + b) \cdot x + dx_\beta \right) \right)_{x = e} \left( f + \frac{q}{2} \left( (d + b') \cdot x + dx_\beta \right) \right)_{x = e}(l) = \sum_d C \left( f + \frac{q}{2} \left( (d + b) \cdot e + dx_\beta \right) \right)_{x = e} \left( f + \frac{q}{2} \left( (d + b') \cdot e + dx_\beta \right) \right)_{x = e}(l).
$$

(13)

The above sum can be rewritten as

$$
\sum_d C \left( f + \frac{q}{2} \left( (b + b') \cdot e + dx_\beta \right) \right)_{x = e} \left( f + \frac{q}{2} \left( (d + b') \cdot e + dx_\beta \right) \right)_{x = e}(l) = \sum_d C \left( f + \frac{q}{2} \left( dx_\beta \right) \right)_{x = e}(l).
$$

(14)

Note that

$$
\sum_d C \left( f + \frac{q}{2} \left( dx_\beta \right) \right)_{x = e} \left( f + \frac{q}{2} \left( dx_\beta \right) \right)_{x = e}(l) = A \left( f \mid x = e \right)(l) + A \left( f + \frac{q}{2} \left( dx_\beta \right) \right)_{x = e}(l)
$$

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

$$
A \left( f \mid x = e \right)(0) = A \left( f + \frac{q}{2} \left( dx_\beta \right) \right)_{x = e}(0) = 2^{m-h}
$$

(16)

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

$$
\sum_d C \left( f + \frac{q}{2} \left( (b \cdot e + dx_\beta) \right) \right)_{x = e} \left( f + \frac{q}{2} \left( (d + b') \cdot e + dx_\beta \right) \right)_{x = e}(0) = (-1)^{b \cdot b' \cdot e} \cdot 2^{m-h+1}
$$

(17)

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

$$
\sum_e (-1)^{b \cdot b' \cdot e} \cdot 2^{m-h+1} = 0.
$$

The codeword represented by the quadratic $Q$ will be in the second-order RM code. In our construction, $\tilde{Q}$ 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 $x_0, x_1, \ldots, x_{n-1}$, we denote by $\tilde{f}$, the function $f(1-x_0, 1-x_1, \ldots, 1-x_{n-1})$. Let $\tilde{x}$ denote the vector $1 - x$. For a complex sequence $a$, let $a$ denote the sequence obtained by reversing $a$ and $a^*$ 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 $\beta$ be the label of either end vertex in this path (or the single vertex of the graph when $k = m - 1$). Then for each $0 \leq t < 2^k$, the ordered set $\tilde{S}_t$ given by

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

(18)

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

Consider the set $\tilde{S}_t$ (with the natural order induced by the binary vector $[d_0 d_1 \cdots d_{k-1}]$), the following corollary is evident from Theorem 3.3.

**Corollary 3.5**: The complementary sets $\tilde{S}_t$ and $\tilde{S}_{t'}$ 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 $S_t$. 

Authorized licensed use limited to: INDIAN INSTITUTE OF TECHNOLOGY KANPUR. Downloaded on September 30, 2009 at 03:12 from IEEE Xplore. Restrictions apply. 
Theorem 3.6: Suppose that the quadratic function \( f \) is as in Lemma 3.4, then the \( 2^{k+1} \) complementary sets given by

\[
\{ S_t : 0 \leq t < 2^k \} \cup \{ S_0^t : 0 \leq t < 2^k \}
\]

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 \( S_{t_2} \).

\[
\sum_d C \left( f + \frac{q}{2} (d + b) \cdot x + x_\beta \right) \left( \tilde{f}^* + \frac{q}{2} (d + b') \cdot \tilde{x} \right)(l)
+ C \left( f + \frac{q}{2} (d + b) \cdot x \right) \left( \tilde{f}^* + \frac{q}{2} (d + b') \cdot \tilde{x} + x_\beta \right)(l)
= L
\]

(19)

where

\[
L = \sum_{d} \sum_{e_1, e_2} C \left( f + \frac{q}{2} (d + b) \cdot x + x_\beta \right) \left( \tilde{f}^* + \frac{q}{2} (d + b') \cdot \tilde{x} \right)(l)
+ C \left( f + \frac{q}{2} (d + b) \cdot x \right) \left( \tilde{f}^* + \frac{q}{2} (d + b') \cdot \tilde{x} + x_\beta \right)(l).
\]

(20)

For a given \( e_1 \) and \( e_2 \), consider the following sum of the first correlation term in (20)

\[
\sum_d C \left( f + \frac{q}{2} (d + b) \cdot x + x_\beta \right) \left( \tilde{f}^* + \frac{q}{2} (d + b') \cdot \tilde{x} \right)(l)
= \sum_d C \left( f + \frac{q}{2} (d + b) \cdot x + x_\beta \right) \left( \tilde{f}^* + \frac{q}{2} (d + b') \cdot \tilde{x} \right)(l)
+ C \left( f + \frac{q}{2} (d + b) \cdot x \right) \left( \tilde{f}^* + \frac{q}{2} (d + b') \cdot \tilde{x} + x_\beta \right)(l)
= C \left( f + \frac{q}{2} (x_\beta) \right) \tilde{f}^* |_{x = e_1} \tilde{f}^* |_{x = e_2} (l)
\cdot \sum_d (-1)^{b \cdot e_1 \cdot b' \cdot e_2 \cdot e_1 \cdot e_2 + 1} \cdot (-1)^{d \cdot (d + b') \cdot 1} \cdot (-1)^{d \cdot (d + b') \cdot 1}.
\]

(21)

The sum in (22) is zero whenever \( (e_1 \cdot e_2) \neq 1 \). So when \( (e_1 = e_2) \), the first correlation term in (20) vanishes. Thus, summing (22) over all \( e_1 \neq e_2 \), we obtain

\[
\sum_{e_1 \neq e_2} C \left( f + \frac{q}{2} (x_\beta) \right) \tilde{f}^* |_{x = e_2} (l)
\cdot (-1)^{b \cdot e_1 \cdot b' \cdot e_2 \cdot b' \cdot 1} \cdot 2^k
= \sum_{e_1} C \left( f + \frac{q}{2} (x_\beta) \right) \tilde{f}^* |_{x = e_1} (l)
\cdot (-1)^{b \cdot e_1 \cdot b' \cdot 1} \cdot 2^k
\cdot (-1)^{b \cdot b' \cdot e}.
\]

(22)

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

\[
\sum_d C \left( f + \frac{q}{2} (d + b) \cdot x \right) \tilde{f}^* |_{x = e_1} \tilde{f}^* |_{x = e_2} (l)
= \sum_e C \left( f |_{x = e} \cdot \tilde{f}^* |_{x = (e + 1)} (l)
- 2^k \cdot (-1)^{b \cdot b' \cdot e}.
\]

Thus

\[
L = \sum_{e} C \left( f + \frac{q}{2} (x_\beta) \right) \tilde{f}^* |_{x = e} (l)
+ C \left( f |_{x = e} \cdot \tilde{f}^* + \frac{q}{2} (x_\beta) \right) |_{x = (e + 1)} (l)
\cdot 2^k.
\]

(25)

By Lemma 2.9

\[
C \left( f + \frac{q}{2} (x_\beta) \right) \tilde{f}^* |_{x = (e + 1)} (l)
= C \left( f + \frac{q}{2} (x_\beta) \right) \tilde{f}^* |_{x = (e + 1) 0} (l)
+ C \left( f + \frac{q}{2} (x_\beta) \right) \tilde{f}^* |_{x = (e + 1) 1} (l)
+ C \left( f + \frac{q}{2} (x_\beta) \right) \tilde{f}^* |_{x = (e + 1) 0} (l)
+ C \left( f + \frac{q}{2} (x_\beta) \right) \tilde{f}^* |_{x = (e + 1) 1} (l)
= C \left( f |_{x = e} \cdot \tilde{f}^* |_{x = (e + 1) 0} (l)
+ C \left( f |_{x = e} \cdot \tilde{f}^* |_{x = (e + 1) 1} (l)
- C \left( f |_{x = e} \cdot \tilde{f}^* |_{x = (e + 1) 0} (l)
- C \left( f |_{x = e} \cdot \tilde{f}^* |_{x = (e + 1) 1} (l).
\]

(26)

Similarly

\[
C \left( f + \frac{q}{2} (x_\beta) \right) \tilde{f}^* |_{x = (e + 1)} (l)
= C \left( f |_{x = e} \cdot \tilde{f}^* |_{x = (e + 1) 0} (l)
- C \left( f |_{x = e} \cdot \tilde{f}^* |_{x = (e + 1) 1} (l)
+ C \left( f |_{x = e} \cdot \tilde{f}^* |_{x = (e + 1) 0} (l)
- C \left( f |_{x = e} \cdot \tilde{f}^* |_{x = (e + 1) 1} (l).
\]

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

\[ L = 2 \sum_{\epsilon} \left( C \left( f|_{x, \beta=e_0}, \tilde{f}^* |_{x, \beta=(e \oplus 1)0} \right)(I) \right) - C \left( f|_{x, \beta=e_1}, \tilde{f}^* |_{x, \beta=(e \oplus 1)1} \right)(I) \cdot g^2 \cdot (-1)^{(b \oplus b') \cdot \epsilon}. \]  

(28)

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

\[ f|_{x-e} = \frac{q}{2} \sum_{i=0}^{m-1} x^i g_i + g \]  

for some permutation \( \pi \), and \( g, g' \in \mathbb{Z}_2 \).

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

\[ h_1 = \frac{q}{2} \sum_{i=0}^{m-1} x^i g_i + g \]  

\[ h_2 = h_1 + \frac{q}{2} x^i \pi(m-k-1) + g \cdot m \cdot k - 1. \]  

(31)

The nonzero components of the complex vectors \( a = f|_{x, \beta=e_0} \) and \( b = f|_{x, \beta=e_1} \) are given by the functions \( h_1 \) and \( h_2 \) respectively. The nonzero components of the vector \( f|_{x, \beta=(e \oplus 1)0} \) are given by the function

\[ h_0 = \frac{q}{2} \sum_{i=0}^{m-1} (1 - x^i)(1 - x^i) \]  

\[ + \sum_{i=0}^{m-k-1} (1 - x^i) g_i + g' + \frac{q}{2} (1 - x^i m-k-2) \]  

\[ + g \cdot m \cdot k - 1. \]  

(32)

and similarly the function corresponding to the sequence \( f|_{x, \beta=(e \oplus 1)1} \) is \( h_1 \).

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

\[ C(a, b^*)(I) = C(b, a^*)(-I) = C(b, a^*)(I). \]

Thus

\[ C \left( f|_{x, \beta=e_0}, \tilde{f}^* |_{x, \beta=(e \oplus 1)0} \right)(I) = C \left( f|_{x, \beta=e_1}, \tilde{f}^* |_{x, \beta=(e \oplus 1)1} \right)(I) \]

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\(^8\) (which can be easily extended to any complementary set with even 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


\(^8\)Mutually orthogonal Golay complementary pairs were referred to as mates in their work.
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 $C_1$ and $C_2$ 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 $C_1$ and $C_2$, the abelian group structure of the intersection codes $C_1 \cap C_2$ 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 $F^n$ be the $n$-dimensional vector space of all $n$-tuples over the finite field $F = \mathbb{Z}_2$. The Hamming distance $d(v, s)$ between two vectors $v, s \in F^n$ is the number of coordinates in which $v$ and $s$ differ. A binary code $C$ of length $n$ is a nonempty subset of $F^n$. 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 $\epsilon = \lfloor \frac{d-1}{2} \rfloor$ and $C$ is called an $\epsilon$-error correcting code. Two binary codes $C_1$ and $C_2$ of length $n$ are isomorphic if there exists a coordinate permutation $\pi$ such that $C_2 = \{ \pi(c) \mid c \in C_1 \}$. They are equivalent if there exists a vector $a \in F^n$ and a coordinate permutation $\pi$ 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 $F^n$, with minimum distance $d = 3$, such that all the vectors in $F^n$ are within distance one from a codeword. For any $t \geq 1$ 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

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

0018-9448/$25.00 © 2008 IEEE