Identifying a Class of Multiple Shift Complementary Sequences in the Second Order Cosets of the First Order Reed-Muller Codes

Wen Chen
Department of Electrical and Computer Engineering
University of Alberta, Edmonton, AB, Canada, T6G 2V4
Email: wenchen@ece.ualberta.ca

Chintha Tellambura
Department of Electrical and Computer Engineering
University of Alberta, Edmonton, AB, Canada, T6G 2V4
Email: chintha@ece.ualberta.ca

Abstract—Multiple-shift complementary sequences (MCS), a generalized form of Golay complementary sequences, have recently been introduced to encode OFDM signals, allowing a better trade-off between the code rate and peak-to-mean envelope power ratio (PMEPR). However, a table of such sequences needs to be constructed by exhaustive search, a practically impossible task for a moderately large number of sub-carriers. As has been done for Golay complementary sequences and generalized Golay complementary sequences, this paper successfully identifies a class of MCS as the second order cosets of the first order Reed-Muller codes. We also present a new proof for the PMEPR of MCS.

I. INTRODUCTION

Orthogonal frequency division multiplexing (OFDM) provides excellent immunity to impulse noise and alleviates the need for equalizers, also enabling efficient hardware implementations using fast Fourier transform (FFT) algorithms. However, a major drawback is the high peak-to-mean envelope power ratio (PMEPR) of the OFDM signal. A number of PMEPR reduction techniques have been proposed including signal distortion techniques [1], [2], coding [3], [4], [5], [6], multiple signal representation [7], [8], [9], [10], modified signal constellation [11], pilot tone methods [12] and others.

An idea introduced in [13] and developed in [14] is to use the Golay complementary sequences [15] to encode OFDM signals with a PMEPR at most 2. Recently Davis and Jedwab [3] made further advances on this work and observed that the 2\textsuperscript{m}-ary Golay complementary sequences (GCS) of length 2\textsuperscript{n} can be obtained from certain second order cosets of the classical first order Reed-Muller code. As consequence of this intrinsic observation, Davis and Jedwab [4] were able to obtain, for a small number of carriers, a range of binary, quaternary and actuary OFDM codes with good error-correcting capabilities, efficient encoding and decoding, and a PMEPR at most 2. Since the code rate of GCS is prohibitively low for a moderate to large number of sub-carriers, a follow-up work done in [6] investigated the trade-offs between code rate and PMEPR using Generalized Golay complementary sequences [16].

Xin and Fair [17] have recently introduced another generalization of GCS called multiple-shift complementary sequences (MCS). The autocorrelation of a pair of MCS of length \( n \) sums to zero at delays which are multiples of a certain number \( L \) whereas the autocorrelation of a classical GSC pair sums to zero at all delays between 1 and \( n - 1 \). If \( L \) is set to 1, then MCS reduces to classical GSC. Clearly, any Golay sequence is a multiple-shift sequence, but the converse is not always true. Thus, there are more members of MCS than those of GCS. This translates to higher coding rate and reduced PMEPR [17]. While several properties and the PMEPR of MCS are discussed in [17], the sequences are generated by exhaustive computer search, a practically impossible task for even a moderately large number of sub-carriers. Therefore an algebraic method to construct a sufficient number of code-words is desirable. In this paper, we successfully identify a class of MCS in the second order cosets of the first order Reed-Muller codes and specify the trade-off between the code rate and PMEPR when MCS are used to encode OFDM signals. This identification enables finding distinct MCS. We prove the PMEPR of MCS and this proof immediately reveals how GCS, Generalized GCS and MCS are related.

For an \( M \)-ary phase shift keying, let \( \xi_M = \{ \xi^k : k \in \mathbb{Z}_M \} \), where \( \xi = \exp(2\pi j/M) \) and \( \mathbb{Z}_M = \{0, \ldots, M-1\} \). For a codeword \( c = (c_0, \ldots, c_{n-1}) \) with \( c_{\ell} \in \xi_M^{2^n} \), the \( n \) sub-carrier complex baseband OFDM signal may be represented as

\[
s_c(z) := \sum_{\ell=0}^{n-1} c_{\ell} z^\ell ,
\]

where \( z = e^{j2\pi t} \). The instantaneous power of the complex envelope \( s_c(z) \) is defined by

\[
P_c(z) := |s_c(z)|^2 .
\]

The peak-to-mean-power ratio (PMEPR) of codeword \( c \) is defined as

\[
PMEPR(c) := \frac{1}{n} \sup_{|z|=1} P_c(z) .
\]

II. PMEPR OF MCS

We next investigate the PMEPR of MCS and compare it with those of GCS and the generalized GCS. First we briefly review Golay sequences.
Two $\xi^{Z_M}$-sequences $a$ and $b$ of length $n$ are said to form a Golay complementary pair [15] if $P_a(z) + P_b(z) = 2n$. Each sequence $a$ or $b$ is called a Golay complementary sequence. It is easy to see $\text{PMEPR}(a) \leq 2$ if $a$ is a GSC. A generalization of Golay complementary pair, known as the Golay complementary set of element $N$ [16], $\{a^0, \ldots, a^{N-1}\}$, is defined by $P_{a^0}(z) + \cdots + P_{a^{N-1}}(z) = Nn$. Any $\xi^{Z_M}$-sequence $a_\ell$ in the complementary set is called an $N$-generalized GSC. Clearly, $\text{PMEPR}(a) \leq N$ if $a$ is an $N$-generalized GSC. In particular, a 2-generalized GSC is an ordinary GSC. Using the aperiodic auto-correlation function $R_a(\cdot)$ of a sequence $a \in \mathbb{C}^n$, defined by

$$R_a(\ell) := \begin{cases} \sum_{k=0}^{n-\ell-1}a_k\bar{a}_{k+\ell}, & \ell = 0, 1, \ldots, n-1, \\ 0, & \text{otherwise}, \end{cases}$$

where $\bar{z}$ is the complex conjugate of $z$, the Golay complementary set of $N$ can be alternatively defined by

$$R_{a^0}(\ell) + \cdots + R_{a^{n-1}}(\ell) = Nn\delta(\ell).$$

where the Dirac function $\delta(\ell)$ is defined by $\delta(0) = 1$ and $\delta(\ell) = 0$ for $\ell \neq 0$. Another generalization of GSCs is called multiple shift complementary sequences, first introduced in [17]. Their fundamental properties have been investigated in [17], but an explicit algebraic construction for them is unknown so far. We next identify a certain class of MCSs as second order cosets of the first order Reed-Muller codes.

**Definition 1:** Let $L$ be a positive integer. Two $\xi^{Z_M}$-sequence $a$ and $b$ of length $n$ are said to form a multiple shift complementary pair of $L$ (or $L$-shift complementary pair) if

$$R_a(\ell) + R_b(\ell) = 2n\delta(\ell), \quad \ell \mod L = 0. \quad (4)$$

$a$ or $b$ is called a multiple shift complementary sequence of $L$ (or an $L$-shift complementary sequence).

A 1-shift complementary sequence is a Golay complementary sequence. In the following, we present a new proof to show that the PMEPR of an $L$-shift complementary sequence is at most $2L$. While the PMEPR of MCSs has been discussed in [17], our new proof immediately reveals the relation between generalized Golay GCS and MCS.

**Theorem 1:** The PMEPR of an $L$-shift complementary sequence is at most $2L$.

**Proof:** Suppose that $a$ and $b$ form an $L$-shift complementary pair. Let $\zeta = \exp(j2\pi/L)$. For a $\xi^{Z_M}$-sequence $a = (a_0, a_1, \ldots, a_{n-1})$, define the sequences $a^u \in \mathbb{C}^n$ for $u = 0, 1, \ldots, L-1$ as

$$a^u = (a_0\zeta^{0u}, a_1\zeta^{1u}, a_2\zeta^{2u}, \ldots, a_{n-1}\zeta^{(n-1)u}).$$

Then $a = a^0$ and

$$\sum_{u=0}^{L-1}P_{a^u}(z) = \sum_{u=0}^{L-1} \sum_{k=0}^{n-1} a_k \bar{a}_{k+\ell} \zeta^{\ell u} = \left| \sum_{u=0}^{L-1} \sum_{k=0}^{n-1} a_k \bar{a}_{k+\ell} \zeta^{\ell u} \right|^2 = \left( \sum_{u=0}^{L-1} \sum_{k=0}^{n-1} R_a(\ell) \zeta^{\ell u} + \bar{R}_a(\ell) \zeta^{-\ell u} \right)^2.$$

where $\bar{R}(\cdot)$ is the real part of a complex number. Since

$$\sum_{u=0}^{L-1} \sum_{k=0}^{n-1} R_a(\ell) \zeta^{\ell u} = \{ L, \ell \mod L = 0, 0, \text{otherwise}, $$

follows that

$$\sum_{u=0}^{L-1} P_{a^u}(z) = L + 2L \Re \left( \sum_{u=0}^{L-1} \sum_{k=0}^{n-1} R_a(\ell) \zeta^{\ell u} \right).$$

Similarly, for a $\xi^{Z_M}$-sequence $b = (b_0, b_1, \ldots, b_{n-1})$, we can define

$$b^u = (b_0\zeta^{0u}, b_1\zeta^{1u}, b_2\zeta^{2u}, \ldots, b_{n-1}\zeta^{(n-1)u})$$

for $u = 0, \ldots, L-1$, and show that

$$\sum_{u=0}^{L-1} P_{b^u}(z) = L + 2L \Re \left( \sum_{u=0}^{L-1} \sum_{k=0}^{n-1} R_b(\ell) \zeta^{\ell u} \right).$$

Since $a$ and $b$ form an $L$-shift complementary pair, these yield

$$\sum_{u=0}^{L-1} [P_{a^u}(z) + P_{b^u}(z)] = 2L.$$
being a Boolean function \( f : (y_1, \cdots, y_m) \to y \). Consider the \( 2^m \) monomials
\[
1, x_1, \ldots, x_m, x_1 x_2, x_1 x_3, \ldots, x_{m-1} x_m, \ldots, x_1 \cdots x_m.
\]
Then any Boolean function \( f \) can be uniquely expressed as a linear combination over \( \mathbb{Z}_M \) of these monomials. Let \( i = \sum_{\ell=1}^m i_\ell 2^{m-\ell} \) be the binary expression of a number \( i \in \mathbb{Z}_{2^m} \). For a Boolean function \( f \), define a sequence \( f \) of length \( 2^m \) by abusing the symbol \( f \), such that the \( i \)th component of \( f \) is \( f(i_1, \ldots, i_m) \).

The \( r \)-th order Reed-Muller code \( \text{RM}_M(r, m) \) of length \( 2^m \) is generated by the monomials \( x_i \) of degree at most \( r \). Alternatively, \( \text{RM}_M(r, m) \) is the linear code over \( \mathbb{Z}_M \) whose generator matrix is identical to that of binary Reed-Muller code \( \text{RM}_2(r, m) \). The number of monomials in the \( x_i \), of degree \( \ell \), is \( \binom{m}{\ell} \), so \( \text{RM}_M(r, m) \) contains \( M^r \) codewords. As an advantage of Reed-Muller code, the minimum Hamming distance of \( \text{RM}_M(r, m) \) is \( 2^m-r \).

In addition, for a codeword \( c \in \text{RM}_M(2, m) \), \( c + \text{RM}_M(1, m) \) is called a second order coset of the first order Reed-Muller code \( \text{RM}_M(1, m) \).

Now we are going to identify a class of \( L \)-shift complementary sequences of length \( 2^m \) in the second order cosets of the first order Reed-Muller code. Consider the case \( L = 2^d \) for some integers \( d \geq 0 \). Define the quadratic form
\[
\begin{align*}
 f(x_1, \ldots, x_m) & := \frac{M}{2} \sum_{k=1}^{m-d} x_{\pi(k)} x_{\pi(k+1)} \\
 & + \sum_{k=1}^{m} \sum_{k \neq \ell}^{m} c_{k, \ell} x_k x_\ell \\
 & + \sum_{\ell=1}^{m} c_{\ell} x_\ell,
\end{align*}
\]
where \( \pi \) is the permutation of the set \( \{1, 2, \ldots, m-d\} \) and \( c_{k, \ell}, c_\ell \in \mathbb{Z}_M \). Then we have the following identification theorem.

**Theorem 2:** Suppose that the sequences \( a, b \) over \( \mathbb{Z}_M \) are defined by
\[
\begin{align*}
a(x_1, \cdots, x_m) & := f(x_1, \cdots, x_m) + c, \\
b(x_1, \cdots, x_m) & := f(x_1, \cdots, x_m) + 2^{b-1} x_{\pi(1)} + c',
\end{align*}
\]
Then the \( \xi^{2^d} \)-sequences \( \xi^a \) and \( \xi^b \) form a \( 2^d \)-shift complementary pair of length \( 2^m \) for any \( c, c' \in \mathbb{Z}_M \).

Proof: Consider \( m > 1 \) since it degenerates to the trivial case of GCS for \( m = 1 \). For a given \( x \in \mathbb{Z}_m \), let \( y = x + u \) for some \( u \neq 0 \) and \( u \mod 2^d = 0 \). Suppose that the binary representation of \( x \) and \( y \) are \( (x_1, \cdots, x_m) \) and \( (y_1, \cdots, x_m) \) respectively. Then
\[
b_x - a_x = \frac{M}{2} x_{\pi(1)} + c' - c.
\]
We now discuss (5) for two cases.

**Case 1:** \( y_{\pi(1)} \neq x_{\pi(1)} \). Then
\[
(a_x - a_y) - (b_x - b_y) = \frac{M}{2} (y_{\pi(1)} - x_{\pi(1)}) = \frac{M}{2}.
\]
Recall \( \xi = \exp(2\pi j/M) \), this implies
\[
\xi^{a_x-a_y} / \xi^{b_x-b_y} = \xi^{M/2} = -1.
\]
Therefore \( \xi^{a_x-a_y} + \xi^{b_x-b_y} = 0 \), which obviously implies that \( R_a(u) + R_b(u) = 0 \). Therefore \( \xi^a \) and \( \xi^b \) form a \( 2^d \)-shift complementary sequence pair.

**Case 2:** \( y_{\pi(1)} = x_{\pi(1)} \). Since \( y \neq x \), there is some \( \ell \in \{1, \cdots, m-d\} \) such that \( y_\ell \neq x_\ell \). Since \( \pi \) is the permutation of \( \{1, \cdots, m-d\} \), we can assume that \( \ell \) is the smallest integer for which \( x_{\pi(\ell)} \neq y_{\pi(\ell)} \). Let \( x' \) be the integer whose binary representation
\[
(x_1, x_2, \cdots, 1 - x_{\pi(\ell)-1}, \cdots, x_{m-d+1}, \cdots, x_m)
\]
differs from that of \( x \) only in \( \pi(v-1) \)th coordinate. Similarly define \( y' \) to have the binary representation
\[
(y_1, y_2, \cdots, 1 - y_{\pi(v)-1}, \cdots, y_{m-d+1}, \cdots, y_m).
\]
So \( y' = x' + u \) due to \( x_{\pi(v)} = y_{\pi(v)} \). By the definition of the quadratic form \( f \), we have
\[
f_{x'} - f_x = \frac{M}{2} x_{\pi(v-2)} + \frac{M}{2} x_{\pi(v)} + d_{\pi(v)} - 2x_{\pi(v)} - 1 \sum_{\ell=m-d+1}^{m} c_{\pi(v-1)} x_{\pi(1)}
\]
Since \( y \mod 2^d = x \), we have \( x_\ell = y_\ell \) for \( \ell = m-d+1, \ldots, m \). Since \( x_{\pi(v)} = y_{\pi(v)} \), and \( x_{\pi(1)} \neq y_{\pi(1)} \), we obtain
\[
(a_x - a_y) - (a_{x'} - a_{y'}) = \frac{M}{2}.
\]
This together with (5) implies that
\[
(b_x - b_y) - (b_{x'} - b_{y'}) = (a_x - a_y) - (a_{x'} - a_{y'}) = \frac{M}{2}.
\]
Then
\[
\xi^{b_x-b_y} / \xi^{b_{x'}-b_{y'}} = \xi^{a_x-a_y} / \xi^{a_{x'}-a_{y'}} = -1,
\]
which implies that
\[
\xi^{a_x-a_y} + \xi^{a_{x'}-a_{y'}} = 0 = \xi^{b_x-b_y} + \xi^{b_{x'}-b_{y'}}.
\]
Therefore,
\[
R_a(u) + R_b(u) = 0,
\]
which completes the proof.

Using Theorem 2, we identify \( \frac{(m-d)!M}{2^m} d(m-d) + (d-1)/2 + m+1 \) numbers of \( 2^d \)-shift complementary sequences in the second order cosets of first order Reed-Muller codes. Therefore the resulting code rate is
\[
\frac{d(m-d) + [d(d-1)/2] + m + 1}{2^m log_2 M}.
\]
Fig. 1 shows the code rate versus PMEPR for these identified MCS for \( n = 16 \). Since these sequences constitute a subset of the second order Reed-Muller code \( \text{RM}_M(2, m) \), their code rate is lower than that of second order Reed-Muller codes.
Theorem 2 guarantee that the minimum Hamming distance is not guaranteed for larger sets of MCS.

Thus it may be possible to find high-coding-rate schemes using MCS. Note however that the sequences in Theorem 2. Thus it may be possible to find high-coding-rate schemes using MCS. There are many more MCS than those are identified in Theorem 2.

Fig. 1 compares this class of MCS and MCS found by exhaustive computer search. There are many more MCS than those are identified in Theorem 2. Thus it may be possible to construct an encoding scheme of high code rate using MCS. But such an encoding scheme may not guarantee that the minimum Hamming distance is $2^{m-2}$, a guarantee which may not hold for larger sets of MCS.

IV. CONCLUSION

In this paper, we have shown that the PMEPR of an L-shift complementary sequence is at most 2L. This suggests a relationship between MCS and generalized GCS. An M-ary L-shift complementary sequence is a 2L-generalized Golay complementary sequence if $M \mod L = 0$. GSC and generalized GSC both have intimate links to Reed-Muller codes [6]; similarly, this paper identifies a class of MCS as second order cosets of the classical first order Reed-Muller code.

The trade-off between the code rate and PMEPR for this class of MCS has been determined. Simulation results show that there are many more MCS than those are identified in Theorem 2. Thus it may be possible to construct an encoding scheme of high code rate using MCS. But such an encoding scheme may not guarantee that the minimum Hamming distance is $2^{m-2}$.

REFERENCES