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^h-ary Golay complementary sequences (GCS) of length 2^m 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 codewords 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 $\xi^{\mathbb{Z}_M} = \{\xi^k : k \in \mathbb{Z}_M\}$, where $\xi = \exp(2\pi j/M)$ and $\mathbb{Z}_M = \{0, \cdots, M-1\}$. For a codeword $c = (c_0, \ldots, c_{n-1})$ with $c_\ell \in \xi^{\mathbb{Z}_M}$, the n sub-carrier complex baseband OFDM signal may be represented as

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

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

$$P_c(z) := |s_c(z)|^2. \tag{2}$$

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

$$\mathrm{PMEPR}(c) := \frac{1}{n} \sup_{|z|=1} P_c(z). \tag{3}$$

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 $\xi^{\mathbb{Z}_M}$-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 $\mathrm{PMEPR}(a) \leq 2$ if a is a GSC. A generalization of Golay complementary pair, known as the *Golay complementary set* of element N [16], $\{a^0, \cdots, a^{N-1}\}$, is defined by $P_{a^0}(z) + \cdots + P_{a^{N-1}}(z) = Nn$. Any $\xi^{\mathbb{Z}_M}$-sequence a_ℓ in the complementary set is called an N*-generalized GSC*. Clearly, $\mathrm{PMEPR}(a) \leq N$ 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

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

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 GCSs 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 $\xi^{\mathbb{Z}_M}$-sequence a and b of length n are said to form a *multiple shift complementary pair* of L (or L-shift complementary pair) if

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

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 $\xi^{\mathbb{Z}_M}$-sequence $a = (a_0, a_1, \cdots, a_{n-1})$, define the sequences $a^u \in \mathbb{C}^n$ for $u = 0, 1, \ldots, L-1$ as

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

Then $a = a^0$ and

$$\begin{aligned} \sum_{u=0}^{L-1} P_{a^u}(z) &= \sum_{u=0}^{L-1} \left| \sum_{k=0}^{n-1} a_k \zeta^{ku} z^k \right|^2 \\ &= \sum_{u=0}^{L-1} \left(n + \sum_{\ell=0}^{N-1} R_a(\ell)\zeta^{u\ell}z^\ell + \bar{R}_a(\ell)\zeta^{-u\ell}z^{-\ell} \right) \\ &= Ln + 2\Re\left(\sum_{\ell=0}^{n-1} R_a(z) z^\ell \sum_{u=0}^{L-1} \zeta^{u\ell} \right), \end{aligned}$$

where $\Re(\cdot)$ is the real part of a complex number. Since

$$\sum_{u=0}^{L-1} \zeta^{u\ell} = \begin{cases} L, & \ell \mod L = 0, \\ 0, & \text{otherwise}, \end{cases}$$

follows that

$$\sum_{u=1}^{L-1} P_{a^u}(z) = Ln + 2L\Re\left(\sum_{\ell \mod L = 0, \ell \neq 0} R_a(\ell) z^\ell \right).$$

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

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

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

$$\sum_{u=0}^{L-1} P_{b^u}(z) = Ln + 2L\Re\left(\sum_{\ell=0 \mod L, \ell \neq 0} R_b(\ell) z^\ell \right).$$

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

$$\sum_{u=0}^{L-1} [P_{a^u}(z) + P_{b^u}(z)] = 2Ln.$$

It shows that $\mathrm{PMEPR}(a) \leq 2L$ and hence completes the proof. ■

The argument in the proof shows that $\{a^0, \cdot, a^{L-1}, b^0, \cdots, b^{L-1}\}$ is a Golay complementary set if $\zeta \in \xi^{\mathbb{Z}_M}$, that is,

$$M \mod L = 0.$$

For an example, a 2-shift complementary binary sequence is a 4-generalized Golay complementary sequence. Therefore the L-shift complementary sequences constitute a subset of the N-generalized GCS if $M \mod L = 0$. But this result may not hold generally.

III. Encoding of MCS

We next identify a class of MCS in the second order cosets of the first order Reed-Muller code. We also investigate the trade-off between the code rate and PMEPR when MCS are used to encode OFDM signals. We use the frameworks of Boolean functions and Reed-Muller code in our discussion [18].

A *Boolean function* is a mapping f from $\mathbb{Z}_2^m$ to $\mathbb{Z}_M$. For any $x = (x_1, \ldots, x_m) \in \mathbb{Z}_2^m$, we regard each variable x_i as itself being a Boolean function $x_i : (y_1, \cdots, y_m) \to y_i$. Consider the 2^m monomials

$$1, x_1, \ldots, x_m, x_1x_2, x_1x_3, \cdots, x_{m-1}x_m, \cdots, x_1 \cdots x_m.$$

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 ith coordinate of f is $f(i_1, \ldots, i_m)$.

The r-th order *Reed-Muller code* $\mathrm{RM}_M(r, m)$ of length 2^m is generated by the monomials in Boolean functions x_i of degree at most r. Alternatively, $\mathrm{RM}_M(r, m)$ is the linear code over $\mathbb{Z}_M$ whose generator matrix is identical to that of binary Reed-Muller code $\mathrm{RM}_2(r, m)$. The number of monomial in the x_i of degree ℓ is $\binom{m}{\ell}$, so $\mathrm{RM}_M(r, m)$ contains $M^{\sum_{\ell=0}^{r}\binom{m}{\ell}}$ codewords. As an advantage of Reed-Muller code, the minimum Hamming distance of $\mathrm{RM}_M(r, m)$ is 2^{m-r}. In addition, for a codeword $c \in \mathrm{RM}_M(2, m)$, $c + \mathrm{RM}_M(1, m)$ is called a second order coset of the first order Reed-Muller code $\mathrm{RM}_M(1, m)$.

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-Muler code. Consider the case $L = 2^d$ for some integers $d \geq 0$. Define the quadratic form

$$\begin{aligned} f(x_1, \ldots, x_m) : \;=\; & \frac{M}{2} \sum_{k=1}^{m-d} x_{\pi(k)} x_{\pi(k+1)} \\ & + \sum_{k=1, k\neq \ell}^{m} \sum_{\ell=m-d+1}^{m} c_{k,\ell} x_k x_\ell \\ & + \sum_{\ell=1}^{m} c_\ell x_\ell. \end{aligned}$$

where π 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 and b over $\mathbb{Z}_M$ are defined by

$$\begin{aligned} a(x_1, \cdots, x_m) &:= f(x_1, \cdots, x_m) + c, \\ b(x_1, \cdots, x_m) &:= f(x_1, \cdots, x_m) + 2^{h-1} x_{\pi(1)} + c'. \end{aligned}$$

Then the $\xi^{\mathbb{Z}_M}$-sequences ξ^a and ξ^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 $x \in \mathbb{Z}_n$, 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

$$b_x - a_x = \frac{M}{2} x_{\pi(1)} + c' - c. \tag{5}$$

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 ξ^a and ξ^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 π is the permutation of $\{1, \cdots, m-d\}$, we can assume that v is the smallest integer for which $x_{\pi(v)} \neq y_{\pi(v)}$. Let x' be the integer whose binary representation

$$(x_1, x_2, \cdots, 1 - x_{\pi(v-1)}, \cdots, x_{m-d+1}, \cdots, x_m)$$

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 $x_{\pi(v-1)} = y_{\pi(v-1)}$. By the definition of the quadratic form f, we have

$$\begin{aligned} f_{x'} - f_x \;=\; & \frac{M}{2} x_{\pi(v-2)} + \frac{M}{2} x_{\pi(v)} + d_{\pi(v-1)}(1 - 2x_{\pi(v-1)}) \\ & + \sum_{\ell=m-d+1}^{m} c_{\pi(v-1),\ell} x_{\pi(v-1)} x_\ell (1 - 2x_{\pi(v-1)}). \end{aligned}$$

Since $y \mod 2^d = x$, we have $x_\ell = y_\ell$ for $\ell = m-d+1, \ldots, m$. Since $x_{\pi(v-1)} = y_{\pi(v-1)}$, and $x_{\pi(v)} \neq y_{\pi(v)}$, 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 $\frac{(m-d)!}{2} M^{d(m-d)+d(d-1)/2+m+1}$ numbers of 2^d-shift complementary sequences in the second order cosets of first order Reed-Muller codes. Therefore the resulting code rate is

$$\frac{d(m-d) + \lfloor d(d-1)/2 \rfloor + m + 1}{2^m} + \frac{\lfloor \log_2 (m-d)! - 1 \rfloor}{2^m \log_2 M}.$$

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 $\mathrm{RM}_M(2, m)$, their code rate is lower than that of second order Reed-Muller codes.

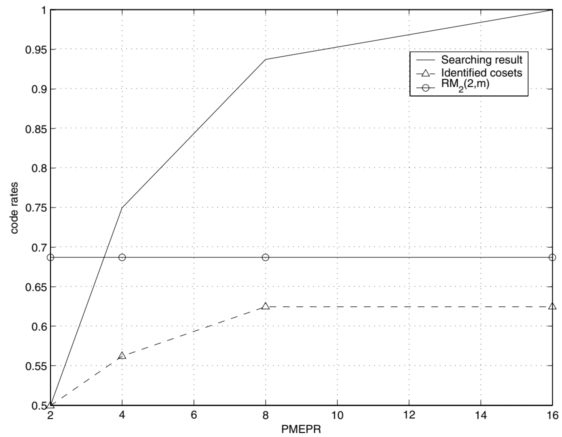

Fig. 1. The code rates of MCS found by computer search, the second order Reed-Muller code and MCS identified in Theorem 2 versus the PMEPR for $n = 16$.

Fig. 1 compares this class of MCS and MCS found by exhaustive computer search. There are many more MCS than found by Theorem 2. Thus it may be possible to find high-coding-rate schemes using MCS. Note however that the sequences in Theorem 2 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

[1] H. Ochiai and H. Imai, "On the clipping for peak power reduction of OFDM signals," in *IEEE GLOBECOM*. San Francisco, USA: IEEE, 2000, pp. 731–735.

[2] W. G. Jeon, K. H. Chang, and Y. S. Cho., "An adaptive data predistorter for compensation of nonlinear distortion in OFDM systems." *IEEE Trans. Commun.*, vol. 45, no. 10, pp. 1167–1171, Oct. 1997.

[3] J. A. Davis and J. Jedwab, "Peak-to-mean power control and error correction for OFDM transmission using Golay sequences and Reed-Muller codes," *IEE Elect. Lett.*, vol. 33, no. 4, pp. 267–268, Feb. 1997.

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

[5] K. G. Paterson and V. Tarokh, "On the existence and construction of good codes with low peak-to-average power ratio," *IEEE Trans. Inform. Theory*, vol. 46, no. 6, pp. 1974–1987, Sept. 2000.

[6] K. G. Paterson, "Generalized Reed-Muller codes and power control in OFDM modulation," *IEEE Trans. Inform. Theory*, vol. 46, no. 1, pp. 104–120, Jan. 2000.

[7] H. Breiling, S. H. Muller-Weinfurtner, and J. B. Huber, "SLM peak-power reduction without explicit side information," *IEEE Commun. Lett.*, vol. 5, no. 6, pp. 239–241, 2001.

[8] R. W. Bauml, R. F. H. Fischer, and J. B. Huber, "Reducing the peak-to-average power ratio of multicarrier modulation by selected mapping," *IEE Elect. Lett.*, vol. 32, no. 22, pp. 2056–2057, Oct. 1996.

[9] G. Hill, M. Faulkner, and J. Singh, "Cyclic shifting and time inversion of partial transmit sequences to reduce the peak-to-average power ratio in OFDM," in *IEEE PIMRC*, vol. 2. Piscataway, NJ, USA.: IEEE, 2000, pp. 1256–1259, conference Paper.

[10] P. V. Eetvelt, G. Wade, and M. Thompson, "Peak to average power reduction for OFDM schemes by selected scrambling," *IEE Elect. Lett.*, vol. 32, no. 21, pp. 1963–1964, Oct. 1996.

[11] P. K. Frenger and N. A. B. Sevensson, "Parallel combinatory OFDM signalling," *IEEE Trans. Commun.*, vol. 47, no. 4, pp. 558–567, Apr. 1999.

[12] J. Tellado and J. M. Cioffi, "PAR reduction in multicarrier transmission systems," Stanford University," Technical Report, 1998.

[13] S. Boyd, "Multitone signals with low crest factors," *IEEE Trans. Circuits Syst.*, vol. CAS-33, no. 10, pp. 1018–1022, Oct 1986.

[14] B. M. Popovic, "Synthesis of power efficient multitone signals with flat amplitude spectrum," *IEEE Trans. Commun.*, vol. 39, pp. 1031–1033, July 1991.

[15] M. J. E. Golay, "Complementary series," *IRE. Trans. Inform. Theory*, vol. IT-7, pp. 82–87, Apr. 1961.

[16] C. Tseng and C. Liu, "Complementary sets of sequences," *IEEE Trans. Inform. Theory.*, vol. 18, no. 5, pp. 644–652, Sept. 1972.

[17] Y. Xin and I. J. Fair, "Multiple-shift complementary sequences and their peak-to-average power ratio values," in *IEEE ISIT*, July 2004.

[18] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting codes, Part II*. North-Holland Publishing Company, 1977.