A Good Trade-Off Performance between the Code Rate and PMEPR for OFDM Signals Using Generalized Rudin-Shapiro Polynomials

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*— Generalized Golay complementary sequences and multiple-shift complementary sequences have recently been introduced to encode orthogonal frequency division multiplexing (OFDM) signals, reducing the peak-to-mean envelope power ratio (PMEPR). Certain classes of these complementary sequences have been identified as a subset of second order cosets of the first order Reed-Muller codes. Since the code rates of these encoding schemes are prohibitively low for a large number of sub-carriers, it is necessary to find an efficient algebraic way to produce sufficient number of codewords such that the code rate of the encoding scheme is high enough. In this paper, we introduce generalized Rudin-Shapiro polynomials, a subset generalized Golay complementary sequences, to encode OFDM signals. In our encoding scheme, a matrix equation recursively produces a sufficient number of Rudin-Shapiro polynomials such that the code rate increases linearly with respect to the PMEPR. Therefore, it offers an excellent trade-off performance between the code rate and the PMEPR.**

I. Introduction

Orthogonal frequency division multiplexing (OFDM) eliminates the need for complex equalizers in wide-band fading channels, while efficient hardware implementations can be realized using fast Fourier transform (FFT). However, a major drawback of OFDM signals is the high peak-to-mean envelope power ratio (PMEPR) of the uncoded OFDM signal. Many PMEPR reduction techniques include 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.

Golay complementary sequences (GCS) [13] are used with multi-carrier signals in [14] and their PMEPR is established in [15]. Encoding OFDM signals with GCS provides a PMEPR at most 2. Recently Davis and Jedwab [3] observed that the 2^h-ary GCS of length 2^m can be obtained from certain second order cosets of the classical first order Reed-Muller code. As a result, Davis and Jedwab [4] derived an explicit algebraic construction for some GCS.

A follow-up work done in [6] investigated the trade-offs between code rate and PMEPR by using Generalized GCS [16], in which a class of generalized GCS is identified in the second order cosets of the first order Reed-Muller code. Multiple-shift complementary sequence [17] has also been introduced to encode OFDM signals, by which the code rate substantially increases. However, an enccoding scheme based on multiple-shift complementary sequences requires a code book generated by exhaustive computer search, which is extremely impossible for a large number of sub-carriers. As has been done for GCS and the generalized GCS, a class of multiple-shift complementary sequences has recently been identified in the second order cosets of the first order Reed-Muller code by the authors [18]. Since the code rate of the second order Reed-Muller code is low for a moderately large number of sub-carriers, it is necessary to find an efficient algebraic way to produce sufficient number of codewords ensuring a high code rate.

In this paper, we introduce generalized Rudin-Shapiro Polynomials [19] and show that they constitute a subset of generalized GCS, from which the PMEPR of generalized Rudin-Shapiro Polynomials immediately follows. We introduce an encoding scheme for OFDM signals using these polynomials. In our encoding scheme, a sufficient number of generalized Rudin-Shapiro polynomials is recursively produced by a matrix formula so that the code rate increases linearly with respect to the PMEPR. Therefore, it offers an excellent trade-off performance between the code rate and the PMEPR.

A. OFDM and PMEPR

Let j be the imaginary unit, i.e., $j^2 = -1$. For an M-ary phase modulation OFDM, 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 subcarrier complex baseband OFDM signal can be mathematically simplified 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

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

0-7803-8938-7/05/$20.00 (C) 2005 IEEE

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

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

II. Generalized Rudin-Shapiro Polynomials and PMEPR

In this section, we introduce generalized Rudin-Shapiro Polynomials, and show that they constitute a subset of generalized GCS. We first review GCS and generalized GCS.

A. GCS and generalized GCS

Two $\xi^{\mathbb{Z}_M}$-sequences a and b of length n is said to form a *Golay complementary pair* [13] if

$$P_a(z) + P_b(z) = 2n.$$

Each sequence a or b are called a *Golay complementary sequence*. It is easy to see $\mathrm{PMEPR}(a) \leq 2$ if a is a Golay complementary sequence. 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 Golay complementary sequence*. Clearly, $\mathrm{PMEPR}(a) \leq N$ if a is a N-generalized Golay complementary sequence. In particular, a 2-generalized Golay complementary sequence is a Golay complementary sequence.

B. Generalized Rudin-Shapiro polynomials

We first introduce the classical Rudin-Shapiro polynomials [20], which have already been used to construct encoding and decoding schemes for OFDM [21].

1) Rudin-Shapiro polynomials: For a $k \geq 0$, a Rudin-Shapiro polynomial pair $(A(z), B(z))$ is recursively defined as

$$\begin{cases} A_{k+1}(z) = A_k(z) + \xi_k z^{2^k} B_k(z), \\ B_{k+1}(z) = A_k(z) - \xi_k z^{2^k} B_k(z), \end{cases} \qquad (4)$$

where $A_0(z) = B_0(z) = 1$ and ξ_k is an element in $\xi^{\mathbb{Z}_M}$. Formula (4) recursively produces the polynomials $A_k(z)$ and $B_k(z)$ for any $k > 0$. For examples, for $k = 1, 2, 3$, one has

$$\begin{cases} A_1(z) = 1 + \xi_0 z, \\ B_1(z) = 1 - \xi_0 z. \end{cases}$$
$$\begin{cases} A_2(z) = 1 + \xi_0 z + \xi_1 z^2 - \xi_1\xi_0 z^3, \\ B_2(z) = 1 + \xi_0 z - \xi_1 z^2 + \xi_1\xi_0 z^3. \end{cases}$$
$$\begin{cases} A_3(z) = & 1 + \xi_0 z + \xi_1 z^2 - \xi_1\xi_0 z^3 \\ & +\xi_2 z^4 + \xi_2\xi_0 z^5 - \xi_2\xi_1 z^6 + \xi_2\xi_1\xi_0 z^7, \\ B_3(z) = & 1 + \xi_0 z + \xi_1 z^2 - \xi_1\xi_0 z^3 \\ & +\xi_2 z^4 - \xi_2\xi_0 z^5 + \xi_2\xi_1 z^6 - \xi_2\xi_1\xi_0 z^7. \end{cases}$$

In general, for $n = 2^m$, let the sequences a and b be respectively the coefficients of the polynomials $A_m(z)$ and $B_m(z)$. The 2^m-subcarrier OFDM signals are $s_a(z) = A_m(z)$ and $s_b(z) = B_m(z)$. For example, for $m = 3$, we have $n = 8$ and the codewords

$$\begin{cases} a = (1 \;\; \xi_0 \;\; \xi_1 \;\; -\xi_1\xi_0 \;\; \xi_2 \;\; \xi_2\xi_0 \;\; -\xi_2\xi_1 \;\; \xi_2\xi_1\xi_0), \\ b = (1 \;\; \xi_0 \;\; \xi_1 \;\; -\xi_1\xi_0 \;\; \xi_2 \;\; -\xi_2\xi_0 \;\; \xi_2\xi_1 \;\; -\xi_2\xi_1\xi_0). \end{cases}$$

2) PMEPR of a Rudin-Shapiro polynomial: From (4), it is clear that

$$P_a(z) + P_b(z) = |s_a(z)|^2 + |s_b(z)|^2 = |A_m(z)|^2 + |B_m(z)|^2$$

Noting $|A_m(z)|^2 + |B_m(z)|^2 = 2\left[|A_{m-1}(z)|^2 + |B_{m-1}(z)|^2\right]$ and repeating the process, we have

$$P_a(z) + P_b(z) = 2^m\left[|A_0(z)|^2 + |B_0(z)|^2\right] = 2n.$$

This shows that a and b form a Golay complementary pair. Therefore, Rudin-Shapiro polynomials constitute a subset of GCS. Hence the PMEPR of a Rudin-Shapiro polynomial is at most 2.

3) Generalized Rudin-Shapiro Polynomials: Alternatively, we can re-write the formula (4) in matrix form as

$$\mathbf{A}^2_{k+1}(z) = \mathbf{T}^2_k \mathbf{B}^2_k(z),$$

where

$$\mathbf{A}^2_k(z) = \begin{pmatrix} A_k(z) \\ B_k(z) \end{pmatrix}, \; \mathbf{B}^2_k(z) = \begin{pmatrix} A_k(z) \\ z^{2^k} B_k(z) \end{pmatrix}, \; \mathbf{T}^2_k = \begin{pmatrix} 1 & \xi_k \\ 1 & -\xi_k \end{pmatrix}.$$

This immediately suggests an extension of Rudin-Shapiro polynomial [19]. Let $\theta = \exp(j2\pi/N)$. Extend $\mathbf{A}^2_k(z)$, $\mathbf{B}^2_k(z)$ and $\mathbf{T}^2_k$ respectively to $\mathbf{A}^N_k(z)$, $\mathbf{B}^N_k(z)$ and $\mathbf{T}^N_k$ for $N \geq 2$, as

$$\mathbf{A}^N_k(z) = \begin{pmatrix} A^0_k(z) \\ A^1_k(z) \\ \vdots \\ A^{N-1}_k(z) \end{pmatrix}, \; \mathbf{B}^N_k(z) = \begin{pmatrix} A^0_k(z) \\ z^{N^k} A^1_k(z) \\ \vdots \\ z^{(N-1)N^k} A^{N-1}_k(z) \end{pmatrix},$$

$$\mathbf{T}^N_k = \begin{pmatrix} 1 & \xi^1_k & \xi^2_k & \cdots & \xi^{N-1}_k \\ 1 & \theta\xi^1_k & \theta^2\xi^2_k & \cdots & \theta^{N-1}\xi^{N-1}_k \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \theta^{N-1}\xi^1_k & \theta^{2(N-1)}\xi^2_k & \cdots & \theta^{(N-1)(N-1)}\xi^{N-1}_k \end{pmatrix},$$

where $A^0_0 = \cdots = A^{N-1}_0 = 1$ and $\xi^1_k, \ldots, \xi^{N-1}_k$ are uniform random variables that have equal possibility to take the elements in $\xi^{\mathbb{Z}_M}$. Then generalized Rudin-Shapiro polynomials are defined as

$$\mathbf{A}^N_{k+1}(z) = \mathbf{T}^N_k \mathbf{B}^N_k(z). \qquad (5)$$

Clearly, this degenerates to ordinary Rudin-Shapiro Polynomial if $N = 2$. We are interested in the case $N > 2$. For example, for $N = 3$, we have $\theta = e^{j2\pi/3}$ and

$$\begin{pmatrix} A^0_{k+1}(z) \\ A^1_{k+1}(z) \\ A^2_{k+1}(z) \end{pmatrix} = \begin{pmatrix} 1 & \xi^1_k & \xi^2_k \\ 1 & \theta\xi^1_k & \theta^2\xi^2_k \\ 1 & \theta^2\xi^1_k & \theta^4\xi^2_k \end{pmatrix} \begin{pmatrix} A^0_k(z) \\ z^{3^k} A^1_k(z) \\ z^{2\cdot 3^k} A^2_k(z) \end{pmatrix}.$$

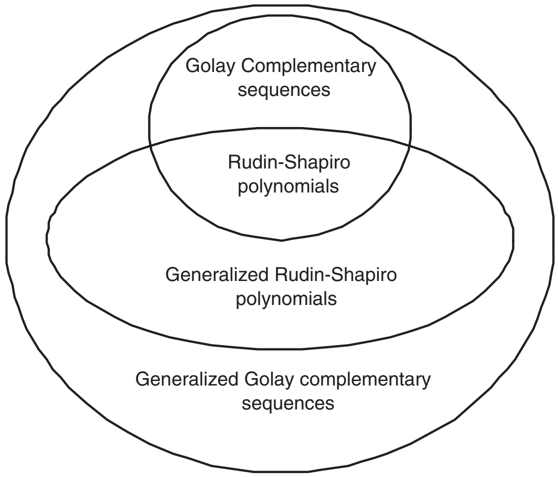
Golay Complementary sequences
Rudin-Shapiro polynomials
Generalized Rudin-Shapiro polynomials
Generalized Golay complementary sequences

Fig. 1. The relationship among GCS, generalized GCS, Rudin-Shapiro polynomials and generalized Rufin-Shapiro polynomials.

For $k = 1, 2$, that is

$$\begin{cases} A_1^0(z) = 1 + \xi_0^1 z + \xi_0^2 z^2, \\ A_1^1(z) = 1 + \theta\xi_0^1 z + \theta^2\xi_0^2 z^2, \\ A_1^2(z) = 1 + \theta^2\xi_0^1 z + \theta^4\xi_0^2 z^2. \end{cases}$$

$$\begin{cases} A_2^0(z) = & 1 + \xi_0^1 z + \xi_0^2 z^2 + \xi_1^1 z^3 + \theta\xi_1^1\xi_0^1 z^4 \\ & +\theta^2\xi_1^1\xi_0^2 z^5 + \xi_1^2 z^6 + \theta^2\xi_1^2\xi_0^1 z^7 + \theta^4\xi_1^2\xi_0^2 z^8, \\ A_2^1(z) = & 1 + \xi_0^1 z + \xi_0^2 z^2 + \theta\xi_1^1 z^3 + \theta^2\xi_1^1\xi_0^1 z^4 \\ & +\theta^3\xi_1^1\xi_0^2 z^5 + \theta^2\xi_1^2 z^6 + \theta^4\xi_1^2\xi_0^1 z^7 + \theta^6\xi_1^2\xi_0^2 z^8, \\ A_2^2(z) = & 1 + \xi_0^1 z + \xi_0^2 z^2 + \theta^2\xi_1^1 z^3 + \theta^3\xi_1^1\xi_0^1 z^4 \\ & +\theta^4\xi_1^1\xi_0^2 z^5 + \theta^4\xi_1^2 z^6 + \theta^6\xi_1^2\xi_0^1 z^7 + \theta^8\xi_1^2\xi_0^2 z^8. \end{cases}$$

For $n = N^m$, let the sequences a^k be the coefficients of the polynomial $A_m^k(z)$ for $0 \le k \le N-1$ respectively. Then the 2^m-subcarrier OFDM signals are $s_{a^k}(z) = A_m^k(z)$ for $0 \le k \le N-1$. For example, for $N = 3$, $m = 2$, we have $n = 9$ and the codewords

$$\begin{cases} a^0 = (1 \;\; \xi_0^1 \;\; \xi_0^2 \;\; \xi_1^1 \;\; \theta\xi_1^1\xi_0^1 \;\; \theta^2\xi_1^1\xi_0^2 \;\; \xi_1^2 z^6 \;\; \theta^2\xi_1^2\xi_0^1 \;\; \theta^4\xi_1^2\xi_0^2), \\ a^1 = (1 \;\; \xi_0^1 \;\; \xi_0^2 \;\; \theta\xi_1^1 \;\; \theta^2\xi_1^1\xi_0^1 \;\; \theta^3\xi_1^1\xi_0^2 \;\; \theta^2\xi_1^2 \;\; \theta^4\xi_1^2\xi_0^1 \;\; \theta^6\xi_1^2\xi_0^2), \\ a^2 = (1 \;\; \xi_0^1 \;\; \xi_0^2 \;\; \theta^2\xi_1^1 \;\; \theta^3\xi_1^1\xi_0^1 \;\; \theta^4\xi_1^1\xi_0^2 \;\; \theta^4\xi_1^2 \;\; \theta^6\xi_1^2\xi_0^1 \;\; \theta^8\xi_1^2\xi_0^2). \end{cases}$$

In order to make $a^k \in \xi^{\mathbb{Z}_M}$ for $k \ge 0$, M must be an integral multiple of N, i.e.,

$$M \mod N = 0.$$

Thus one can use ordinary Rudin-Shapiro polynomials only to construct binary GCS, and cannot use generalized Rudin-Shapiro polynomials ($N > 2$) to construct binary generalized GCS.

III. PMEPR OF GENERALIZED RUDIN-SHAPIRO POLYNOMIALS

We now show that generalized Rudin-Shapiro polynomials constitute a subset of generalized GCS, from which, the PMEPR immediately follows. By formula (5), it is easy to see that

$$\begin{aligned} P_{a^0}(z) + \cdots + P_{a^{N-1}}(z) &= \sum_{\ell=0}^{N-1} |s_{a^\ell}(z)|^2 = \sum_{\ell=0}^{N-1} |A_m^\ell(z)|^2 \\ &= \left(\mathbf{A}_m^N\right)^\top \cdot \overline{\mathbf{A}_m^N}, \end{aligned}$$

where $\left(\mathbf{A}_m^N\right)^\top$ is the transpose of the matrix $\mathbf{A}_m^N$. Since $\mathbf{T}_{m-1}^N$ is an orthogonal matrix, we have $\left(\mathbf{T}_{m-1}^N\right)^\top \overline{\mathbf{T}_{m-1}^N} = N\mathbf{I}_N$ and

$$\begin{aligned} \left(\mathbf{A}_m^N\right)^\top \cdot \overline{\mathbf{A}_m^N} &= \left(\mathbf{B}_{m-1}^N(z)\right)^\top \left(\mathbf{T}_{m-1}^N\right)^\top \overline{\mathbf{T}_{m-1}^N \mathbf{B}_{m-1}^N(z)} \\ &= N\left(\mathbf{B}_{m-1}^N(z)\right)^\top \overline{\mathbf{B}_{m-1}^N(z)}, \end{aligned}$$

where the $\mathbf{I}_N$ is the identity matrix of degree N. By the definition of the vector $\mathbf{B}_{m-1}^N(z)$, we have $\left(\mathbf{B}_{m-1}^N(z)\right)^\top \overline{\mathbf{B}_{m-1}^N(z)} = N\left(\mathbf{A}_{m-1}^\ell(z)\right)^\top \overline{\mathbf{A}_{m-1}^\ell(z)}$. We deduce that

$$\left(\mathbf{A}_m^N\right)^\top \cdot \overline{\mathbf{A}_m^N} = N\left(\mathbf{A}_{m-1}^\ell(z)\right)^\top \overline{\mathbf{A}_{m-1}^\ell(z)}.$$

Repeating the process and noting $\left(\mathbf{A}_0^\ell(z)\right)^\top \overline{\mathbf{A}_0^\ell(z)} = N$, finally we have

$$P_{a^0}(z) + \cdots + P_{a^{N-1}}(z) = N^m\left(\mathbf{A}_0^\ell(z)\right)^\top \overline{\mathbf{A}_0^\ell(z)} = nN.$$

This clearly shows that $\{a^0, \cdots, a^{N-1}\}$ are Golay complementary set, and hence a^ℓ for $0 \le \ell \le N-1$ is a generalized Golay complementary sequences (see Fig. 1). Hence, it immediately implies that the PMEPR of a generalized Rudin-Shapiro polynomial is at most N.

IV. ENCODING USING GENERALIZED RUDIN-SHAPIRO POLYNOMIALS

We now investigate the code rate of encoding using generalized Rudin-Shapiro polynomials. We are particularly interested in the trade-off performance between the code rate and the PMEPR and we make comparison with encoding using generalized GSC in the second order cosets of the first order Reed-Muller codes [4]. Let us briefly review the encoding and code rate investigated in [4]. We shall need the frameworks of Boolean functions introduced in the Appendix.

A. Code rate of generalized GCS in the second order cosets of the first order Reed-Muller codes

For $n = 2^m$ and $x \in \mathbb{Z}_m$, let the binary representation of x be $x = \sum_\ell x_\ell 2^{m-\ell}$. For an even number M and an integer $d \ge 0$, define the quadratic form f using Boolean function as

$$\begin{aligned} f(x_1, \cdots x_m) &= \frac{M}{2}\sum_{k=1}^{m-d-1} x_{\pi(k)}x_{\pi(k+1)} \\ &\quad + \sum_{k=1}^{m-d}\sum_{\ell=m-d+1}^{m} c_{k\ell}^1 x_{\pi(k)}x_{\pi(\ell)} \\ &\quad + \sum_{m-d<k<\ell\le m} c_{k\ell}^2 x_{\pi(k)}x_{\pi(\ell)}, \end{aligned}$$

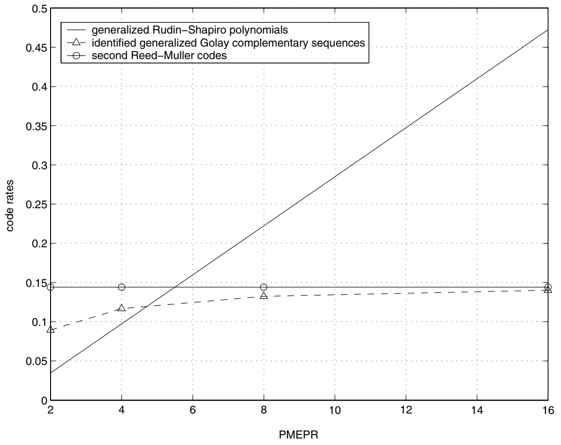

Fig. 2. The code rates of coset based encoding and generalized Rudin-Shapiro polynomial based encoding versus PMEPR for $n = 256$.

where π is a permutation of $\{1, \cdots, m\}$ and $a_{k\ell}, c_{k\ell} \in \mathbb{Z}_M$. Define a $\xi^{\mathbb{Z}_M}$-sequence a as

$$a(x_1, \cdots, x_m) = \xi^{f(x_1, \cdots, x_m) + \ _{\ell=1}^{m} c_\ell x_\ell + c},$$

where $c_\ell, c \in \mathbb{Z}_M$. Using the graph theory and the quadratic form, Paterson [6] showed that a is a 2^{d+1}-generalized Golay complementary sequence, which coincides with the Golay complementary sequence for $d = 0$. Since different permutations may result in the same generalized GCS, it is difficult to count the distinct generalized GCS generated by this construction. But for some special cases, such as the cases of $d = 1$ or binary sequences, Paterson [6] obtained some results.

1) $d = 1$: There are $\frac{m!}{2} M^{m+1} |\mathcal{G}_m|$ distinct 4-generalized Golay complementary sequences, where $|\mathcal{G}_m| = M^{m-1} - (Mm - M - 2m + 4)2^{m-2}$. Then the code rate is

$$\text{Rate1} = \frac{m+1}{2^m} + \frac{\lfloor \log_2 m! - 1 \rfloor + \lfloor \log_2 |\mathcal{G}_m| \rfloor}{2^m \log_2 M}.$$

2) Binary sequences: There are $\frac{m!}{2} 2^{m+1} |\mathcal{G}_m|$ distinct 2^{d+1}-generalized Golay complementary sequences, where $|\mathcal{G}_m| = \binom{S_{m-d}}{k}$ and $S_{m-d} = 2^{m-d} - \binom{m-d}{3} - \binom{m-d}{2} - (m-d) - 1$. When $m - d \gg d$, $|\mathcal{G}_m|$ is approximately $2^{(m-d)d}/d!$. Therefore the code rate is approximately

$$\text{Rate2} = \frac{(m-d)d + m - 1}{2^m} + \frac{\lfloor \log_2 m! - 1 \rfloor - \lfloor \log_2 d! \rfloor}{2^m}.$$

B. Code rate of generalized Rudin-Shapiro polynomials

For $n = 2^m$, there are totally $m(N-1)$ random variables involved in $A_m^0(z)$. Hence one can construct $M^{m(N-1)}$ number of distinct generalized Rudin-Shapiro polynomials. Since for any $\eta \in \xi^{\mathbb{Z}_M}$, ηa is a generalized Golay complementary sequence if a is a generalized Rudin-Shapiro polynomial, one can totally construct $M^{m(N-1)+1}$ number of distinct generalized Rudin-Shapiro polynomials using the formula (5). For an integer $d \geq 0$ and $N = 2^{d+1}$, the the code rate of encoding using generalized Rudin-Shapiro polynomials is

$$\text{Rate3} = \frac{m(2^{d+1} - 1) + 1}{2^m}.$$

C. Numerical results

Fig. 2 shows the code rates of coset based encoding and generalized Rudin-Shapiro polynomial based encoding versus PMEPR for $n = 256$. For $\text{PMEPR} < 5$, coset based encoding provides a trade-off between the code rate and the PMEPR. However, for $\text{PMEPR} > 5$, the code rate of generalized Rudin-Shapiro polynomial exceeds that of coset based encoding . The code rate of generalized Rudin-Shapiro polynomial based encoding increases linearly with respect to PMEPR; while that of coset based encoding reaches a limit given by the code rate of second order Reed-Muller codes, when PMEPR is large enough. Therefore, for $\text{PMEPR} > 5$, generalized Rudin-Shapiro polynomial based encoding gives a better trade-off between the code rate and PMEPR. Sufficient numbers of codewords can be recursively produced by a matrix equation in generalized Rudin-Shapiro polynomial based encoding.

V. Conclusions

In this paper, we investigated generalized Rudin-Shapiro polynomials to encode OFDM signals. By showing that they constitute a subset of generalized GCS, we obtained the PMEPR of generalized Rudin-Shapiro polynomials. In an encoding scheme using these polynomials, a matrix formula recursively produces a sufficient number of codewords that the code rate increases linearly with respect to the PMEPR. Therefore, it offers an excellent trade-off performance between the code rate and PMEPR.

Appendix
Boolean functions and Reed-Muller codes

A Boolean function is a mapping f from $\mathbb{Z}_2^m$ to $\mathbb{Z}_M$. For any $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Z}_2^m$, 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 2^m-dimensional vector $\mathbf{f} \in \mathbb{Z}_M^{2^m}$ such that the ith coordinate of $\mathbf{f}$ is $f(i_1, \ldots, i_m)$. For example, for $m = 3$ we have

$$\begin{aligned} \mathbf{f} \;\; = \;\; & (f(0,0,0), f(0,0,1), f(0,1,0), f(0,1,1), f(1,0,0), \\ & f(1,0,1), f(1,1,0), f(1,1,1)), \end{aligned}$$

and $\mathbf{1} = (11111111)$, $\mathbf{x}_1 = (00001111)$, $\mathbf{x}_2 = (00110011)$, $\mathbf{x}_3 = (01010101)$, $\mathbf{x}_1\mathbf{x}_2 = (00000011)$, $\mathbf{x}_2\mathbf{x}_3 = (00010001)$, $\mathbf{x}_1\mathbf{x}_3 = (00000101)$, and $\mathbf{x}_1\mathbf{x}_2\mathbf{x}_3 = (00000001)$. Then we can write an vector $\mathbf{f}$ induced by any Boolean function $f : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_M$ as

$$\begin{aligned}\mathbf{f} &= c_0 + c_1\mathbf{x}_1 + c_2\mathbf{x}_2 + c_3\mathbf{x}_3 + c_{12}\mathbf{x}_1\mathbf{x}_2 + c_{23}\mathbf{x}_2\mathbf{x}_3 \\ &\quad + c_{13}\mathbf{x}_1\mathbf{x}_3 + c_{123}\mathbf{x}_1\mathbf{x}_2\mathbf{x}_3,\end{aligned}$$

where the coefficients $c_0, \cdots, c_{123}$ are taken from $\mathbb{Z}_M$. For example, for $M = 3$, $2\mathbf{x}_1\mathbf{x}_2 = (00000022)$ and $\mathbf{x}_1\mathbf{x}_2 + 2\mathbf{x}_1\mathbf{x}_3 = (00000210)$.

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 $M^{\quad_{\ell=0}^{r}\binom{m}{\ell}}$ 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 $\mathrm{RM}_M(1, m)$. See [22] for the details about Boolean functions and the Reed-Muller codes.

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. coiffi, "PAR reduction in multicarrier transmission systems," Stanford University," Technical Report, 1998.

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

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

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

[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] W. Chen and C. Tellambura, "Identifying a class of multiple shift complementary sequences in the second order cosets of the first order reed-muller codes," in *IEEE ICC*. Seoul, Korea: IEEE, 2005.

[19] Z. X. Lei, "Some properties of generalized rudin-shapiro polynomials," *Chinese Ann. Math.*, no. 2, pp. 145–153, 1991.

[20] W. Rudin, "Some theorems on Fourier coefficients," *Proc. Amer. Math. Soc.*, vol. 10, pp. 855–859, 1959.

[21] A. J. Grant and R. Van Nee, "Efficient maximum-likelihood decoding of Q-ary modulated Reed-Muller codes," *IEEE Commun. Lett.*, vol. 2, no. 5, pp. 134–136, may 1998.

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