

Construction of M -QAM Sequences Based on Generalized Rudin-Shapiro Polynomials

Yajun Wang, Wen Chen, and Wei Chen

Department of Electronic Engineering

Shanghai Jiaotong University

800 Dongchuan Road, Minhang, Shanghai, China 200240

Email: {wangyj1859, wenchen, chx_ufo}@sjtu.edu.cn

Abstract—A construction scheme of M -QAM (quaternary amplitude modulation) signals using quaternary phase-shift keying (QPSK) constellations for the orthogonal frequency division multiplexing (OFDM) has been proposed, when $M = 2^k$ and k is an even number. In this paper, we extend Rudin-Shapiro polynomials (RSP) to the generalized Rudin-Shapiro polynomials (GRSP). Based on the generalized Rudin-Shapiro polynomials (GRSP), upper bound of peak-to-mean envelope power ratio (PMEPR), code rate, the minimum Hamming distance for the M -QAM sequences are derived.

I. INTRODUCTION

Orthogonal frequency division multiplexing (OFDM) is a multicarrier modulation technique that has been adopted for many kinds of applications in wireless systems, such as wireless local-area networks [1] and digital video broadcasting [2]. However, a major drawback of OFDM signals is the high peak-to-mean envelope power ratio (PMEPR) of the uncoded OFDM signal. Some popular PMEPR reduction techniques include signal distortion techniques [3], [4], coding [5], [6], [7], [8], multiple signal representation [12], [13], [16], [27], modified signal constellation [21], pilot tone methods [31] and others.

Several schemes to use so-called Golay complementary sequences [18] to encode the OFDM signals with PMEPR of at most 2 have been studied [11], [19], [20], [28]. Davis and Jedwab made an main theoretical advance on this work and observed that the 2^h -ary Golay sequences of length 2^m can be obtained from certain second order cosets of the classical first order Reed-Muller code [5]. Davis and Jedwab's construction were able to obtain $(m!/2)2^{h(m+1)}$ codewords (DJ-code) for the phase shift keying (PSK) OFDM signals of 2^m carriers with good error-correcting capabilities, efficient encoding and decoding, and a PMEPR of at most 2. Its main drawback is that the code rate rapidly decreases for larger block lengths. Futher work on DJ-code has been done in [8], which provides a trade-off between the code rate and PMEPR by employing generalized Golay complementary sequences [30].

Since M -quadrature amplitude modulation (M -QAM) sequences are widely used in OFDM, RöBing and Tarokh[22], Chong and Tarokh [23] has studied the Golay sequences for 16-QAM OFDM signals. As a simple way to construct Golay sequences, the Rudin-Shapiro polynomials (RSP) [29] have been studied in [14], [15], [24], [25], [26]. Further study

to general M -QAM OFDM sequences with low PMEPR has been reported in [9], [10]. In this paper, we develop a simple way to design the M -QAM OFDM signals using the generalized Rudin-Shapiro polynomials(GRSP) [14], [15]. The upper bound of peak-to-mean envelope power ratio (PMEPR), code rate, the Hamming distance for these M -QAM sequences are derived.

II. PRELIMINARIES

Let j be the imaginary unit, i.e., $j^2 = -1$. For an H -ary phase modulation OFDM, let $\xi^{\mathbb{Z}_H} = \{\xi^k : k \in \mathbb{Z}_H\}$, where $\xi = \exp(2\pi j/H)$, H is a positive integer, and $\mathbb{Z}_H = \{0, \dots, H-1\}$.

A. OFDM Signals, Instantaneous Power and PMEPR

Let a codeword $\mathbf{c} = (c_0, \dots, c_{n-1})$ with $c_\ell \in \xi^{\mathbb{Z}_H}$, the frequency separation between any two adjacent subcarriers is $\Delta f = 1/T$. Then the n subcarrier complex baseband OFDM signal can be represented as

$$s_{\mathbf{c}}(t) = \sum_{\ell=0}^{n-1} c_\ell e^{j2\pi\ell\Delta ft}, \quad (1)$$

where $0 \leq t < T$. The instantaneous power of the complex envelope $s_{\mathbf{c}}(t)$ is defined by

$$P_{\mathbf{c}}(t) = |s_{\mathbf{c}}(t)|^2. \quad (2)$$

So the peak-to-mean power ratio (PMEPR) of the codeword \mathbf{c} is defined by

$$\text{PMEPR}(\mathbf{c}) = \frac{1}{n} \sup_{0 \leq t < T} |s_{\mathbf{c}}(t)|^2. \quad (3)$$

B. Rudin-Shapiro Polynomials

The construction of encoding and decoding schemes for OFDM by means of Rudin-Shapiro polynomials (RSP) [29] can be found in [17].

For a $k \geq 0$, an RSP pair $(A(z), B(z))$ is recursively defined as

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

where $A_0(z) = B_0(z) = 1$ and ξ_k is any element in $\xi^{\mathbb{Z}_H}$.

Formula (4) recursively produces the polynomials $A_k(z)$ and $B_k(z)$ of degree $2^k - 1$ for any $k > 0$. 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 $m = 3$, the corresponding codewords are

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

C. Generalized Rudin-Shapiro Polynomials

We rewrite the formula (4) in the matrix form. Let

$$\mathbf{A}_k^2(z) = \begin{pmatrix} A_k(z) \\ B_k(z) \end{pmatrix}, \quad \mathbf{B}_k^2(z) = \begin{pmatrix} A_k(z) \\ z^{2^k} B_k(z) \end{pmatrix},$$

and

$$\mathbf{T}_k^2 = \begin{pmatrix} 1 & \xi_k \\ 1 & -\xi_k \end{pmatrix}.$$

Then one can rewrite formula (4) in the matrix form as

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

We can attain an extension of RSP. Let $\theta = \exp(j2\pi/N)$, where N is a positive integer. Extend $\mathbf{A}_k^2(z)$, $\mathbf{B}_k^2(z)$ and \mathbf{T}_k^2 respectively to $\mathbf{A}_k^N(z)$, $\mathbf{B}_k^N(z)$ and \mathbf{T}_k^N as follows:

$$\mathbf{A}_k^N(z) = \begin{pmatrix} A_{k+1}^0(z) \\ A_{k+1}^1(z) \\ \vdots \\ A_{k+1}^{N-1}(z) \end{pmatrix}, \quad \mathbf{B}_k^N(z) = \begin{pmatrix} A_k^0(z) \\ z^{N^k} A_k^1(z) \\ \vdots \\ z^{(N-1)N^k} A_k^{N-1}(z) \end{pmatrix},$$

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

where $A_0^0 = \dots = A_0^{N-1} = 1$ and $\xi_k^1, \dots, \xi_k^{N-1}$ are any symbols taken from the constellations $\xi^{\mathbb{Z}_H}$. Each polynomial entry in $\mathbf{A}_k^N(z)$ is called a generalized Rudin-Shapiro polynomials (GRSP). Naturally, GRSP vector is iteratively defined by the formula

$$\mathbf{A}_k^N(z) = \mathbf{T}_k^N \mathbf{B}_k^N(z). \quad (5)$$

Obviously, the GRSP degenerates to the ordinary RSP if $N = 2$. Particular cases of interest are the case $N > 2$.

For example, for $N = 4$, this is more practical in encoding OFDM signals. Then $\theta = j$ and

$$\begin{pmatrix} A_{k+1}^0(z) \\ A_{k+1}^1(z) \\ A_{k+1}^2(z) \\ A_{k+1}^3(z) \end{pmatrix} = \begin{pmatrix} 1 & \xi_k^1 & \xi_k^2 & \xi_k^3 \\ 1 & \theta\xi_k^1 & \theta^2\xi_k^2 & \theta^3\xi_k^3 \\ 1 & \theta^2\xi_k^1 & \theta^4\xi_k^2 & \theta^6\xi_k^3 \\ 1 & \theta^3\xi_k^1 & \theta^6\xi_k^2 & \theta^9\xi_k^3 \end{pmatrix} \begin{pmatrix} A_k^0(z) \\ z^{4^k} A_k^1(z) \\ z^{2 \cdot 4^k} A_k^2(z) \\ z^{3 \cdot 4^k} A_k^3(z) \end{pmatrix}.$$

For $k = 0$, we have

$$\begin{aligned} A_1^0(z) &= 1 + \xi_0^1 z + \xi_0^2 z^2 + \xi_0^3 z^3, \\ A_1^1(z) &= 1 + j\xi_0^1 z - \xi_0^2 z^2 - j\xi_0^3 z^3, \\ A_1^2(z) &= 1 - \xi_0^1 z + \xi_0^2 z^2 - \xi_0^3 z^3, \\ A_1^3(z) &= 1 - j\xi_0^1 z - \xi_0^2 z^2 + j\xi_0^3 z^3. \end{aligned}$$

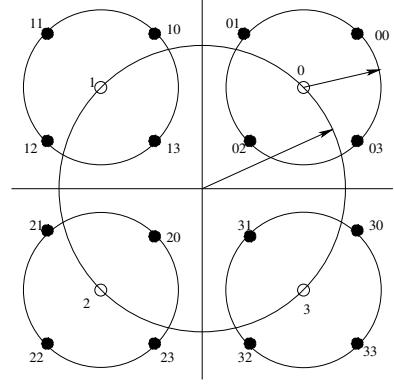


Fig. 1. Construction of 16-QAM from two QPSK.

For $k = 1$, we have

$$\begin{aligned} A_2^0(z) &= 1 + \xi_0^1 z + \xi_0^2 z^2 + \xi_0^3 z^3 \\ &\quad + \xi_1^1 z^4 + j\xi_1^1 \xi_0^1 z^5 - \xi_1^1 \xi_0^2 z^6 - j\xi_1^1 \xi_0^3 z^7 \\ &\quad + \xi_1^2 z^8 - \xi_1^2 \xi_0^1 z^9 + \xi_1^2 \xi_0^2 z^{10} - \xi_1^2 \xi_0^3 z^{11} \\ &\quad + \xi_1^3 z^{12} - j\xi_1^3 \xi_0^1 z^{13} - \xi_1^3 \xi_0^2 z^{14} + j\xi_1^3 \xi_0^3 z^{15}. \\ A_2^1(z) &= 1 + \xi_0^1 z + \xi_0^2 z^2 + \xi_0^3 z^3 \\ &\quad + j\xi_1^1 z^4 - \xi_1^1 \xi_0^1 z^5 - j\xi_1^1 \xi_0^2 z^6 + \xi_1^1 \xi_0^3 z^7 \\ &\quad - \xi_1^2 z^8 + \xi_1^2 \xi_0^1 z^9 - \xi_1^2 \xi_0^2 z^{10} + \xi_1^2 \xi_0^3 z^{11} \\ &\quad - j\xi_1^3 z^{12} - \xi_1^3 \xi_0^1 z^{13} + j\xi_1^3 \xi_0^2 z^{14} + \xi_1^3 \xi_0^3 z^{15}. \\ A_2^2(z) &= 1 + \xi_1^1 z + \xi_1^2 z^2 + \xi_1^3 z^3 \\ &\quad - \xi_1^1 z^4 - j\xi_1^1 \xi_0^1 z^5 + \xi_1^1 \xi_0^2 z^6 + j\xi_1^1 \xi_0^3 z^7 \\ &\quad + \xi_1^2 z^8 - \xi_1^2 \xi_0^1 z^9 + \xi_1^2 \xi_0^2 z^{10} - \xi_1^2 \xi_0^3 z^{11} \\ &\quad - \xi_1^3 z^{12} + j\xi_1^3 \xi_0^1 z^{13} + \xi_1^3 \xi_0^2 z^{14} - j\xi_1^3 \xi_0^3 z^{15}. \\ A_2^3(z) &= 1 + \xi_0^1 z + \xi_0^2 z^2 + \xi_0^3 z^3 \\ &\quad - j\xi_1^1 z^4 + \xi_1^1 \xi_0^1 z^5 + j\xi_1^1 \xi_0^2 z^6 - \xi_1^1 \xi_0^3 z^7 \\ &\quad - \xi_1^2 z^8 + \xi_1^2 \xi_0^1 z^9 - \xi_1^2 \xi_0^2 z^{10} + \xi_1^2 \xi_0^3 z^{11} \\ &\quad + j\xi_1^3 z^{12} + \xi_1^3 \xi_0^1 z^{13} - j\xi_1^3 \xi_0^2 z^{14} - \xi_1^3 \xi_0^3 z^{15}. \end{aligned}$$

This generates the codewords of length 4^2 from the coefficients of the polynomials $A_2^0(z), \dots, A_2^3(z)$. In general, for $n = N^m$, let the sequences a^k be the coefficients of the polynomial $A_m^k(z)$ for $0 \leq k \leq N-1$ respectively. Then the 2^m -subcarrier OFDM signals are $\mathcal{S}_{a^k}(z) = A_m^k(z)$ for $0 \leq k \leq N-1$.

D. Construction of M -QAM Signals from QPSK Constellations

The QPSK constellation can be realized as $\text{QPSK} = \{j^{x_i}\}$, where $x_i \in \mathbb{Z}_4 = \{0, 1, 2, 3\}$. Thus any QPSK sequence $\mathbf{a} = (a_0 a_1 \dots, a_{n-1})$ can be associated with another sequence $x_i = (x_i^0 x_i^1 \dots x_i^{N-1})$, where the elements of x_i are in \mathbb{Z}_4 . One can use shift and rotation operation to produce M -QAM constellations from QPSK symbols. Fig. 1 shows the construction of a 16-QAM symbol from two QPSK symbols. In general, M -QAM constellation can be written as

$$M - \text{QAM} = \sum_{i=0}^{\frac{N}{2}-1} 2^{i-1} \sqrt{2} (j^{x_i}) \exp(j\pi/4), \quad (6)$$

where $M = 2^n$, n is an even integer, $x_i^k \in \mathbb{Z}_4$. In this way, we can associate any M -QAM sequences

$\mathbf{a} = (a_0 a_1 \dots, a_{N-1})$ with a unique sequences, $x_0^0 x_1^0 \dots x_{\frac{n}{2}-1}^0, x_1^0 x_1^1 \dots x_{\frac{n}{2}-1}^1, \dots x_0^{N-1} x_1^{N-1} \dots x_{\frac{n}{2}-1}^{N-1} \in \mathbb{Z}_4^N \times \mathbb{Z}_4^N \times \dots \times \mathbb{Z}_4^N$. In particular, the signal $\mathcal{S}_{\mathbf{a}}(t)$ can be written as

$$\mathcal{S}_{\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{\frac{n}{2}-1}}(t) = \sum_{k=0}^{N-1} \sum_{i=0}^{\frac{n}{2}-1} 2^{i-1} \sqrt{2}(j)^{x_i^k} \times \exp(2j\pi(f_0 + kf_s)t + j\pi/4). \quad (7)$$

Let

$$\mathcal{S}_{\mathbf{x}_i}(t) = \sum_{k=0}^{N-1} (j)^{x_i^k} \exp(2j\pi(f_0 + kf_s)t + j\pi/4). \quad (8)$$

Simplifying (7), the instantaneous envelop power is given by

$$P_{\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{\frac{n}{2}-1}}(t) = \left| \sum_{k=0}^{N-1} \sum_{i=0}^{\frac{n}{2}-1} (2^{i-1}) \sqrt{2} j^{x_i^k} \times \exp(2j\pi kf_s t) \right|^2 = \left| \sum_{i=0}^{\frac{n}{2}-1} (2^{i-1}) \sqrt{2} \mathcal{S}_{\mathbf{x}_i}(t) \right|^2. \quad (9)$$

We will use the above results to compute PMEPR bounds when the sequences based on GRSP is constructed.

III. NEW CONSTRUCTION OF M -QAM SEQUENCES

Our construction of M -QAM sequences is based on GRSP and the decomposition of M -QAM symbols.

A. PMEPR of M -QAM Sequences by GRSP

Let $U = (u_0, \dots, u_{n-1})$ and $V = (v_0, \dots, v_{n-1})$ be the two QPSK sequences of length n from GRSP. Then we have

Theorem 1: The PMEPR of QPSK sequences from GRSP is at most 4.

Proof: Let $Z = (1, z, \dots, z^{n-1})^T$, U and V be two QPSK sequences constructed by GRSP. Assume $U^1 Z, U^2 Z, U^3 Z$ and $U^0 Z (= UZ)$ form GRSP vector. From (5), we have

$$\begin{aligned} \sum_{\ell=0}^3 |s_{U^\ell}(z)|^2 &= \sum_{\ell=0}^3 |A_m^\ell(z)|^2 \\ &= (\mathbf{A}_m^4)^\top \cdot \overline{\mathbf{A}_m^4}, \end{aligned}$$

where $(\mathbf{A}_m^4)^\top$ is the transpose of the matrix \mathbf{A}_m^4 . Since \mathbf{T}_{m-1}^N

is an orthogonal matrix, we have $(\mathbf{T}_{m-1}^4)^\top \overline{\mathbf{T}_{m-1}^4} = 4\mathbf{I}_4$ and

$$\begin{aligned} \sum_{\ell=0}^3 |s_{U^\ell}(z)|^2 &= (\mathbf{B}_{m-1}^4(z))^\top (\mathbf{T}_{m-1}^4)^\top \overline{\mathbf{T}_{m-1}^4} \mathbf{B}_{m-1}^4(z) \\ &= 4(\mathbf{B}_{m-1}^4(z))^\top \mathbf{I}_4 \overline{\mathbf{B}_{m-1}^4(z)} \\ &= 4 \sum_{\ell=0}^3 (\mathbf{B}_{m-1}^\ell(z))^\top \overline{\mathbf{B}_{m-1}^\ell(z)} \\ &= 4 \sum_{\ell=0}^3 (\mathbf{A}_{m-1}^\ell(z))^\top \overline{\mathbf{A}_{m-1}^\ell(z)} \\ &= \dots \\ &= 4^m \sum_{\ell=0}^3 (\mathbf{A}_0^\ell(z))^\top \overline{\mathbf{A}_0^\ell(z)} \\ &= 4^{m+1} = 4n, \end{aligned}$$

where \mathbf{I}_4 is the identity 4×4 matrix. This shows that $\text{PMEPR}(U) = 4$. Similarly, $\text{PMEPR}(V) = 4$.

Using the PMEPR of GRSP, one can obtain the PMEPR of M -QAM sequences, which is summarized in the following theorem.

Theorem 2: If $\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{\frac{n}{2}-1}$ are QPSK sequences constructed from GRSP, then $P_{\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{\frac{n}{2}-1}}(t) \leq (2^{n/2-1})^2 2N$. Proof from (9), we have

$$\begin{aligned} P_{\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{\frac{n}{2}-1}}(t) &= \left| \sum_{i=0}^{\frac{n}{2}-1} (2^{i-1}) \sqrt{2} \mathcal{S}_{\mathbf{x}_i}(t) \right|^2 \\ &\leq \left\{ \sum_{i=0}^{\frac{n}{2}-1} |(2^{i-1}) \sqrt{2} \mathcal{S}_{\mathbf{x}_i}(t)| \right\}^2. \end{aligned} \quad (10)$$

We can use inequality

$$P_{\mathbf{a}}(t) = |\mathcal{S}_{\mathbf{a}}(t)|^2 \leq 4N, \quad (11)$$

to conclude that

$$P_{\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{\frac{n}{2}-1}}(t) \leq \left| \sum_{i=0}^{\frac{n}{2}-1} (2^{i-1}) \sqrt{2} \right|^2 4N = (2^{\frac{n}{2}} - 1)^2 2N. \quad (12)$$

Lemma 1: ([10], Lemma IV.1) Let \mathbf{x}_i^k be independent sequences of length N and each element of them are equiprobable, such that $E(\mathcal{S}_{\mathbf{x}_i}(t) \mathcal{S}_{\mathbf{x}_j}(t)) = 0$. Then the mean envelop power is $P_{\mathbf{av}} = N/6 \times (2^n - 1)$.

By means of *Theorem 2* and *Lemma 1*, we can immediately get the PMEPR of QPSK sequences from GRSP.

Theorem 3: Let $\mathcal{A} \subseteq \mathbb{Z}_4^N$ be the set of QPSK sequences from GRSP. The PMEPR for $Z := \mathcal{A}^1 \times \dots \times \mathcal{A}^{\frac{n}{2}-1}$ is bounded by $12(2^{\frac{n}{2}} - 1)^2 / 2^n - 1$, provided that $\mathcal{A}^1 \times \dots \times \mathcal{A}^{\frac{n}{2}-1}$ is used for equiprobable M -QAM OFDM transmission.

Proof: By *Theorem 2*, the peak transmitted envelop power is bounded by $(2^{\frac{n}{2}} - 1)^2 / 2^n - 1$. The mean envelop power by *Lemma 1* is $P_{\mathbf{av}} = N/6 \times (2^n - 1)$. Thus the PMEPR is bounded above by $12(2^{\frac{n}{2}} - 1)^2 / 2^n - 1$.

TABLE I

COMPARISON OF CODE RATES BETWEEN 16-QAM SEQUENCES
CONSTRUCTED IN [23] AND THOSE BASED ON GRSP

$n = 4^m$	$\mathcal{R}(\mathcal{C}_{2.0})$	$\mathcal{R}(\mathcal{C}_{2.8})$	$\mathcal{R}(\mathcal{C}_{3.6})$	$\mathcal{R}(\mathcal{C}_{7.2})$
4	2.3962	2.7925	2.81	4
16	1.1192	1.2182	1.22	1.75
64	0.4266	0.4513	0.45	0.625
256	0.1464	0.1526	0.15	0.20

B. Code Rate of M -QAM by GRSP

For the GRSP of degree $N^k - 1$, there are $(N-1)k$ variables involved in $A_k^0(z)$, and each variable has 4 choices. Hence, one can construct $4^{(N-1)k}$ QPSK sequences by GRSP. Since for any $\xi \in \xi^{\mathbb{Z}_4}$, ξa is a GRSP, if a is a GRSP, one can totally construct $4^{(N-1)k+1}$ distinct QPSK sequences by GRSP. Since we can choose different QPSK sequences to construct the M -QAM OFDM signals, we have totally $[4^{(N-1)k+1}]^{\frac{n}{2}}$ different choices. This gives the code rate of the M -QAM by GRSP.

Theorem 4: For the M -QAM codes of length N^k constructed by GRSP, the code rate is

$$\frac{\log_2[4^{(N-1)k+1}]^{\frac{n}{2}}}{N^k} = \frac{[(N-1)k+1]n}{N^k}.$$

Let $n = 4$. This correspond to 16-QAM modulation. The code rate is $[(N-1)k+1]/4/N^k$. Let $N = 4$, the corresponding code rate is $(3k+1)/4^{k-1}$, which is higher than that of the constructions presented in [23]. The comparison between code rates of the constructed 16-QAM sequences in [23] and those of GRSP is shown in Table I, where $\mathcal{R}(\mathcal{C}_d)$ represents the code rate of the code whose PMEPR is bounded above by d . From Table I, we can discover that the code rate is higher than that of 16-QAM sequences constructed in [23]. One will see our performance is better than [23] for the moderately large carriers. On the other hand, the PMEPR of 16-QAM sequences based on GRSP method in this paper is larger than that of 16-QAM Sequences from [23], but the method is simple.

C. Minimum Hamming Distance of M -QAM by Generalized RSP

Take an M -QAM sequence

$$M-QAM = \sum_{i=0}^{\frac{n}{2}-1} 2^{i-1} \sqrt{2} U_i \exp(j\pi/4), \quad (13)$$

where U_i are QPSK sequences. Then the Hamming distance d_H of M -QAM sequence is the smallest one between the Hamming distances of U_i and U_k , $i \neq k$, $0 \leq i, k \leq \frac{n}{2} - 1$. In the following theorem, the Hamming distance of M -QAM sequences based on GRSP is given.

Theorem 5: For the M -QAM sequences of length N^k by GRSP, the minimum Hamming distance is N^{k-1} .

Proof: Take any M -QAM sequence

$$M-QAM = \sum_{i=0}^{\frac{n}{2}-1} 2^{i-1} \sqrt{2} U_i \exp(j\pi/4), \quad (14)$$

TABLE II

GENERAL FORMULAE ON THE PMEPR, CODE RATE AND MINIMUM HAMMING DISTANCES FOR 16-QAM CODES FROM DISTANT SCHEMES

construction	PMEPR	code rate	d_H
Golay [23]	3.6	$\frac{2(m+1)+\log_2[(7+6m)(m!)]}{2^m}$	2^{m-2}
RSP [26]	3.6	$\frac{8+\log_2(4^{m-1} \times m - m + 1)}{2^m}$	2^{m-1}
GRSP	7.2	$\frac{1}{2^m}$	2^{m-1}

of length N^k . Since the Hamming distance of M -QAM is determined by those of U_i and U_k , we only find out the Hamming distances of U_i and U_k , $i \neq k$, $0 \leq i, k \leq \frac{n}{2} - 1$. In the following, we will use induction to show that the minimum Hamming distances of U_i and U_k are N^{k-1} .

For the minimum case $k = 1$, we have $A_1^0(z) = 1 + \xi_0^1 z + \xi_0^2 z^2 + \xi_0^3 z^3 + \dots + \xi_0^{N-1} z^{N-1}$. For different choices of $\xi_0^1, \xi_0^2, \dots, \xi_0^{N-1}$, we obtain different codes. Then the minimum Hamming distance of U_i is $1 = N^{k-1}$.

For the case $k = m + 1$, we have $A_{m+1}^0(z) = A_m^0(z) + \xi_m^1 z^{N^m} A_m^1(z) + \xi_m^2 z^{2 \cdot N^m} A_m^2(z) + \dots + \xi_m^{N-1} z^{N-1 \cdot N^m} A_m^{N-1}(z)$. Since the degrees of $A_m^0(z), \dots, A_m^{N-1}(z)$ are $N^m - 1$, the coefficients of $z^0, \dots, z^{N-1 \cdot N^m}$ will not add to each other. For the different choices of $\xi_m^\ell, 0 \leq \ell \leq N - 1$, the derived codes are different at least at N^m places, the length of A_m^ℓ . For the case of fixed choice of ξ_m^ℓ , assume that the Hamming distance of the code by A_m^ℓ are N^{m-1} . Since each A_m^ℓ includes all ξ_i^ℓ for $\ell = 0, 1, 2, \dots, N - 1$ and $0 \leq i < m$, there must be one ξ_i^ℓ changes. This implies that all A_m^ℓ are not fixed choices for two different A_{m+1}^0 . Therefore the minimum Hamming distance of the codes is $N \times N^{m-1} = N^m = N^{(m+1)-1}$.

By induction, this proves that the minimum Hamming distance of U_i and U_k is N^{k-1} . Therefore the minimum Hamming distance of M -QAM is N^{k-1} , which completes the proof.

Table II gives the general formulae on the PMEPR, code rate and minimum Hamming distances for 16-QAM codes from distant schemes. By given distant values for m , we can get the PMEPR, code rate and minimum Hamming distances from three kinds of distant methods. We can find out that our method offers a trade-off among minimum Hamming distance, code rate, and PMEPR by a simple numeration.

IV. CONCLUSIONS

In this paper, we introduce the generalized Rudin-Shapiro polynomials, and a large number of QPSK sequences can be recursively produced from this method. Then we use these QPSK sequences to construct M -QAM codewords for OFDM signals. By this construction, we can obtain $[4^{(N-1)k+1}]^{\frac{n}{2}}$ M -QAM codewords of length N^m , while controlling the PMEPR by $12(2^{\frac{n}{2}} - 1)^2 / 2^n - 1$. Moreover, we find that the minimum Hamming distance is N^{k-1} for this code of length N^m . Our scheme provides a trade-off between minimum Hamming distance, code rate, and PMEPR.

V. ACKNOWLEDGEMENT

This work is supported by NSF China #60672067, by Cultivation Fund of the Key Scientific and Technical Innovation Project, Ministry of Education of China #706022, by Program for New Century Excellent Talents in University #NCET-06-0386, by PUJIANG Talents #07PJ4046, by Huawei Fund for Sciences and Technologies in Universities #YJCB2008048WL, and by National 973 Project #2009CB824900.

REFERENCES

- [1] M. Aldinger, "Multicarrier COFDM scheme in high bit rate radio local area network," In *Proc. 5th IEEE Int.Symp.Personal,Indoor and Mobile Radio Communications*, The Hague, The Netherlands, sept,pp. 969-973, 1994
- [2] M. Alard and R. Lassalle, "Principles of modulation and channel coding for digital broadcasting for mobile receivers" *EBU Rev.*no. 224, pp. 47-69, Aug. 1987
- [3] H. Ochiai and H. Imai, "On the clipping for peak power reduction of OFDM signals," in *IEEE GLOBE-COM*, pp. 731-735, 2000 (San Francisco, USA).
- [4] W. G. Jeon, K. H. Chang, and Y. S. Cho, "An adaptive data predistorter for compensation of nonlinear distortion in OFDM systems," *IEEE Trans. Communications*, vol. 45, pp. 1167-1171, 1997.
- [5] J. A. Davis, and J. Jedwab, "Peak-to-mean power control for OFDM transmission using Golay sequences and Reed-Muller codes," *Electron. Letters*, vol. 33, pp. 267-268, 1997.
- [6] J. A. Davis, and J. Jedwab, "Peak to mean power control in OFDM, Golay complementary sequences and Reed-Miller codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 7, pp. 2397-2417, Nov., 1999.
- [7] K. G. Paterson, "Generalized Reed-Muller code and power control in OFDM modulation," *IEEE Trans. Information Theory*, vol. 46, no. 1, pp. 104-120, Jan., 2001.
- [8] K. G. Paterson, and V. Tarokh, "On the existence of construction of good codes with low peak-to-average power ratios," *IEEE Trans. Information Theory*, vol. 46, no. 6, pp. 1974-1987, Sep. 2000.
- [9] B. Tarokh and H. R. Sadjadpour, "Construction of non-square M -QAM sequences with low PMEPR for OFDM systems," *IEE Proc. Commun.*, vol. 151, no. 1, pp. 20-24, Feb, 2004.
- [10] B. Tarokh and H. R. Sadjadpour, "Construction of M -QAM sequences with low peak-to-average power ratio," *IEEE Trans. Communications*, vol. 51, no. 1, pp. 25-28, Jan, 2003.
- [11] S. Boyd, "Multitone signals with low crest factor," *IEEE Trans. Circuits and Systems*, vol. 33, pp. 1018-1022, 1986.
- [12] R. W. Bauml, R. F. H. Fisher, and J. B. Huber, "Reducing the peak-to-average power ratio of multicarrier modulation by selected mapping," *IEEE Elect. Letter*, vol. 32, pp. 2056-2057, 1996.
- [13] M. Breiling, S. Muller-Weinfurter, and J. Huber, "SLM peak-power reduction without explicit side information," *IEEE Commun. Letter*, vol. 5, no. 6, pp. 239-241, 2001.
- [14] W. Chen, and C. Tellambura, "A simple construction of 16-QAM codewords with low PMEPR for OFDM signals "In *IEEE ICCT*. Guilin, China, pp. 1397-1400, 2006.
- [15] W. Chen, and C. Tellambura, "A good trade-off performance between the code rate and the PMEPR for OFDM signals using the generalized Rudin-shapiro polynomials", In *IEEE ICC*. Seoul,Korea: *IEEE*, pp. 373-377. 2004.
- [16] P. V. Eetvelt, G. Wade, and M. Thompson, "Peak to average power reduction for OFDM schemes by selected scrambling," *IEEE Elect. Letter*, vol. 32, pp. 1963-1964, 1996.
- [17] A. J. Grant, and R. D. V. Nee, "Efficient Maximum-Likeli-hood Decoding of Q -ary Modulation Reed-Muller codes," *IRE Trans. Information Theory*, vol. 7, pp. 82-87, 1961.
- [18] M. J. E. Golay, "Complementary series." *IRE Trans.Inf.theory*, vol. IT-7,no. 2,pp. 82-87,Apr.1961
- [19] T. A. Wilkinson and A. E. Jones, "Minimization of the peak to mean envelop power ratio of multicarrier transmission schemes by block coding," *Proc. IEEE Vehicular Technology Conf.(VTC)*, Chicago,IL,Jul. 1995,pp. 825-829
- [20] H. Ochiai and H. Imai, "Block coding scheme based on complementary sequences for multicarrier signals." *IEICE Trans. Fundamentals*, vol. E80-A,pp. 2136-2146,1997
- [21] P. K. Frenger, and N. A. B. Sevensson, "Parallel combinatory OFDM signalling," *IEEE Trans. Communications*, vol. 47, pp. 558-567, 1999.
- [22] C. RöBing and V. Tarokh, "A construction of OFDM 16-QAM sequences having low peak powers," *IEEE Trans. Information Theory*, vol. 47, no. 11, pp. 2091-2094, Nov. 2001.
- [23] C. V. Chong, R. Venkataramani and V. Tarokh, "A new construction of 16-QAM Golay complementary sequences," *IEEE Trans. Information Theory*, vol. 49, no. 11, pp. 2953-2959, Nov. 2003.
- [24] J. Zhao, "A peal-to-mean power control scheme: the extended Rudin-Shapiro construction," In *VTC*, vol. 1. Los Angeles,USA:*IEEE* , 2004, pp. 373 377.
- [25] J. Zhao, "Efficient identification of the codewords with low peak-to-mean envelope power ratio of multicarrier transmission," In *VTC*, vol. 1. Los Angeles, USA: *IEEE* , 2004, pp. 621 625.
- [26] J. Zhao, "A new construction of 16-QAM codewords with low peak power," In *Trans. Engineering,computer and technology*, vol. 11. pp. 210-215, Feb, 2006,
- [27] G. Hill, M. Faulkner, and J. Singh, "Cyclic shifting and time inversion of partial transmit sequence OFDM," in *IEEE PIMRC*,. vol. 2, pp. 1256-1259, 2000 (Piscataway, USA).
- [28] B. M. Popovic, "Synthesis of power efficient multitone signals with flat amplitude spectrum," *IEEE Trans. Communications*,. vol. 39, pp. 1031-1033, 1991.
- [29] W. Rudin, "Some theorems on Fourier coefficients," *Proc. AMS*,. vol. 10, pp.855-859, 1959.
- [30] C.-C. Tseng, and C. L. Liu, "Complementary sets of sequences," *IEEE Trans. Information Theory*, vol. 18, no. 5,pp. 644-652, Sept. 1972.
- [31] J. Tellado, and J. M. Coiffi, "PAR reduction in multicarrier transmission system," *Technical Report*, Stanford University, 1998.