Complementary Sets, Generalized Reed–Muller Codes, and Power Control for OFDM

Kai-Uwe Schmidt

Abstract

The use of error-correcting codes for tight control of the peak-to-mean envelope power ratio (PMEPR) in orthogonal frequency-division multiplexing (OFDM) transmission is considered in this correspondence. By generalizing a result by Paterson, it is shown that each q-phase (q is even) sequence of length 2^m lies in a complementary set of size 2^{k+1}, where k is a nonnegative integer that can be easily determined from the generalized Boolean function associated with the sequence. For small k this result provides a reasonably tight bound for the PMEPR of q-phase sequences of length 2^m. A new 2^h-ary generalization of the classical Reed–Muller code is then used together with the result on complementary sets to derive flexible OFDM coding schemes with low PMEPR. These codes include the codes developed by Davis and Jedwab as a special case. In certain situations the codes in the present correspondence are similar to Paterson's code constructions and often outperform them.

Index Terms

Code, complementary, correlation, Golay, orthogonal frequency-division multiplexing (OFDM), peak-to-mean envelope power ratio (PMEPR), Reed–Muller, sequence, set

I. Introduction

In some applications the advantages of the orthogonal frequency-division multiplexing (OFDM) modulation technique are outweighed by the typically high peak-to-mean envelope power ratio (PMEPR) of uncoded OFDM signals. Among various approaches to solve this power-control issue, the use of block coding across the subcarriers [8], [7] is one of the more promising concepts [13]. Here the goal is to design error-correcting codes that contain only codewords with low PMEPR.

Sequences lying in *complementary pairs* [5], also called *Golay sequences*, are known to have PMEPR at most 2 in q-ary phase-shift keying (PSK) modulation [14]. In [4] Davis and Jedwab developed a powerful theory linking Golay sequences with generalized Reed–Muller codes. More

The author is with Communications Laboratory, Dresden University of Technology, 01062 Dresden, Germany, e-mail: schmidtk@ifn.et.tu-dresden.de, web: http://www.ifn.et.tu-dresden.de/∼schmidtk/

specifically, it was shown that a family of binary Golay sequences of length 2^m organizes in $m!/2$ cosets of $\mathrm{RM}_2(1,m)$ inside $\mathrm{RM}_2(2,m)$, where $\mathrm{RM}_2(r,m)$ is the Reed–Muller code of order r and length 2^m [9]. Similarly for $h > 1$ [4] identifies $m!/2$ cosets of $\mathrm{RM}_{2^h}(1,m)$ comprised of polyphase Golay sequences inside $\mathrm{ZRM}_{2^h}(2,m)$. Here $\mathrm{RM}_{2^h}(r,m)$ and $\mathrm{ZRM}_{2^h}(r,m)$ are generalizations of the classical Reed–Muller code over 2^h-ary alphabets. For small m, say $m \leq 5$, the union of these cosets yields powerful code with good error-correcting properties and strictly bounded PMEPR.

However the rate of this code rapidly tends to zero when the block length increases. Therefore Davis and Jedwab proposed [4] to include further cosets of $\mathrm{RM}_{2^h}(1,m)$ in order to increase the code rate at the cost of a slightly larger PMEPR. While in [4] such cosets have been identified with an exhaustive search, a more sophisticated theory was developed by Paterson in [12]; it was shown that each coset of $\mathrm{RM}_{2^h}(1,m)$ inside $\mathrm{RM}_{2^h}(2,m)$ can be partitioned into *complementary sets* of size 2^{k+1}, where k is a nonnegative integer that can be easily determined from a representative of the coset. Since the PMEPR of each sequence lying in a complementary set of size N has PMEPR at most N, [12] provides an upper bound on the PMEPR of arbitrary second-order cosets of $\mathrm{RM}_{2^h}(1,m)$. This result was then exploited in various ways to obtain coding schemes for OFDM, which extend those proposed in [4].

Several further constructions linking complementary sets and Reed–Muller codes have been described in [16], [11], [2]. Although these results often provide better upper bounds on the PMEPR than the work in [12], it seems difficult to use them to derive practicable coding schemes for OFDM.

In this correspondence we generalize the results from [12]. We will establish a construction of sequences that are contained in higher-order generalized Reed–Muller codes and lie in complementary sets of a given size. It appears that [12, Theorem 12] is a special case of this result. We will then relate this construction to a new generalization of the classical Reed–Muller code, which we call the *effective-degree Reed–Muller code*. In this way, we derive a number of new flexible OFDM coding schemes with low PMEPR. In contrast to the work in [12], all these codes arise in a uniform way from a general framework. Moreover they often outperform the coding options presented in [12]. The proposed codes are unions of cosets of a linear code over $\mathbb{Z}_{2^h}$ that contains in general more codewords than $\mathrm{RM}_{2^h}(1,m)$, although this linear code itself is a union of cosets of $\mathrm{RM}_{2^h}(1,m)$. Compared to the approaches in [4] and [12], this makes our codes more amenable to efficient encoding and decoding algorithms.

The remainder of this correspondence is organized as follows. In the next section we describe a simplified OFDM model, establish our main notation (which essentially follows that in [12]), and present some known results from [12]. Section III contains our results on complementary

sets. In Section IV we introduce the effective-degree Reed–Muller code and derive OFDM codes with low PMEPR. We close with a discussion in Section V.

II. Preliminaries

A. The OFDM Coding Problem

We consider an OFDM system with n subcarriers. The transmitted OFDM signal corresponding to the codeword $\boldsymbol{C} = (C_0, C_1, \ldots, C_{n-1}) \in \mathbb{C}^n$ is the real part of the *complex envelope*, which can be written as

$$S(\boldsymbol{C})(\theta) = \sum_{i=0}^{n-1} C_i \, e^{\sqrt{-1}2\pi(i+\zeta)\theta}, \quad 0 \le \theta < 1,$$

where ζ is a positive constant. In the following it is assumed that the elements of $\boldsymbol{C}$ are taken from a q-ary PSK constellation, i.e., $C_i = \xi^{c_i}$ with $\xi = e^{\sqrt{-1}2\pi/q}$ and $c_i \in \mathbb{Z}_q$. Then $\boldsymbol{C}$ is a polyphase sequence. This assumption together with Parseval's identity implies that the complex envelope has mean power equal to n. The PMEPR of the codeword $\boldsymbol{C}$ (or of the corresponding complex envelope) is then defined to be

$$\text{PMEPR}(\boldsymbol{C}) \triangleq \frac{1}{n} \sup_{0 \le \theta < 1} |S(\boldsymbol{C})(\theta)|^2.$$

The PMEPR is always less than or equal to n, where the maximum occurs, for example, if $\boldsymbol{C}$ is the all-one word. We aim at constructing codes $\mathcal{C}$ that have error-correcting capabilities and for which the value

$$\max_{\boldsymbol{C} \in \mathcal{C}} \text{PMEPR}(\boldsymbol{C})$$

is substantially lower than n.

B. Aperiodic Correlations and Complementary Sets

Given two complex-valued sequences $\boldsymbol{A} = (A_0, A_1 \ldots, A_{n-1})$ and $\boldsymbol{B} = (B_0, B_1 \ldots, B_{n-1})$ of length n, their *aperiodic cross-correlation* at a displacement $\ell \in \mathbb{Z}$ is defined to be

$$C(\boldsymbol{A}, \boldsymbol{B})(\ell) \triangleq \begin{cases} \sum_{i=0}^{n-\ell-1} A_{i+\ell} B_i^* & 0 \le \ell < n \\ \sum_{i=0}^{n+\ell-1} A_i B_{i-\ell}^* & -n < \ell < 0 \\ 0 & \text{otherwise,} \end{cases}$$

where $(.)^*$ denotes complex conjugation. The *aperiodic auto-correlation* of $\boldsymbol{A}$ at a displacement $\ell \in \mathbb{Z}$ is defined as

$$A(\boldsymbol{A})(\ell) \triangleq C(\boldsymbol{A}, \boldsymbol{A})(\ell).$$

Definition 1: A set of N sequences $\{\boldsymbol{A}^0, \boldsymbol{A}^1, \ldots, \boldsymbol{A}^{N-1}\}$ is a *complementary set of size* N if

$$\sum_{i=0}^{N-1} A(\boldsymbol{A}^i)(\ell) = 0 \quad \text{for each } \ \ell \neq 0.$$

If $N = 2$, the set is called a *complementary pair* (or *Golay complementary pair*) [5] and the sequences therein *Golay sequences*.

Golay sequences have found applications in many different areas of signal processing. The work of Popović [14], where it was essentially proved that polyphase Golay sequences have PMEPR at most 2, motivated the use of such sequences as codewords in OFDM [18], [17], [10], [4]. Paterson [12] generalized these results by proving:

Theorem 2 ([12]): Each polyphase sequence lying in a complementary set of size N has PMEPR at most N.

C. Generalized Boolean Functions, Associated Sequences and their Correlations

A *generalized Boolean function* f is defined as a mapping $f : \{0,1\}^m \to \mathbb{Z}_q$. Such a function can be written uniquely in the polynomial form

$$f(x_0, x_1, \ldots, x_{m-1}) = \sum_{i \in \{0,1\}^m} c_i \prod_{\alpha=0}^{m-1} x_\alpha^{i_\alpha}, \quad c_i \in \mathbb{Z}_q,$$

called the *algebraic normal form* of f. Sometimes we write f in place of $f(x_0, x_1, \ldots, x_{m-1})$. If $c_i = 1$ for exactly one i and zero otherwise, then f is called a *monomial*. Let $\deg(f)$ denote the algebraic degree of f.

A generalized Boolean function may be equally represented by sequences of length 2^m. Therefore suppose $0 \leq i < 2^m$ has binary expansion $(i_0, i_1, \ldots, i_{m-1})$ such that $i = \sum_{\alpha=0}^{m-1} i_\alpha 2^\alpha$ and $i_\alpha \in \{0,1\}$, and write $f_i = f(i_0, i_1, \ldots, i_{m-1})$. We define

$$\psi(f) \triangleq (f_0, f_1, \ldots, f_{2^m-1})$$

as the *$\mathbb{Z}_q$-valued sequence associated with* f and

$$\Psi(f) \triangleq (\xi^{f_0}, \xi^{f_1}, \ldots, \xi^{f_{2^m-1}})$$

as the *polyphase sequence associated with* f, where $\xi = e^{\sqrt{-1}2\pi/q}$.

In what follows we recall the technique of restricting generalized Boolean functions and their associated polyphase sequences. This technique was introduced in [12] in order to expand aperiodic correlations, as we shall see in Lemma 3.

Suppose that $f : \{0,1\}^m \to \mathbb{Z}_q$ is a generalized Boolean function in the variables $x_0, x_1, \ldots, x_{m-1}$, and let $\boldsymbol{F} = \Psi(f)$. Let a list of k indices be given by $0 \leq j_0 < j_1 < \cdots < j_{k-1} < m$, and

write $\boldsymbol{x} = (x_{j_0}, x_{j_1}, \ldots, x_{j_{k-1}})$. Let $\boldsymbol{d} = (d_0, d_1, \ldots, d_{k-1})$ be a binary word of length k, and let $(i_0, i_1, \ldots, i_{m-1})$ be the binary expansion of $0 \leq i < 2^m$. The *restricted sequence* $\boldsymbol{F}|_{\boldsymbol{x}=\boldsymbol{d}}$ is a sequence of length 2^m that coincides with $\boldsymbol{F}$ at the positions i where $i_{j_\alpha} = d_\alpha$ for each $0 \leq \alpha < k$. Otherwise $\boldsymbol{F}|_{\boldsymbol{x}=\boldsymbol{d}}$ is equal to zero. For $k = 0$ we define $\boldsymbol{F}|_{\boldsymbol{x}=\boldsymbol{d}} \triangleq \boldsymbol{F}$.

A sequence that is restricted in k variables comprises $2^m - 2^{m-k}$ zero entries and 2^{m-k} nonzero entries. Those nonzero entries are determined by a function, which is denoted as $f|_{\boldsymbol{x}=\boldsymbol{d}}$ and called a *restricted generalized Boolean function*. This function is a generalized Boolean function in $m-k$ variables and is obtained by replacing the variables x_{j_α} by d_α for all $0 \leq \alpha < k$ in the algebraic normal form of f. The restricted sequence $\boldsymbol{F}|_{\boldsymbol{x}=\boldsymbol{d}}$ is then recovered by associating a polyphase sequence of length 2^{m-k} with $f|_{\boldsymbol{x}=\boldsymbol{d}}$ and inserting $2^m - 2^{m-k}$ zeros at the corresponding positions. Similarly to a disjunctive normal form of a Boolean function [9], the original function f can be reconstructed from the functions $f|_{\boldsymbol{x}=\boldsymbol{d}}$ by

$$f = \sum_{\boldsymbol{d} \in \{0,1\}^k} f|_{\boldsymbol{x}=\boldsymbol{d}} \prod_{\alpha=0}^{k-1} x_{j_\alpha}^{d_\alpha} (1 - x_{j_\alpha})^{(1-d_\alpha)}.$$

Lemma 3 ([12]): Suppose that $f : \{0,1\}^m \to \mathbb{Z}_q$ is a generalized Boolean function, and let $\boldsymbol{F} = \Psi(f)$. Let $0 \leq j_0 < j_1 < \cdots < j_{k-1} < m$ be a list of k indices. Write $\boldsymbol{x} = (x_{j_0}, x_{j_1}, \ldots, x_{j_{k-1}})$, and let $\boldsymbol{d}, \boldsymbol{d}_1, \boldsymbol{d}_2 \in \{0,1\}^k$. Then we have

$$A(\boldsymbol{F})(\ell) = \sum_{\boldsymbol{d}} A(\boldsymbol{F}|_{\boldsymbol{x}=\boldsymbol{d}})(\ell) + \sum_{\boldsymbol{d}_1 \neq \boldsymbol{d}_2} C(\boldsymbol{F}|_{\boldsymbol{x}=\boldsymbol{d}_1}, \boldsymbol{F}|_{\boldsymbol{x}=\boldsymbol{d}_2})(\ell).$$

D. A Known Construction of Complementary Pairs

Next we recall a construction of complementary pairs from [12]. A quadratic polynomial f over $\mathbb{Z}_q$ in the $\{0,1\}$-valued variables $x_{i_0}, x_{i_1}, \ldots, x_{i_{m-1}}$ is generally given by

$$f(x_{i_0}, \ldots, x_{i_{m-1}}) = \sum_{0 \leq j < k < m} b_{jk} x_{i_j} x_{i_k} + a(x_{i_0}, \ldots, x_{i_{m-1}}),$$

where $b_{jk} \in \mathbb{Z}_q$ and a is an affine form over $\mathbb{Z}_q$. With each such a polynomial one can associate a labeled graph, denoted by $G(f)$. The vertices of this graph are labeled with $i_0, i_1, \ldots, i_{m-1}$, and the edge between vertex i_j and vertex i_k is labeled with b_{jk}.

Such a graph is called a *path* in m vertices if q is even and $m = 1$ (then the graph consists of a single vertex) or if q is even, $m \geq 2$, and f is of the form

$$f(x_{i_0}, \ldots, x_{i_{m-1}}) = \frac{q}{2} \sum_{\alpha=0}^{m-2} x_{i_{\pi(\alpha)}} x_{i_{\pi(\alpha+1)}} + a(x_{i_0}, \ldots, x_{i_{m-1}}),$$

where π is a permutation of $\{0, 1, \ldots, m-1\}$. The indices $i_{\pi(0)}$ and $i_{\pi(m-1)}$ are called *end vertices* of the path. If the path consists of a single vertex, this vertex is called an end vertex as well.

We are now in a position to quote:

Theorem 4 ([12]): Suppose $m > k$. Let $0 \le j_0 < j_1 < \cdots < j_{k-1} < m$ be a list of k indices, write $\boldsymbol{x} = (x_{j_0}, x_{j_1}, \ldots, x_{j_{k-1}})$, and let $\boldsymbol{d} \in \{0,1\}^k$. Suppose $f : \{0,1\}^m \to \mathbb{Z}_q$ is a generalized Boolean function such that $f|_{\boldsymbol{x}=\boldsymbol{d}}$ is quadratic and $G(f|_{\boldsymbol{x}=\boldsymbol{d}})$ is a path in $m-k$ vertices. Write $\boldsymbol{F} = \Psi(f)$ and $\boldsymbol{F}' = \Psi(f + (q/2)x_a + c')$. Then $\boldsymbol{F}|_{\boldsymbol{x}=\boldsymbol{d}}$ and $\boldsymbol{F}'|_{\boldsymbol{x}=\boldsymbol{d}}$ form a complementary pair. Here, a is an end vertex of the path $G(f|_{\boldsymbol{x}=\boldsymbol{d}})$ and $c' \in \mathbb{Z}_q$.

In particular, if $k = 0$, the preceding theorem identifies $(m!/2)q^{m+1}$ polyphase sequences lying in complementary pairs [12, Corollary 11], which generalizes the original result by Davis and Jedwab [4, Theorem 3] from q being a power of 2 to even q.

III. A Construction of Complementary Sets

In what follows we prove that each polyphase sequence of length 2^m lies in a complementary set, whose size can be easily determined by inspecting the generalized Boolean function associated with the sequence.

Theorem 5: Suppose $m > k$. Let $0 \le j_0 < j_1 < \cdots < j_{k-1} < m$ be a list of k indices, and write $\boldsymbol{x} = (x_{j_0}, x_{j_1}, \ldots, x_{j_{k-1}})$. Let $f : \{0,1\}^m \to \mathbb{Z}_q$ be a generalized Boolean function such that for each $\boldsymbol{d} \in \{0,1\}^k$ the restricted function $f|_{\boldsymbol{x}=\boldsymbol{d}}$ is quadratic and $G(f|_{\boldsymbol{x}=\boldsymbol{d}})$ is a path in $m-k$ vertices. Then $\Psi(f)$ lies in a complementary set of size 2^{k+1}, and the PMEPR of $\Psi(f)$ is at most 2^{k+1}.

Proof: Write $\boldsymbol{d} = (d_0, d_1, \ldots, d_{k-1})$ and $\boldsymbol{c} = (c_0, c_1, \ldots, c_{k-1})$. Define

$$\boldsymbol{F}_{\boldsymbol{c}c'} = \Psi\left(f \;+\; \frac{q}{2}\sum_{\alpha=0}^{k-1} c_\alpha\, x_{j_\alpha} + \frac{q}{2}\, c'\, e\right),$$

where $\boldsymbol{c} \in \{0,1\}^k$, $c' \in \{0,1\}$,

$$e = \sum_{\boldsymbol{d}\in\{0,1\}^k} x_{a_{\boldsymbol{d}}} \prod_{\alpha=0}^{k-1} x_{j_\alpha}^{d_\alpha}(1-x_{j_\alpha})^{(1-d_\alpha)},$$

and $a_{\boldsymbol{d}}$ is an end vertex of the path $G(f|_{\boldsymbol{x}=\boldsymbol{d}})$. We claim that the set

$$\left\{\boldsymbol{F}_{\boldsymbol{c}c'} \mid \boldsymbol{c} \in \{0,1\}^k, c' \in \{0,1\}\right\},$$

which contains $\Psi(f)$, is a complementary set of size 2^{k+1}. To prove this, it has to be shown that the sum of auto-correlations $\sum_{\boldsymbol{c},\,c'} A\left(\boldsymbol{F}_{\boldsymbol{c}c'}\right)(\ell)$ is zero for each $\ell \neq 0$. We employ Lemma 3 and write

$$\sum_{\boldsymbol{c},\,c'} A(\boldsymbol{F}_{\boldsymbol{c}c'})(\ell) = S_1 + S_2,$$

where

$$S_1 = \sum_{\boldsymbol{c},\, c'} \sum_{\boldsymbol{d}} A(\boldsymbol{F}_{\boldsymbol{c}c'}|_{\boldsymbol{x}=\boldsymbol{d}})(\ell)$$
$$S_2 = \sum_{\boldsymbol{c},\, c'} \sum_{\boldsymbol{d}_1 \neq \boldsymbol{d}_2} C(\boldsymbol{F}_{\boldsymbol{c}c'}|_{\boldsymbol{x}=\boldsymbol{d}_1}, \boldsymbol{F}_{\boldsymbol{c}c'}|_{\boldsymbol{x}=\boldsymbol{d}_2})(\ell).$$

We first focus on the term S_1, which can be written as

$$S_1 = \sum_{\boldsymbol{c}} \sum_{\boldsymbol{d}} \left[A(\boldsymbol{F}_{\boldsymbol{c}0}|_{\boldsymbol{x}=\boldsymbol{d}})(\ell) + A(\boldsymbol{F}_{\boldsymbol{c}1}|_{\boldsymbol{x}=\boldsymbol{d}})(\ell) \right].$$

Note that $e|_{\boldsymbol{x}=\boldsymbol{d}} = x_{a_{\boldsymbol{d}}}$. Thus the restricted functions corresponding to $\boldsymbol{F}_{\boldsymbol{c}0}|_{\boldsymbol{x}=\boldsymbol{d}}$ and $\boldsymbol{F}_{\boldsymbol{c}1}|_{\boldsymbol{x}=\boldsymbol{d}}$ are of the form

$$f|_{\boldsymbol{x}=\boldsymbol{d}} + \frac{q}{2} \sum_{\alpha=0}^{k-1} c_\alpha\, d_\alpha$$
$$f|_{\boldsymbol{x}=\boldsymbol{d}} + \frac{q}{2} \sum_{\alpha=0}^{k-1} c_\alpha\, d_\alpha + \frac{q}{2}\, x_{a_{\boldsymbol{d}}},$$

respectively. Notice that the term containing the sum over α is a constant occurring in both functions. Hence, by hypothesis and by Theorem 4, $\boldsymbol{F}_{\boldsymbol{c}0}|_{\boldsymbol{x}=\boldsymbol{d}}$ and $\boldsymbol{F}_{\boldsymbol{c}1}|_{\boldsymbol{x}=\boldsymbol{d}}$ form a complementary pair. It follows that the inner term of S_1 is zero for each $\ell \neq 0$. Thus also S_1 itself is zero for each $\ell \neq 0$.

It remains to show that the sum S_2 is zero. This part of the proof follows more or less the same reasoning as the second part of the proof of [12, Theorem 12]. □

We have a number of notes on Theorem 5. If $k = 0$, Theorem 5 applies to $(m!/2)q^{m+1}$ polyphase sequences lying in complementary pairs. These are exactly those identified by setting $k = 0$ in Theorem 4. For $k > 0$ Theorem 5 essentially generalizes [12, Theorem 12]; if f is constrained to be a quadratic generalized Boolean function, then Theorem 5 virtually reduces to [12, Theorem 12].

The proof of Theorem 5 shows that the sequence $\Psi(f)$ lies in a complementary set that can be decomposed into 2^k complementary pairs identified by Theorem 4. By reversing this process, the sequence $\Psi(f)$ can be constructed by interleaving 2^k Golay sequences from Theorem 4. However the sole application of such an interleaving method would not directly admit the construction of sequences corresponding to generalized Boolean functions of a specific degree, which will be required to derive flexible coding schemes in the next section.

We also remark that it cannot be expected that Theorem 5 provides tight PMEPR bounds for each individual sequence, especially when k is large. Indeed [16] (in particular [16, Theorem 3.6]) and the recent work [2] contain significant improvements of Theorem 5 in certain situations.

However it seems difficult to exploit these results to derive coding schemes that admit efficient encoding and decoding.

In summary, the usefulness of Theorem 5 lies in the fact that it provides a relatively simple method to identify sets of sequences that correspond to generalized Boolean functions of a given (preferably low) degree and whose PMEPR is bounded above by a given power of 2.

We close this section with an example for the application of Theorem 5.

Example 6: We take $q = 2$ and $m = 4$. Let $f : \{0,1\}^4 \to \mathbb{Z}_2$ be given by

$$f(x_0, x_1, x_2, x_3) = x_0x_1x_2 + x_0x_1x_3 + x_0x_2 + x_1x_3 + x_2x_3.$$

By restricting f in x_0 (i.e., $\boldsymbol{x} = (x_0)$), we obtain the two restricted functions

$$f|_{x_0=0} = x_1x_3 + x_2x_3$$
$$f|_{x_0=1} = x_1x_2 + x_2x_3 + x_2,$$

which are quadratic and their associated graphs are paths in 3 vertices. Hence, by Theorem 5, the PMEPR of $\Psi(f)$ is at most 4. By direct computation it can be observed that the true PMEPR of $\Psi(f)$ is approximately 3.32.

IV. OFDM Codes with Low PMEPR

A. The Effective-Degree Reed–Muller Code

A code of length n over the ring $\mathbb{Z}_{2^h}$ is linear if it is a submodule of $\mathbb{Z}_{2^h}^n$. A coset of a linear code $\mathcal{C} \subseteq \mathbb{Z}_{2^h}^n$ is defined to be $\{\boldsymbol{a} + \boldsymbol{c} \,|\, \boldsymbol{c} \in \mathcal{C}\}$, where $\boldsymbol{a} \in \mathbb{Z}_{2^h}^n$ is a representative of this coset. Despite the fact that a linear code $\mathcal{C}$ defined over a ring does not necessarily have a basis, one can associate a generator matrix with $\mathcal{C}$ such that the codewords of $\mathcal{C}$ are all distinct $\mathbb{Z}_{2^h}$-linear combinations of the rows of this matrix. For background on linear codes over rings we refer to [6] and [1].

In what follows we generalize the classical Reed–Muller codes [9] to linear codes over $\mathbb{Z}_{2^h}$. We begin with defining the effective degree of a generalized Boolean function.

Definition 7: Let $f : \{0,1\}^m \to \mathbb{Z}_{2^h}$ be a generalized Boolean function. We define the *effective degree of* f to be

$$\max_{0 \le i < h} \left[\deg \left(f \bmod 2^{i+1} \right) - i \right].$$

For instance, the function $f : \{0,1\}^3 \to \mathbb{Z}_8$ given by $f = 4x_0x_1x_2 + x_1$ has effective degree equal to 1. Now let $\mathcal{F}(r, m, h)$ be the set of all generalized Boolean functions $\{0,1\}^m \to \mathbb{Z}_{2^h}$ of effective degree at most r. A simple counting argument leads to

$$\log_2 \left| \mathcal{F}(r, m, h) \right| = \sum_{i=0}^{r} h \binom{m}{i} + \sum_{i=1}^{h-1} (h - i) \binom{m}{r+i}. \tag{1}$$

Definition 8: For $0 \leq r \leq m$ we define the *effective-degree Reed–Muller code* as

$$\mathrm{ERM}(r,m,h) \triangleq \{\psi(f) \,|\, f \in \mathcal{F}(r,m,h)\}\,.$$

It follows that $\mathrm{ERM}(r,m,h)$ is a linear code over $\mathbb{Z}_{2^h}$ and, since the effective degree and the algebraic degree coincide for $h=1$, $\mathrm{ERM}(r,m,1)$ is the classical Reed–Muller code [9]. A generator matrix for $\mathrm{ERM}(r,m,h)$ has rows corresponding to the words associated with monomials in the variables $x_0, x_1, \ldots, x_{m-1}$ of degree at most r together with 2^i times the monomials of degree $r+i$, where $i = 1, \ldots, h-1$. For example a generator matrix for $\mathrm{ERM}(0,3,3)$ is given by:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 \\ 0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 4 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 & 4 \end{bmatrix} \begin{matrix} 1 \\ 2x_0 \\ 2x_1 \\ 2x_2 \\ 4x_0x_1 \\ 4x_0x_2 \\ 4x_1x_2. \end{matrix}$$

Now let $\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1})$ be a word with elements in $\mathbb{Z}_{2^h}$. The Lee weight of $\boldsymbol{a}$ is defined to be

$$\mathrm{wt}_L(\boldsymbol{a}) \triangleq \sum_{i=0}^{n-1} \min\{a_i, 2^h - a_i\},$$

and its squared Euclidean weight (when the entries of $\boldsymbol{a}$ are mapped onto a 2^h-ary PSK constellation) is given by

$$\mathrm{wt}_E^2(\boldsymbol{a}) \triangleq \sum_{i=0}^{n-1} \left|\xi^{a_i} - 1\right|^2,$$

where $\xi = e^{\sqrt{-1}2\pi/2^h}$. Let $\mathrm{d}_L(\boldsymbol{a},\boldsymbol{b}) \triangleq \mathrm{wt}_L(\boldsymbol{a}-\boldsymbol{b})$ and $\mathrm{d}_E^2(\boldsymbol{a},\boldsymbol{b}) \triangleq \mathrm{wt}_E^2(\boldsymbol{a}-\boldsymbol{b})$ be the Lee and squared Euclidean distance between $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}_{2^h}^n$, respectively. We shall use the standard notation $\mathrm{d}_L(\mathcal{C})$ and $\mathrm{d}_E^2(\mathcal{C})$ to refer to the respective minimum distances (taken over all distinct codewords) of a code $\mathcal{C} \subseteq \mathbb{Z}_{2^h}^n$. The minimum squared Euclidean distance of a code essentially determines the performance of the code when employed for transmission over a white Gaussian noise channel at high signal-to-noise ratios.

Theorem 9: We have

$$\begin{aligned} \mathrm{d}_L(\mathrm{ERM}(r,m,h)) &= 2^{m-r} \\ \mathrm{d}_E^2(\mathrm{ERM}(r,m,h)) &= 2^{m-r+2}\sin^2\left(\frac{\pi}{2^h}\right). \end{aligned}$$

Proof: Since $\mathrm{ERM}(r,m,h)$ is linear, its minimum Lee distance is equal to the minimum Lee weight of the nonzero codewords. We shall first find a lower bound for the minimum Lee weight. It is then shown at the end of the proof that this bound is tight. Since $\mathrm{ERM}(r,m,1)$ is the classical Reed–Muller code, the theorem holds for $h=1$ (cf. [9]). This case serves as the anchor for the following induction. Let $\boldsymbol{a}=(a_0,a_1,\ldots,a_{n-1})$ be a nonzero codeword in $\mathrm{ERM}(r,m,h)$. For $h>1$ let $b_i=a_i \pmod{2^{h-1}}$. Then $\boldsymbol{b}=(b_0,b_1,\ldots,b_{n-1})$ is a codeword in $\mathrm{ERM}(r,m,h-1)$. Since $a_i\in\{b_i,b_i+2^{h-1}\}$, it holds $\min\{a_i,2^h-a_i\}\geq\min\{b_i,2^{h-1}-b_i\}$, and therefore, $\mathrm{wt}_L(\boldsymbol{a})\geq\mathrm{wt}_L(\boldsymbol{b})\geq 2^{m-r}$, by induction on h.

Now let us prove a lower bound on the minimum squared Euclidean distance. Again we have to find the minimum of $\mathrm{wt}_E^2(\boldsymbol{a})$ taken over all nonzero words $\boldsymbol{a}\in\mathrm{ERM}(r,m,h)$. For any $u\in\mathbb{Z}_{2^h}$ we have

$$\begin{aligned}|\xi^u-1|^2&=4\sin^2\left(u\frac{\pi}{2^h}\right)\\&=4\sin^2\left(\mathrm{wt}_L(u)\frac{\pi}{2^h}\right).\end{aligned}$$

For $1\leq w\leq 2^{h-1}$ it can be shown that

$$\sin^2\left(w\frac{\pi}{2^h}\right)\geq w\sin^2\left(\frac{\pi}{2^h}\right).$$

Let $N_{\boldsymbol{a}}(w)$ denote the number of entries in $\boldsymbol{a}$ with Lee weight equal to w. Indeed

$$\begin{aligned}\mathrm{wt}_E^2(\boldsymbol{a})&=4\sum_{w=1}^{2^{h-1}}N_{\boldsymbol{a}}(w)\sin^2\left(w\frac{\pi}{2^h}\right)\\&\geq 4\sin^2\left(\frac{\pi}{2^h}\right)\sum_{w=1}^{2^{h-1}}wN_{\boldsymbol{a}}(w)\\&=4\sin^2\left(\frac{\pi}{2^h}\right)\mathrm{wt}_L(\boldsymbol{a}).\end{aligned}\tag{2}$$

It remains to exhibit a codeword in $\mathrm{ERM}(r,m,h)$, for which the lower bounds are tight. Such a word is, for example, the word associated with the monomial $x_0\,x_1\cdots x_r$. This word has Lee weight 2^{m-r}, and since it only contains zeros and ones, equality holds in (2). □

Next we relate $\mathrm{ERM}(r,m,h)$ to the codes $\mathrm{RM}_{2^h}(r,m)$ and $\mathrm{ZRM}_{2^h}(r,m)$ given in [4]. These codes also generalize the binary Reed–Muller code to linear codes over $\mathbb{Z}_{2^h}$. We have

$$\mathrm{RM}_{2^h}(r,m)\subseteq\mathrm{ERM}(r,m,h),$$

where the inclusion is proper if $h>1$ and $r<m$. Hence for $h>1$ and $r<m$ the code $\mathrm{ERM}(r,m,h)$ contains more codewords than $\mathrm{RM}_{2^h}(r,m)$, while both codes have minimum Lee distance equal to 2^{m-r}. For $h\geq 2$

$$\mathrm{ZRM}_{2^h}(r+1,m)\subseteq\mathrm{ERM}(r,m,h),$$

which is a proper inclusion if $h > 2$ and $r < m-1$. Hence for $h > 2$ and $r < m-1$ the code $\mathrm{ERM}(r,m,h)$ contains more codewords than $\mathrm{ZRM}_{2^h}(r+1,m)$, while their minimum Lee distances are equal to 2^{m-r}.

B. OFDM Code Constructions

We begin with defining a linear code over $\mathbb{Z}_{2^h}$.

Definition 10: For $0 \le k < m$, $0 \le r \le k+1$, and $h \ge 1$ we define the code $\mathcal{A}(k,r,m,h)$ to be the set of words corresponding to the set of polynomials

$$\left\{ \sum_{i=0}^{m-k-1} x_\alpha g_i(x_{m-k},\ldots,x_{m-1}) + g(x_{m-k},\ldots,x_{m-1}) \,\middle|\, g_0,\ldots,g_{m-k-1} \in \mathcal{F}(r-1,k,h), g \in \mathcal{F}(r,k,h) \right\}.$$

Notice that $\mathcal{A}(0,1,m,h)$ is equal to the generalized first-order Reed–Muller code $\mathrm{RM}_{2^h}(1,m)$, described in [4]. It follows from Definition 10 that $\mathcal{A}(k,r,m,h)$ is a linear code over $\mathbb{Z}_{2^h}$. Moreover

$$\mathcal{A}(k,r,m,h) \subseteq \mathrm{ERM}(r,m,h),$$

and therefore, the minimum distances of $\mathcal{A}(k,r,m,h)$ can be lower-bounded with Theorem 9. We remark that, similarly as in the proof of Theorem 9, a particular word in $\mathcal{A}(k,r,m,h)$ can be identified showing that the lower bounds are in fact tight. The number of codewords in $\mathcal{A}(k,r,m,h)$ is equal to 2^s, where

$$s = (m-k)\cdot \log_2 \left|\mathcal{F}(r-1,k,h)\right| + \log_2 \left|\mathcal{F}(r,k,h)\right|, \tag{3}$$

which can be computed with (1).

As an example consider $\mathcal{A}(1,0,3,3)$. This code is a linear subcode of $\mathrm{ERM}(0,3,3)$ and has a generator matrix:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 4 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 & 4 \end{bmatrix} \begin{matrix} 1 \\ 2x_0 \\ 2x_1 \\ 2x_2 \\ 4x_0x_2 \\ 4x_1x_2. \end{matrix}$$

Now let $\mathcal{R}(k,m,h)$ be the set of words associated with the following polynomials over $\mathbb{Z}_{2^h}$

$$2^{h-1} \sum_{\boldsymbol{d}\in\{0,1\}^k} \sum_{i=0}^{m-k-2} x_{\pi_{\boldsymbol{d}}(i)} x_{\pi_{\boldsymbol{d}}(i+1)} \prod_{j=0}^{k-1} x_{m-k+j}^{d_j} (1-x_{m-k+j})^{(1-d_j)},$$

where $\boldsymbol{d} = (d_0, d_1, \ldots, d_{k-1})$ and $\pi_{\boldsymbol{d}}$ are 2^k permutations of $\{0, 1, \ldots, m-k-1\}$.

Corollary 11: The corresponding polyphase words in the cosets of $\mathcal{A}(k, r, m, h)$ with coset representatives in $\mathcal{R}(k, m, h)$ have PMEPR at most 2^{k+1}.

Proof: The corollary is a consequence of Theorem 5 and the following observations. By restricting any function corresponding to a word in $\mathcal{A}(k, r, m, h)$ in the variables $x_{m-k}, \ldots, x_{m-1}$, we obtain an affine function, and by restricting any function associated with a word in $\mathcal{R}(k, m, h)$ in the same variables, we obtain a quadratic polynomial, whose graph is a path of length $m-k$. □

We are now in a position to construct a simple code.

Construction 12: Take a single coset of $\mathcal{A}(k, r, m, h)$ that contains a word in $\mathcal{R}(k, m, h)$. The polyphase versions of the words in this code have PMEPR at most 2^{k+1}. The code has minimum Lee and squared Euclidean distance equal to 2^{m-r} and $2^{m-r+2}\sin^2\left(\frac{\pi}{2^h}\right)$, respectively, and the number of encoded bits per codeword is equal to $s = \log_2 |\mathcal{A}(k, r, m, h)|$, which is given in (3).

In order to obtain a more elaborate code construction, we prove:

Lemma 13: For $m - k > 1$ and $r > 2 - h$ the set $\mathcal{R}(k, m, h)$ contains

$$\left[\frac{(m-k)!}{2}\right]^{2^{\min\{r+h-3,k\}}} \tag{4}$$

words corresponding to a generalized Boolean function of effective degree at most r.

Proof: The set $\mathcal{R}(k, m, h)$ contains exactly $[(m-k)!/2]^{2^k}$ words, all having effective degree at most $k+3-h$. Hence the lemma is true for $r \geq k+3-h$. It is also clear that the expression in (IV-B) has algebraic degree at least 2, so the effective degree is at least $3-h$. Now suppose that $3-h \leq r < k+3-h$, and write $\ell = r+h-3$, where $0 \leq \ell < k$. By factoring out terms in the outer sum in (IV-B), it can be verified that, if

$$\pi_{(d_0,\ldots,d_{\ell-1},\, d_\ell,\ldots,d_{k-1})} = \pi_{(d_0,\ldots,d_{\ell-1},\, 1-d_\ell,\ldots,1-d_{k-1})},$$

then (IV-B) is independent of the variables $x_{m-k+\ell}, \ldots, x_{m-1}$ and, therefore, has effective degree at most $r = \ell + 3 - h$. This leaves the choice of $2^\ell = 2^{r+h-3}$ permutations of the symbols $\{0, 1, \ldots, m-k-1\}$ that are distinct under reversal (e.g., all permutations satisfying $\pi(0) < \pi(m-k-1)$) to obtain distinct words in $\mathcal{R}(k, m, h)$ with effective degree at most $\ell + 3 - h$. This leads in total to the number given in (4). □

Construction 14: Suppose $m - k > 1$. Let $2 \leq r \leq k+2$ when $h = 1$ and $1 \leq r \leq k+1$ when $h > 1$. Write $r' = \min\{r, k+1\}$. Let 2^t be the largest power of 2 not exceeding (4). Now take the union of 2^t distinct cosets of $\mathcal{A}(k, r', m, h)$, each containing a word in $\mathcal{R}(k, m, h)$ with effective degree at most r. The PMEPR of the corresponding polyphase words in this code is at most 2^{k+1}, and one can encode $s + t$ bits, where $s = \log_2 |\mathcal{A}(k, r', m, h)|$. Since the code is

a subcode of $\mathrm{ERM}(r, m, h)$, its minimum Lee and squared Euclidean distance is at least 2^{m-r} and $2^{m-r+2}\sin^2\left(\frac{\pi}{2^h}\right)$, respectively. These are tight bounds if $r = r'$.

We remark that, when $k = 0$, Construction 14 essentially restates the construction by Davis and Jedwab [4]. A list of coding options having PMEPR at most 4 and at most 8 is compiled in Tables I and II, respectively. The quantities d_L and d_E^2 indicate lower bounds for the minimum Lee and the minimum squared Euclidean distance of the codes, respectively. The code with rate $R_1 = s/2^m$ is obtained with Construction 12, and the code with rate $R_2 = (s + t)/2^m$ arises from Construction 14. Notice that our definition of the code rate differs from the common one $\log_{2^h} |\mathcal{C}|/2^m$. The present definition has the advantage that it allows a fair comparison of codes over different alphabets on the basis of code rate and minimum squared Euclidean distance.

Finally, we wish to sketch how the proposed codes can be generally encoded and decoded. Encoding of the code $\mathcal{A}$ is straightforward by using a generator matrix for $\mathcal{A}$. Encoding of a union of cosets of $\mathcal{A}$ can be performed by using the information symbols partly to encode a word from $\mathcal{A}$ and partly to select a coset representative from a stored list. For decoding one needs to have an efficient algorithm to decode the linear code $\mathcal{A}$. This already provides a decoder for the codes from Construction 12. Then codes from Construction 14 can be decoded by applying the supercode decoding method, as described in [3] and [4]. Such a concept involves subtracting all possible coset representatives from the received word in turn, and passing the resulting words to a decoder for the code $\mathcal{A}$. Among those decoder outputs the word that is closest to the received word determines the final decoding result.

V. Discussion and Relations to Previous Constructions

It can be observed that QPSK (quaternary PSK) codes are always better than BPSK (binary PSK) codes, i.e., we can always construct a QPSK code with higher code rate and the same minimum Euclidean distance as a BPSK code. By moving to larger alphabets, the code rate can be increased further, but only at the cost of a smaller minimum Euclidean distance.

It should be noted that Corollary 11 and the arising code constructions do not exploit Theorem 5 in the most general way. The generalized Boolean functions corresponding to the words in the cosets identified in Corollary 11 are characterized by the property that by restricting the functions in the variables $x_{m-k}, \ldots, x_{m-1}$, we obtain quadratic functions whose graphs are paths in the vertices $0, \ldots, m-k-1$. In order to increase the size of the codes in Constructions 12 and 14, we can, according to Theorem 5, apply any permutation to the m variables in the functions corresponding to the codewords (instead of only to a fixed set of $m-k$ variables). This, however, has the unwanted effect that some codewords are generated more than once. Such an approach, coupled with rather complicated techniques to remove multiple codewords, has been used in [12],

TABLE I

CODING OPTIONS WITH PMEPR AT MOST 4

m	h	r	s	t	R_1	R_2	d_L	d_E^2
4	1	2	8	1	0.50	0.56	4	16.00
		3	8	3	—	0.69	2	8.00
	2	1	13	1	0.81	0.88	8	16.00
		2	16	3	1.00	1.19	4	8.00
	3	1	21	3	1.31	1.50	8	4.69
		2	24	3	1.50	1.69	4	2.34
5	1	2	10	3	0.31	0.41	8	32.00
		3	10	7	—	0.53	4	16.00
	2	1	16	3	0.50	0.59	16	32.00
		2	20	7	0.63	0.84	8	16.00
	3	1	26	7	0.81	1.03	16	9.37
		2	30	7	0.94	1.16	8	4.69
6	1	2	12	5	0.19	0.27	16	64.00
		3	12	11	—	0.36	8	32.00
	2	1	19	5	0.30	0.38	32	64.00
		2	24	11	0.38	0.55	16	32.00
	3	1	31	11	0.48	0.66	32	18.75
		2	36	11	0.56	0.73	16	9.37

where the functions are constrained to have quadratic degree. Our approach has the advantage that these difficulties are avoided. Moreover, compared to the concept in [12], it allows us to construct our codes as unions of relatively few cosets of a relatively large linear code, which presumably simplifies the decoding process. The penalty of this simplification is a loss of at most $\log_2 \binom{m}{k}$ encodable information bits (since, instead of $\binom{m}{k}$ possible index sets, we choose just one set of $m-k$ indices that form the vertices of the paths in the graphs of the restricted functions). This loss is moderate for typical choices of m and k.

Finally we wish to compare the codes arising from Construction 14 with those in [4] and [12]. The codes in the latter references are contained in $\mathrm{RM}_{2^h}(2,m)$ or $\mathrm{ZRM}_{2^h}(2,m)$, which ensures a minimum Lee distance of at least 2^{m-2} or 2^{m-1}, respectively. So we compare these codes with codes arising from Construction 14 having the same lower bound on the minimum Lee distance, i.e., we let $r \in \{1,2\}$. Also we let $k=1$, which covers the majority of the codes in [4] and [12] having PMEPR greater than 2.

For $h=1$, $r=2$, and $m \geq 3$ the code from Construction 14 can be used to encode

$$\lfloor \log_2(m-1)! \rfloor + 2m - 1$$

bits. This yields 13 and 17 bits for $m=5$ and $m=6$, respectively. These values should be

TABLE II

CODING OPTIONS WITH PMEPR AT MOST 8

m	h	r	s	t	R_1	R_2	d_L	d_E^2
5	1	2	13	1	0.41	0.44	8	32.00
		3	16	3	0.50	0.59	4	16.00
		4	16	6	—	0.69	2	8.00
	2	1	19	1	0.59	0.63	16	32.00
		2	29	3	0.91	1.00	8	16.00
		3	32	6	1.00	1.19	4	8.00
	3	1	35	3	1.09	1.19	16	9.37
		2	45	6	1.41	1.59	8	4.69
		3	48	6	1.50	1.69	4	2.34
6	1	2	16	3	0.25	0.30	16	64.00
		3	20	7	0.31	0.42	8	32.00
		4	20	14	—	0.53	4	16.00
	2	1	23	3	0.36	0.41	32	64.00
		2	36	7	0.56	0.67	16	32.00
		3	40	14	0.63	0.84	8	16.00
	3	1	43	7	0.67	0.78	32	18.75
		2	56	14	0.88	1.09	16	9.37
		3	60	14	0.94	1.16	8	4.69

compared with 11 and 17 bits in [12, Table I], which suggests that for $h = 1$ and for small m our construction is slightly stronger than that in [12]. However for $h = 1$ and $m \geq 8$ it was stated in [12] that the number of encoded bits of the codes in [12] is equal to $\lfloor \log_2 m! \rfloor + 2m - 2$. Hence for large m the binary code from [12] allows to encode either $\lfloor \log_2 m \rfloor$ or $\lfloor \log_2 m \rfloor - 1$ bits more than a comparable code arising from Construction 14. We arrive at a similar conclusion for $h = 2$ and $r = 1$. For $m \geq 3$ we can encode

$$\lfloor \log_2 (m-1)! \rfloor + 3m$$

bits, which is, compared to a code in [12] with the same minimum distance, slightly larger for small m and is either $\lfloor \log_2 m \rfloor$ or $\lfloor \log_2 m \rfloor - 1$ bits less for $m \geq 8$.

For $h \geq 2$, $r = 2$, and $m \geq 3$ Construction 14 yields a code, which can be used to encode

$$\lfloor 2 \cdot \log_2 (m-1)! \rfloor + 2hm - 2$$

bits. When $m \geq 4$, the number of encoded bits for a comparable code in [12] is equal to $\lfloor \log_2 m! \rfloor + 2hm - 2$. This is $\lfloor \log_2 m! - 2 \cdot \log_2 m \rfloor$ or $\lfloor \log_2 m! - 2 \cdot \log_2 m \rfloor + 1$ bits less than the code from Construction 14. Similar results can be established for $h > 2$ and $r = 1$.

In summary, except for large m in the cases $(h, r) = (1, 2)$ and $(h, r) = (2, 1)$, the codes from Construction 14 outperform coding schemes proposed proposed in [12].

Based on exhaustive computational search, [4] reports codes that outperform the codes given in the first and the third row of Table I by one encoded information bit and the codes in the seventh and ninth row of Table I by two encoded information bits. These observations can be partly explained using a variety of individual theorems from [15], [12], [16], [2] and show that stronger constructions are possible in some situations. However the description of such codes (and therefore encoding and decoding) tends to be unwieldy.

REFERENCES

[1] A. R. Calderbank and N. J. A. Sloane, "Modular and p-adic cyclic codes," *Designs, Codes and Cryptography*, vol. 6, pp. 21–35, 1995.

[2] C.-Y. Chen, C.-H. Wang, and C.-C. Chao, "Complementary sets and Reed–Muller codes for peak-to-average power ratio reduction in OFDM," *Proc. of 16th AAECC Symp. (Lecture Notes in Computer Science)*, vol. 3857, pp. 317–327, 2006.

[3] J. H. Conway and N. J. A. Sloane, "Soft decoding techniques for codes and lattices, including the Golay code and the Leech lattice," *IEEE Trans. Inf. Theory*, vol. 32, no. 1, pp. 41–50, Jan. 1986.

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

[5] M. J. E. Golay, "Complementary series," *IRE Trans. Inf. Theory*, vol. 7, no. 2, pp. 82–87, Apr. 1961.

[6] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 301–319, Mar. 1994.

[7] A. E. Jones and T. A. Wilkinson, "Combined coding for error control and increased robustness to system nonlinearities in OFDM," *Proc. of IEEE 46th Vehicular Technology Conf. (VTC), Atlanta, GA*, pp. 904–908, Apr. 1996.

[8] A. E. Jones, T. A. Wilkinson, and S. K. Barton, "Block coding scheme for reduction of peak to mean envelope power ratio of multicarrier transmission schemes," *IEE Electron. Lett.*, vol. 30, no. 25, pp. 2098–2099, Dec. 1994.

[9] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North Holland Mathematical Library, 1977.

[10] H. Ochiai and H. Imai, "Block coding scheme based on complementary sequences for multicarrier signals," *IEICE Transactions on Fundamentals*, vol. E80-A, pp. 2136–2146, Nov. 1997.

[11] M. G. Parker and C. Tellambura, "A construction for binary sequence sets with low peak-to-average power ratio," *Report No. 242, Department of Informatics, University of Bergen, Norway*, Feb. 2003. [Online]. Available: http://www.ii.uib.no/~matthew/ConstructReport.pdf

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

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

[14] B. M. Popović, "Synthesis of power efficient multitone signals with flat amplitude spectrum," *IEEE Trans. Commun.*, vol. 39, no. 7, pp. 1031–1033, Jul. 1991.

[15] K.-U. Schmidt, "On cosets of the generalized first-order Reed–Muller code with low PMEPR," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3220-3232, Jul. 2006.

[16] T. E. Stinchcombe, "Aperiodic autocorrelations of length 2^m sequences, complementarity, and power control for OFDM," Ph.D. dissertation, University of London, Apr. 2000. [Online]. Available: http://www.isg.rhul.ac.uk/alumni/thesis/stinchcombe_t.pdf

[17] R. D. J. van Nee, “OFDM codes for peak-to-average power reduction and error correction,” *Proc. of IEEE Global Telecommunications Conference (GLOBECOM), London, U.K.*, pp. 740–744, Nov. 1996.

[18] T. A. Wilkinson and A. E. Jones, “Minimisation of the peak to mean envelope power ratio of multicarrier transmission schemes by block coding,” *Proc. of IEEE Vehicular Technology Conference (VTC), Chicago, IL*, pp. 825–829, Jul. 1995.