On Codes with Low Peak-to-Average Power Ratio for Multi-Code CDMA

Kenneth G. Paterson, *Member, IEEE*

Abstract

Codes which reduce the peak-to-average power (PAPR) in multi-code code division multiple access (MC-CDMA) communications systems are systematically studied. The problem of designing such codes is reformulated as a new coding-theoretic problem: codes with low PAPR are ones in which the codewords are far from the first-order Reed-Muller code. Bounds on the trade-off between rate, PAPR and error-correcting capability of codes for MC-CDMA follow. The connections between the code design problem, bent functions and algebraic coding theory (in particular, the Kerdock codes and Delsarte-Goethals codes) are exploited to construct code families with flexible parameters for the small values of n of practical interest. In view of their algebraic structure, these codes enjoy efficient encoding and decoding algorithms. The paper concludes by listing open problems in algebraic coding theory and Boolean functions motivated by the paper.

Keywords

CDMA, rate adaptation, multi-code, Walsh-Hadamard transform, envelope, power, bent function, Reed-Muller, Kerdock

I. Introduction

Code-Division Multiple-Access (CDMA) in one form or another is likely to be at the heart of future cellular wireless communications systems, third generation and beyond: eight out of ten proposals that have been made for IMT-2000 are based on Direct Sequence CDMA (DS-CDMA) [34]. Already, some second-generation systems using DS-CDMA have been deployed, especially in North America, for example systems based upon the IS-95 standard [13].

A challenge for DS-CDMA systems is to support rate adaptation for users who demand widely varying data rates for different applications. For voice applications, a few kbits per second on both the forward (base station to mobile) and the reverse (mobile to base station) links suffice. But internet access, file transfer, streaming video and multimedia applications will demand much higher rates, of the order of hundreds of kbits per second and up, in both directions.

Several methods for rate adaptation in CDMA systems have already been proposed [19], including variable spreading factor CDMA, where the number of chips per data bit is reduced for users who require higher data rates, time-slotting methods and multi-code CDMA, [12]. Multi-code CDMA, the focus of this paper, is a very simple, backwards-compatible technique in which a mobile user who wishes to transmit at a higher data rate is simply assigned additional channels, and appears to the base station as multiple users. Implementation requires only replication of the appropriate hardware. We note that the abbreviation MC-CDMA has been widely used for both multi-carrier CDMA, where characteristics of OFDM and CDMA systems are combined [10], and multi-code CDMA. Here we use it to abbreviate the latter.

In effect, the transmitted signal in an MC-CDMA system is a sum of some number n of basic rate signals, where n is the rate multiple required by a user. As we shall see below, this means that the peak signal power in an MC-CDMA system can be as large as n times the average signal power. Typically $n = 2^m$ where m lies between 2 and 6. Thus an MC-CDMA signal can have a significantly higher peak-to-average power ratio (PAPR) than a basic rate signal. So to transmit MC-CDMA signals without distortion requires either a more expensive power amplifier that is linear across a wider range of amplitudes, or a power amplifier which is operated only in its linear region, where conversion of DC to RF power is inefficient [12], [24]. As with OFDM, this is a significant barrier to the adoption of MC-CDMA in practice. The problem is particularly

K.G. Paterson was with Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol BS34 8QZ, U.K. He is now with Information Security Group, Royal Holloway, University of London, Egham, SUrrey TW20 0EX, U.K.

acute on reverse links where low cost components and low power consumption are vital [24] but it is also an important consideration on forward links [2], [15].

In order to avoid self-interference due to the use of multiple spreading codes in MC-CDMA, *subcode concatenation* has been proposed [11]. Here, a user is assigned n orthogonal channels and n bits in parallel from n different data streams (usually already coded for error correction and scrambled) are used to modulate the spreading sequences on these channels. The transmitted signal is the sum of the n orthogonal signals on the individual channels and the user's rate is n times the basic data rate. Typically, the channel orthogonalisation is achieved by using length $n = 2^m$ Walsh-Hadamard sequences as synchronous spreading sequences on the n channels, see Section II. In this case, the transmitted signal is effectively the Walsh-Hadamard transform of the vector of n data bits.

In MC-CDMA with subcode concatenation, coding across the n channels can be used to reduce the PAPR of the transmitted signals [23], [24], [30], [31], [32]. With coding, the user's rate is reduced to nR times the basic rate for some $R < 1$: nR bits at a time from nR parallel data streams are encoded onto n bits using a specially chosen rate R block code. These n bits are in turn used to modulate the Walsh-Hadamard sequences. Thus the block encoder is inserted between the user's data streams and the Walsh-Hadamard transform. The block code is selected to produce MC-CDMA signals with low PAPR and the approach trades transmission rate for reduced PAPR. This is analogous to coding methods that have recently been developed for OFDM [6], [7], [14], [20], [22], [25]. In [31], ad hoc methods were used to produce constant amplitude MC-CDMA codes (i.e. codes with best possible PAPR of 1) for $n = 4$ and $n = 16$. In [30], it is shown that using bent functions to define codewords gives constant amplitude signals. In [23], [24], heuristic search methods for constructing codes were introduced. These are based on a connection between the PAPR of a codeword and its Hamming distance to chip vectors. (The work in [23], [24] does not restrict attention to Walsh-Hadamard sequences and so a larger set of values of n can be considered.) In [24], analytic expressions for the codewords of some of the codes are derived. These expressions are however rather unwieldy. It has been pointed out in [32] and demonstrated by simulation in [24] that the redundancy introduced by coding can be exploited for error-correction. The technique also introduces some additional complexity at the transmitter (encoding circuitry) and at the receiver (decoding circuitry).

In this paper, we make a thorough study of codes which reduce PAPR in MC-CDMA. We introduce a simple model for MC-CDMA which captures the key features of an MC-CDMA reverse link in Section II. We reformulate the problem of designing codes as a new coding-theoretic problem in Section III, showing that codes with low PAPR are ones in which the codewords are far from the first-order Reed-Muller code $\mathrm{RM}(1, m)$. This allows us to prove in Section IV bounds on the trade-off between rate, PAPR and error-correcting capability of codes for MC-CDMA (c.f. the work in [27] for OFDM). We also show that asymptotically good families of codes exist with PAPR growing only as $O(\log n)$. More pragmatically, in Section V, we exploit the connections between the code design problem, bent functions and algebraic coding theory (in particular, the Kerdock codes and Delsarte-Goethals codes) to systematically develop families of codes with flexible parameters for the small values of n of practical interest. In view of their algebraic structure, these codes enjoy efficient encoding and decoding algorithms. This represents a significant advance over previous work in [24], [31], [32].

Our focus is on codes with PAPR equal to 1, but we also consider constructions for codes with higher PAPR. We conclude in Section VI by stating some problems in algebraic coding theory and the theory of Boolean functions which are motivated by this work.

This paper develops a theory of coding for MC-CDMA that parallels the theory for OFDM developed in [6], [7], [14], [20], [22], [25], [27]. Indeed, since the Walsh-Hadamard transform is a discrete version of the Fourier transform inherent in OFDM, our work on MC-CDMA can be seen as a discrete-time analogue of the OFDM theory. For further discussion on the similarities and differences between the two approaches, see Section VI.

II. Communication Model

In this section we describe our model of the reverse link of an MC-CDMA system. Our model is a simplified version of the model given in [23]. Throughout the paper n will be a power of two. We write $n = 2^m$.

The Walsh-Hadamard matrix WH_n can be defined recursively by $\mathrm{WH}_1 = (1)$ and

$$\mathrm{WH}_{2^j} = \begin{pmatrix} \mathrm{WH}_{2^{j-1}} & \mathrm{WH}_{2^{j-1}} \\ \mathrm{WH}_{2^{j-1}} & -\mathrm{WH}_{2^{j-1}} \end{pmatrix}$$

This matrix is a $\{+1, -1\}$-matrix and is symmetric and orthogonal, so that:

$$\mathrm{WH}_n \cdot \mathrm{WH}_n = nI_n$$

where I_n denotes the $n \times n$ identity matrix. Thus the rows (or columns) of WH_n are orthogonal vectors of length n, called Walsh-Hadamard sequences.

Our model of the reverse link of an MC-CDMA system is a discrete-time one. We begin by considering an MC-CDMA system without coding. We have n parallel streams of bits and the signal transmitted by a user on the reverse link corresponding to a vector $c = (c_0, c_1, \ldots, c_{n-1})$ of data bits (one bit $c_i \in \{0, 1\}$ from each stream) is the time-domain vector of real values $S(c) = (S(c)_0, S(c)_1, \ldots S(c)_{n-1})$ where

$$S(c)_t = \sum_{j=0}^{n-1} (-1)^{c_j} (\mathrm{WH}_n)_{jt}. \tag{1}$$

Writing $(-1)^c = ((-1)^{c_0}, (-1)^{c_1}, \ldots, (-1)^{c_{n-1}})$, we have

$$S(c) = (-1)^c \cdot \mathrm{WH}_n.$$

We can now see that each data bit c_j is used to modulate a Walsh-Hadamard sequence (a row of the matrix WH_n) and the time-domain signal is the sum of these modulated spreading sequences: we have

$$S(c) = \sum_{j=0}^{n-1} (-1)^{c_j} a_j$$

where a_j denotes the j-th row of WH_n. Thus a user acts like n basic rate users transmitting in parallel in a synchronous CDMA system, each such user spreading a single bit c_j.

In a real MC-CDMA system, the power required to transmit a signal is proportional to the square of the signal value. Since we are interested only in ratios of powers, we define the instantaneous power of the signal $S(c)$ at time t to be $P(c)_t = S(c)_t^2$. From (1), the peak (i.e. largest) value of $P(c)_t$ can be as large as n^2. An easy calculation using the orthogonality of the matrix WH_n shows that the average value of $P(c)_t$ over $0 \le t < n$ is equal to n. Therefore we define the peak-to-average power ratio of the vector of data bits c (and the corresponding signal $S(c)$) to be

$$\mathrm{PAPR}(c) = \frac{1}{n} \max_{0 \le t < n} P(c)_t.$$

From the above discussion we know that $1 \le \mathrm{PAPR}(c) \le n$.

We note that our model omits many important features of the transmit chain of the reverse link of an MC-CDMA system, including the use of long user-specific spreading codes (called primary codes in [12]), pulse-shaping of chip waveforms and the spreading of user data by Gray mapping over both I and Q components. However, these features do not have a major impact on PAPR, the key parameter that we study here.

Now we consider coding for MC-CDMA. We let C be an arbitrary binary code of length n and rate R, that is a set of 2^{nR} binary length n vectors. An encoder for C maps $k = nR$ information bits at a time onto vectors $c \in C$. In MC-CDMA with coding, we have k parallel data streams which are fed into an encoder for C and thence to a Walsh-Hadamard transform. Thus only codewords c in C are selected for transmission, though (1) still describes the transmitted signal. The rate of a user in an MC-CDMA scheme with precoding is $k = nR$ times that of a basic rate user.

We define the PAPR of the code C to be

$$\mathrm{PAPR}(C) = \max_{c \in C} \mathrm{PAPR}(c).$$

A code C with $\mathrm{PAPR}(C) = 1$ is called a constant amplitude code. Such a code attains the lowest and therefore best possible value of PAPR. We reiterate that [24], [32] have already shown that the redundancy in C can be used for additional error correction. The two main problems that we study in this paper can now be stated as:

- How can we construct codes for MC-CDMA with small PAPR, large R (so as to maintain high data rates) and large minimum Hamming distance d that are practical, i.e. efficiently encodable and decodable?
- what are the trade-offs between the parameters R, d and $\mathrm{PAPR}(C)$ for MC-CDMA codes?

III. A Coding-Theoretic Formulation

In this and the following sections, we assume the reader has a basic familiarity with the Reed-Muller codes and we draw heavily on results in [17, Chaps. 13 – 15]. In particular, we assume that every length $n = 2^m$ word c can be identified with a Boolean function $c(x_0, x_1, \ldots, x_{m-1})$ in variables $x_0, x_1, \ldots, x_{m-1}$ (where we note our change from the standard numbering of these variables) and that component i of $c = (c_0, c_1, \ldots, c_{n-1})$ can be obtained by evaluating the corresponding Boolean function at $(i_0, i_1, \ldots, i_{m-1})$. We will denote both the codeword and the associated Boolean function by the same symbol. Indeed we will not distinguish between the two objects. We recall the code $\mathrm{RM}(r, m)$ consisting of all those words whose Boolean functions have non-linear order at most r has minimum distance 2^{m-r} and is linear of dimension $1 + \binom{m}{1} + \cdots + \binom{m}{r}$. To be explicit,

$$\begin{bmatrix} 1111 & 1111 & \cdots & 1111 \\ 0101 & 0101 & \cdots & 0101 \\ 0011 & 0011 & \cdots & 0011 \\ \vdots & \vdots & & \vdots \\ 0000 & 0000 & \cdots & 1111 \end{bmatrix} \begin{matrix} 1 \\ x_0 \\ x_1 \\ \vdots \\ x_{m-1} \end{matrix}$$

denotes a generator matrix for $\mathrm{RM}(1, m)$.

We assert that the matrix WH_n has t-th row (and column) equal to the vector $(-1)^{\sum_{k=0}^{m-1} t_k x_k}$ where $t = \sum_{k=0}^{m-1} t_k 2^k$. Thus the rows (and columns) of WH_n are related to codewords of $\mathrm{RM}(1, m)$, i.e. linear functions. This can be proved by comparing the recursive definition of WH_n with the fact that words of $\mathrm{RM}(1, m)$ all have the form (c, c) or $(c, \overline{c})$ where $c \in \mathrm{RM}(1, m-1)$.

Now let $c \in C$ be a codeword for transmission. Then we have

$$\begin{aligned} S(c)_t &= \sum_{j=0}^{n-1} (-1)^{c_j} (\mathrm{WH}_n)_{jt} \\ &= \sum_{j=0}^{n-1} (-1)^{c_j + (\sum_{k=0}^{m-1} t_k x_k)_j} \\ &= n - 2d_H(c, \sum_{k=0}^{m-1} t_k x_k) \end{aligned}$$

where $d_H(x, y)$ denotes the Hamming distance between vectors x and y. Therefore

$$\mathrm{PAPR}(c) = \frac{1}{n} \max_t \left(n - 2d_H(c, \sum_{k=0}^{m-1} t_k x_k) \right)^2 .$$

Notice that if $P(c)_t$ equals $\mathrm{PAPR}(c)$ but $d_H(c, \sum_{k=0}^{m-1} t_k x_k) \geq 2^{m-1}$ then $2d_H(c, 1 + \sum_{k=0}^{m-1} t_k x_k) = 2n - 2d_H(c, \sum_{k=0}^{m-1} t_k x_k)$ and

$$P(c)_t = \left(n - 2d_H(c, \sum_{k=0}^{m-1} t_k x_k) \right)^2 = \left(n - 2d_H(c, 1 + \sum_{k=0}^{m-1} t_k x_k) \right)^2$$

where $1 + \sum_{k=0}^{m-1} t_k x_k \in \mathrm{RM}(1,m)$ and $d_H(c, 1 + \sum_{k=0}^{m-1} t_k x_k) \leq 2^{m-1}$. Hence we have proved

Lemma 1: For any word c of length n,

$$\mathrm{PAPR}(c) = n\left(1 - \frac{2d_*(c)}{n}\right)^2,$$

where $d_*(c) := \min\{d_H(c,w) : w \in \mathrm{RM}(1,m)\}$ denotes the minimum Hamming distance between c and the first-order Reed-Muller code of length 2^m.

Because $\mathrm{RM}(1,m)$ is closed under complementation, it is clear that $d_*(c) \leq n/2$, so the quantity $1-2d_*(c)/n$ above is always non-negative.

If we write $d_*(C) = \min\{d_*(c) : c \in C\}$, then we have $\mathrm{PAPR}(C) = n(1 - \frac{2d_*(C)}{n})^2$. Thus codes which are far from $\mathrm{RM}(1,m)$ will have small PAPR, and our first problem can be restated as constructing good codes having this property.

Occasionally it will be useful to write $d_*(C)$ in terms of $\mathrm{PAPR}(C)$. We have:

$$d_*(C) = \frac{n}{2}\left(1 - \left(\frac{\mathrm{PAPR}(C)}{n}\right)^{1/2}\right). \tag{2}$$

IV. Bounds on Codes

In this section, we use the connection between PAPR and Hamming distance developed above to prove bounds relating the rate and a minimum distance of a code C with $\mathrm{PAPR}(C)$. We prove analogues of the Gilbert-Varshamov and Hamming bounds for MC-CDMA codes. We perform an asymptotic analysis of the former bound and exhibit a code that is (almost) non-trivial and 'perfect' with respect to the latter. Our analysis is analogous to that carried out for OFDM in [27], but simplified because here we work in Hamming space rather than in an n-dimensional complex Euclidean space.

A. A Gilbert-Varshamov-style lower bound

For any $0 \leq r \leq n$, let $H(r)$ denote the number of words in a Hamming sphere of radius r in dimension n, so $H(r) = \sum_{k=0}^{r} \binom{n}{k}$.

We have:

Lemma 2: Suppose that $0 \leq d_* < n/2$ and that

$$2n \cdot H(d_*) + 2^{nR} \cdot H(d) \leq 2^n.$$

Then there exists a code C of length n, rate R and minimum distance d with

$$\mathrm{PAPR}(C) \leq n\left(1 - \frac{2d_*}{n}\right)^2.$$

Proof: Any set of words with each word lying at least distance d_* from $\mathrm{RM}(1,m)$ and each pair of words lying at least distance d from each other will have PAPR at most $n(1 - \frac{2d_*}{n})^2$ by Lemma 1. Such a set C of size 2^{nR} can be chosen provided $2nH(d_*) + 2^{nR}H(d) \leq 2^n$, by firstly removing from Hamming space of dimension n the $2n$ disjoint spheres of radius d_* about $\mathrm{RM}(1,m)$ and then sequentially chosing codewords and removing spheres of radius d around these codewords in the remaining space. ■

We note that the left-hand side of the bound in Lemma 2 contains a term $2^{nR}H(d)$ appearing in the standard Gilbert-Varshamov bound, c.f. [16, Thm. 5.1.7], and a term $2nH(d_*)$ in which d_* determines the resulting PAPR of the code. It is instructive to examine the asymptotic behaviour of our bound. We have:

Theorem 3: Suppose that $0 \leq R < 1$ and $0 \leq \delta < 1/2$ satisfy

$$R < 1 - H_2(\delta)$$

where $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ denotes the binary entropy function. Then there exists a length n code of rate R and minimum distance δn satisfying $\mathrm{PAPR}(C) \leq 2\log(2n)$ for all sufficiently large n.

Proof: By Lemma 2, it suffices to show that for all sufficiently large n,

$$2^{-n} \cdot 2n \cdot H\left(\frac{n}{2}(1-y)\right) + 2^{n(R-1)} \cdot H(\delta n) \leq 1 \tag{3}$$

where

$$y = \left(\frac{2\log(2n)}{n}\right)^{1/2}.$$

For R and δ satisfying the hypothesis in the theorem the second term in left-hand side of this expression tends to zero as $n \to \infty$, c.f. the proof of the asymptotic form of the standard Gilbert-Varshamov bound in [16, Thm. 5.1.9]. Next we consider the logarithm of the first term. We note that $0 \leq y < 1$ for large n. Then

$$\begin{aligned}
\log_2 2^{-n} \cdot 2n \cdot H\left(\frac{n}{2}(1-y)\right) &= -n + \log_2(2n) + \log_2 H\left(\frac{n}{2}(1-y)\right) \\
&\leq -n + \log_2(2n) + H_2\left(\frac{1}{2}(1-y)\right) \quad \text{by [16, Thm. 1.4.5]} \\
&= -n + \log_2(2n) + n\left(1 - (\log_2 e)\sum_{s=1}^{\infty}\frac{y^{2s}}{2s(2s-1)}\right)
\end{aligned}$$

where we have used the expansion

$$H_2\left(\frac{1}{2}(1-y)\right) = (\log_2 e)\sum_{s=1}^{\infty}\frac{y^{2s}}{2s(2s-1)}, \quad |y| < 1$$

obtained from the Taylor series for $\log(1-y)$ and $\log(1+y)$. Extracting the first term in this series, we can write

$$\log_2 2^{-n} \cdot 2n \cdot H(\frac{n}{2}(1-y)) \leq \log_2(2n) - (\log_2 e)\frac{ny^2}{2} - O(ny^4).$$

Replacing y by $(\frac{2\log(2n)}{n})^{1/2}$ and simplifying, we see that the error term $O(ny^4)$ tends to ∞ as $n \to \infty$ and we deduce that

$$\log_2 2^{-n} \cdot 2n \cdot H(\frac{n}{2}(1-y)) \to -\infty \text{ as } n \to \infty.$$

This establishes that the first term in (3) tends to zero for large n and completes the proof. ■

B. A Hamming-style upper bound

Theorem 4: Suppose that there exists a length n code C with rate R and minimum distance d. Then

$$2^{-n} \cdot 2n \cdot H\left(d_* - \lfloor\frac{d+1}{2}\rfloor\right) + 2^{n(R-1)} \cdot H\left(\lfloor\frac{d-1}{2}\rfloor\right) \leq 1$$

where

$$d_* = \frac{n}{2}\left(1 - \left(\frac{\mathrm{PAPR}(C)}{n}\right)^{1/2}\right).$$

Proof: The 2^{nR} Hamming spheres of radius $\lfloor\frac{d-1}{2}\rfloor$ around codewords of C must be mutually disjoint. Moreover, it follows from Lemma 1 that none of these spheres can intersect any of the $2n$ spheres of radius $d_* - \lfloor\frac{d+1}{2}\rfloor$ around words in $\mathrm{RM}(1,m)$. These $2n$ spheres are disjoint because the minimum distance of $\mathrm{RM}(1,m)$ is $2^{m-1} \geq d_*$. ■

No asymptotic analysis of the above bound can yield a condition connecting R, d and $\mathrm{PAPR}(C)$: the first term is the only one depending on $\mathrm{PAPR}(C)$ and is essentially a Hamming bound term for a code with only $2n$ codewords. So it grows so slowly with n that even for $\mathrm{PAPR}(C) = 1$, the term converges to zero. Indeed the bound does not preclude the existence of an asymptotically good sequence of codes (i.e. one with both rate

and d/n bounded away from zero as $n \to \infty$) with PAPR equal to 1. However, the bound can be interesting at small values of n, as the following example shows.

Example 5: Consider the length 4 code $x_0x_1 + \mathrm{RM}(1,2)$, a coset of the first-order Reed-Muller code which consists of all odd weight words of length 4. It is an easy exercise to check that this code has minimum distance 2, rate 3/4 and PAPR equal to 1. It also meets the bound in Theorem 4 with equality. Therefore it can be regarded as a 'perfect' code. This code has the same parameters as the length 4 code of [31].

We will consider generalisations of the code in this example in the next section.

V. Families of Codes

Here, we develop the connections between codes for MC-CDMA with low PAPR, bent functions and Reed-Muller codes. Our objective is to produce families of codes and a large number of coding options trading-off R, d and $\mathrm{PAPR}(C)$ for small values of n.

A. Walsh-Hadamard Transforms and Bent Functions

Given a Boolean function f in m variables, the Walsh-Hadamard transform of f (or the binary vector corresponding to f, or the real vector $(-1)^f$) is defined in [17, p. 414] to be the function $\hat{f}$ where

$$\hat{f}(u) = \sum_{v \in \{0,1\}^m} (-1)^{f(v)+L_u(v)}, \qquad u \in \{0,1\}^m$$

where

$$L_u = \sum_{k=0}^{m-1} u_k x_k \in \mathrm{RM}(1,m).$$

Comparing this definition with those in Section II, we see that

$$S(c)_t = \hat{c}(t_0, t_1, \ldots, t_{m-1}), \qquad t = \sum_{k=0}^{m-1} t_k 2^k$$

so that the vector $S(c)$ corresponding to the transmitted signal has components that are Walsh-Hadamard transform components of c. From Lemma 1, we also have

$$\hat{c}(t_0, t_1, \ldots, t_{m-1}) = S(c)_t = n - 2d_H(c, \sum_{k=0}^{m-1} t_k x_k)$$

so that the Walsh-Hadamard transform coefficients of c give us information about $d_*(c)$, c.f. [17, p. 415, Thm. 1].

It is an easy exercise ([17, p. 416, Cor. 3] to show that $\sum_{u \in \{0,1\}^m} \hat{c}(u)^2 = n^2$. The following lemma is now immediate:

Lemma 6: Let c be a word of length $n = 2^m$. Then

$$\mathrm{PAPR}(c) = \frac{1}{n} \max_u |\hat{c}(u)|^2.$$

Moreover c has PAPR equal to 1 if and only if $|\hat{c}(u)| = \sqrt{n}$ for every $u \in \{0,1\}^m$.

We also have the following lemma, useful in constructing codes:

Lemma 7: Every codeword in a coset $c + \mathrm{RM}(1,m)$ has the same PAPR.

Proof: Let $w \in \mathrm{RM}(1,m)$. Then

$$\widehat{(c+w)}(u) = \sum_{v \in \{0,1\}^m} (-1)^{c(v)+L_w(v)+L_u(v)} = \hat{c}(w+u)$$

so that c and $c+w$ have the same Walsh-Hadamard transform spectrum. ■

A *bent function* is defined to be a Boolean function all of whose Walsh-Hadamard transform coefficients are equal in magnitude to $2^{m/2} = \sqrt{n}$. Clearly m must be even for such a function to exist. A bent function corresponds to a word with PAPR equal to 1. From the preceding discussion, such a word satisfies $d_*(c) = \frac{1}{2}(n - \sqrt{n}) = 2^{m-1} - 2^{\frac{m}{2}-1}$ and is maximally distant from $\mathrm{RM}(1, m)$. Thus:

Theorem 8: C is a constant amplitude code if and only if every codeword of C is a bent function. In particular, constant amplitude codes of length $n = 2^m$ exist only for m even.

We note that Wada [30] has also recently recognised the connection between bent functions and PAPR reduction in MC-CDMA. Bent functions have received a good deal of attention, see for example [1], [4], [5], [8], [28], [29], [33], and a brief overview can be found in [17, Chap. 14, Sec. 5]. It is known that any bent function has non-linear order at most $m/2$, that is, lies in the code $\mathrm{RM}(m/2, m)$. The following construction of bent functions is attributed to Maiorana and McFarland in [21]. The same set of functions are called linear-based bent sequences in [1].

Result 9: Let π be a permutation on $\{0, 1\}^t$ and let g be any Boolean function in t variables. Then

$$f(x_0, \ldots, x_{2t-1}) = \pi(x_0, \ldots, x_{t-1}) \cdot (x_t, \ldots, x_{2t-1}) + g(x_0, \ldots, x_{t-1})$$

is a bent function of $2t$ variables. (Note that we interpret π as a vector of t Boolean functions in t variables).

Of importance to us will be bent functions in $\mathrm{RM}(2, m)$. The codewords of $\mathrm{RM}(2, m)$ can be identified with quadratic functions in m variables, and each coset of $\mathrm{RM}(1, m)$ inside $\mathrm{RM}(2, m)$ is represented by a quadratic form in m variables. According to results of [17, Chap. 15, Sec. 2], with each such form Q can be associated an even number, called the rank of the form, denoted $\mathrm{rank}(Q)$. This number determines the weight distribution of the coset $Q + \mathrm{RM}(1, m)$, [17, p. 441, Thm. 5]. Moreover, for m even, a quadratic form in m variables is bent if and only if it has full rank m. More generally, we have:

Lemma 10: Let Q be a quadratic form in m variables of rank $2h$. Then the codewords of the coset $Q + \mathrm{RM}(1, m)$ have PAPR equal to 2^{m-2h}.

Proof: From [17, p. 441, Thm. 5], the coset $Q + \mathrm{RM}(1, m)$ has codewords of weights 2^{m-1} and $2^{m-1} \pm 2^{m-h-1}$. Hence $d_*(Q) = 2^{m-1} - 2^{m-h-1}$ and so $\mathrm{PAPR}(Q) = n\left(1 - \frac{2d_*(c)}{n}\right)^2 = 2^{m-2h}$. The result now follows from Lemma 7. ■

According to [17, p. 436, Thm. 2], the quadratic forms of rank $2h$ are in 1-1 correspondence with $m \times m$ symplectic matrices of rank $2h$ over GF(2) and their number is equal to

$$N(m, 2h) = \frac{(2^m - 1)(2^{m-1} - 1) \cdots (2^{m-2h+1} - 1)}{(2^{2h} - 1)(2^{2h-2} - 1) \cdots (2^2 - 1)} \cdot 2^{h(h-1)}.$$

Much less is known about Boolean functions that are 'approximately bent' in the case where m is odd. From Lemma 10, for m odd, the smallest PAPR that a codeword of $\mathrm{RM}(2, m)$ can have is 2. For higher non-linear orders, the problem of determining the 'flattest' possible Walsh-Hadamard spectrum is an open problem related to the determination of the covering radius of $\mathrm{RM}(1, m)$. We refer the reader to [3] for recent results on this problem.

B. Families of Constant Amplitude Codes from Bent Functions

We know that constant amplitude codes consist of bent functions. In this section, we construct some families of codes with this property. Our aim is to construct families which are practical for small (necessarily even) m. In view of Lemma 7, all of our codes will consist of cosets of $\mathrm{RM}(1, m)$. For pragmatic reasons, we restrict to codes in which the number of cosets is a power of 2, so that the codes encode an whole number of data bits. The codes can all be conveniently encoded and decoded using techniques similar to those developed for OFDM codes in [7] and [26].

Construction 11: A first family of constant amplitude codes can be obtained by generalising the code of Example 5. We let m be even and let Q be any bent function on m variables, for example $Q = x_0x_1 + x_2x_3 + \cdots + x_{m-2}x_{m-1}$ ([17, p. 429, Cor. 11]). Then we take as our code the coset $Q + \mathrm{RM}(1, m)$. This code has rate $(m + 1)/2^m$, minimum distance 2^{m-1} and PAPR 1.

Construction 12: A second family of constant amplitude codes is obtained by taking as the code at length $n = 2^m$, m even, a union of many second-order cosets corresponding to quadratic forms of full rank m. Such a code has minimum distance at least 2^{m-2} as it is a subcode of $\mathrm{RM}(2, m)$. For $m = 4$, the total number of full rank forms is $N(4, 4) = 28$, and a pictorial list of the forms can be found on [17, p. 429]. Selecting any 16 of these forms gives a code of rate 9/16, minimum distance 4 and PAPR equal to 1. This code has the same parameters as length 16 codes in [24], [31]. For $m = 6$, the number of full rank quadratic forms is equal to $N(6, 6) = 217 \times 2^6$, yielding a code of rate 20/64, minimum distance 16 and PAPR equal to 1. Generally, $N(m, m) \geq 2^{m(\frac{m}{2}-1)}$ and we obtain a code of rate at least $\frac{m(\frac{m}{2}+1)}{2^m}$, minimum distance 2^{m-2} and PAPR 1. In order to make these codes practical for larger values of m, it would be useful to have an algorithm for encoding data bits directly onto full rank forms.

Construction 13: A third family of constant amplitude codes can be obtained from Result 9, which identifies a set of $2^{2^t} \cdot (2^t)!$ bent functions in $m = 2t$ variables. Because the non-linear order of the functions is at most t, this set is a subcode of $\mathrm{RM}(t, 2t)$ and so has minimum distance at least $2^{m-t} = 2^t$. By restricting to functions g of non-linear order at most $\ell \leq t$ and permutations π of non-linear order at most $\ell - 1$, we can obtain codes with larger minimum distance $2^{m-\ell}$ at the expense of lower rate. It is not hard to see from Result 9 that this code will consist of a union of cosets of $\mathrm{RM}(1, m)$. In the case $\ell = 2$, we note that this construction does not in general produce all the bent quadratic functions, so the rate of the resulting codes is lower than that of the codes in Construction 12. However, for larger ℓ, it can attain higher rates. As an example, for $m = 6$ and $\ell = 3$, we obtain a code with minimum distance 8, rate 23/64 and PAPR 1. To make these codes practical, an efficient algorithm for encoding data bits into functions of the type appearing in Result 9 is required. This is straightforward in the cases $\ell = t$ (where encoding 2^t bits onto functions g is trivial, and π can be any permutation of $\{0, 1\}^t$) and $\ell = 2$ (where π can be represented by a non-singular $m \times m$ matrix and g can be obtained from an encoder for $\mathrm{RM}(2, t)$).

The above constructions give further motivation to the longstanding open problems of enumerating, constructing and classifying bent functions — as well as being interesting for their own sake, progress on these problems is likely to lead to better constant amplitude codes. For example, for $m = 6$ it should in principal be possible to obtain a code of rate 1/2 and minimum distance 8 since the number of bent functions for $m = 6$ is known to exceed 2^{32} [28]. However, we know of no simple method for generating this number of bent functions.

C. Families of Constant Amplitude Codes from Kerdock and Delsarte-Goethals Codes

In this section we generate more coding options by exhibiting subcodes of the Kerdock and Delsarte-Goethals codes with constant PAPR.

We begin by recalling some terminology from [17, Chap. 15, Sec. 5 and Chap. 21, Sec. 8].

A set Y of quadratic forms in m variables is called an (m, h)-set if for any $Q, Q' \in Y$, the quadratic form $Q + Q'$ has rank at least $2h$. If such a set Y contains the all-zero form, then clearly every non-zero form in Y also has rank at least $2h$. The code

$$\bigcup_{Q \in Y} Q + \mathrm{RM}(1, m)$$

obtained from such a set contains $|Y| \cdot 2^{m+1}$ codewords and has minimum distance $2^{m-1} - 2^{m-h-1}$ (because the distance between any two words in the same coset of $\mathrm{RM}(1, m)$ is 2^{m-1} and the distance between any two words in different cosets is at least $2^{m-1} - 2^{m-h-1}$, being determined by the rank of the sum of the two forms). It is shown in [17, p. 667, Thm. 13] that for any (m, h)-set Y, $|Y| \leq c^{\lfloor m/2 \rfloor - h + 1}$, where $c = 2^m$ for m odd and $c = 2^{m-1}$ for m even. Explicit constructions for maximal (m, h)-sets are given in terms of trace functions in [17, p. 454-455, Thms. 15 and 16] for m odd and [17, p. 457, eqn. (33), p. 461, eqn. (37)] for m even. In the even case, these sets give rise to the Kerdock and Delsarte-Goethals codes.

For the remainder of this section, we assume that m is even.

Construction 14: An $(m, m/2)$-set is called a Kerdock set. For each even m, a Kerdock set is constructed in [17, p. 457, eqn. (33)]. The set contains the zero quadratic form and $2^{m-1}-1$ quadratic forms of full rank. The resulting code $\mathcal{K}(m)$, known as the Kerdock code, contains $\mathrm{RM}(1,m)$ as a subcode, has minimum distance $2^{m-1}-2^{(m/2)-1}$ and rate $2m/2^m$. Selecting any 2^{m-2} of the $2^{m-1}-1$ non-zero cosets of $\mathrm{RM}(1,m)$ in the Kerdock code gives a subcode with the same minimum distance, rate $(2m-1)/2^m$ and PAPR 1. This subcode has higher rate than the code of Construction 11, but nearly the same minimum distance. For $m=4$, we obtain a code of rate 7/16 and minimum distance 6 (which is a subcode of the Nordstrom-Robinson code) and for $m=6$, a code of rate 11/64 and minimum distance 28.

It is unfortunate that we had to remove the zero coset from the Kerdock code in the above construction, since it reduced the rate from $2m/2^m$ to $(2m-1)/2^m$. However, it is not hard to show that any Kerdock set of quadratic forms must contain the zero form. We ask: does there exist a code with the same parameters as the Kerdock code which consists entirely of bent functions? In particular, is there a Boolean function g (necessarily of non-linear order greater than 2) such that the set $g+\mathcal{K}(m)$ contains only bent functions?

Next we attempt to generalise this Kerdock-based construction to the Delsarte-Goethals codes [17, p. 461, Thm. 19]. The code $\mathcal{DG}(m,h)$, where $1 \le h \le m/2$, is constructed from a maximal (m,h)-set and has minimum distance $2^{m-1}-2^{m-h-1}$ and contains $2^{(m-1)(m/2-h+1)+m+1}$ codewords, arranged in cosets of $\mathrm{RM}(1,m)$. The particular (m,h)-set of quadratic forms used to construct $\mathcal{DG}(m,h)$ is not described explicitly in the construction of [17], nevertheless it can be derived from the (m,h)-set used to construct $\mathcal{K}(m)$ and a related $(m-1,h)$-set appearing in [17, p. 454-455, Thm. 16].

The quadratic forms in the (m,h)-set include the zero form and so every non-zero form in the set has rank at least $2h$. But to construct a constant amplitude MC-CDMA subcode of $\mathcal{DG}(m,h)$, Lemma 10 tells us we must include only full rank quadratic forms. To evaluate the rate of this subcode, we must find the number of such forms in the (m,h)-set used to construct the Delsarte-Goethals codes. We resort to the results of [17, Chap. 21, Secs. 7 and 8]. Given a set of quadratic forms Y, we define the *inner distribution* of Y to be the $(m+1)$-tuple of real numbers $(B_0, B_1, \ldots, B_{m/2})$ where

$$B_i = \frac{1}{|Y|}|\{(Q,Q') \in Y \times Y : \mathrm{rank}(Q+Q') = 2i\}|.$$

For Y the (m,h)-set used to construct $\mathcal{DG}(m,h)$, we would like to know the numbers $(A_0, A_1, \ldots, A_{m/2})$ where

$$A_i = |\{Q \in Y : \mathrm{rank}(Q) = 2i\}|,$$

in particular the number $A_{m/2}$. We have the following Lemma:

Lemma 15: Let Y be the (m,h)-set used to construct $\mathcal{DG}(m,h)$ and let A_i, B_i be defined as above. Then

$$A_i = B_i, \qquad 0 \le i \le m/2$$

Proof: The code $\mathcal{DG}(m,h)$ is the Gray image of a code that is linear over $\mathbb{Z}_4$ [9] and so is distance invariant, i.e. the weight distribution and distance distribution of $\mathcal{DG}(m,h)$ are equal. But by virtue of the code's construction from quadratic cosets of $\mathrm{RM}(1,m)$, these two distributions are determined entirely by the numbers A_i and B_i respectively, with the number of words of weight $2^{m-1} \pm 2^{m-i-1}$ being determined by A_i and the number of times $2^{m-1} \pm 2^{m-i-1}$ appears in the distance distribution being determined by B_i. To obtain equality of these distributions we must then have $A_i = B_i$, $0 \le i \le m/2$. This result can be proved without recourse to $\mathbb{Z}_4$-linerity by carefully examining the form of codewords in $\mathcal{DG}(m,h)$ given by [17, eqn. (37), p. 461]. ■

The inner distribution $(B_0, B_1, \ldots, B_{m/2})$ of Y, a maximal (m,h)-set is known exactly from [17, p. 668, Thm. 14]. We have:

$$B_{m/2-i} = \sum_{j=i}^{m/2-h} (-1)^{j-i} C_{i,j}$$

(R, d)	Reference
$(5/16, 8)$	Construction 11, single coset
$(7/16, 6)$	Construction 14, subcode of $\mathcal{K}(4)$
$(9/16, 4)$	Construction 12

TABLE I
PARAMETERS OF CONSTANT AMPLITUDE CODES FOR $m = 4$

where

$$C_{i,j} = 4^{\binom{j-i}{2}} \left[\begin{array}{c} j \\ i \end{array} \right] \left[\begin{array}{c} m/2 \\ j \end{array} \right] (2^{(m-1)(m/2-h+1-j)} - 1).$$

Here, $\left[\begin{array}{c} x \\ y \end{array} \right]$ denotes a 4-ary Gaussian binomial coefficient [17, p. 443].

Lemma 16: With notation as above, we have

$$C_{0,j} \geq C_{0,j+1} \quad \text{for all } j \geq 1.$$

Proof: Examining the ratio $C_{0,j+1}/C_{0,j}$ and using simple approximations shows that for $j \geq 1$, $C_{0,j+1}/C_{0,j} \leq 2^{-1-2j}$. ■

Lemma 17: With notation as above, we have

$$A_{m/2} \geq 2^{(m-1)(m/2-h+1)-2}$$

Proof: From the preceding lemmas, we have

$$A_{m/2} = B_{m/2} = (C_{0,0} - C_{0,1}) + (C_{0,2} - C_{0,3}) + \cdots \geq C_{0,0} - C_{0,1}.$$

Now

$$\begin{aligned} C_{0,0} - C_{0,1} &= 2^{(m-1)(m/2-h+1)} - 1 - \frac{4^{m/2} - 1}{3} \cdot \left(2^{(m-1)(m/2-h)} - 1 \right) \\ &\geq 2^{(m-1)(m/2-h+1)} \left(1 - \frac{2^m - 1}{3 \cdot 2^{m-1}} \right) \\ &\geq \frac{1}{3} \cdot 2^{(m-1)(m/2-h+1)} \end{aligned}$$

and the lemma follows. ■

Construction 18: Lemma 17 shows that considering only cosets of $\mathrm{RM}(1, m)$ corresponding to the full rank forms in the (m, h)-set used in constructing $\mathcal{DG}(m, h)$ results in a subcode which encodes 2 bits less than the entire code. Since $\mathcal{DG}(m, h)$ always contains the zero form, this is just one bit less than we would have obtained by considering all the non-zero cosets in the code. This full rank subcode has minimum distance $2^{m-1} - 2^{m-h-1}$, rate $(m-1)(m/2-h+2)/2^m$ and PAPR 1. Taking all the non-zero cosets in the the code $\mathcal{DG}(m, h)$ would result in a subcode with the same minimum distance, rate $[(m-1)(m/2-h+2)+1]/2^m$ but PAPR 2^{m-2h}. For small values of m, the full rank quadratic forms in the (m, h)-set can be obtained by direct calculation. It would be convenient to find a simple method of selecting such forms directly for larger values of m.

Finally in this subsection, we bring together all the preceding constructions in the cases $m = 4, 6$ to produce two tables of constant amplitude codes, Tables I and II.

(R, d)	Reference
$(7/64, 32)$	Construction 11, single coset
$(11/64, 28)$	Construction 14, subcode of $\mathcal{K}(6)$
$(15/64, 24)$	Construction 18, subcode of $\mathcal{DG}(6, 2)$
$(20/64, 16)$	Construction 12
$(23/64, 8)$	Construction 13, $\ell = 3$

TABLE II
PARAMETERS OF CONSTANT AMPLITUDE CODES FOR $m = 4$

D. Codes with PAPR greater than 1

We have seen that codes with PAPR equal to 1 can exist only for m even. We have also seen that the rates of codes with PAPR 1 are constrained. In this subsection, we give three constructions for codes with higher PAPR for both odd and even m. These further extend the available coding options (though we do not explore those options in any detail). In particular, they produce codes with PAPR 2 for odd m. For odd m (and indeed even m), there may exist good codes with PAPR significantly less than 2 and indeed close to 1. These would arise from sets of words that are 'nearly bent', that is, words whose minimum distance to $\mathrm{RM}(1, m)$ is close to $2^{m-1} - \lceil 2^{\frac{m}{2}-1} \rceil$. We leave as a major open problem the question of constructing such codes, though we note that when m is odd, they cannot arise from subcodes of $\mathrm{RM}(2, m)$ because of the connection between rank and PAPR in Lemma 10.

We begin with a lemma generalising a result of [18]:

Lemma 19: Let f and g be Boolean functions of m variables $x_0, \ldots, x_{m-1}$. Suppose that both f and g have PAPR at most w. Then the Boolean function

$$c(x_0, \ldots, x_{m-1}, x_m) = (1 + x_m) \cdot f(x_0, \ldots, x_{m-1}) + x_m \cdot g(x_0, \ldots, x_{m-1})$$

has PAPR at most $2w$

Proof: We have $\hat{f}(u_0, \ldots, u_{m-1}), \hat{g}(u_0, \ldots, u_{m-1}) \leq (nw)^{1/2}$ for every choice of $(u_0, \ldots, u_{m-1}) \in \{0, 1\}^m$. It is easy to show that

$$\hat{c}(u_0, \ldots, u_{m-1}, u_m) = \hat{f}(u_0, \ldots, u_{m-1}) + (-1)^{u_m} \hat{g}(u_0, \ldots, u_{m-1}).$$

Hence

$$|\hat{c}(u_0, \ldots, u_{m-1}, u_m)| \leq |\hat{f}(u_0, \ldots, u_{m-1})| + |\hat{g}(u_0, \ldots, u_{m-1})| \leq 2(nw)^{1/2}$$

and from Lemma 6, we have

$$\mathrm{PAPR}(c) = \frac{1}{2n} \max_{u \in \{0,1\}^{m+1}} |\hat{c}(u)|^2 \leq 2w.$$

■

Notice that the length $2n$ codeword corresponding to c in the above lemma is formed by concatenating the length n words f and g. This simple concatenation construction allows us to convert any construction for a code C of length $n = 2^m$, rate R and minimum distance d into a construction for a code C' of length $2n = 2^{m+1}$ which also has rate R but, according to Lemma 19, with $\mathrm{PAPR}(C') \leq 2 \cdot \mathrm{PAPR}(C)$. The double-length code C' consists of all codewords of the form $(1 + x_m)f + x_m g$ where $f, g \in C$. The minimum Hamming distance of this code is the same d as that of the original code (though most pairs of words in C' will differ in at least $2d$ positions, d positions in each 'half'). Recall, with notation as above, that

$$\hat{c}(u_0, \ldots, u_{m-1}, u_m) = \hat{f}(u_0, \ldots, u_{m-1}) + (-1)^{u_m} \hat{g}(u_0, \ldots, u_{m-1}).$$

Taking $f = g$ and $u_m = 0$, we get

$$\hat{c}(u_0, \ldots, u_{m-1}, 0) = 2\hat{f}(u_0, \ldots, u_{m-1}).$$

It follows from this that in fact we have $\mathrm{PAPR}(C') = 2 \cdot \mathrm{PAPR}(C)$.

For example, this idea allows us to convert all of our constructions for constant amplitude codes for even m into constructions of codes with PAPR equal to 2 for odd m. Hence Tables I and II can be essentially replicated for $m = 5$ and $m = 7$, but now the codes have PAPR 2. Of course the concatenation can be repeated multiple times.

Our second construction generalises Result 9 to construct Boolean functions whose Walsh-Hadamard transforms are small. In the special case $\delta = 0$, our construction is identical to that of Result 9.

Lemma 20: Suppose $t + \delta \geq t \geq 1$ are integers. Let $\pi : \{0,1\}^{t+\delta} \to \{0,1\}^t$ be a 2^δ-to-1 map (regarded as a vector of t Boolean functions in $t + \delta$ variables) and let $g(x_0, \ldots, x_{t+\delta-1})$ be any Boolean function in $t + \delta$ variables. Finally, let

$$f(x_0, \ldots, x_{2t+\delta-1}) = \pi(x_0, \ldots, x_{t+\delta-1}) \cdot (x_{t+\delta}, \ldots, x_{2t+\delta-1}) + g(x_0, \ldots, x_{t+\delta-1})$$

be a Boolean function in $2t + \delta$ variables. Then $\mathrm{PAPR}(f) \leq 2^\delta$.

Proof: By Lemma 6, it is enough to show that $|\hat{f}(u)| \leq 2^{t+\delta}$ for every choice of $u = (a, b)$, where $a \in \{0,1\}^{t+\delta}, b \in \{0,1\}^t$. We have

$$\begin{aligned} \hat{f}(a,b) &= \sum_{v \in \{0,1\}^{2t+\delta}} (-1)^{f(v)+L_u(v)} \\ &= \sum_{c \in \{0,1\}^{t+\delta}} \sum_{d \in \{0,1\}^t} (-1)^{g(c)+(\pi(c)+b)\cdot d + a \cdot c} \end{aligned}$$

where $v = (c, d)$.

Now if $\pi(c) + b = 0$, then the inner sum is equal to

$$\sum_{d \in \{0,1\}^t} (-1)^{g(c)+a\cdot c}$$

in which the summand is independent of d. Hence in this case, which occurs for 2^δ choices of c, the inner sum is equal to $\pm 2^t$.

On the other hand if $\pi(c) + b \neq 0$, then the inner sum is equal to

$$\sum_{d \in \{0,1\}^t} (-1)^{g(c)+a\cdot c+\gamma\cdot d} = (-1)^{g(c)+a\cdot c} \cdot \sum_{d \in \{0,1\}^t} (-1)^{\gamma \cdot d}$$

in which $\gamma = \pi(c) + b$ is not the zero vector. In this case, the inner sum is equal to 0.

Considering all contributions to the sum over c, we see that

$$|\hat{f}(u)| \leq 2^\delta \cdot 2^t = 2^{t+\delta}.$$

■

This lemma can be used to generate codes in the same way as in Construction 13. It identifies $2^{2^{t+\delta}} \cdot (2^{t+\delta})!/(2^\delta!)^{2^t}$ distinct Boolean functions with PAPR at most 2^δ and non-linear order at most $t + \delta$. This last fact is true because each of the t component Boolean functions in π must be balanced and so has non-linear order at most $t + \delta - 1$. Thus the codes will, as subcodes of $\mathrm{RM}(t + \delta, 2t + \delta)$, have minimum distance at least 2^t. For example, taking $t = \delta = 2$, the lemma can in principal be used to produce a code of length 64, rate 41/64, minimum distance 4 and PAPR 4. By restricting the non-linear orders of π and g as in Construction 13, we can trade-off rate and minimum distance. We note that the construction cannot be used to produce codes with PAPR of, say, 2 when m is even.

Our third construction is concerned with the analogues of the Delsarte-Goethals codes in the case m odd. These codes are described via (m, h)-sets in [17, p. 454-455, Thms. 15, 16, Cor. 17]. In the m odd case, two linear codes with rate $[m(\lfloor m/2 \rfloor - h + 2) + 1]/2^m$ and minimum distance $2^{m-1} - 2^{\lfloor m/2 \rfloor - h - 1}$ are constructed from two different maximal (m, h)-sets for each h and m, $1 \leq h \leq \lfloor m/2 \rfloor$. Each of these sets contains $2^{m(\lfloor m/2 \rfloor - h + 1)}$ quadratic forms, one of which is the zero form. Every non-zero form in the two sets has rank greater than $2h$ (whereas this was true of the sum of two forms from the set in the even case). As before, we can select from each (m, h)-set just the forms of maximum rank (equal to $m - 1$ when m is odd), to obtain two subcodes with the same minimum distance as before, but with PAPR of only 2 instead of 2^{m-2h}. The only remaining questions are to determine the rate of the subcodes, and to find a method for generating the maximum rank forms in the sets. We can settle the first question using the same techniques as were used in the even case, the results of [17, Chap. 21, Secs. 7 and 8] applying here too. In fact the result is slightly easier to derive because the codes are linear. Using the same notation as in Section V-C, we can show that $A_{(m-1)/2}$, the number of maximum rank forms in a maximal (m, h)-set, is at least $2^{m(\lfloor m/2 \rfloor - h + 1) - 1}$. This is half as many forms as are in the complete (m, h)-set (but recall that we had to remove the zero form in any case). The subcodes obtained from these sets of forms have rate $m(\lfloor m/2 \rfloor - h + 2)/2^m$ and now we only lose one encoded bit as compared to the entire codes.

As examples, for $m = 5$ and $h = 1$, we obtain codes with rate 10/32, minimum distance 12 and PAPR 2, while for $m = 5$ and $h = 2$, we obtain codes with rate 15/32, minimum distance 8 and PAPR 2. These should be compared to codes obtained from Table II and our rate doubling construction.

VI. Conclusions and Open Problems

We have seen how coding for MC-CDMA can significantly reduce PAPR at the expense of rate, and how the additional redundancy can be exploited for error-correction. We have quantified this by formulating bounds on the parameters of rate, minimum distance and PAPR of a code. We have also developed the connections between PAPR, Reed-Muller codes, Walsh-Hadamard transforms and bent functions.

To finish, we gather together a number of areas requiring further investigation and some open problems.

We hinted in our description of the MC-CDMA system that in real systems, QPSK modulation is used rather than BPSK modulation and a user actually transmits data simultaneously on I and Q channels. Furthermore, different data can be transmitted on the I and Q channels. Can better rates and PAPR performance be obtained by considering code design on the two channels jointly? Quaternary codes and bent functions may be useful in addressing these questions.

The coding techniques developed here are also applicable to forward links, where PAPR is also a concern [2], [15]. Indeed the methods might be used directly (i.e. without the need for subcode concatenation) in systems like IS-95 where modulated Walsh-Hadamard sequences are used directly to transmit data to users. Even though it is not possible to code across multiple channels intended for different mobile recipients, we can still have a situation where a single user demands a high transmission rate on the forward link. Variable spreading factor schemes for rate adaptation in CDMA also exploit certain orthogonality properties of the Walsh-Hadamard sequences, namely that concatenations of modulated short sequences can be orthogonal to longer sequences. Our coding techniques can be applied to a combined multi-code, variable spreading factor scenario on the forward link, in which, for example, the coding might be applied across short sequences to produce a very high rate transmission channel with low PAPR to one mobile user. This channel would still be orthogonal to lower rate channels used to transmit to other users. The rates and PAPRs attainable in this situation should be explored further.

In Example 5, we gave an instance of a 'perfect' MC-CDMA code. Are there any more non-trivial codes meeting our Hamming-style bound with equality?

We have seen that bent functions have ideal power properties in MC-CDMA transmissions. This underlines the need to find new constructions for large numbers of bent functions and the problem of classifying all bent functions. We ask: can the recursive construction of bent-based bent sequences in [1] be written in terms of Boolean functions and made amenable to encoding? Can the recent constructions in [8] or the new characterisations in [4], [5] be exploited for coding purposes?

The work in this paper also gives further motivation to the old problem of finding the covering radius of

$\mathrm{RM}(1,m)$ for m odd: solving this and then constructing large numbers of words at the covering radius would give codes with best possible PAPR. We have also seen that the problem of finding a code with the same parameters as the Kerdock code which consists entirely of bent functions has practical consequences. We have yet to solve the important practical problem of finding methods for selecting maximum rank forms from the (m,h)-sets considered in Section V. There is also the problem of finding more and better constructions for large numbers of 'approximately bent' functions.

Finally, we speculate on the similarity between the codes for MC-CDMA described here and the codes for OFDM developed in [6], [7], [20], [22], [25]. In the binary case, the OFDM codes are also either implicitly or explicitly constructed from cosets of $\mathrm{RM}(1,m)$. In both situations, an orthogonal transform is used to transform data prior to transmission and the problem is to design codes which reduce the size of the transform values. The Walsh-Hadamard transform used here is a discrete analogue of the Fourier transform inherent in OFDM, so similar coding solutions might be expected. Indeed, in [7] it is shown that for m even, certain cosets of $\mathrm{RM}(1,m)$ which consist of binary Golay complementary sequences and have PAPR at most 2 are bent cosets. However the Reed-Muller code appears to arise for different reasons in the two cases. For OFDM, an explanation relating the particular Boolean functions yielding Golay complementary sequences and the recursive constructions for those sequences was given in [25]. In MC-CDMA, the Reed-Muller code plays a role because of the connection between rows of the Walsh-Hadamard matrix and the codewords of $\mathrm{RM}(1,m)$ (though this link has a recursive proof). A detailed explanation of the double appearance of the Reed-Muller codes may give greater insight into both practical and theoretical questions.

Acknowledgements

I am grateful to R. Castle and J. Davis for their careful comments on the paper and L. Porter for comments on the introduction. My thanks also to A. Lauder for his early interest in the work and for his help with the analysis in Section IV.

References

[1] C.M. Adams and S.E. Tavares, "Generating and counting binary bent sequences," *IEEE Trans. Inform. Theory*, vol. 36, no. 5, pp. 1170–1173, Sept. 1990.

[2] R.N. Braithwaite, "Using Walsh code selection to reduce the power variance of band-limited forward-link CDMA waveforms," *IEEE J. on Selected Areas in Communications*, vol. 18, no. 11, pp. 2260–2269, Nov. 2000.

[3] A. Canteaut, "On the weight distributions of optimal cosets of the first-order Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 1, pp. 407–413, Jan. 2001.

[4] C. Carlet and P. Guillot, "A characterization of binary bent functions," *J. Combin. Theory Ser. A*, vol. 76, no. 2, pp. 328–335, 1996.

[5] C. Carlet and P. Guillot, "An alternate characterization of the bentness of binary functions, with uniqueness," *Des. Codes Cryptogr.*, vol. 14, no. 2, pp. 133–140, 1998.

[6] J. A. Davis and J. Jedwab, "Peak-to-mean power control and error correction for OFDM transmission using Golay sequences and Reed-Muller codes," *Elec. Lett.*, vol. 33, pp. 267–268, 1997.

[7] J. A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences and Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2397–2417, Nov. 1999.

[8] H. Dobbertin, "Construction of bent functions and balanced Boolean functions with high nonlinearity," in *Lecture Notes in Computer Science*, vol. 1008, pp. 61–74, Springer, Berlin, 1995.

[9] A.R. Hammons, Jr., 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. Inform. Theory*, vol. 40, pp. 301–319, 1994.

[10] S. Hara and R. Prasad, "Overview of multicarrier CDMA,", *IEEE Communications Magazine*, vol. 35, no. 12, pp. 126–133, 1997.

[11] C.-L. I and R.D. Gitlin, "Multi-code CDMA wireless personal communications networks" in *Proc. ICC'95*, Seattle, Wash., pp. 1060–1064, 1995.

[12] C.-L. I, C.A. Webb III, H.C. Huang, S. ten Brink, S. Nanda and R.D. Gitlin, "IS-95 enhancements for multimedia services," *Bell Labs Tech. J.*, vol. 1, no. 2, pp. 60–87, 1996.

[13] TIA/EIA standard "Mobile station-base station compatibility standard for wideband spread spectrum cellular systems," TIA/EIA-95-B, Mar. 1999.

[14] 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," *Elec. Lett.*, vol. 30, pp. 2098–2099, 1994.

[15] V.K.N. Lau, "On the analysis of peak-to-average ratio (PAR) for IS95 and CDMA2000 systems," *IEEE Trans. Vehic. Tech.*, vol. 49, no. 6, pp. 2174–2188, Nov. 2000.

[16] J.H. van Lint, An introduction to coding theory, 2nd edition, Springer, Berlin, 1992.

[17] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
[18] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," in *Proc. EuroCrypt89*, Lecture Notes in Computer Science, vol. 434, pp. 549–562, Springer, Berlin, 1990.
[19] S. Nanda, K. Balachandran and S. Kumar, "Adaptation techniques in wireless packet data services," *IEEE Communications Magazine*, vol. 38, no. 1, pp. 54–64, 2000.
[20] R.D.J. van Nee, "OFDM codes for peak-to-average power reduction and error correction," in *Proc. IEEE Globecom 1996*, pp. 740–744, London, 1996.
[21] K. Nyberg, "Construction of bent functions and difference sets," in *Proc. EuroCrypt90*, Lecture Notes in Computer Science, vol. 473, pp. 151–160, Springer, Berlin, 1991.
[22] H. Ochiai and H. Imai, "Block coding scheme based on complementary sequences for multicarrier signals," *IEICE Trans. Fundamentals*, pp. 2136–2143, 1997.
[23] T. Ottosson, "Precoding in multicode DS-CDMA Systems," in *Proc. IEEE Int. Symp. Info. Thy.*, Ulm, Germany, June 29 - July 4th, 1997, p. 351.
[24] T. Ottosson, "Precoding for minimization of envelope variations in multicode DS-CDMA systems," *Wireless Personal Communications*, vol. 13, pp. 57–78, May 2000.
[25] K. G. Paterson, "Generalised Reed-Muller codes and power control in OFDM modulation," *IEEE Trans. Inform. Theory*, vol. 46, pp. 104–120, Jan. 2000.
[26] K.G. Paterson and A.E. Jones, "Efficient decoding algorithms for generalised Reed-Muller Codes, *IEEE Trans. Commun.*, vol. 48, no. 8, pp. 1272–1285, 2000.
[27] K. G. Paterson and V. Tarokh, "On the existence and construction of good codes with low peak-to-average power ratios," *IEEE Trans. Inform. Theory*, vol. 46, no. 6, pp. 1974–1987, Sept. 2000.
[28] B. Preneel, W. van Leekwijck, L. van Linden, R. Govaerts and J. Vandewalle, "Propagation characteristics of boolean functions," in *Proc. EuroCrypt90*, Lecture Notes in Computer Science, vol. 473, pp. 161–173, Springer, Berlin, 1991.
[29] O.S. Rothaus, "On "bent" functions", *J. Comb. Thy. Ser. A*, vol. 20, pp. 300–305, 1976.
[30] T. Wada, "Characteristic of bit sequences applicable to constant amplitude orthogonal multicode systems," *IEICE Trans. Fundamentals*, vol. E83-A, no. 11, pp. 2160–2164, Nov 2000.
[31] T. Wada, T. Yamazato, M. Katayama and A. Ogawa, "A constant amplitude coding for orthogonal multi-code CDMA systems," *IEICE Trans. Fundamentals*, vol. E80-A, no. 12, pp. 2477–2484, Dec. 1997.
[32] T. Wada, T. Yamazato, M. Katayama and A. Ogawa, "Error correcting capability of constant amplitude coding for orthogonal multi-code CDMA systems," *IEICE Trans. Fundamentals*, vol. E81-A, no. 10, pp. 2166–2169, Oct. 1998.
[33] J. Wolfmann, "Bent functions and coding theory," in *Difference sets, sequences and their correlation properties (Bad Windsheim, 1998)*, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 542, Kluwer Acad. Publ., Dordrecht, pp. 393–418, 1999
[34] M. Zeng, A. Annamalai and V.K. Bhargava, "Recent Advances in Cellular Wireless Communications," *IEEE Communications Magazine*, vol. 37, no. 9, pp. 28–138, 1999.