Sequences for OFDM and Multi-Code CDMA: Two Problems in Algebraic Coding Theory

Kenneth G. Paterson

Hewlett-Packard Laboratories,
Filton Road, Stoke Gifford,
Bristol BS34 8QZ, UK.

Abstract. We study the peak-to-average power ratio (PAPR) problem for two different kinds of communications systems, Orthogonal Frequency Division Multiplexing (OFDM) and Multi-Code Code-Division Multiple Access (MC-CDMA). We describe a common coding theoretic approach to reducing the PAPR of both kinds of transmissions. In both cases, the classical Reed-Muller codes turn out to play a critical role. There is an intimate connection between Reed-Muller codes and Golay complementary sequences which can be exploited to produce codes suitable for OFDM. For MC-CDMA, it turns out that bent functions lead to transmissions with ideal power characteristics. In this way, the problem of finding good codes for OFDM and MC-CDMA can be closely related to some old and new problems in algebraic coding theory and sequence design.

1 Introduction

In this paper, we study the peak-to-average power ratio (PAPR) problem for two different kinds of communications systems, Orthogonal Frequency Division Multiplexing (OFDM) and Multi-Code Code-Division Multiple Access (MC-CDMA).

OFDM is a method of transmitting data simultaneously over multiple equally-spaced carrier frequencies, using Fourier transform processing for modulation and demodulation [2,8]. The method has been proposed for many types of radio systems such as wireless local area networks [1] and digital audio and digital video broadcasting [44]. OFDM offers many well-documented advantages for multicarrier transmission at high data rates, particularly in mobile applications.

Code-Division Multiple-Access (CDMA) dominates amongst proposals for 3rd Generation cellular communications systems [56]. Multi-code CDMA is a very simple, backwards-compatible technique for supporting users who demand widely varying data rates for different applications. In MC-CDMA, a user who wishes to transmit at a higher data rate is simply assigned additional orthogonal transmission channels and appears to the base station as multiple users [21,22]. (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 [20], and multi-code CDMA. Here we use it to abbreviate the latter.)

Both OFDM and MC-CDMA involve signals that are the sums of some number of basic signals from an orthogonal set. In the former case, these are continuous-time sinusoidal signals and in the latter, discrete-time Walsh-Hadamard sequences. In both cases, the signal is an orthogonal transform of the data to be transmitted: in OFDM, the signal is related to a Fourier transform and in MC-CDMA, it is simply a Walsh-Hadamard transform. Because of 'constructive interference' in the summation of basic signals, both systems can suffer from high PAPR, a severe handicap in low-cost mobile applications [4,22,23,26,34].

Coding, selecting for transmission only those sequences with low PAPR, is a possible solution to the PAPR problem. For OFDM, it turns out that Golay complementary sequences have excellent PAPR properties. Recently, Davis and Jedwab gave an explicit description of a large class (possibly all) of Golay complementary sequences in terms of certain cosets of the first order Reed-Muller codes [10,11]. Because of this intimate connection to algebraic coding theory, the codes for OFDM in Davis and Jedwab's work have not only low PAPR but also simple encoding algorithms and good error-correcting properties. We will review this work and some generalisations [35,42,45,46] and present some new problems in algebraic coding and sequence design which arise from it.

Then we'll turn our attention to the PAPR problem for MC-CDMA. Here, the sequences with optimal PAPR are those whose Walsh-Hadamard transforms are uniformly small. These correspond to the class of Boolean functions known in the literature as bent functions. Based on this connection, we will describe some classes of codes for MC-CDMA. These codes include earlier coding schemes of Ottosson [33,34] and Wada *et al* [52,53] as special cases. In view of the relationship between the Walsh-Hadamard transform and Reed-Muller codes, it is perhaps not surprising that the Reed-Muller codes will once again play a crucial role. We will develop links to old and new problems about bent functions, Kerdock codes and their relatives, the Delsarte-Goethals codes.

We will close by speculating on the connections between coding for OFDM and coding for MC-CDMA.

This paper draws heavily on material contained in [11,35,36]. These references contain full details and proofs as well as a full account of independent work on Golay complementary sequences [30,32], and on power control in OFDM and MC-CDMA. Further work adopting different approaches to coding for OFDM can be found in [38,47].

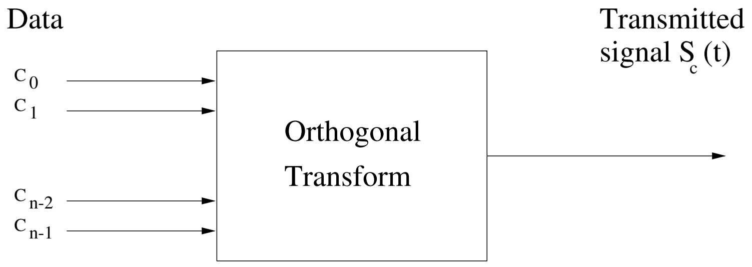

Fig. 1. Model for communication by orthogonal transforms

2 Communication by Orthogonal Transforms

2.1 Model of Communications Systems

In this section, we outline a general model for communication which includes OFDM and MC-CDMA. This model allows us to examine the common features shared by OFDM and MC-CDMA.

In our model (Fig. 1), a binary data vector $c = (c_0, c_1, \ldots, c_{n-1})$ is input to an *orthogonal transform*. Each data bit c_i modifies the sign of one of n orthogonal functions $f_i(t)$ of time t, and the output is the sum of these n modulated functions, the transmitted signal $S_c(t)$. So

$$S_c(t) = \sum_{i=0}^{n-1} (-1)^{c_i} f_i(t)$$

At the receiver (not shown in the figure), a noise-corrupted version of the signal is received. By virtue of orthogonality, computing the inner product of each of the orthogonal functions with the received signal recovers an estimate for each data bit c_i. In practice, the inner products are computed simultaneously via computation of the *inverse transform*.

For OFDM, the orthogonal transform is actually a kind of *Fourier* transform. The resulting signal is resistant to multi-path fading, which makes OFDM an attractive transmission technique in certain wireless environments. More specifically, we have $f_i(t) = e^{2\pi j(f+i\Delta f)t}$ where $j = \sqrt{-1}$, and given $c = (c_0, c_1, \ldots, c_{n-1})$, the OFDM signal is:

$$S_c(t) = \sum_{i=0}^{n-1} (-1)^{c_i} f_i(t) = \sum_{i=0}^{n-1} (-1)^{c_i} e^{2\pi j(f+i\Delta f)t}.$$

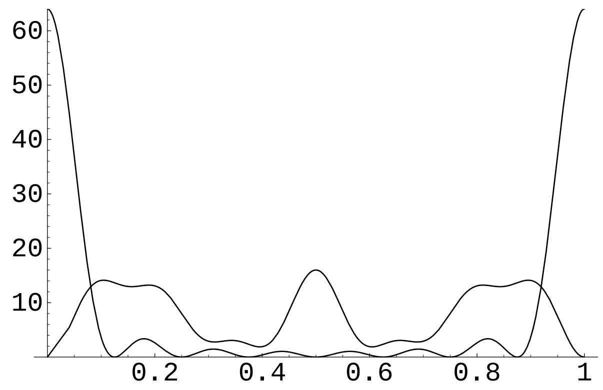

Fig. 2. (Envelope) powers of OFDM signals for $c = 00000000$ and $c = 00011101$, with t normalised to $[0,1]$ by taking $\Delta f = 1$

Here, the n functions f_i are called *carriers* and are orthogonal on the interval $t \in [0, 1/\Delta f]$ with respect to the inner product

$$\langle f, g \rangle = \int_t f(t) g(t)^* dt.$$

In fact, the transmitted signal for OFDM is actually the real part of the complex function $S_c(t)$. However, it is more mathematically convenient (and a good approximation when considering power properties as we shall) to work with this complex signal, called the envelope signal. Fig. 2 shows the function $|S_c(t)|^2$ for two different OFDM signals. Typically $n = 2^m$ where m is small, say 4 up to 6 or so for mobile applications and as large as 10 or 11 for digital TV.

For multi-code CDMA, the transform is a *Walsh-Hadamard* transform. The system transmits at n times the rate of a basic CDMA system and thus caters for users demanding higher data rates. Given $c = (c_0, c_1, \ldots, c_{n-1})$ where $n = 2^m$, we model an MC-CDMA signal by:

$$S_c(t) = \sum_{i=0}^{n-1} (-1)^{c_i} \mathrm{WH}(n)_{it}, \quad t = 0, 1, \ldots, n-1,$$

where

$$\mathrm{WH}(2^m) = \begin{pmatrix} \mathrm{WH}(2^{m-1}) & \mathrm{WH}(2^{m-1}) \\ \mathrm{WH}(2^{m-1}) & -\mathrm{WH}(2^{m-1}) \end{pmatrix}, \qquad \mathrm{WH}(1) = (1)$$

is a $2^m \times 2^m$ Walsh-Hadamard matrix whose rows (and columns) are easily shown by induction to be orthogonal vectors. Notice that, in contrast

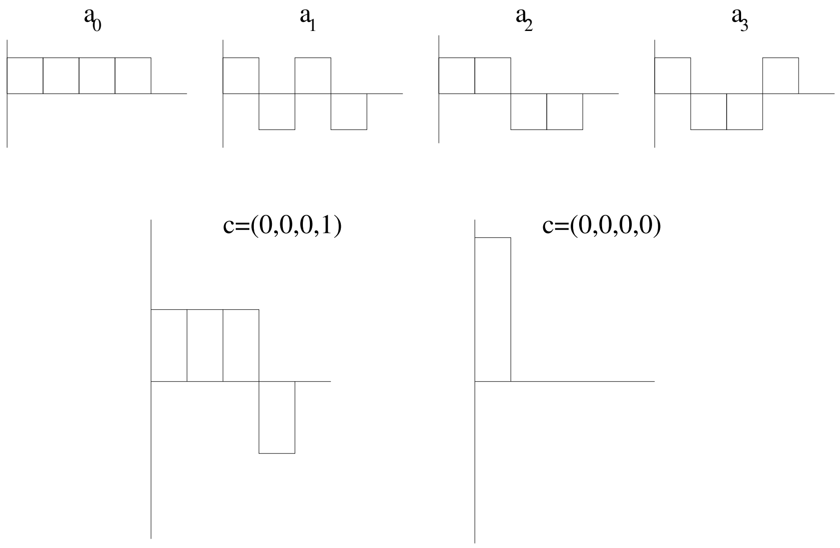

Fig. 3. MC-CDMA signal for $n = 4$

to OFDM, our MC-CDMA signal is modelled as a *discrete-time* signal and involves a *discrete* transform. We can write

$$S_c = (S_c(0), S_c(1), \dots, S_c(n-1)) = \sum_{i=0}^{n-1} (-1)^{c_i} f_i$$

where f_i is the i-th row of $\mathrm{WH}(n)$. Thus we once again have that the signal is a sum of orthogonal functions (vectors in this case) and the transmitted signal is the sum of modulated versions of these signals. Fig. 3 shows the formation of two different MC-CDMA signals in the case $n = 4$. Typically in applications $n = 2^m$ with m between 2 and 6.

In both the OFDM and the MC-CDMA case, our model is only a rough approximation to what happens in a real system. Nevertheless, it captures the key parameter, power, that we want to study.

2.2 Peak-to-Average Power Ratio

Now consider the power of the transmitted signals in a system using an orthogonal transform.

We define the instantaneous power of the signal at time t for data c to be:

$$P_c(t) = |S_c(t)|^2.$$

In the context of OFDM, this real-valued function is usually called the *envelope power* of the signal. If we assume that each of the n orthogonal functions f_i is normalised so that it satisfies $\langle f_i, f_i \rangle = n$, then it is easy to show using orthogonality that the average value of the function $P_c(t)$ is equal to n. On the other hand, as is easily verified, for both OFDM and MC-CDMA, the signal $S_c(t)$ in the case $c = (0, 0, \ldots, 0)$ satisfies $S_c(0) = n$ so that $P_c(0) = n^2$. Informally, this arises because of a temporal alignment of peaks in the orthogonal functions, a kind of 'constructive interference' in the transform. This behaviour can be seen in both Figs. 3 and 2.

We define the *peak-to-average power ratio (PAPR)* of data c to be:

$$\mathrm{PAPR}(c) = \frac{1}{n} \cdot \max_t |S_c(t)|^2.$$

For OFDM, this function is more commonly referred to as the peak-to-mean envelope power ratio (PMEPR), with PAPR being reserved for the ratio $\frac{1}{n} \cdot \max_t \mathrm{R}e(S_c(t))^2$, representing the peak-to-average power ratio of the actual transmitted OFDM signal. Of course, this last function is bounded above by what we call here PAPR(c). Working with the complex signal $S_c(t)$ is somewhat easier than working with the actual transmitted signal.

The above discussion shows that PAPR(c) can be as large as n in a communication system using an orthogonal transform. If the peak power is subject to a design or regulatory limit then this has the effect of reducing the allowed average power relative to that which would be allowed with any constant power transmission scheme. This reduces the effective range of the transmissions and is particularly acute in mobile applications where battery power is a constraint. Moreover, to prevent signal distortions and spectral growth due to non-linearities inherent in electronic components, power amplifiers must be operated below their compression point where power is converted most efficiently. This results in more expensive and inefficiently used components. In summary, high PAPR is a serious drawback to both OFDM and MC-CDMA.

2.3 The Coding Solution

How then can the PAPR of transmissions be controlled? A very simple idea is to use coding: find a code $C \subset \{0, 1\}^n$ in which every word has small PAPR and select for transmission only words $c \in C$. Thus we sacrifice transmission rate for PAPR reduction, inserting an encoder for C between data and orthogonal transform. At the receiver, the original data is recovered by performing the inverse transform and then decoding the resulting received word. This idea, perhaps obvious with the benefit of hindsight, appears to date back to the series of papers [23,24,55] for OFDM and to [33,52] for MC-CDMA. We illustrate the idea schematically in Fig. 4.

Several basic questions immediately arise from the idea of using coding to control PAPR:

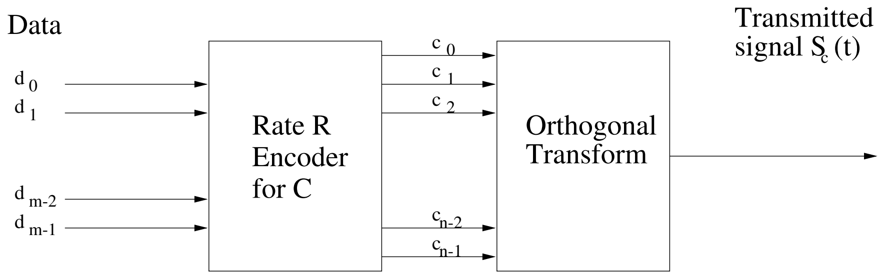

Fig. 4. Model for communication by orthogonal transforms with coding. Here R denotes the rate of the code C and $m = Rn$ is the number of data bits input to the encoder

- Given an orthogonal transform, which words can be used to form a code C with low PAPR?
- What is the maximum rate R that can be achieved while keeping the PAPR of C below a certain value?
- Can the redundancy introduced to reduce PAPR be exploited for error-correction?
- If so, for what triples $(R, d, \mathrm{PAPR}(C))$ can we construct codes? Here d denotes the minimum distance of C and $\mathrm{PAPR}(C)$ the peak-to-average power ratio of C.
- Are there efficient encoders (and decoders) for the code C?

In Secs. 3 and 4, we will describe at least partial answers to these questions for OFDM and MC-CDMA.

3 Coding for OFDM

3.1 Golay Complementary Pairs and Sets

A *Golay complementary pair* is a pair $\{c, d\}$ of binary sequences of length n such that:

$$A_c(u) + A_d(u) = 0, \quad u \neq 0$$

where

$$A_c(u) = \sum_i (-1)^{c_i - c_{i+u}}$$

is the *aperiodic auto-correlation* function of c (in which the summation is understood to be over only those integer values for which both i and $i + u$ lie within $\{0, 1, \ldots, n-1\}$).

Each member of a Golay complementary pair is called a *Golay complementary sequence.*

We are interested in using Golay complementary sequences as OFDM codewords because the resulting OFDM signals have PAPR of at most 2, a substantial and practically very useful reduction from the maximum value of n. This result in [39] generalises earlier work of [3]:

Theorem 1. *The PAPR of any Golay complementary sequence is at most 2.*

Proof. We have

$$\begin{aligned}
P_c(t) &= S_c(t) \cdot S_c(t)^* \\
&= \sum_{i=0}^{n} (-1)^{c_i} e^{2\pi j(f+i\Delta f)t} \cdot \sum_{k=0}^{n} (-1)^{-c_k} e^{-2\pi j(f+k\Delta f)t} \\
&= \sum_{\substack{i-k=u \\ 0\leq i,k<n}} (-1)^{c_i - c_k} \cdot e^{2\pi j u \Delta f t} \\
&= \sum_{u=1-n}^{n-1} A_c(u) e^{2\pi j u \Delta f t} \\
&= A_c(0) + 2 \cdot \mathrm{Re} \sum_{u=1}^{n-1} A_c(u) e^{2\pi j u \Delta f t}.
\end{aligned}$$

Using the fact that $A_c(u) + A_d(u) = 0$ for every $u \neq 0$, we obtain

$$P_c(t) + P_d(t) = A_c(0) + A_d(0) = 2n.$$

Since the function $P_a(t)$ is real-valued and non-negative, we deduce that $P_a(t) \leq 2n$ and the theorem follows.

An illustration of this theorem can be seen in Fig. 5. Notice how the sum of the two powers is exactly 16 for every time t, so that each of the sequences has instantaneous power at most 16 and hence PAPR at most 2.

Binary Golay complementary pairs were introduced by Golay [15,16] in connection with infrared multislit spectrometry and have since found application in a variety of fields [29,48]. They are known to exist for all lengths $n = 2^\alpha 10^\beta 26^\gamma$, where $\alpha, \beta, \gamma \geq 0$ [50], but do not exist for length n having any prime factor congruent to 3 modulo 4 [13]. A variety of recursive and direct constructions for Golay complementary pairs were given in [17]. For a survey of previous results on non-binary Golay complementary pairs, see [14, Chap. 13].

Golay complementary sets were introduced in [49] as a generalisation of Golay complementary pairs. For $1 \leq j \leq N$, let $c^j = (c_0^j, c_1^j, \ldots, c_{n-1}^j)$ be a

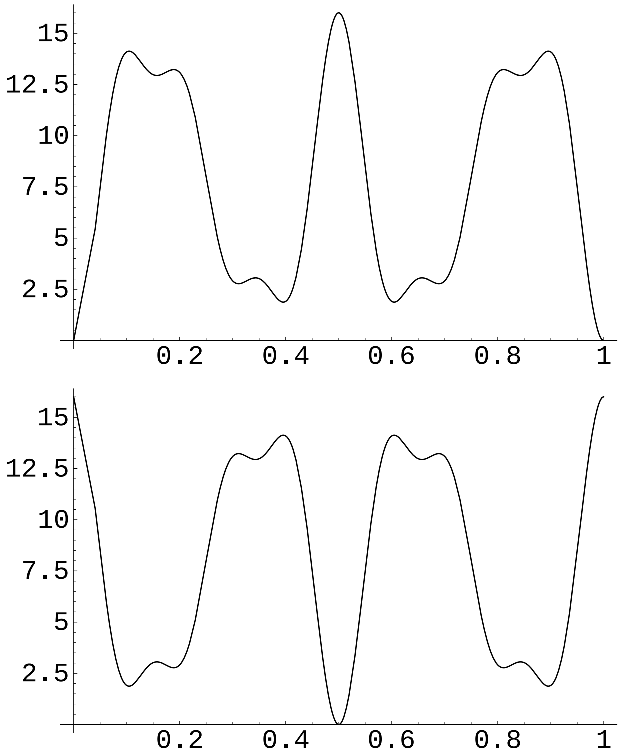

Fig. 5. OFDM Power for Golay Complementary Pair $\{00011101, 00010010\}$

binary sequence of length n. Let $\mathcal{C} = \{c^1, c^2, \ldots, c^N\}$ The set $\mathcal{C}$ is called a *Golay complementary set of size* N if

$$\sum_{j=1}^{N} A_{c^j}(u) = 0 \quad \text{for each } u \neq 0.$$

Clearly, a Golay complementary set of size 2 is a Golay complementary pair. A survey of previous work on these sets and their applications can also be found in [14, Chap. 13].

As with Golay complementary sequences, our motivation for studying Golay complementary sets is that their sequences can have low PAPR. We have the following straightforward generalisation of Thm. 1.

Theorem 2. *The PAPR of any sequence from a Golay complementary set of size N is at most N.*

To make use of Golay complementary sequences (and more generally sequences from Golay complementary sets) to reduce PAPR in OFDM, we at least need to find large numbers of sequences. To build a practical system, we also need to answer the basic questions of how to encode and decode. Thus we need some structure in the set of sequences. But the received wisdom prior to the work of [10,11] was that *aperiodic* correlations are relatively difficult to understand and that sequences with controlled aperiodic correlations do not have any particular regularity. With this context, the results of [10,11] that we describe in Sect. 3.3 below are even more surprising.

3.2 Reed-Muller Codes

We recall the definition of the classical binary Reed-Muller codes $\mathrm{RM}(r,m)$, $0 \leq r \leq m$, from [28, Chap. 13]: the code $\mathrm{RM}(r,m)$ has

$$(n,k,d) = (2^m, \sum_{i=0}^{r} \binom{m}{i}, 2^{m-r})$$

and a generator matrix whose rows are vectors related to certain Boolean functions in m variables $x_0, x_1, \ldots, x_{m-1}$. Each row is obtained by evaluating a monomial function of non-linear order at most r over all 2^m possible inputs $(x_0, x_1, \ldots, x_{m-1})$ in their natural ordering. Notice that we label the codewords of the Reed-Muller codes somewhat unconventionally, c.f. [11,28]. The following example should clarify our notation:

Example 1. $\mathrm{RM}(2,3)$ has length 8, dimension 7, minimum distance 2 and generator matrix:

$$\begin{array}{cc} \begin{bmatrix} 1111\ 1111 \\ 0101\ 0101 \\ 0011\ 0011 \\ 0000\ 1111 \\ 0001\ 0001 \\ 0000\ 0101 \\ 0000\ 0011 \end{bmatrix} & \begin{array}{c} 1 \\ x_0 \\ x_1 \\ x_2 \\ x_0x_1 \\ x_0x_2 \\ x_1x_2 \end{array} \end{array}$$

Each codeword c of $\mathrm{RM}(r,m)$ is obtained from a unique Boolean function in m variables in which the maximum non-linear order is r. We use the two notions of codeword and Boolean function interchangeably in what follows, using c to denote both.

3.3 Golay Complementary Pairs and Sets from Reed-Muller Codes

Theorem 3. *[10,11] Let*

$$Q_\pi = x_{\pi(0)}x_{\pi(1)} + x_{\pi(1)}x_{\pi(2)} + \cdots + x_{\pi(m-2)}x_{\pi(m-1)}$$

where π is a permutation of $\{0,1,\ldots,m-1\}$. Then the coset $Q_\pi + RM(1,m) \subset RM(2,m)$ consists entirely of Golay complementary sequences. The Golay complementary pairs include:

$$\{Q_\pi + w, Q_\pi + w + x_{\pi(0)}\}$$
$$\{Q_\pi + w, Q_\pi + w + x_{\pi(m-1)}\}$$

for each $w \in RM(1,m)$.

Thm. 3 explicitly determines $2^{m+1} \cdot m!/2$ binary Golay complementary sequences of length 2^m (using the factor $m!/2$ rather than $m!$ because the expression $\sum_{k=0}^{m-2} x_{\pi(k)} x_{\pi(k+1)}$ is invariant under the mapping $\pi \mapsto \pi'$, where $\pi'(k) = \pi(m-1-k)$). Exhaustive computations for $m \leq 6$ by T. Stinchcombe (personal communication) have shown that, for these parameters, Thm. 3 accounts for all binary Golay complementary sequences.

Open Problem 1 *Are there any more binary Golay complementary sequences of length 2^m?*

Each of the $2^{m+1} \cdot m!/2$ Golay complementary sequences of length 2^m identified in Thm. 3 has PAPR at most 2. They are neatly arranged in $m!/2$ second order cosets of $\mathrm{RM}(1,m)$, i.e. they occur as a subcode of $\mathrm{RM}(2,m)$. Each coset is identified with a quadratic form of the type Q_π. Therefore this set has all the properties that we need to build practical OFDM systems: a structure which can be exploited for encoding, a certain minimum distance (of at least 2^{m-2} determined by the minimum distance of $\mathrm{RM}(2,m)$) and a relationship to well-understood error-correcting codes which can be used to build efficient decoders. For full details of the variety of coding options trading-off rate, minimum distance and PAPR that can be developed from this result, see [11]. For details on the important issue of efficient decoding, see [11,18,37]. We give just one example of the kind of trade-offs that can be made:

Example 2. In the case $m = 4$, Thm. 3 identifies 12 cosets of $\mathrm{RM}(1,4)$ inside $\mathrm{RM}(2,4)$ in which every word has PAPR at most 2. Selecting any 8 of these cosets (so that the number of encoded bits is an integer, easing implementation), we get an OFDM code with $(R, d, \mathrm{PAPR}) = (1/2, 4, 2)$. We can increase the minimum distance at the expense of rate by considering just a single coset, giving a code with parameters $(5/16, 8, 2)$.

Extensive computations reported in [11] indicate that other second order cosets of $\mathrm{RM}(1,m)$ have amazingly regular (but larger) PAPR. Where does this structure come from? The answer, as we shall see, is connected with Golay complementary sets. We need to introduce one further concept first. With each quadratic form Q in m variables $x_0, \ldots, x_{m-1}$, we can associate a labelled graph $G(Q)$ on m vertices, $0, 1, \ldots, m-1$. An example should make the correspondence clear:

Fig. 6. The graph corresponding to Q_π

Example 3. $Q_\pi = \sum_{i=0}^{m-2} x_{\pi(i)} x_{\pi(i+1)}$ has as its graph what we call a *path* on m vertices, as depicted in Fig. 6.

With the concept of the graph of a quadratic form in hand, we can now state:

Theorem 4. *[35] Suppose Q is a quadratic form in m variables. Suppose further that $G(Q)$ contains a set of $\ell \geq 0$ distinct vertices labelled $j_1, \ldots, j_\ell$ with the property that deleting those ℓ vertices and all their edges results in a path graph (necessarily on $m - \ell$ vertices). Let t be the label of either vertex of degree 1 in this path graph. Then for any choice of $c, c_k \in \mathbb{Z}_2$,*

$$\left\{ Q + \sum_{k=0}^{m-1} c_k x_k + c + \sum_{k=1}^{\ell} d_k x_{j_k} + d x_t \mid d_k, d \in \mathbb{Z}_2 \right\}$$

is a Golay complementary set of size $2^{\ell+1}$.

Thm. 4 provides a partial answer to an open problem posed in [49]:

Open Problem 2 *Obtain direct construction procedures for complementary sets with given parameters, namely, the number of sequences in the set and their lengths.*

Example 4. Let $m = 4$ and

$$Q = x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_2x_3.$$

The graph $G(Q)$ is shown in Fig. 7. We see that deleting the vertex labelled 0 results in a path graph on vertices $1, 2$ and 3. Applying Thm. 4 with $\ell = 1$, we get, for each choice of $c, c_0, c_1, c_2, c_3 \in \mathbb{Z}_2$, the following Golay complementary set of size 4:

$$\begin{aligned}
\{\ & Q + \textstyle\sum_{k=0}^{3} c_k x_k + c, \\
& Q + \textstyle\sum_{k=0}^{3} c_k x_k + c + x_0, \\
& Q + \textstyle\sum_{k=0}^{3} c_k x_k + c + x_1, \\
& Q + \textstyle\sum_{k=0}^{3} c_k x_k + c + x_0 + x_1\ \}.
\end{aligned}$$

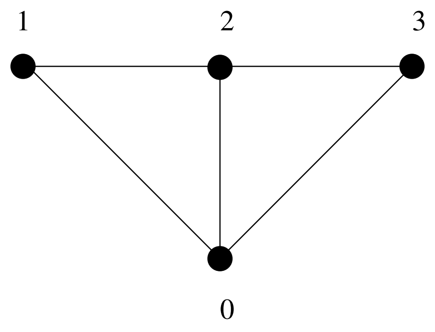

Fig. 7. The graph of the quadratic form $Q = x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_2x_3$

Using Thm. 4, it is possible to give an explicit form (in terms of Boolean functions and graphs) for a large class of binary sequences that lie in Golay complementary sets of size $2^{\ell+1}$. These sequences all have PAPR at most $2^{\ell+1}$. The theorem also gives a bound for the PAPR of each second order coset $Q + \mathrm{RM}(1, m)$ in terms of a graph-theoretic parameter, the minimum number of vertices in $G(Q)$ whose deletion leads to a path. This bound goes some way to explaining the PAPR behaviour of second order cosets observed in [11]. We can also use the theorem and the bound it gives to construct codes for OFDM – see [35] for details.

Thm. 4 is also a generalisation of Thm. 3: the special case $\ell = 0$ of the latter theorem recovers the former. However, the methods that were used to prove the two results are rather different: [11] contains a direct proof of the result on Golay complementary pairs, while [35] uses a recursive approach containing as an intermediate step a result on a generalisation of binary Golay complementary pairs to alphabets $\{+1, -1, 0\}$. The direct approach has the benefit of being quick, but the recursive approach can be used to shed light on why the particular quadratic forms Q_π appear in the theorems.

3.4 Non-binary Sequences and Codes

So far, we have only considered binary sequences and binary modulation for OFDM. In practice, other kinds of modulation are also used, resulting in increased transmission rates. Here the OFDM signal becomes

$$S_c(t) = \sum_{i=0}^{n-1} z_i e^{2\pi j(f+i\Delta f)t}.$$

where $z_i \in \mathcal{Z}$ is some finite subset of the complex numbers, called a *constellation* or *signal set*. For the binary modulation considered so far, we have

$\mathcal{Z} = \{+1, -1\}$ and one bit of information is transported on each carrier. Another common form of modulation is *phase-shift keying.* In q-PSK, we have $\mathcal{Z} = \{\omega^i, 0 \leq i < q\}$ where q is some fixed integer and $\omega = e^{2\pi j/q}$ is a complex q-th root of unity. Typically $q = 2$ (which coincides with our usual binary modulation), 4 (2 bits per carrier, also called QPSK) or 8 (3 bits per carrier). Another important family are the QAM constellations, see [40, Chap. 4] for details.

There are nice (and practically valuable) generalisations of Thms. 3 and 4 to q-ary alphabets which lend themselves to q-PSK modulation. We sketch these generalisations next. In what follows q will be any even integer. We consider the generator matrix for $\mathrm{RM}(r, m)$, but now take linear combinations of rows modulo q. This defines a code that is linear over $\mathbb{Z}_q$, and which we denote $\mathrm{RM}_q(r, m)$. The code $\mathrm{RM}_q(r, m)$ is distinct from other generalisations of the binary Reed-Muller codes [25], but is closely connected to the quaternary code $\mathrm{ZRM}(r, m)$ introduced in [19]. It can be shown [11,35] that the code has the same minimum Hamming distance 2^{m-r} and 'dimension' as the classical binary code. The minimum Lee distance can also be calculated. Each codeword can be associated with a (generalised) Boolean function in m variables with coefficients from $\mathbb{Z}_q$.

We also need to define aperiodic correlation functions and Golay complementary sequences, pairs and sets for sequences over $\mathbb{Z}_q$. To do so, we simply replace -1 by $\omega = e^{2\pi j/q}$ in the definition of aperiodic correlation.

The motivation for the above definitions is the following pair of theorems:

Theorem 5. *[10,11] Let $q = 2^h$ where $h \geq 1$. Then the cosets $2^{h-1}Q_\pi + RM_q(1, m)$ are composed of q-ary Golay complementary sequences.*

Theorem 6. *[35] Let $q = 2h$ be any even integer. Suppose Q is a quadratic form in m variables. Associate with Q a labelled graph $G(Q)$ in which there is an edge between vertices i and j labelled q_{ij} whenever $q_{ij}x_ix_j$ appears as a non-zero term in Q. Suppose further that $G(Q)$ contains a set of $\ell \geq 0$ distinct vertices labelled $j_1, \ldots, j_\ell$ with the property that deleting those ℓ vertices and all their edges results in a path graph in which each edge is labelled h. Then every word of the coset $Q + RM_q(1, m)$ is a sequence lying in a q-ary Golay complementary set of size $2^{\ell+1}$.*

Both theorems can be refined to explicitly identify the pair/set which contains any particular codeword. As well as being of theoretical interest, these theorems can be used to develop many OFDM coding options enjoying low PAPR for non-binary modulations. This is because Thms. 1 and 2 generalise straightforwardly to q-ary sequences. Details can be found in [11,35].

OFDM codes designed for 16-QAM alphabets were introduced in [42]: the codes there are constructed by cleverly decomposing the 16-QAM constellation into a sum of two 4-PSK constellations and using the two sequences from quaternary Golay complementary pairs to determine the modulation in the two signal sets. The resulting OFDM signals have PAPR at most 5.

Table 1. The weight distribution of $Q + \mathrm{RM}(1,m)$, $\mathrm{rank}(Q) = 2h$

Weight	Number of words
$2^{m-1} - 2^{m-h-1}$	2^{2h}
2^{m-1}	$2^{m+1} - 2^{2h+1}$
$2^{m-1} + 2^{m-h-1}$	2^{2h}

Yet another direction was explored in [46]: here, 4-PSK codes are obtained by using a binary code twice, once to encode bits onto a constellation $\{+1,-1\}$ and a second time onto $\{+j,-j\}$. The resulting OFDM signals have PAPR at most 4.

3.5 Ranks of Quadratic Forms and Lower Bounds on PAPR

Let Q be a (binary) quadratic form, $Q = \sum_{i<j} q_{ij}x_ix_j$. Let $A = (q_{ij})$ be an $m \times m$ matrix and $B = A + A^T$. Then the *rank* of the quadratic form Q, denoted $\mathrm{rank}(Q)$, is defined to be the rank of the matrix B (over $\mathbb{Z}_2$). The rank of a quadratic form is a fundamental invariant of the form. As one example of its importance we have:

Theorem 7. *[28, p. 441, Thm. 5] Let Q be a binary quadratic form in m variables. Then rank$(Q) = 2h$ is even. The coset $Q + RM(1,m)$ has the weight distribution given in Table 1.*

We can use the notion of rank to obtain *lower* bounds on the PAPR of cosets. Recall that

$$S_c(t) = \sum_{i=0}^{n-1} (-1)^{c_i} e^{2\pi j(f+i\Delta f)t}.$$

Cammarano and Walker [5] first suggested considering power in the special case $t = 0$. Doing so, we get:

$$|S_c(0)| = \sum_{i=0}^{n-1} (-1)^{c_i} = n - 2\mathrm{wt}(c)$$

where $\mathrm{wt}(c)$ denotes the Hamming weight of c. So

$$\mathrm{PAPR}(c) \geq \frac{1}{n}\left(n - 2\mathrm{wt}(c)\right)^2$$

and it immediately follows that

$$\mathrm{PAPR}(Q + \mathrm{RM}(1,m)) \geq 2^{m-\mathrm{rank}(Q)}.$$

This bound can be used to show that the PAPR bounds on cosets given by Thms. 3 and 4 are often tight. For example, consider the cosets Q_π+RM$(1,m)$ in Thm. 3 when m is odd: in this case, the maximum possible rank of Q_π is $m-1$ and hence PAPR$(Q_\pi + \mathrm{RM}(1,m)) \geq 2$. This technique can be pushed further [35], but there are still many situations where the upper and lower bounds do not match.

The thesis [45] extends the graph theoretical methods of [35]. For example, it is shown that under certain conditions, up to two vertices of degree 0 (i.e. vertices with no incident edges) created in the process of deleting vertices in a graph $G(Q)$ can be ignored. The result is the identification of smaller Golay sets than are predicted by Thm. 6 and therefore, better bounds on PAPR of cosets. Improved lower bounds on the PAPR of binary cosets are also developed in [45], by examining more carefully the values $S_c(0)$. These can be used to demonstrate that degree 0 vertices cannot always be ignored and that certain sequences must lie in large Golay complementary sets. In this way, PAPR can be a useful tool in the study of the Golay set structure of cosets of RM$_q(1,m)$, itself a theoretically interesting sequence problem

Little more is known about lower bounds in the non-binary case. One result in [5] is that the quaternary cosets $2Q_\pi$+RM$_4(1,m)$ have PAPR exactly 2 when m is even. A result of [31] shows that certain cosets of RM$_8(1,m)$ have PAPR at least 3. Earlier computations in [11] suggest that these cosets should have PAPR exactly 3. But this PAPR behaviour cannot arise from Golay complementary sets of size 3 because such sets must be of even size over $\mathbb{Z}_8$.

Open Problem 3 *Obtain stronger lower and upper bounds on the PAPR of second order cosets of RM$_q(1,m)$.*

3.6 Kerdock Codes and Golay Pairs

Here we briefly outline another series of interesting open problems on binary Golay complementary pairs, motivated by the desire to generate more coding options.

We define an (m,h)-set to be a set of quadratic forms $\mathcal{Y}$ in m variables such that:

$$\mathrm{rank}(Q+Q') \geq 2h \quad \forall Q, Q' \in \mathcal{Y}.$$

If such a set $\mathcal{Y}$ contains the all-zero form, then clearly every non-zero form in $\mathcal{Y}$ also has rank at least $2h$. The code

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

obtained from such a set contains $|\mathcal{Y}| \cdot 2^{m+1}$ 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). This can be substantially larger than the minimum distance of $\mathrm{RM}(2,m)$. It is shown in [28, p. 667, Thm. 13] that for any (m,h)-set $\mathcal{Y}$, $|\mathcal{Y}| \le c^{\lfloor m/2\rfloor-h+1}$, where $c=2^m$ for m odd and $c=2^{m-1}$ for m even. In the even case, maximal (m,h)-sets give rise to the notorious Kerdock and Delsarte-Goethals codes.

How can these sets be used to produce better OFDM codes? It is shown in [11] that when $m=4$, there is an $(m,m/2)$-set $\mathcal{Y}$ of size 6 in which every quadratic form is of the type Q_π for some π. Selecting any 4 of the forms and taking the union of cosets they determine leads to a binary OFDM code with parameters $(R,d,\mathrm{PAPR})=(7/16,6,2)$. This gives an attractive coding option which is midway between the codes of Example 2 in terms of rate and minimum distance. Actually the set of 6 forms $\mathcal{Y}$ in this case is a subset of the 'standard Kerdock set' pictured in [27, p. 55]. This example raises a series of open questions:

Open Problem 4 *Suppose m is even. What is the maximum size of an $(m,m/2)$-set containing only quadratic forms of the type Q_π?*

In fact, a simple argument proves an upper bound of $\binom{m}{2}$ on this intersection. Because of the special type of quadratic forms under consideration, the first rows of the corresponding matrices B have a 0 as their first entry and must have weight 1 or 2. A simple count shows that there are $\binom{m}{2}$ possible first rows. For the pair-wise sums of the forms in the set to have rank m, the matrices B must all have distinct first rows. Thus there are at most $\binom{m}{2}$ forms in the set. This bound is attained for $m=4$. Is there a general construction? Does studying the problem in the $\mathbb{Z}_4$-domain help?

The problem can be doubly generalised to consider (m,h) sets as well as the more general quadratic forms considered in Thm. 4:

Open Problem 5 *What is the maximum size of an (m,h)-set containing only quadratic forms Q for which the deletion of some ℓ vertices in $G(Q)$ gives a path graph?*

Nothing is known about this more general formulation. Its solution may lead to interesting OFDM codes with high minimum distances and rates.

4 Coding for Multi-code CDMA

4.1 Reed-Muller Codes, Walsh-Hadamard Transforms and Bent Functions

We recall our discrete time model for an MC-CDMA system from Sect. 2.1. We have:

$$S_c = (S_c(0), S_c(1), \ldots, S_c(n-1)) = \sum_{i=0}^{n-1} (-1)^{c_i} f_i$$

where the f_i, $0 \le i < 2^m$, are the rows of the orthogonal matrix $\mathrm{WH}(2^m)$. The following key result depends on the observation that f_i is just the ± 1 version of the word $\sum_{k=0}^{m-1} i_k x_k \in \mathrm{RM}(1,m)$, where $i = \sum_{k=0}^{m-1} i_k x_k$ is the binary expansion of i.

Theorem 8. *[36] For any word c of length $n = 2^m$,*

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

where $d_*(c) := \min\{d_H(c,w) : w \in RM(1,m)\}$ is the minimum Hamming distance between c and the first-order Reed-Muller code of length 2^m. In particular, $PAPR(c) = 1$ (the minimum possible value) if and only if $d_*(c) = 2^{m-1} - 2^{\frac{m}{2}-1}$.

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 for MC-CDMA. This idea is exploited in [36] to prove analogues of the Hamming and Gilbert-Varshamov sphere-packing bounds for MC-CDMA codes. Similar results for OFDM codes, involving more sophisticated technical machinery, can be found in [38].

The *Walsh-Hadamard transform* of the Boolean function c is defined to be the function $\hat{c}$ with

$$\hat{c}(u) = \sum_{v \in \mathbb{Z}_2^m} (-1)^{c(v)+L_u(v)}, \qquad u \in \mathbb{Z}_2^m$$

where

$$L_u = \sum_{k=0}^{m-1} u_k x_k \in \mathrm{RM}(1,m), \quad u = (u_0, u_1, \ldots, u_{m-1}).$$

Alternatively, working with vectors, the Walsh-Hadamard transform of c is just the vector $(-1)^c \cdot \mathrm{WH}(2^m)$. Thus the vector S_c containing the signal values for codeword c has components that are just the Walsh-Hadamard transform coefficients of c. We have:

Theorem 9. *Let c be a word of length $n = 2^m$. Then*

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

Moreover c has PAPR equal to 1 if and only if $|\hat{c}(u)| = \sqrt{n}$ for every $u \in \mathbb{Z}_2^m$.

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. Equivalently, a bent function corresponds to a word satisfying $d_*(c) = 2^{m-1} - 2^{\frac{m}{2}-1}$, i.e. at maximum distance from $\mathrm{RM}(1,m)$. Thus:

Theorem 10. *[36,51] C is a constant amplitude MC-CDMA code, i.e. a code with PAPR equal to 1, 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.*

Bent functions have received a good deal of attention, see for example [6,7,12,41,43,54] and the brief overview in [28, Chap. 14, Sect. 5]. It is known that any bent function has non-linear order at most $m/2$, that is, lies in the code $\mathrm{RM}(m/2, m)$. So any code of bent functions will automatically have minimum distance at least $2^{m/2}$.

We are also interested in MC-CDMA codes with low PAPR in the case where m is odd. We know that $\mathrm{PAPR}(C) = 1$ cannot be achieved in this case. We are therefore motivated to pose:

Open Problem 6 *When m is odd, how close to being uniform can the Walsh-Hadamard transform of a length 2^m word be? Additionally, how many words achieve this most uniform transform and what, if any, coding structure do they have?*

The first part of this problem is equivalent to determining the covering radius of $\mathrm{RM}(1, m)$ for odd m. See [9] for further information on this old and difficult problem.

4.2 Codes from Bent Functions

In this section, we give several constructions of constant amplitude codes for MC-CDMA from bent functions. For the remainder of the paper, m will be even. It is easy to see that if c is bent, then so is every word of the coset $c + \mathrm{RM}(1, m)$. So as with codes for OFDM, our codes will tend to be formed from unions of cosets of $\mathrm{RM}(1, m)$. In this way, they are amenable to decoding techniques developed for OFDM codes, [11,18,37].

Example 5. The code $Q + \mathrm{RM}(1, m)$ where Q is any bent function in m variables (for example $Q = x_0x_1 + x_2x_3 + \cdots + x_{m-2}x_{m-1}$) is a constant amplitude code of rate $(m+1)/2^m$ and minimum distance 2^{m-1}. When $m = 2$ this gives a code equivalent to that obtained in an *ad hoc* fashion in [52]. See also [53].

Example 6. A second family of constant amplitude codes is obtained by taking as the code at length $n = 2^m$ a union of many second-order cosets corresponding to quadratic forms Q of full rank m: combining Thms. 7 and 8, it is easy to see that such a code will have PAPR 1. Any code formed in this way 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 equal to 28, and a pictorial list of them can be found in [28, p. 429]. Selecting any 16 of these forms gives a code with $(R, d, \mathrm{PAPR}) = (9/16, 4, 1)$. This code has the same parameters as length 16 codes obtained by searching in [34] and an *ad hoc* construction in [52]. In the general case, the number of full rank forms is at least $2^{m(\frac{m}{2}-1)}$ 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, an algorithm for encoding data bits directly onto full rank forms is needed.

Yet more families of codes can be obtained from what is known as the Maiorana-McFarland construction for bent functions:

Theorem 11. *Let π be a permutation on $\{0,1\}^t$ and let g be any Boolean function in t variables. Then*

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

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

This construction produces a large number of bent functions with controllable non-linear order. It can be exploited to produce a variety of coding options. We refer to [36] for the details. To make these codes practical, efficient algorithms for encoding data bits into functions of the type appearing in Thm. 11 are required.

The above code families give new motivation to a longstanding research topic:

Open Problem 7 *Enumerate, construct and classify bent functions.*

As well as being interesting for its own sake, progress on this problem is likely to lead to better families of constant amplitude codes for MC-CDMA.

4.3 Codes from Kerdock and Delsarte-Goethals Codes

In this section we generate more coding options for MC-CDMA by considering subcodes of the Kerdock and Delsarte-Goethals codes.

We recall the definition of an (m,h)-set from Sect. 3.6. An $(m,m/2)$-set is called a Kerdock set. For each even m, a Kerdock set is constructed in [28, 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 an MC-CDMA code with the same minimum distance, rate $(2m-1)/2^m$ and PAPR 1. For example, for $m=4$, we obtain a code with $(R,d,\mathrm{PAPR}) = (7/16,6,1)$ which is a subcode of the Nordstrom-Robinson code.

It is unfortunate that we had to remove the zero coset from the Kerdock code here, since it forced us to reduce the rate from $2m/2^m$ to $(2m-1)/2^m$. It is not hard to show that any Kerdock set of quadratic forms must contain the zero form. However, moving to bent functions with higher non-linear order may help.

Open Problem 8 *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 consider subcodes of the Delsarte-Goethals codes [28, 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, 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 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 $\mathcal{DG}(m,h)$, we must include only full rank quadratic forms. So to evaluate the rate of this subcode, we must find the number of full rank forms in the (m,h)-set used to construct the Delsarte-Goethals codes. Fortunately, this number can be calculated, using the results of [28, Chap. 21, Secs. 7 and 8]. We sketch this calculation next.

Given a set of quadratic forms $\mathcal{Y}$, we define the *inner distribution* of $\mathcal{Y}$ to be the $(m+1)$-tuple of real numbers $(B_0, B_1, \dots, B_{m/2})$ where

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

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

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

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

Lemma 1. *Let $\mathcal{Y}$ 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 $\mathbb{Z}_4$ and so is distance invariant, i.e. the weight distribution and distance distribution of $\mathcal{DG}(m,h)$ are equal. (We refer to [19] for details of the Gray map and $\mathbb{Z}_4$-linearity.) But by virtue of the code's construction from second order 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 $A_i = B_i$, $0 \le i \le m/2$.

The inner distribution $(B_0, B_1, \dots, B_{m/2})$ of any maximal (m,h)-set is known exactly from [28, p. 668, Thm. 14]. We have:

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

where

$$C_{i,j} = 4^{\binom{j-i}{2}} \begin{bmatrix} j \\ i \end{bmatrix} \begin{bmatrix} m/2 \\ j \end{bmatrix} (2^{(m-1)(m/2-h+1-j)} - 1).$$

Here, $\begin{bmatrix} x \\ y \end{bmatrix}$ denotes a 4-ary Gaussian binomial coefficient [28, p. 443].

The following result is proved in [36] by carefully examining these coefficients:

Theorem 12. *With notation as above, we have*

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

Thm. 12 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. 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.

4.4 Further Codes for MC-CDMA

Here we briefly mention two other areas worthy of further exploration.

We have concentrated exclusively on binary codes for MC-CDMA. But, as with OFDM, QPSK and other modulations may be used in place of BPSK in MC-CDMA.

Open Problem 9 *What can be said about quaternary (and larger alphabet) MC-CDMA codes with low PAPR?*

We have only looked at constant amplitude MC-CDMA codes, these having optimal PAPR and a nice connection to bent functions. But codes with approximately constant PAPR may also be useful in practice (especially for m odd where bent functions do not exist). Some ideas in this direction can be found in [36].

Open Problem 10 *Find constructions for large numbers of 'approximately bent' functions and study the trade-offs between rate, PAPR and minimum distance which can be made.*

5 Conclusions

We have seen how the practical problem of designing codes which reduce the PAPR of OFDM and MC-CDMA transmissions leads to new problems in sequence design and algebraic coding theory. We have also seen new motivation for attacking some well-known (and difficult) problems on Reed-Muller codes and bent functions.

Finally, we speculate on the similarities and differences between codes for OFDM and codes for MC-CDMA. In both cases, 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 is a discrete analogue of the Fourier transform inherent in OFDM, so similar coding solutions might be expected. Indeed, in [11] it is shown that for m even, the $m!/2$ cosets of $\mathrm{RM}(1,m)$ which consist of binary Golay complementary sequences are bent cosets. Thus a code formed from these cosets will simultaneously enjoy low OFDM PAPR and ideal MC-CDMA PAPR. However the Reed-Muller code, and the constructions as unions of cosets of $\mathrm{RM}(1,m)$, appear 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 [35]. 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 also 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.

Finally, we ask:

Open Problem 11 *Are there more examples of orthogonal transforms in communications theory waiting to be identified? Are PAPR considerations important and if so, what structure do good codes have?*

Acknowledgements

I am grateful to Prof. J.A. Davis and the anonymous referee for comments which significantly improved the paper.

References

1. M. Aldinger, "Multicarrier COFDM scheme in high bitrate radio local area networks," in *5th IEEE Int. Symp. on Personal, Indoor and Mobile Radio Commun., The Hague*, pp. 969–973, 1994.
2. J.A.C. Bingham, "Multicarrier modulation for data transmission: an idea whose time has come," *IEEE Commun. Magazine*, vol. 28, pp. 5–14, May 1990.
3. S. Boyd, "Multitone signals with low crest factor," *IEEE Trans. Circuits and Systems* vol. CAS-33, pp. 1018–1022, 1986.

4. 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.
5. M.W. Cammarano and M.L. Walker, "Integer maxima in power envelopes of Golay codewords," Technical Report TR-99-02, Dept. Math. Comp. Science, University of Richmond, 1997.
6. C. Carlet and P. Guillot, "A characterization of binary bent functions," *J. Combin. Theory Ser. A*, vol. 76, no. 2, pp. 328–335, 1996.
7. 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.
8. L.J. Cimini, Jr., "Analysis and simulation of a digital mobile channel using orthogonal frequency division multiplexing," *IEEE Trans. Commun.*, vol. 33, pp. 665–675, July 1985.
9. G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering codes*, North-Holland, Amsterdam, 1997.
10. 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.
11. 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.
12. 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.
13. S. Eliahou, M. Kervaire and B. Saffari, "A new restriction on the lengths of Golay complementary sequences," *J. Combin. Theory (A)* vol. 55, pp. 49–59, 1990.
14. P. Fan and M. Darnell, *Sequence Design for Communications Applications*, Communications Systems, Techniques and Applications, Research Studies Press, Taunton, 1996.
15. M.J.E. Golay, "Multislit spectroscopy," *J. Opt. Soc. Amer.* vol. 39, pp. 437–444, 1949.
16. M.J.E. Golay, "Static multislit spectrometry and its application to the panoramic display of infrared spectra," *J. Opt. Soc. Amer.* vol. 41, pp. 468–472, 1951.
17. M.J.E. Golay, "Complementary series," *IRE Trans. Inform. Theory*, vol. IT-7, pp. 82–87, 1961.
18. A.J. Grant and R.D.J. van Nee, "Efficient maximum-likelihood decoding of Q-ary modulated Reed-M-uller codes," *IEEE Comm. Lett.*, vol. 2, pp. 134–136, 1998.
19. 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.
20. S. Hara and R. Prasad, "Overview of multicarrier CDMA,", *IEEE Communications Magazine*, vol. 35, no. 12, pp. 126–133, 1997.
21. C.-L. I and R.D. Gitlin, "Multi-code CDMA wireless personal communications networks" in *Proc. ICC'95*, Seattle, Wash., pp. 1060–1064, 1995.

22. 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.
23. 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.
24. A.E. Jones and T.A. Wilkinson, "Combined coding for error control and increased robustness to system nonlinearities in OFDM," in *IEEE 46th Vehicular Technology Conference*, Atlanta, USA, pp. 904–908, April–May 1996.
25. T. Kasami, S. Lin, and W. Peterson, "New generalizations of Reed-Muller codes, Part I: primitive codes," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 189–199, 1968.
26. 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.
27. J.H. van Lint, *An introduction to coding theory*, 2nd edition, Springer, Berlin, 1992.
28. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.
29. M. Nazarathy, S.A. Newton, R.P. Giffard, D.S. Moberly, F. Sischka and W.R. Trutna, Jr., "Real-time long range complementary correlation optical time domain reflectometer," *IEEE J. Lightwave Technology*, vol. 7, pp. 24–38, 1989.
30. 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.
31. K.M. Nieswand and K.N. Wagner, "Octary codewords with power envelopes of $3*2^m$," Technical Report TR-99-03, Dept. Math. Comp. Science, University of Richmond, 1998.
32. H. Ochiai and H. Imai, "Block coding scheme based on complementary sequences for multicarrier signals," *IEICE Trans. Fundamentals*, pp. 2136–2143, 1997.
33. T. Ottosson, "Precoding in multicode DS-CDMA Systems," in *Proc. 1997 IEEE Int. Symp. Info. Thy.*, Ulm, Germany, June 29 - July 4th, 1997, p. 351.
34. T. Ottosson, "Precoding for minimization of envelope variations in multicode DS-CDMA systems," *Wireless Personal Communications*, vol. 13, pp. 57–78, May 2000.
35. K.G. Paterson, "Generalised Reed-Muller codes and power control in OFDM modulation," *IEEE Trans. Inform. Theory*, vol. 46, pp. 104–120, Jan. 2000.
36. K.G. Paterson, "On codes with low peak-to-average power ratio for multicode CDMA," HP Laboratories Technical Report HPL-2001-115, May 2001. Submitted.
37. 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.
38. 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.
39. B.M. Popović, "Synthesis of power efficient multitone signals with flat amplitude spectrum," *IEEE Trans. Commun.*, vol. 39, pp. 1031–1033, 1991.
40. J.G. Proakis, *Digital Communications (3rd Edition)*, McGraw-Hill, Inc., 1995.

41. 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.
42. C. Rössing, “Golay complementary sequences for OFDM with 16-QAM,” in *Proc. 2000 IEEE Int. Symp. Info. Thy.*, Sorrento, Italy, June 25 - 30, 2000, p. 331.
43. O.S. Rothaus, “On “bent” functions”, *J. Comb. Thy. Ser. A*, vol. 20, pp. 300–305, 1976.
44. P. Shelswell, “The COFDM modulation system: the heart of digital audio broadcasting,” *Elec. Commun. Eng. J.*, pp. 127–136, June 1995.
45. T.E. Stinchcombe, “Aperiodic correlations of length 2^m sequences, complementarity, and power control for OFDM,” Ph.D. thesis, University of London, 2000.
46. V. Tarokh and C. Chong, “A simple encodable/decodable OFDM QPSK code with low peak envelope to average power ratio,” *Proc. 2001 IEEE Int. Symp. Info. Thy.*, Washington D.C., USA, June 24 - 29, 2001.
47. V. Tarokh and H. Jafarkhani, “On Reducing the Peak to Average Power Ratio in Multicarrier Communications,” *IEEE Trans. Comm.*, vol. 48, pp. 37–44, 2000.
48. C.-C. Tseng, “Signal multiplexing in surface-wave delay lines using orthogonal pairs of Golay’s complementary sequences,” *IEEE Trans. Sonics and Ultrasonics*, vol. SU-18, pp. 103–107, 1971.
49. C.-C. Tseng and C.L. Liu, “Complementary sets of sequences,” *IEEE Trans. Inform. Theory*, vol. IT-18(5), pp. 644–652, Sept. 1972.
50. R.J. Turyn, “Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings,” *J. Combin. Theory (A)*, vol. 16, pp. 313–333, 1974.
51. 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.
52. 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.
53. 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.
54. 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
55. T.A. Wilkinson and A.E. Jones, “Minimisation of the peak to mean envelope power ratio of multicarrier transmission schemes by block coding,” in *IEEE 45th Vehicular Technology Conference*, pp. 825–829, Chicago, July 1995.
56. 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.