Generalised Reed-Muller Codes and Power Control in OFDM Modulation

Kenneth G. Paterson, *Member, IEEE*

Abstract

Controlling the peak-to-mean envelope power ratio (PMEPR) of Orthogonal Frequency Division Multiplexed (OFDM) transmissions is a notoriously difficult problem, though one which is of vital importance for the practical application of OFDM in low-cost applications. The utility of Golay complementary sequences in solving this problem has been recognised for some time. In this paper, a powerful theory linking Golay complementary sets of polyphase sequences and Reed-Muller codes is developed. Our main result shows that any second order coset of a q-ary generalisation of the first order Reed-Muller code can be partitioned into Golay complementary sets whose size depends only on a single parameter that is easily computed from a graph associated with the coset. As a first consequence, recent results of Davis and Jedwab on Golay pairs, as well as earlier constructions of Golay, Budišin and Sivaswamy are shown to arise as special cases of a unified theory for Golay complementary sets. As a second consequence, the main result directly yields bounds on the PMEPRs of codes formed from selected cosets of the generalised first order Reed-Muller code. These codes enjoy efficient encoding, good error correcting capability and tightly controlled PMEPR, and significantly extend the range of coding options for applications of OFDM using small numbers of carriers.

Keywords

OFDM; multicarrier; encoding; power; PMEPR; Golay; complementary; sequence; set; Reed-Muller; code.

I. Introduction

Multicarrier communications is a technique that has recently seen rising popularity in wireless and wireline applications [1], [2], [6], [7]. The increasing interest in the technique, also known as orthogonal frequency division multiplexing (OFDM) or discrete multi-tone (DMT), can be ascribed to the advancing capabilities of digital signal processors. International standards making use of OFDM for wireless LANs are currently being established by IEEE 802.11 and ETSI BRAN committees. For wireless applications, OFDM-based systems can be of interest because they can provide a greater immunity to impulse noise and fast fades and eliminate the need for equalisers, while efficient hardware implementations for small numbers of carriers can be realised using FFT techniques.

A major barrier to the widespread acceptance of OFDM is the high peak-to-mean envelope power ratio (PMEPR) of uncoded OFDM signals. If the peak transmit power is limited, either by regulatory or application constraints, this has the effect of reducing the average power allowed under OFDM relative to that under constant power modulation techniques. This in turn reduces the range of OFDM transmissions. Moreover, to prevent spectral growth of the OFDM signal in the form of intermodulation amongst subcarriers and out-of-band radiation, the transmit amplifier must be operated in its linear region (i.e. with a large input back-off), where the conversion from DC to RF power is inefficient. This may have a deleterious effect on battery lifetime in mobile applications. In many low-cost applications the drawbacks of high PMEPR outweigh all the potential benefits of OFDM systems.

A number of approaches have been proposed to deal with this power control problem [13], [19], [23], [25], [29], [40], [43]. One of the more attractive ideas, introduced in [21] and developed further in [42] is to use block coding across the subcarriers and to select codewords which minimise or reduce the PMEPR. This approach suffers from the need to perform an exhaustive search to find the best codes and to store large look-up tables for encoding and decoding. Moreover, this approach does not address the problem of error correction. A more sophisticated approach proposed in [20] is to use codewords drawn from offsets of a linear code. The work in [36] goes further, giving a computationally efficient algorithm which, given any code and a maximum

The material in this paper was presented in part at the 1998 IEEE International Symposium on Information Theory, MIT, Cambridge, MA USA, 16-21 August, 1998

The author is with Hewlett-Packard Laboratories, Filton Road, Stoke-Gifford, Bristol BS34 8QZ, U.K.

likelihood decoding algorithm for that code, finds good offsets. But there is no guarantee about the size of PMEPR reductions that can be obtained with this approach, though the results obtained in [36] for practical convolutional codes are quite encouraging.

On the other hand, it has been known since the work of Popović [32], generalising work of Boyd [3], that the use of *Golay complementary sequences* [16] as codewords to control the modulation of carrier signals results in OFDM signals with PMEPR of at most 2. More recently, Davis and Jedwab [9] made a major theoretical advance, announcing that the large sets of binary length 2^m Golay complementary pairs described in [16] can be obtained from certain second-order cosets of the classical first order Reed-Muller code. Thus Davis and Jedwab found a highly effective way of combining the block coding approach (with all of the encoding, decoding and error correcting capability that this entails) and the use of Golay complementary sequences (with their attractive power control properties). They also reported that 2^h-ary Golay complementary pairs can be similarly obtained from cosets of an appropriate generalisation of the Reed-Muller codes. As a consequence of this intrinsic structure, Davis and Jedwab in [10], the full version of [9], were able to obtain, at least for small numbers of carriers, a range of binary, quaternary and octary OFDM codes with good error correcting capabilities, efficient encoding and decoding, high code rates and enjoying tightly controlled PMEPR. A limited subset of these OFDM codes were also identified in [29], [40], but without making the vital connection to Reed-Muller codes and the consequent powerful and rich theory that this entails.

It was further observed in [10] that, for binary, quaternary and octary codes of lengths 4, 8, 16 and 32, the second order cosets of the first order generalised Reed-Muller code organise themselves naturally into groups according to maximum PMEPR *taken over all the words of a coset*. A first group contains cosets composed of Golay complementary pairs and having PMEPR at most 2, a larger second group appears to consist of cosets having PMEPR at most 4, and so on. Codewords with high PMEPR also appear to be isolated into groups by this classification into cosets. By selecting second order cosets from an ordered list of cosets ranked according to increasing PMEPR, a discrete set of trade-offs between code rate, PMEPR and minimum distance can be obtained [10]. This approach works very well when the number $n = 2^m$ of carriers is small (up to, say, $n = 32$) but becomes infeasible for larger values of n because of the amount of computation needed to numerically evaluate the PMEPRs of complete cosets. Unfortunately, the approach gives no *a priori* guarantee of the achievable code rate for a maximum tolerable PMEPR, since it makes no predictions about the number of cosets satisfying a given upper bound on PMEPR.

The main result of this paper, Theorem 12, generalises the result of [10] on Golay complementary pairs in two ways. Firstly, we work with q-ary alphabets, q even, rather than with 2^h-ary alphabets. Secondly, and more importantly, we consider *general* second order cosets of a q-ary generalisation of the first order Reed-Muller code, which we denote by $\mathrm{RM}_q(1, m)$. We show that the codewords of such a coset lie in *Golay complementary sets* of size 2^{k+1}, where k is an integer depending only on $G(Q)$, a graph naturally associated with the quadratic form Q in m variables which defines the coset. It turns out that the cosets shown to yield Golay complementary pairs in [10] are exactly those arising when $k = 0$ and $q = 2^h$ in our result. Our main result also gives an explicit, non-recursive construction of q-phase Golay complementary sets, answering a long-standing open problem from [38].

As a stepping-stone to our main theorem on Golay complementary sets, we prove an intermediate result on Golay complementary pairs, using a new, inductive approach. On carefully interpreting the proof of this result, we are able to give further insight into why Golay's binary complementary pairs and their generalisations in [9], [10] arise from particular cosets of the Reed-Muller code (while the proof of this in [10] is concise, it gives little clue as to why this should be so). Our approach also gives a unified view of the earlier direct and recursive constructions for Golay complementary pairs in [4], [16], [34].

Since any sequence lying in a Golay complementary set of size 2^{k+1} has PMEPR at most 2^{k+1}, Theorem 12 immediately gives upper bounds on the PMEPRs of complete second order cosets of $\mathrm{RM}_q(1, m)$. We will also develop a lower bound on the PMEPRs of second order cosets of $RM_2(1, m)$ that depends on the rank of the quadratic form Q defining the coset. The two bounds explain much, though not all, of the PMEPR behaviour of cosets empirically observed in [9], [10].

Our final use of Theorem 12 is to develop new codes for OFDM, thereby extending the range of coding options available for practical applications. We use the language of graph theory to explicitly describe large numbers of second order cosets of $\mathrm{RM}_q(1,m)$ having PMEPR bounded by 2,4,8, etc. In each case, coset representatives can be conveniently obtained from a basic set of quadratic forms by applying certain permutations to the m variables appearing in the forms. In this way, we obtain efficient encoding algorithms for the codes. This approach to developing OFDM codes overcomes some of the shortcomings of the coset ranking method of [10] and is mathematically more satisfying.

Since our codes, like those of [10], are constrained to lie inside the full second order Reed-Muller codes, they enjoy high minimum Hamming and Lee distances. But this constraint also implies a strong limitation on the achievable rates for large numbers of carriers. In [26], [33], approximations to the distribution of PMEPR for random binary codewords are derived. Assuming these approximations to be accurate, these papers show that in principle, only a small amount of redundancy needs to be introduced in order to obtain codes with significantly reduced PMEPR. In this light, the OFDM codes presented in [9], [10] and here appear to be far from optimal. But an important *caveat* must be made. These distributional results are about achievable rates of codes of a given PMEPR but say nothing about the error correcting properties of such codes. Indeed recent work in [31] makes precise the notion that there is a more sophisticated trade-off than previously anticipated between the rate, minimum distance and power ratio of codes. Put simply, [31] establishes that one cannot simply impose a PMEPR limit, calculate a rate that should be achievable according to the theoretical distribution and then hope, given that rate and PMEPR limit, to find an error correcting code whose minimum distance is as large as one would predict from coding theoretic considerations alone. So the comparisons that can be made with purely distributional results like those in [26], [33] are of limited value when evaluating OFDM codes simultaneously enjoying good error correcting capability and low PMEPR.

The structure of the remainder of our paper is as follows. In the next section, we establish most of our notation, give a brief description of OFDM modulation and define the generalised Reed-Muller codes that we use. In Section III, we concentrate on Golay complementary pairs of sequences, as a prelude to our main result in Section IV on Golay complementary sets derived from Reed-Muller codes. We then develop our new OFDM codes in Section V. In Section VI, we prove a lower bound on PMEPR for second order cosets of the classical Reed-Muller code and compare it to the upper bound provided by our main result. We close with some conclusions and open problems.

II. Further Background and Notation

A. Correlations of Vectors

Let $\mathbf{A} = [A_0 A_1 \ldots A_{n-1}]$ and $\mathbf{B} = [B_0 B_1 \ldots B_{n-1}]$ be two length n complex-valued vectors and let ℓ be an integer. Define

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

and

$$A(\mathbf{B})(\ell) = C(\mathbf{B},\mathbf{B})(\ell).$$

These functions are called the aperiodic cross-correlation function of $\mathbf{A}$ and $\mathbf{B}$ and the aperiodic auto-correlation function of $\mathbf{B}$ respectively.

We also want to define correlation functions for $\mathbb{Z}_q$-valued vectors. We do this by defining $\omega = e^{2\pi i/q}$ and associating with each vector $\mathbf{a} = [a_0 a_1 \ldots a_{n-1}]$, where $a_i \in \mathbb{Z}_q$, a complex-valued vector $\mathbf{A} = [A_0 A_1 \ldots A_{n-1}]$ in which $A_i = \omega^{a_i}$. If $\mathbf{a}$ and $\mathbf{b}$ are $\mathbb{Z}_q$-valued vectors, then we define (by abuse of notation) the function $C(\mathbf{a},\mathbf{b})(\cdot)$ to be the cross-correlation function of the associated complex-valued vectors $\mathbf{A}$ and $\mathbf{B}$. Similarly for auto-correlations.

Definition 1: A set of N length n vectors $\mathbf{a}^0, \mathbf{a}^1, \ldots, \mathbf{a}^{N-1}$ is said to be a *Golay complementary set* if

$$A(\mathbf{a}^0)(\ell) + A(\mathbf{a}^1)(\ell) + \cdots + A(\mathbf{a}^{N-1})(\ell) = 0, \quad \ell \neq 0.$$

Notice that our definition applies equally to $\mathbb{Z}_q$-valued and complex-valued vectors.

A Golay complementary set of size 2 is called a *Golay complementary pair*, and any sequence in such a pair is called a *Golay complementary sequence.*

Golay complementary pairs were introduced by Golay in his seminal work on infrared multislit spectrometry [14], [15] and have since found applications in many other fields [27], [41], [37]. Their application in multicarrier modulation dates back to [3], [32]. Golay complementary sets were introduced in [38]; a good survey of existing work on these sets and their applications can be found in [12].

B. OFDM Transmission and Golay Complementary Pairs

In this section we give a short introduction to OFDM, as a means of establishing notation.

For an n-carrier OFDM signal with carrier frequencies $f_0 + jf_s, (0 \le j < n)$, we have n time-varying carrier signals

$$e^{2\pi i(f_0+jf_s)t} \quad (0 \le j < n)$$

and with q-PSK modulation, the OFDM signal for the word $\mathbf{a} = [a_0 a_1 \dots a_{n-1}]$ (where $a_j \in \mathbb{Z}_q$) can be modelled as the real part of:

$$S(\mathbf{a})(t) = \sum_{j=0}^{n-1} \omega^{a_j} e^{2\pi i(f_0+jf_s)t} \tag{1}$$

where $\omega = e^{2\pi i/q}$ is a complex q-th root of unity.

For ease of implementation, the number of carriers n is often taken to be a power of 2, $n = 2^m$: in this situation, the signal processing required to compute the OFDM signal can be efficiently performed using fast Fourier transforms. Typically, $q = 2$, 4 or 8, and we speak of BPSK, QPSK or 8-PSK modulation. Carrier modulation schemes other q-PSK, notably 16-QAM and 64-QAM, are also often used in OFDM systems, but we do not consider them here.

We define the *instantaneous envelope power* of the OFDM signal to be the function

$$P(\mathbf{a})(t) = |S(\mathbf{a})(t)|^2.$$

It is an easy exercise to show that

$$\begin{aligned} P(\mathbf{a})(t) &= \sum_{\ell=1-n}^{n-1} A(\mathbf{a})(\ell) e^{2\pi i \ell f_s t} \\ &= A(\mathbf{a})(0) + 2 \cdot \mathrm{Re} \sum_{\ell=1}^{n-1} A(\mathbf{a})(\ell) e^{2\pi i \ell f_s t}. \end{aligned}$$

where $A(\mathbf{a})(\ell)$ is the aperiodic auto-correlation function of the word $\mathbf{a}$. From this last expression, we see that the time-averaged envelope power of $S(\mathbf{a})(t)$ is equal to n. We define the *peak-to-mean envelope power ratio (PMEPR)* of the signal $S(\mathbf{a})(t)$ and the word $\mathbf{a}$ to be

$$\frac{1}{n} \sup_{0 \le f_s t < 1} P(\mathbf{a})(t).$$

The largest value that the PMEPR of an n-carrier OFDM signal can have is n. For example, at $t = 0$, the all-zero word attains this figure. It is this potentially high value of PMEPR and the large dynamic range of OFDM signals that it implies that handicaps OFDM when compared to constant envelope modulation techniques.

The key contribution of [32], generalising work in [3], is to consider words that are Golay complementary sequences: suppose $\mathbf{a}^0, \mathbf{a}^1$ are a Golay complementary pair of length n over $\mathbb{Z}_q$. Then we have:

$$\begin{aligned} P(\mathbf{a}^0)(t) + P(\mathbf{a}^1)(t) &= \sum_{\ell=1-n}^{n-1} \left[A(\mathbf{a}^0)(\ell) + A(\mathbf{a}^1)(\ell)\right] e^{2\pi i \ell t/n} \\ &= A(\mathbf{a}^0)(0) + A(\mathbf{a}^1)(0) \\ &= 2n \end{aligned}$$

and hence (since each power function is non-negative and real-valued)

$$0 \le P(\mathbf{a}^j)(t) \le 2n, \quad j = 0, 1.$$

So the instantaneous envelope power of a multi-carrier signal modulated by a word $\mathbf{a}^j$ from a Golay complementary pair is at most $2n$, and the peak-to-mean envelope power ratio (PMEPR) is at most 2, a substantial and practically useful reduction over the values of PMEPR that can be attained by unrestricted words.

In an entirely analogous fashion, it can be shown that if $\mathbf{a}^0, \ldots, \mathbf{a}^{N-1}$ is a Golay complementary set of size N then

$$0 \le P(\mathbf{a}^j)(t) \le nN, \quad 0 \le j < N.$$

Thus the instantaneous envelope power of a multi-carrier signal modulated by a word $\mathbf{a}^j$ from a Golay complementary set of size N is at most nN, and the PMEPR of such a signal is at most N.

So we are motivated to use words drawn from Golay complementary sets of small size in OFDM. But to obtain reasonable data transmission rates, we need to use very many such words. If we let $\mathcal{C}$ denote the set of words used, then the usual measure of rate for q-PSK modulation with n carriers is $(\log_q |\mathcal{C}|)/n$. To obtain practical OFDM schemes, we need efficient methods for encoding raw information bits to and from words of $\mathcal{C}$. Moreover, the OFDM channel is usually noisy, typically subject to severe multipath fading in wireless applications. Ideally then, the set of words $\mathcal{C}$ used for modulation should form a powerful error correcting code with high rate as well as consisting of words with low PMEPR. This appears at the outset to be a very severe set of requirements.

C. Some Families of Codes

We introduce the families of codes that we use in this paper.

For $q \ge 2$, we define a length n linear code over $\mathbb{Z}_q$ to be a set of $\mathbb{Z}_q$-valued vectors (called codewords) of length n that is closed under the operation of taking $\mathbb{Z}_q$-linear combinations of vectors. With any such code $\mathcal{C}$ we can associate a generator matrix G: the defining property of a generator matrix is that the $\mathbb{Z}_q$-linear combinations of the rows of G should yield the set $\mathcal{C}$. We say that the rows *generate* the code. By a coset of $\mathcal{C}$, we mean a set of the form $\mathbf{a} + \mathcal{C}$ where $\mathbf{a}$ is some fixed vector over $\mathbb{Z}_q$. The vector $\mathbf{a}$ is called a coset representative for the coset $\mathbf{a} + \mathcal{C}$.

We are interested in linear codes derived from *generalised Boolean functions.* To make our later presentation easier, we use a different notation to that adopted in [10]: we define such a function to be a mapping $f : \{0,1\}^m \to \mathbb{Z}_q$ of $\{0,1\}$-valued variables $x_0, x_1, \ldots, x_{m-1}$. A routine counting argument shows that every such function can be written in algebraic normal form as a sum of monomials of the form $x_{j_0} x_{j_1} \ldots x_{j_{r-1}}$ (in which $j_0, j_1 \ldots, j_{r-1}$ are distinct). With each generalised Boolean function f we identify a length 2^m, $\mathbb{Z}_q$-valued vector $\mathbf{f} = [f_0 f_1 \ldots f_{2^m-1}]$ in which

$$f_i = f(i_0, i_1, \ldots, i_{m-1})$$

where $[i_0 i_1 \ldots i_{m-1}]$ is the binary expansion of the integer i (so that $i = \sum_{j=0}^{m-1} i_j 2^j$). We also associate a complex-valued vector $\mathbf{F}$ with f, where $F_i = \omega^{f_i}$, $0 \le i < 2^m$ and ω is a complex q-th root of unity. From now on, we will ignore the distinction between the generalised Boolean function f and the associated $\mathbb{Z}_q$-valued and complex-valued vectors $\mathbf{f}$ and $\mathbf{F}$, using the notation f to refer to all three. The context will make clear to which we are referring in any given situation.

In the binary case, $q = 2$, the r-th order Reed-Muller code $\mathrm{RM}(r, m)$ is defined to be the binary code whose codewords are (the vectors identified with) the Boolean functions of degree at most r in $x_0, x_1, \dots, x_{m-1}$. The code $\mathrm{RM}(r, m)$ is linear, has minimum Hamming distance 2^{m-r} and has a generator matrix whose rows are the words corresponding to the distinct monomials in $x_0, x_1, \dots, x_{m-1}$ of degree at most r. For details, see [24], [39].

We introduce non-binary generalisations of the classical Reed-Muller codes. Our codes generalise those of [10] from 2^h-ary alphabets to the q-ary case. The codes of [10] in turn generalised the classical Reed-Muller codes and the quaternary Reed-Muller codes $\mathrm{ZRM}(r, m)$ defined in [18]. The reader should note that our codes are again different from the earlier generalisations of the binary Reed-Muller codes introduced in [11], [22].

Definition 2: • For $q \geq 2$ and $0 \leq r \leq m$, $\mathrm{RM}_q(r, m)$ is defined to be the linear code over $\mathbb{Z}_q$ that is generated by the $\mathbb{Z}_q$-valued vectors corresponding to the monomials of degree at most r in $x_0, x_1, \dots, x_{m-1}$. Alternatively, $\mathrm{RM}_q(r, m)$ is the linear code over $\mathbb{Z}_q$ whose generator matrix is formally identical to that of the binary code $\mathrm{RM}(r, m)$ (but which is interpreted over $\mathbb{Z}_q$).
• For $q \geq 4$ with q even and for $0 \leq r \leq m + 1$, $\mathrm{ZRM}_q(r, m)$ is defined to be the linear code over $\mathbb{Z}_q$ that is generated by the monomials of degree at most $r - 1$ together with the degree r monomials of the form $2x_{j_0} x_{j_1} \dots x_{j_{r-1}}$ (in which $j_0, j_1 \dots, j_{r-1}$ are distinct and with the convention that monomials of degree -1 and $m + 1$ are equal to zero).

Clearly, $\mathrm{ZRM}_q(r, m)$ is a subcode of $\mathrm{RM}_q(r, m)$. Moreover, for $r \geq 2$, $\mathrm{RM}_q(r, m)$ and $\mathrm{ZRM}_q(r, m)$ are both unions of cosets of $\mathrm{RM}_q(1, m)$. When $r = 2$, an appropriate set of quadratic forms in m variables can be taken as the coset representatives.

Example 3: The code $\mathrm{RM}_4(2, 3)$ is the linear code over $\mathbb{Z}_4$ with generator matrix:

$$\begin{array}{cc}
\begin{bmatrix} 11111111 \\ 01010101 \\ 00110011 \\ 00001111 \\ 00010001 \\ 00000101 \\ 00000011 \end{bmatrix} &
\begin{array}{c} 1 \\ x_0 \\ x_1 \\ x_2 \\ x_0 x_1 \\ x_0 x_2 \\ x_1 x_2 \end{array}
\end{array}$$

while $\mathrm{ZRM}_4(2, 3)$ is the linear code over $\mathbb{Z}_4$ with generator matrix:

$$\begin{array}{cc}
\begin{bmatrix} 11111111 \\ 01010101 \\ 00110011 \\ 00001111 \\ 00020002 \\ 00000202 \\ 00000022 \end{bmatrix} &
\begin{array}{c} 1 \\ x_0 \\ x_1 \\ x_2 \\ 2x_0 x_1 \\ 2x_0 x_2 \\ 2x_1 x_2 \end{array}
\end{array}$$

Now let $\mathbf{a} = [a_0 a_1 \dots a_{n-1}]$ and $b = [b_0 b_1 \dots b_{n-1}]$ be two $\mathbb{Z}_q$-valued vectors. We recall the standard definitions of the Hamming weight $\mathrm{wt_H}(\mathbf{a})$ of $\mathbf{a}$, the Hamming distance $\mathrm{d_H}(\mathbf{a}, \mathbf{b})$ between $\mathbf{a}$ and $\mathbf{b}$, and the minimum Hamming distance $\mathrm{d_H}(\mathcal{C})$ of a code $\mathcal{C}$ over $\mathbb{Z}_q$. We define the Lee weight of the vector $\mathbf{a}$ to be

$$\mathrm{wt_L}(\mathbf{a}) = \sum_{i=0}^{n-1} \min\{a_i, q - a_i\}$$

where each summand is interpreted as being an integer between 0 and $q - 1$. The Lee distance between $\mathbf{a}$ and $\mathbf{b}$, denoted $\mathrm{d_L}(\mathbf{a}, \mathbf{b})$, is defined to be $\mathrm{wt_L}(\mathbf{a} - \mathbf{b} \bmod q)$ where $\mathbf{a} - \mathbf{b} \bmod q$ denotes the vector with components

$a_i - b_i \bmod q$. Finally, we define the minimum Lee distance of a code $\mathcal{C}$ over $\mathbb{Z}_q$ to be:

$$\mathrm{d_L}(\mathcal{C}) = \min\{\mathrm{d_L}(\mathbf{a},\mathbf{b}) : \mathbf{a},\mathbf{b} \in \mathcal{C}, \mathbf{a} \neq \mathbf{b}\}.$$

If $\mathcal{C}$ is linear over $\mathbb{Z}_q$, then the minimum Lee distance of $\mathcal{C}$ is equal to the minimum Lee weight of a non-zero codeword of $\mathcal{C}$.

The following theorem is a straightforward generalisation of a result of [10]:

Theorem 4: We have:

- for $q \geq 2$, $\mathrm{d_H}(\mathrm{RM}_q(r,m)) = \mathrm{d_L}(\mathrm{RM}_q(r,m)) = 2^{m-r}$.
- for $q \geq 4$ with q even, $\mathrm{d_H}(\mathrm{ZRM}_q(r,m)) = 2^{m-r}$ and $\mathrm{d_L}(\mathrm{ZRM}_q(r,m)) = 2^{m-r+1}$.

D. Further Notation

In this subsection we introduce some new notation that will be essential in concisely setting out the proofs of our results on Golay complementary sets of sequences.

Let $f : \{0,1\}^m \to \mathbb{Z}_q$ be a generalised Boolean function in variables $x_0, x_1, \ldots, x_{m-1}$. Let $0 \leq j_0 < j_1 < \ldots < j_{k-1} < m$ be a list of k indices and write $\mathbf{x} = [x_{j_0} x_{j_1} \ldots x_{j_{k-1}}]$. Let $\mathbf{c} = [c_0 c_1 \ldots c_{k-1}]$ be a binary word of length k. Then we define the vector $f|_{\mathbf{x}=\mathbf{c}}$ to be the complex-valued vector with component $i = \sum_{j=0}^{m-1} i_j 2^j$ equal to $\omega^{f(i_0,i_1,\ldots,i_{m-1})}$ if $i_{j_\alpha} = c_\alpha$ for each $0 \leq \alpha < k$, and equal to 0 otherwise. Here ω is a complex q-th root of unity. By convention, in the special case where $\mathbf{x}$ and $\mathbf{c}$ are null (i.e. of length zero), we define $f|_{\mathbf{x}=\mathbf{c}}$ to be the complex-valued vector associated with f.

A simple consequence of the definition is the following vector identity: for any $\mathbf{x}$ defined as above,

$$f = \sum_{\mathbf{c}} f|_{\mathbf{x}=\mathbf{c}}. \tag{2}$$

Example 5: For $q = 2$ and $m = 3$, consider the function $f = x_1$. Writing $+$ for 1 and $-$ for -1, the vector $f|_{x_0=0}$ is equal to $[+0-0+0-0]$, while the vector $f|_{x_0=1}$ is equal to $[0+0-0+0-]$. Adding these vectors, we recover the vector $[++--++--]$, which is the complex-valued vector associated with x_1.

It is apparent that the vector $f|_{\mathbf{x}=\mathbf{c}}$ is equal to the usual complex-valued vector f in components $i = \sum_{j=0}^{m-1} i_j 2^j$ where $[i_{j_0} \ldots i_{j_{k-1}}] = [c_0 \ldots c_{k-1}]$, but is equal to zero in every other position. For example, $f|_{x_0=0}$ and $f|_{x_0=1}$ pick out the even and odd components from the complex-valued vector f, while $f|_{x_{m-1}=0}$ and $f|_{x_{m-1}=1}$ give the left and right halves of f. Alternatively, it's easy to see that $f|_{\mathbf{x}=\mathbf{c}}$ agrees with complex-valued vector f in components where the binary vector corresponding to the generalised Boolean function

$$\prod_{c_\alpha=1} x_{j_\alpha} \prod_{c_\alpha=0} (1 - x_{j_\alpha}).$$

has a 1, and is equal to 0 elsewhere.

The vector $f|_{\mathbf{x}=\mathbf{c}}$ can also be thought of as being constructed from the generalised Boolean function f by substituting $x_{i_\alpha} = c_\alpha$ in the algebraic normal form for f for each $0 \leq \alpha < k$, simplifying to obtain a generalised Boolean function in $m-k$ variables (which we also denote by $f|_{\mathbf{x}=\mathbf{c}}$), then calculating $\omega^{f|_{\mathbf{x}=\mathbf{c}}}$ over the domain of this new function and finally inserting zeros at appropriate locations in the resulting vector. We can synthesise the generalised Boolean function f from the various functions $f|_{\mathbf{x}=\mathbf{c}}$. We have:

$$f = \sum_{\mathbf{c}} f|_{\mathbf{x}=\mathbf{c}} \prod_{c_\alpha=1} x_{j_\alpha} \prod_{c_\alpha=0} (1 - x_{j_\alpha}) \tag{3}$$

which is the functional analogue of the vector equation (2).

Example 6: We take $q = 2$, $m = 4$ and

$$f(x_0, x_1, x_2, x_3) = x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_2x_3$$

corresponding to binary vector [0001011101001101]. Substituting $x_0 = 0$ and $x_0 = 1$ in the algebraic normal form for f, we get

$$f|_{x_0=0} = x_1x_2 + x_2x_3, \quad f|_{x_0=1} = x_1x_2 + x_2x_3 + x_1 + x_2 + x_3$$

with corresponding vectors

$$f|_{x_0=0} = [+0+0+0-0+0+0-0+0], \quad f|_{x_0=1} = [0+0-0-0-0-0+0-0-].$$

Reversing this using (3), we can check that

$$f|_{x_0=0} \cdot (1-x_0) + f|_{x_0=1} \cdot x_0$$

yields the function f and that the complex-valued vector f is the sum of the vectors $f|_{x_0=0}$ and $f|_{x_0=1}$.

The following lemma (whose proof comes from manipulation of components) relates the aperiodic correlations of vectors.

Lemma 7: Let $f, g : \{0,1\}^m \to \mathbb{Z}_q$ be generalised Boolean functions in variables $x_0, x_1, \ldots, x_{m-1}$. Let $0 \le j_0 < j_1 < \ldots < j_{k-1} < m$ be a list of k indices and let $\mathbf{c} = [c_0 c_1 \ldots c_{k-1}]$ and $\mathbf{d} = [d_0 d_1 \ldots d_{k-1}]$ be binary-valued vectors. Write $\mathbf{x} = [x_{j_0} x_{j_1} \ldots x_{j_{k-1}}]$ and suppose $0 \le j < m$ is an index with $j \ne j_0, j_1, \ldots, j_{k-1}$. Then

$$\begin{aligned} C(f|_{\mathbf{x}=\mathbf{c}}, g|_{\mathbf{x}=\mathbf{d}})(\ell) &= C(f|_{\mathbf{x}x_j=\mathbf{c}0}, g|_{\mathbf{x}x_j=\mathbf{d}0})(\ell) + C(f|_{\mathbf{x}x_j=\mathbf{c}0}, g|_{\mathbf{x}x_j=\mathbf{d}1})(\ell) \\ &+ C(f|_{\mathbf{x}x_j=\mathbf{c}1}, g|_{\mathbf{x}x_j=\mathbf{d}0})(\ell) + C(f|_{\mathbf{x}x_j=\mathbf{c}1}, g|_{\mathbf{x}x_j=\mathbf{d}1})(\ell) \end{aligned}$$

Note that the above lemma still holds in the case where $\mathbf{x}$ is null.

As a special case of the above lemma, we have:

$$\begin{aligned} A(f|_{\mathbf{x}=\mathbf{c}})(\ell) &= A(f|_{\mathbf{x}x_j=\mathbf{c}0})(\ell) + A(f|_{\mathbf{x}x_j=\mathbf{c}1})(\ell) \\ &+ C(f|_{\mathbf{x}x_j=\mathbf{c}0}, f|_{\mathbf{x}x_j=\mathbf{c}1})(\ell) + C(f|_{\mathbf{x}x_j=\mathbf{c}1}, f|_{\mathbf{x}x_j=\mathbf{c}0})(\ell) \end{aligned} \tag{4}$$

and as a generalisation of this (with a proof that is a routine induction based on Lemma 7):

Lemma 8: Let $f : \{0,1\}^m \to \mathbb{Z}_q$ be a generalised Boolean function in variables $x_0, x_1, \ldots, x_{m-1}$. Let $0 \le j_0 < j_1 < \ldots < j_{k-1} < m$ be a list of k indices. Write $\mathbf{x} = [x_{j_0} x_{j_1} \ldots x_{j_{k-1}}]$. Then

$$A(f)(\ell) = \sum_{\mathbf{c}} A(f|_{\mathbf{x}=\mathbf{c}})(\ell) + \sum_{\mathbf{c}_1 \ne \mathbf{c}_2} C(f|_{\mathbf{x}=\mathbf{c}_1}, f|_{\mathbf{x}=\mathbf{c}_2})(\ell).$$

III. Golay Complementary Pairs From Reed-Muller Codes

In this section we prove a theorem which identifies a large class of complex-valued Golay complementary pairs whose terms come from the set

$$\{0\} \cup \{\omega^i : i = 0, 1, \ldots, q-1\},$$

where, as in the remainder of this paper, q is even and ω is a complex q-th root of unity. This theorem will be fundamental in our construction of larger Golay complementary sets.

As a corollary of our theorem, we obtain a new inductive proof of the results of [9], [10] on Golay complementary pairs derived from cosets of first order Reed-Muller codes. We also seek to elucidate the relationships between Golay's constructions for pairs [16], the forms identified in [9], [10] and earlier results on the synthesis of Golay complementary pairs in [4], [34].

A. Graphs and Quadratic Forms

Let $Q : \{0,1\}^m \to \mathbb{Z}_q$ be the generalised Boolean function defined by

$$Q(x_0, \ldots, x_{m-1}) = \sum_{0 \le i < j < m} q_{ij} x_i x_j$$

where $q_{ij} \in \mathbb{Z}_q$, so that Q is a quadratic form in m variables over $\mathbb{Z}_q$. We associate a labelled graph $G(Q)$ on m vertices with Q as follows. We label the vertices of $G(Q)$ by $0, 1, \ldots, m-1$ and join vertices i and j by an edge labelled q_{ij} if $q_{ij} \ne 0$. In the case $q = 2$, every edge is labelled 1 and by convention we will omit edge-labels in this case. Of course, from any graph G of this type we can recover a quadratic form Q. If

$f : \{0,1\}^m \to \mathbb{Z}_q$ is a quadratic *function* (i.e. a generalised Boolean function corresponding to a codeword of $\mathrm{RM}_q(2,m)$), then we define $G(f)$ to be the graph $G(Q)$ where Q is the quadratic part of f.

We say that a graph G of the type defined above is a *path* if either

- $m = 1$ (in which case the graph contains a single vertex and no edges), or
- $m \geq 2$ and G has exactly $m-1$ edges, all labelled $q/2$, which form a Hamiltonian path in G.

For $m \geq 2$, a path on m vertices corresponds a quadratic form of the type:

$$\frac{q}{2} \cdot \sum_{\alpha=0}^{m-1} x_{\pi(\alpha)} x_{\pi(\alpha+1)}, \tag{5}$$

where π is a permutation of $\{0, 1, \ldots, m-1\}$.

B. Construction of Golay Complementary Pairs

Let $f : \{0,1\}^m \to \mathbb{Z}_q$ be a generalised Boolean function in variables $x_0, x_1, \ldots, x_{m-1}$. As usual we let $0 \leq j_0 < j_1 < \ldots < j_{k-1} < m$ be a list of k indices, where $0 \leq k \leq m-1$ and write $\mathbf{x} = [x_{j_0} x_{j_1} \ldots x_{j_{k-1}}]$. We also write $0 \leq i_0 < i_1 < \ldots < i_{m-k-1} < m$ for the remaining $m-k$ indices between 0 and $m-1$.

Let $\mathbf{c} = [c_0 c_1 \ldots c_{k-1}]$ be a binary word of length k.

Theorem 9: With notation as above, suppose that the function $f|_{\mathbf{x}=\mathbf{c}}$ (obtained from f by substituting $x_{j_\alpha} = c_\alpha$, $0 \leq \alpha < k$, in the algebraic normal form of f) is a quadratic function and that $G(f|_{\mathbf{x}=\mathbf{c}})$ is a path. Then the complex-valued vector $f|_{\mathbf{x}=\mathbf{c}}$ is a Golay complementary sequence, forming a Golay complementary pair with each vector of the form

$$(f + (q/2)x_a + r)|_{\mathbf{x}=\mathbf{c}}$$

where $r \in \mathbb{Z}_q$ is arbitrary and a is either the single vertex of $G(f|_{\mathbf{x}=\mathbf{c}})$ when $k = m-1$, or an end vertex of the path in $G(f|_{\mathbf{x}=\mathbf{c}})$ when $0 \leq k < m-1$.

Proof: The proof is by induction on k, where we take as an inductive hypothesis the statement of the theorem. The case $k = m-1$ serves as a base case for the induction. In this case Q, the quadratic part of $f|_{\mathbf{x}=\mathbf{c}}$, is identically zero, $G(f|_{\mathbf{x}=\mathbf{c}})$ has a single vertex labelled a and $\mathbf{x}$ omits exactly the variable x_a. From this last fact, it follows that for *any* function h, we have that $h|_{\mathbf{x}=\mathbf{c}}$ is non-zero in exactly two components, namely those numbered $\sum_{j \neq a} c_j 2^j$ and $2^a + \sum_{j \neq a} c_j 2^j$, these components being 2^a positions apart in the vector $h|_{\mathbf{x}=\mathbf{c}}$.

Consider the pair of vectors

$$f|_{\mathbf{x}=\mathbf{c}} \quad \text{and} \quad (f + (q/2)x_a + r)|_{\mathbf{x}=\mathbf{c}},$$

where $r \in \mathbb{Z}_q$ is arbitrary. Now the function $(q/2)x_a + r$ takes on values r and $q/2 + r$ in the two non-zero components. Suppose that $f|_{\mathbf{x}=\mathbf{c}}$ takes on values ω^{f_0} and ω^{f_1} in the two non-zero components. Then the vector $(f + (q/2)x_a + r)|_{\mathbf{x}=\mathbf{c}}$ takes on the values ω^{f_0+r} and $-\omega^{f_1+r}$ in the two non-zero components. It is now simple to show that the vectors $f|_{\mathbf{x}=\mathbf{c}}$ and $(f + (q/2)x_a + r)|_{\mathbf{x}=\mathbf{c}}$ form a Golay complementary pair.

Now suppose the theorem is true in the case where $\mathbf{x}$ contains $k+1$ variables and consider the case of k variables, where $0 \leq k \leq m-2$. The non-zero components of $f|_{\mathbf{x}=\mathbf{c}}$ are determined by the values of the quadratic function $f|_{\mathbf{x}=\mathbf{c}}$ in variables $x_{i_0}, \ldots, x_{i_{m-k-1}}$, where $G(f|_{\mathbf{x}=\mathbf{c}})$ is a path. So for some permutation π of $\{0, 1, \ldots, m-k-1\}$ and some $g_0, \ldots, g_{m-k-1}, g' \in \mathbb{Z}_q$, we can write

$$f|_{\mathbf{x}=\mathbf{c}}(x_{i_0}, \ldots, x_{i_{m-k-1}}) = Q + L$$

where

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

and

$$L(x_{i_0}, \dots, x_{i_{m-k-1}}) = \sum_{\alpha=0}^{m-k-1} g_\alpha x_{i_{\pi(\alpha)}} + g'.$$

We claim that the pair of vectors

$$f|_{\mathbf{x}=\mathbf{c}}, \quad (f + (q/2)x_{i_{\pi(m-k-1)}} + r)|_{\mathbf{x}=\mathbf{c}},$$

where $r \in \mathbb{Z}_q$ is arbitrary, form a Golay complementary pair. The argument that we give to support this claim also applies with minor modifications to the pairs:

$$f|_{\mathbf{x}=\mathbf{c}}, \quad (f + (q/2)x_{i_{\pi(0)}} + r)|_{\mathbf{x}=\mathbf{c}}, \quad r \in \mathbb{Z}_q.$$

Notice that $i_{\pi(0)}$ and $i_{\pi(m-k-1)}$ are the end vertices of the path $G(f|_{\mathbf{x}=\mathbf{c}})$.

Write $a = i_{\pi(m-k-1)}$, let $\ell \neq 0$ be chosen arbitrarily and consider

$$A(f|_{\mathbf{x}=\mathbf{c}})(\ell) + A((f + (q/2)x_a + r)|_{\mathbf{x}=\mathbf{c}})(\ell).$$

Using equation (4), we can decompose this sum as

$$\begin{array}{rl} & A(\mathbf{f}_1)(\ell) + A(\mathbf{f}_2)(\ell) + C(\mathbf{f}_1, \mathbf{f}_2)(\ell) + C(\mathbf{f}_2, \mathbf{f}_1)(\ell) \\ + & A(\mathbf{f}_3)(\ell) + A(\mathbf{f}_4)(\ell) + C(\mathbf{f}_3, \mathbf{f}_4)(\ell) + C(\mathbf{f}_4, \mathbf{f}_3)(\ell) \end{array} \tag{6}$$

where

$$\begin{aligned} \mathbf{f}_1 &= f|_{\mathbf{x}x_a=\mathbf{c}0}, \\ \mathbf{f}_2 &= f|_{\mathbf{x}x_a=\mathbf{c}1}, \\ \mathbf{f}_3 &= (f + (q/2)x_a + r)|_{\mathbf{x}x_a=\mathbf{c}0}, \\ \mathbf{f}_4 &= (f + (q/2)x_a + r)|_{\mathbf{x}x_a=\mathbf{c}1}. \end{aligned}$$

The non-zero components of the vector $\mathbf{f}_1$ come from a function h_1 obtained by substituting $x_a = x_{i_{\pi(m-k-1)}} = 0$ in the function $f|_{\mathbf{x}=\mathbf{c}}$. For $0 \leq k \leq m-3$ we have:

$$h_1(x_{i_{\pi(0)}}, \dots, x_{i_{\pi(m-k-2)}}) = \frac{q}{2} \cdot \sum_{\alpha=0}^{m-k-3} x_{i_{\pi(\alpha)}} x_{i_{\pi(\alpha+1)}} + \sum_{\alpha=0}^{m-k-2} g_\alpha x_{i_{\pi(\alpha)}} + g',$$

while for $k = m-2$ we have:

$$h_1(x_{i_{\pi(0)}}) = g_0 x_{i_{\pi(0)}} + g'.$$

Similarly, the non-zero components of the vector $\mathbf{f}_2$ come from a function h_2 obtained by substituting $x_a = x_{i_{\pi(m-k-1)}} = 1$ in the function $f|_{\mathbf{x}=\mathbf{c}}$. We have:

$$h_2(x_{i_{\pi(0)}}, \dots, x_{i_{\pi(m-k-2)}}) = h_1(x_{i_{\pi(0)}}, \dots, x_{i_{\pi(m-k-2)}}) + (q/2)x_{i_{\pi(m-k-2)}} + g_{m-k-1}.$$

Next consider the vector:

$$\mathbf{f}_2' := (f + (q/2)x_{i_{\pi(m-k-2)}} + g_{m-k-1})|_{\mathbf{x}x_a=\mathbf{c}0}.$$

Substituting $\mathbf{x} = \mathbf{c}$ and then $x_a = 0$ in the expression for $f + (q/2)x_{i_{\pi(m-k-2)}} + g_{m-k-1}$, we obtain the function $h_1 + (q/2)x_{i_{\pi(m-k-2)}} + g_{m-k-1}$, identical to h_2. It follows that the value of the vector $\mathbf{f}_2$ in component i is equal to that of the vector $\mathbf{f}_2'$ in position $i - 2^a$ (that is, in the non-zero positions, $\mathbf{f}_2$ is just a shift of $\mathbf{f}_2'$). Hence the vectors $\mathbf{f}_2$ and $\mathbf{f}_2'$ have identical auto-correlation functions.

Now consider the pair

$$\mathbf{f}_1 = f|_{\mathbf{x}x_a=\mathbf{c}0} \quad \text{and} \quad \mathbf{f}_2' = (f + (q/2)x_{i_{\pi(m-k-2)}} + g_{m-k-1})|_{\mathbf{x}x_a=\mathbf{c}0}.$$

We have seen above that h_1, the generalised Boolean function to which $\mathbf{f}_1$ corresponds, is quadratic and has a graph that is a path on $m-k-1$ vertices. Moreover, either $i_{\pi(m-k-2)}$ is an end vertex of this path, or $k = m-2$ and it is the only vertex in the graph. By the inductive hypothesis, $\mathbf{f}_1$ and $\mathbf{f}_2'$ are a Golay complementary pair, hence

$$A(\mathbf{f}_1)(\ell) + A(\mathbf{f}_2')(\ell) = 0.$$

Since $A(\mathbf{f}_2)(\ell) = A(\mathbf{f}_2')(\ell)$ for every ℓ, we also have

$$A(\mathbf{f}_1)(\ell) + A(\mathbf{f}_2)(\ell) = 0. \tag{7}$$

From the definitions, we have $\mathbf{f}_3 = \omega^r \mathbf{f}_1$ and $\mathbf{f}_4 = -\omega^r \mathbf{f}_2$. It follows that $A(\mathbf{f}_3)(\ell) = A(\mathbf{f}_1)(\ell)$ and $A(\mathbf{f}_4)(\ell) = A(\mathbf{f}_2)(\ell)$ and hence from (7) that

$$A(\mathbf{f}_3)(\ell) + A(\mathbf{f}_4)(\ell) = 0. \tag{8}$$

Moreover $C(\mathbf{f}_3, \mathbf{f}_4)(l) = C(\omega^r \mathbf{f}_1, -\omega^r \mathbf{f}_2)(l) = -C(\mathbf{f}_1, \mathbf{f}_2)(l)$ and so

$$C(\mathbf{f}_1, \mathbf{f}_2)(\ell) + C(\mathbf{f}_3, \mathbf{f}_4)(\ell) = C(\mathbf{f}_2, \mathbf{f}_1)(\ell) + C(\mathbf{f}_4, \mathbf{f}_3)(\ell) = 0 \tag{9}$$

Combining (7) – (9), we see that the sum in (6) is equal to zero. Since $\ell \neq 0$ was arbitrary, the vectors $f|_{\mathbf{x}=\mathbf{c}}$ and $(f + (q/2)x_a + r)|_{\mathbf{x}=\mathbf{c}}$ are a Golay complementary pair. □

Example 10: As in Example 6, we take $q = 2$, $m = 4$ and

$$f(x_0, x_1, x_2, x_3) = x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_2x_3$$

corresponding to binary vector [0001011101001101]. The graph $G(f)$ is shown in Figure 1. Substituting $x_0 = 0$ in the above expression for f, we get $f|_{x_0=0} = x_1x_2 + x_2x_3$, so that $G(f|_{x_0=0})$ is a path. By Theorem 9

$$\begin{aligned} f|_{x_0=0} &= [+0+0+0-0+0+0-0+0], \\ (f+x_1)|_{x_0=0} &= [+0-0+0+0+0-0-0-0] \end{aligned}$$

are a Golay complementary pair. Likewise substituting $x_0 = 1$ in f, we get $f|_{x_0=1} = x_1x_2 + x_2x_3 + x_1 + x_2 + x_3$, so that $G(f|_{x_0=1})$ is again a path. Again the vectors

$$\begin{aligned} f|_{x_0=1} &= [0+0-0-0-0-0+0-0-], \\ (f+x_1)|_{x_0=1} &= [0+0+0-0+0-0-0-0+] \end{aligned}$$

are a Golay complementary pair. Since $f = \sum_{\mathbf{c}} f|_{\mathbf{x}=\mathbf{c}}$, we see that the vector f can be obtained by combining two Golay complementary sequences of length 8.

C. Relation to Previous Constructions

Taking $k = 0$ in the Theorem 9, we obtain a generalisation of a result of [9], [10] from the case of 2^h-ary alphabets to the case of even alphabets.

Corollary 11: Let q be even, let π be a permutation of $\{0, 1, \ldots, m-1\}$ and let $f : \{0,1\}^m \to \mathbb{Z}_q$ be defined by

$$f(x_0, \ldots, x_{m-1}) = \frac{q}{2} \cdot \sum_{i=0}^{m-2} x_{\pi(i)} x_{\pi(i+1)} + \sum_{i=0}^{m-1} g_i x_i + g', \tag{10}$$

where $g_0, g_1, \dots, g_{n-1}, g' \in \mathbb{Z}_q$. Then the vector corresponding to f forms a Golay complementary pair with each of the vectors corresponding to the functions

$$f + (q/2)x_{\pi(0)} + r, \quad f + (q/2)x_{\pi(m-1)} + r, \qquad r \in \mathbb{Z}_q.$$

This corollary identifies a set of $(m!/2)q^{m+1}$ Golay complementary sequences arranged in $m!/2$ cosets of $\mathrm{RM}_q(1,m)$. The coset representatives are the quadratic forms $\frac{q}{2}\cdot\sum_{i=0}^{m-2} x_{\pi(i)}x_{\pi(i+1)}$, where π is any permutation of $\{0,1,\dots,m-1\}$. So these cosets are contained in $\mathrm{RM}_q(2,m)$, and in $\mathrm{ZRM}_q(2,m)$ when q is divisible by 4. The corollary exhibits, for each Golay complementary sequence, $2q$ different Golay complementary pairs in which the sequence lies.

We note that the proof technique of [10] is rather different from the inductive approach developed here. We want to indicate how our approach sheds some light on why the particular quadratic forms which arise in Corollary 11 and in [9], [10] do so. Recall that in the proof of Theorem 9, we considered the pair of vectors

$$f|_{\mathbf{x}=\mathbf{c}} \quad \text{and} \quad (f + (q/2)x_a + r)|_{\mathbf{x}=\mathbf{c}},$$

and decomposed the first of these as

$$f|_{\mathbf{x}=\mathbf{c}} = \mathbf{f}_1 + \mathbf{f}_2$$

where

$$\mathbf{f}_1 = f|_{\mathbf{x}x_{i_{\pi(m-k-1)}}=\mathbf{c}0} \qquad \text{and} \qquad \mathbf{f}_2 = f|_{\mathbf{x}x_{i_{\pi(m-k-1)}}=\mathbf{c}1}$$

are also a Golay complementary pair. Notice that $f|_{\mathbf{x}=\mathbf{c}}$ contains 2^{m-k} non-zero entries while each of $\mathbf{f}_1$ and $\mathbf{f}_2$ contains 2^{m-k-1} non-zero entries. We have a similar decomposition for the vector $(f + (q/2)x_a + r)|_{\mathbf{x}=\mathbf{c}}$ into a second Golay complementary pair of vectors $\mathbf{f}_3$, $\mathbf{f}_4$ which differ from the pair $\mathbf{f}_1$, $\mathbf{f}_2$ only by constant phases. Alternatively, we can think of the vector $f|_{\mathbf{x}=\mathbf{c}}$ as being synthesised by adding the vectors $\mathbf{f}_1$ and $\mathbf{f}_2$, and similarly for the other member of the pair. Using equation (3), we can also synthesise the function $f|_{\mathbf{x}=\mathbf{c}}$ from the functions h_1 and h_2 describing $\mathbf{f}_1$ and $\mathbf{f}_2$. Recall that

$$\begin{aligned} h_1(x_{i_{\pi(0)}}, \dots, x_{i_{\pi(m-k-2)}}) &= \frac{q}{2}\cdot\sum_{\alpha=0}^{m-k-3} x_{i_{\pi(\alpha)}}x_{i_{\pi(\alpha+1)}} + \sum_{\alpha=0}^{m-k-2} g_\alpha x_{i_{\pi(\alpha)}} + g', \\ h_2 &= h_1 + (q/2)x_{i_{\pi(m-k-2)}} + g_{m-k-1} \end{aligned}$$

and so

$$\begin{aligned} f|_{\mathbf{x}=\mathbf{c}} &= h_1\cdot(1 - x_{i_{\pi(m-k-1}}) + h_2\cdot x_{i_{\pi(m-k-1)}} \\ &= h_1 + (h_2 - h_1)x_{i_{\pi(m-k-1)}} \\ &= h_1 + \left(\frac{q}{2}x_{i_{\pi(m-k-2)}} + g_{m-k-1}\right)x_{i_{\pi(m-k-1)}} \\ &= \frac{q}{2}\cdot\sum_{\alpha=0}^{m-k-2} x_{i_{\pi(\alpha)}}x_{i_{\pi(\alpha+1)}} + \sum_{\alpha=0}^{m-k-1} g_\alpha x_{i_{\pi(\alpha)}} + g' \end{aligned}$$

with a similar expression for the function corresponding to the other half of the pair, $(f + (q/2)x_a + r)|_{\mathbf{x}=\mathbf{c}}$. We can then think of the inductive proof of the theorem as providing an iterative method for constructing Golay complementary pairs by adding together Golay complementary pairs containing half as many non-zero entries. In this context, the above analysis shows that if we start with a Golay complementary pair whose generalised Boolean functions both have a quadratic part whose graph is the same path and whose linear parts are appropriately related, then one iterative step builds another Golay complementary pair whose functions have the same property, but where the path has one more edge (identified with the new quadratic term $x_{i_{\pi(m-k-2)}}x_{i_{\pi(m-k-1)}}$). Now the base case of the induction in the proof of Theorem 9 uses pairs with graphs that are paths with no edges, and so the final pairs obtained after $m-1$ iterations will come from graphs that are paths on $m-1$ edges. Thus we have an explanation for why the particular generalised Boolean functions appearing in Corollary 11, in [9], [10] and in [16, Paragraph 13] do so: it may be regarded as a consequence of an iterative construction method applied to Golay complementary pairs of length 2.

We can also explain the relationship to Golay's original interleaving and concatenation constructions for binary complementary pairs in [16]. By appropriately inserting zeros into the complex versions of Golay's sequences, these two iterative construction methods can be interpreted simply as additions of complementary sequences containing fewer non-zero entries, in the way we have described above. Keeping track of the Boolean functions involved, it is not hard to show that the set of length 2^m binary Golay complementary sequences that can be obtained by using combinations of Golay's iterative steps is exactly the same set as described by the case $q=2$ of Corollary 11, this being the same set, after appropriate translation of language, as that directly constructed by Golay himself in [16, Paragraph 13].

The iterative step we have described is also essentially the same as that given in [4], although the latter paper does not restrict itself to just q-phase sequences and begins its iterative construction with pairs of length 1. Nevertheless, we can say that all the q-phase Golay complementary pairs constructed recursively in [4] (and in [34], whose concatenation construction is a special case of that of [4]) can all be obtained directly from Corollary 11.

Thus our corollary provides a unification of these earlier disparate constructions for q-phase Golay complementary sequences.

IV. Golay Complementary Sets from Reed-Muller Codes

In this section we will prove that the codewords of arbitrary second order cosets of $\mathrm{RM}_q(1,m)$ lie in Golay complementary sets, where the set size depends only on a single number that can be computed from the graph associated with the quadratic form defining the coset. This immediately gives bounds on the PMEPRs of complete cosets of $\mathrm{RM}_q(1,m)$ in $\mathrm{RM}_q(2,m)$.

Let $Q:\{0,1\}^m \to \mathbb{Z}_q$ be a quadratic form in m variables $x_0, x_1, \ldots, x_{m-1}$. We write

$$f = Q + \sum_{i=0}^{m-1} g_i x_i + g'$$

where $g', g_i \in \mathbb{Z}_q$ are arbitrary. We define a vertex deletion operation on $G(f)$ as follows: we choose a vertex (say j) in the graph and delete that vertex and all the edges incident with that vertex. Consider the function $f|_{x_j=c}$, obtained by substituting $x_j = c$ in f. This substitution replaces quadratic terms $q_{ij}x_ix_j$ in f with linear terms $q_{ij}cx_i$ and replaces the linear term g_jx_j in f by g_jc. It follows that the graph of the function $f|_{x_j=c}$ is equal to the graph obtained by applying a deletion operation to vertex j of $G(f)$. Notice that this graph does not depend on the value of c. By extension, if we have a list of k indices $0 < j_0 < \ldots < j_{k-1} < m$ and write $\mathbf{x} = x_{j_0} \ldots x_{j_{k-1}}$ and $\mathbf{c} = c_0 \ldots c_{k-1}$ then the graph of the function $f|_{\mathbf{x}=\mathbf{c}}$ is obtained by applying a sequence of deletion operations on vertices $j_0, j_1, \ldots, j_{k-1}$ of $G(f)$. The final graph is independent of the choice of $\mathbf{c}$. So for any $\mathbf{c}$, the quadratic part of the function $f|_{\mathbf{x}=\mathbf{c}}$ is completely described by a graph obtained from $G(f)$ by applying deletion operations.

Theorem 12: Suppose $Q:\{0,1\}^m \to \mathbb{Z}_q$ is a quadratic form in variables $x_0, x_1, \ldots, x_{m-1}$. Suppose further that $G(Q)$ contains a set of k distinct vertices labelled $j_0, j_1, \ldots, j_{k-1}$ with the property that deleting those k vertices and all their edges results in a path. Let a be the label of either end vertex in this path (or the single vertex of the graph when $k=m-1$). Then for any choice of $g', g_i \in \mathbb{Z}_q$,

$$\left\{ Q + \sum_{i=0}^{m-1} g_i x_i + g' + \frac{q}{2}\left(\sum_{\alpha=0}^{k-1} d_\alpha x_{j_\alpha} + d x_a\right) : d, d_\alpha \in \{0,1\} \right\}$$

is a Golay complementary set of size 2^{k+1}.

Proof: Let $\mathbf{x} = x_{j_0}x_{j_1}\ldots x_{j_{k-1}}$ and $\mathbf{d} = d_0 d_1 \ldots d_{k-1}$. Write $f = Q + \sum_{i=0}^{m-1} g_i x_i + g'$ and $\mathbf{d}\cdot\mathbf{x} =$

$\sum_{\alpha=0}^{k-1} d_\alpha x_{j_\alpha}$. Now, using Lemma 8, for any $\ell \neq 0$,

$$\sum_{\mathbf{d},d} A(f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + dx_a))(\ell) = S_1 + S_2$$

where

$$S_1 = \sum_{\mathbf{d},d} \sum_{\mathbf{c}} A((f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + dx_a))|_{\mathbf{x}=\mathbf{c}})(\ell) \tag{11}$$

and

$$S_2 = \sum_{\mathbf{d},d} \sum_{\mathbf{c}_1\neq\mathbf{c}_2} C((f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + dx_a))|_{\mathbf{x}=\mathbf{c}_1}, (f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + dx_a))|_{\mathbf{x}=\mathbf{c}_2})(\ell). \tag{12}$$

From the discussion preceding the statement of the theorem, for every choice of $\mathbf{c}$ and $\mathbf{d}$, the function $(f + (q/2)\mathbf{d}\cdot\mathbf{x})|_{\mathbf{x}=\mathbf{c}}$ has a graph that is a path. Moreover, either a is an end vertex of the path, or it is the single vertex of the graph (when $k = m-1$). So from Theorem 9, for every $\mathbf{d}$ and $\mathbf{c}$, the vectors $(f + (q/2)\mathbf{d}\cdot\mathbf{x})|_{\mathbf{x}=\mathbf{c}}$ and $(f + (q/2)(\mathbf{d}\cdot\mathbf{x} + x_a))|_{\mathbf{x}=\mathbf{c}}$ form a Golay complementary pair. It follows that

$$\begin{aligned} S_1 &= \sum_{\mathbf{c}} \sum_{\mathbf{d}} A((f + \frac{q}{2}\mathbf{d}\cdot\mathbf{x})|_{\mathbf{x}=\mathbf{c}})(\ell) + A((f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + x_a))|_{\mathbf{x}=\mathbf{c}})(\ell) \\ &= 0. \end{aligned}$$

Now consider the rearranged sum S_2:

$$S_2 = \sum_{\mathbf{c}_1\neq\mathbf{c}_2} \sum_{d} \sum_{\mathbf{d}} C((f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + dx_a))|_{\mathbf{x}=\mathbf{c}_1}, (f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + dx_a))|_{\mathbf{x}=\mathbf{c}_2})(\ell)$$

For fixed values of $\mathbf{c}_1, \mathbf{c}_2$, and d we consider the inner sum:

$$\sum_{\mathbf{d}} C((f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + dx_a))|_{\mathbf{x}=\mathbf{c}_1}, (f + \frac{q}{2}(\mathbf{d}\cdot\mathbf{x} + dx_a))|_{\mathbf{x}=\mathbf{c}_2})(\ell)$$

Notice that the vector $\mathbf{x}$ contains all the variables occurring in the sum $\mathbf{d}\cdot\mathbf{x}$. So for $\mathbf{c}_1, \mathbf{c}_2$ and d fixed, we have that the vector $(f + (q/2)(\mathbf{d}\cdot\mathbf{x} + dx_a))|_{\mathbf{x}=\mathbf{c}_j}$ is equal to either the vector $\mathbf{a}_j := (f + (q/2)dx_a)|_{\mathbf{x}=\mathbf{c}_j}$ or to the vector $-\mathbf{a}_j$, the former case occurring when $(q/2)\mathbf{d}\cdot\mathbf{c_j} = 0 \bmod q$ and the latter when $(q/2)\mathbf{d}\cdot\mathbf{c_j} = q/2 \bmod q$.

We aim to show that as $\mathbf{d}$ varies, we get as many correlations of the type I:

$$C(\mathbf{a}_1, \mathbf{a}_2) \quad \text{or} \quad C(-\mathbf{a}_1, -\mathbf{a}_2)$$

as we do correlations of the type II:

$$C(\mathbf{a}_1, -\mathbf{a}_2) \quad \text{or} \quad C(-\mathbf{a}_1, \mathbf{a}_2)$$

in the inner sum above. Because type I and type II correlations are equal in magnitude but opposite in sign, it is then immediate that the inner sum is equal to zero, and hence that S_2 is equal to zero. The theorem will then follow immediately. Notice that a type I correlation arises whenever $\mathbf{d}\cdot\mathbf{c_1} = \mathbf{d}\cdot\mathbf{c_2} \bmod 2$ and that a type II correlation arises whenever $\mathbf{d}\cdot\mathbf{c_1} \neq \mathbf{d}\cdot\mathbf{c_2} \bmod 2$. Because $\mathbf{c_1} \neq \mathbf{c_2}$, we have $\mathbf{c_1} + \mathbf{c_2} \neq \mathbf{0} \bmod 2$, and so the linear functional $\mathbf{d}\cdot(\mathbf{c_1} + \mathbf{c_2}) \bmod 2$ (regarded as a function of $\mathbf{d}$) is not equal to the zero functional. Hence it is balanced, i.e. takes on the values 0 and 1 equally often as $\mathbf{d}$ varies. Thus $\mathbf{d}\cdot\mathbf{c_1}$ and $\mathbf{d}\cdot\mathbf{c_2}$ agree modulo 2 for half the values of $\mathbf{d}$ and disagree modulo 2 for the other half. Hence there are equal numbers of type I and type II correlations. □

Notice that all the words of the Golay complementary set identified in the above theorem are contained in the same coset $Q + \mathrm{RM}_q(1, m)$.

We now present a simple corollary of the theorem:

Corollary 13: Suppose $Q : \{0,1\}^m \to \mathbb{Z}_q$ is a quadratic form in variables $x_0, x_1, \ldots, x_{m-1}$. Suppose further that $G(Q)$ contains a set of k distinct vertices with the property that deleting those k vertices and all their edges results in a path. Then every word of the coset $Q + \mathrm{RM}_q(1,m)$ has PMEPR at most 2^{k+1}.

Taking $k = 0$ in Theorem 12, we see that any form Q whose graph is a path determines a coset of $\mathrm{RM}_q(1,m)$ that consists of Golay complementary sequences. Examining the particular Golay complementary pairs identified in the theorem gives us Corollary 11 again (with the technicality that Corollary 11 is slightly more general because it allows the introduction of an arbitrary constant term r in the second member of each pair). So the results of [9], [10] on Golay complementary pairs can be viewed as a special case of Theorem 12, placing them in the more general context of Golay complementary *sets* derived from second order cosets of $\mathrm{RM}_q(1,m)$. By giving an explicit, non-recursive construction for q-phase Golay complementary sets, the theorem also provides a partial solution to a central open problem from [38]:

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

The PMEPR of individual words in a coset $Q + \mathrm{RM}_q(1,m)$ may vary considerably from the bound of Corollary 13, and indeed the bound may not be tight for *any* word of the coset. In practice however, the corollary seems to give a reasonably good bounds on the PMEPRs of cosets, in many cases being tight and often giving a bound that is the smallest power of two larger than the actual value of PMEPR of the coset. In Section VI, we will derive a lower bound on PMEPR in the case $q = 2$ which shows that the bound is tight in many cases. For now we demonstrate the utility of our bound by showing how to derive much of the PMEPR behaviour of the second order cosets of $\mathrm{RM}_2(1,4)$ that was reported in [10, Table 1].

There are 64 second order cosets of $\mathrm{RM}_2(1,4)$, each determined by a quadratic form Q in variables x_0, x_1, x_2, x_3. Of the 64 cosets, 12 have $G(Q)$ a path and hence have PMEPR bounded by 2. These correspond to the 12 cosets of $\mathrm{RM}(1,4)$ consisting of Golay complementary sequences, [9], [10]. Direct computation over these cosets gives PMEPRs between 1.97 and exactly 2, [10].

There are 37 cosets for which we can take $k = 1$ in Corollary 13, obtaining a bound of 4 on PMEPR for these cosets. From [10, Table I], the PMEPR for these cosets ranges from 3.18 to exactly 4 (in fact 25 out of the 37 cosets have PMEPR equal to exactly 4). So the theorem gives a bound that is the 'correct power of 2' for all of these cosets.

Of the remaining 15 cosets, all bar one (the one corresponding to $Q = 0$) allow us to take $k = 2$ in Corollary 13, giving a bound of 8 on PMEPR. For 11 of these cosets, the PMEPR ranges between 6.18 and 6.85 [10, Table I], so our result again gives the smallest possible power of 2. This leaves 3 cosets, which correspond to the following quadratic forms:

$$x_0x_1 + x_2x_3, \quad x_0x_2 + x_1x_3, \quad x_0x_3 + x_1x_2.$$

The PMEPRs for the cosets determined by these forms are 3.113, 3.124 and 3.117 respectively [10, Table I]. We will say more about these cosets in Section VII.

In summary, Corollary 13 gives reasonably good bounds on PMEPR for many second order cosets of $\mathrm{RM}_2(1,4)$. That this is true for more general binary and non-binary cosets at other lengths is supported by comparing computational results given in [10, Tables 2 and 3] with the predictions of our corollary.

V. OFDM Codes with Low PMEPR

In this section we will use the theory developed above to construct OFDM codes with low PMEPR, good error correcting capabilities and reasonable rates (at least for small numbers of carriers).

A simple way to obtain a code with PMEPR at most 2^{k+1} is to use Corollary 13 to identify a set of quadratic forms Q whose graphs $G(Q)$ satisfy the conditions of the corollary and to take as the code the union of cosets $Q + \mathrm{RM}_q(1,m)$. Efficient encoding is achieved by storing the corresponding list of coset representatives and then using information bits partly to specify a representative from the list and partly to encode a codeword from the q^{m+1} words of $\mathrm{RM}_q(1,m)$ (using a straightforward generalisation of the usual encoding circuit for $\mathrm{RM}_2(1,m)$ given in [24, p. 420]).

A number of approaches can be taken to the decoding of codes formed in this way. The techniques of [10] are applicable in the 2^h-ary case, and maximum likelihood decoding can be obtained by combining supercode decoding [8] with the algorithm of [17] for decoding $\mathrm{RM}_q(1,m)$. Alternatively, [30] contains a number of new high performance algorithms designed to be efficient for codes formed from large numbers of cosets of $\mathrm{RM}_q(1,m)$ inside $\mathrm{RM}_q(2,m)$ and $\mathrm{ZRM}_q(2,m)$. This latter paper also contains a comparison of the various decoding strategies.

Our first step in identifying large sets of quadratic forms comes from applying the following lemma:

Lemma 14: Let $A=(a_{ij})\in(\mathbb{Z}_q)_{(m-k)\times k}$ be an $(m-k)\times k$ matrix over $\mathbb{Z}_q$, and let $C=(c_{ij})\in(\mathbb{Z}_q)_{k\times k}$ be a $k\times k$ upper-triangular matrix over $\mathbb{Z}_q$, so $c_{ij}=0$ for $0\le j\le i<k$. Let $Q_{A,C}$ denote the quadratic form

$$\frac{q}{2}\sum_{i=0}^{m-k-2}x_ix_{i+1}+\sum_{i=0}^{m-k-1}\sum_{j=0}^{k-1}a_{ij}x_ix_{m-k+j}+\sum_{0\le i<j<k}c_{ij}x_{m-k+i}x_{m-k+j}. \tag{13}$$

Finally, let Q be the quadratic form

$$\frac{q}{2}\sum_{i=0}^{m-k-2}x_{\pi(i)}x_{\pi(i+1)}+\sum_{i=0}^{m-k-1}\sum_{j=0}^{k-1}a_{ij}x_{\pi(i)}x_{\pi(m-k+j)}+\sum_{0\le i<j<k}c_{ij}x_{\pi(m-k+i)}x_{\pi(m-k+j)}. \tag{14}$$

obtained from $Q_{A,C}$ by applying a permutation π of $\{0,1,\dots,m-1\}$ to the indices of $x_0,x_1,\dots,x_{m-1}$. Then Q satisfies the conditions of Corollary 13, so the coset $Q+\mathrm{RM}_q(1,m)$ has PMEPR at most 2^{k+1}. Moreover, every quadratic form satisfying the conditions of Corollary 13 can be obtained from some $Q_{A,C}$ in this way.

Proof: The graph $G(Q_{A,C})$ is shown schematically in Figure 2. The graph of the form Q is obtained from this graph by applying the permutation π to the vertex labels. It is clear from the figure that applying k deletion operations to vertices $m-k,\dots,m-1$ of the graph results in a path. So applying k deletion operations to vertices $\pi(m-k),\dots,\pi(m-1)$ of the graph $G(Q)$ also results in a path. The converse is equally easily proved. □

Of course, we already have an exact characterisation of the forms arising in Lemma 14 when $k=0$: they are simply the forms whose graphs are paths, giving the cosets consisting of Golay complementary pairs that were identified in [9], [10] and Corollary 11. The resulting OFDM codes have PMEPR bounded by 2 and were discussed at length for $q=2^h$ in [10]. So in what follows, we focus on codes in which $k\ge 1$ in Lemma 14, in particular developing codes for $k=1$ where the PMEPR is bounded by 4.

Clearly, a list of coset representatives identified by Lemma 14 could be inconveniently large for practical use. It is preferable to have available instead simple, algorithmic methods which use information bits to directly specify coset representatives. The basic idea behind the encoding algorithms that we present here is to use some information bits to jointly specify A, C and a permutation π in Lemma 14. These determine a coset representative Q as in equation (14). Unfortunately, this procedure has the potential to generate some coset representatives more than once. We require methods that generate each coset representative at most once. For convenience, we will describe such methods using graphs rather than working directly with quadratic forms. Of course, each graph corresponds directly to a quadratic form in m variables over $\mathbb{Z}_q$, and consequently to a coset representative of $\mathrm{RM}_q(1,m)$ in $\mathrm{RM}_q(2,m)$. We will specify large subsets $\mathcal{G}_m$ of the set of graphs $G(Q_{A,C})$ and subsets of the set $\mathcal{P}_m$ of permutations on $\{0,1,\dots,m-1\}$ with the property that applying the permutations of $\mathcal{P}_m$ to the vertex labels of graphs in $\mathcal{G}_m$ directly results in $|\mathcal{P}_m|\cdot|\mathcal{G}_m|$ distinct graphs (and corresponding cosets).

In what follows, we define the set $\mathcal{P}_m$ to be the set of permutations π of $\{0,1,\dots,m-1\}$ satisfying $\pi(0)<\pi(m-k-1)$. Clearly, $|\mathcal{P}_m|=m!/2$. For $A=(a_{ij})\in(\mathbb{Z}_q)_{(m-k)\times k}$, we define A_j to be the integer $\sum_{i=0}^{m-k-1}a_{ij}q^i$, $0\le j<k$.

Definition 15: Let G_1 and G_2 be edge- and vertex- labelled graphs on m vertices labelled $0,1,\dots,m-1$. Then G_1 and G_2 are said to be *isomorphic* if there is a permutation π of $\{0,1,\dots,m-1\}$ such that there is a edge labelled w between vertices j_0 and j_1 in G_1 if and only if there is a edge labelled w between vertices $\pi(j_0)$ and $\pi(j_1)$ in G_2. We call any such permutation π an *isomorphism* from G_1 to G_2. We write $\pi(G_1)=G_2$. An automorphism of G_1 is an isomorphism from G_1 to itself. The identity permutation is an automorphism for every graph, called the *trivial automorphism.*

Lemma 16: Let $\mathcal{G}_m$ be a subset of the set of graphs

$$\{G(Q_{A,C}) : A_0 < A_1 < \ldots < A_{k-1}\}$$

having the property that any isomorphism from G_1 to G_2 (with $G_1, G_2 \in \mathcal{G}_m$) induces a permutation of the vertex set $\{m-k, \ldots, m-1\}$. Then $|\mathcal{P}_m| \cdot |\mathcal{G}_m|$ distinct graphs are obtained by applying the permutations of $\mathcal{P}_m$ to the vertices of graphs in $\mathcal{G}_m$.

Proof: Suppose there exist permutations $\pi_1, \pi_2 \in \mathcal{P}_m$ such that

$$\pi_1(G_1) = \pi_2(G_2)$$

where the graphs $G_1 = G(Q_{A,C})$ and $G_2 = G(Q_{B,D})$ lie in the set $\mathcal{G}_m$. Then $\pi = \pi_2^{-1}\pi_1$ is an isomorphism from G_1 to G_2. So π permutes the vertices $m-k, \ldots, m-1$ and so induces an isomorphism from the subgraph of G_1 on vertices $0, 1, \ldots, m-k-1$ to the same subgraph of G_2. But both of these subgraphs are a path on $m-k$ vertices labelled $0, 1, \ldots, m-k-1$ with edges from vertex j to vertex $j+1$ for each $0 \leq j < m-k-1$. So π induces an automorphism of this path. But this path has just two automorphisms: we either have:

$$\pi(j) = j, \quad 0 \leq j \leq m-k-1$$

or

$$\pi(j) = m-k-1-j, \quad 0 \leq j \leq m-k-1.$$

In the latter case we have $\pi(0) = m-k-1$ and $\pi(m-k-1) = 0$ from which we deduce:

$$\pi_1(m-k-1) = \pi_2(0) < \pi_2(m-k-1) = \pi_1(0)$$

a contradiction, since $\pi_1 \in \mathcal{P}_m$. So the former case applies. Now column j of A records the weights of the edges from vertex $m-k+j$ to vertices $0, 1 \ldots, m-k-1$ of G_1 and similarly for B. Since vertices $0, 1, \ldots, m-k-1$ are fixed by π, we deduce that the columns of B are a permutation of the columns of A, column j of A being mapped to column $\pi(m-k+j)-(m-k)$ of B for each $0 \leq j < k$. Since $A_j = \sum_{i=0}^{m-k-1} a_{ij}q^i$ and $B_j = \sum_{i=0}^{m-k-1} b_{ij}q^i$, we see that the B_j must then be a permutation of the A_j. From the fact that $A_0 < A_1 < \ldots < A_{k-1}$ and $B_0 < B_1 < \ldots B_{k-1}$ it follows that $A_j = B_j$ for each j, so that $A = B$ and π fixes each of $m-k, \ldots, m-1$. Then π is the identity permutation and $\pi_1 = \pi_2$. Since $\pi(G_1) = G_2$ we must also have $C = D$. Hence $G_1 = G_2$. □

A. Binary Codes with PMEPR at Most 4

We consider the special case $q = 2$ and $k = 1$ of Lemma 14. Here C is the 1×1 zero matrix, denoted 0, and A is an $(m-1) \times 1$ matrix, i.e. a column vector. We write $A = [a_0, a_1, \ldots, a_{m-2}]^T$ and have:

$$Q_{A,0} = x_0x_1 + \cdots + x_{m-3}x_{m-2} + \sum_{i=0}^{m-2} a_i x_i x_{m-1} \tag{15}$$

We now give an explicit description of a set of graphs $\mathcal{G}_m$ satisfying the condition of Lemma 16:

Lemma 17: Let $m \geq 5$ and let $\mathcal{G}_m$ be the set of graphs $\{G(Q_{A,0}) : \mathrm{wt}_{\mathrm{H}}(A) \geq 4\}$, where $\mathrm{wt}_{\mathrm{H}}(A)$ denotes the Hamming weight of the vector A. Then the set $\mathcal{G}_m$ satisfies the condition of Lemma 16 for $k = 1$.

Proof: Suppose A and B both have Hamming weight at least 4 and suppose $\pi : G(Q_{A,0}) \to G(Q_{B,0})$ is an isomorphism. We have to show that π maps vertex $m-1$ to vertex $m-1$. Now π must preserve the degrees of vertices and the only vertices of degree greater than or equal 4 in our two graphs are the vertices labelled $m-1$. So π must fix vertex $m-1$. □.

A simple counting argument shows that with this definition of $\mathcal{G}_m$,

$$|\mathcal{G}_m| = 2^{m-1} - \left[\binom{m-1}{3} + \binom{m-1}{2} + m\right]$$

so that $|\mathcal{G}_5| = 1$, $|\mathcal{G}_6| = 6$, $|\mathcal{G}_7| = 22$, and $2^{m-2} \leq |\mathcal{G}_m| < 2^{m-1}$ for $m \geq 8$. By Lemma 16, we obtain a set $\mathcal{H}_m$ of $|\mathcal{G}_m| \cdot m!/2$ distinct quadratic forms (and graphs) from the set $\mathcal{G}_m$ by applying the $m!/2$ permutations from the set $\mathcal{P}_m$ to the vertex labels of the graphs in $\mathcal{G}_m$.

For $m \geq 5$, we take as our binary, length 2^m OFDM code the union of cosets of $\mathrm{RM}_2(1, m)$ identified by the quadratic forms in the set $\mathcal{H}_m$. Since these cosets all lie in $\mathrm{RM}_2(2, m)$, the code has minimum Hamming distance at least 2^{m-2}. The code has PMEPR no more than 4 by Lemma 14. It can be used to encode $\lfloor \log_2 m!/2 \rfloor + \lfloor \log_2 |\mathcal{G}_m| \rfloor + m + 1$ bits. For $m \geq 8$, the number of encoded bits is $\lfloor \log_2 m! \rfloor + 2m - 2$. The number of encoded bits and code rate for this code are given for small values of m in Table I. We note that, while the number of encoded bits increases with m, the code rate quickly decreases to zero. This is the price for retaining strict power control and high minimum distance [31].

We next describe an efficient encoding algorithm for the codes.

We write $k_1 = \lfloor \log_2 |\mathcal{G}_m| \rfloor$, $k_2 = \lfloor \log_2 |\mathcal{P}_m| \rfloor$ and let $d_0 d_1 \ldots d_{k_1+k_2+m}$ be information bits. We require the storage of a list of 2^{k_1} distinct vectors $A = [a_0, a_1, \ldots, a_{m-2}]^T$ corresponding to graphs in $\mathcal{G}_m$ and a list of 2^{k_2} permutations from $\mathcal{P}_m$. As an alternative, we can make use of any efficient method which generates arbitrary elements from such lists. The encoding algorithm for the length 2^m code is then as follows:

- Use bits $d_0, d_1, \ldots, d_{k_1-1}$ to select a vector $A = [a_0, a_1, \ldots, a_{m-2}]^T$ from the list of 2^{k_1} vectors A satisfying $\mathrm{wt_H}(A) \geq 4$.
- Use bits $d_{k_1}, \ldots, d_{k_1+1}, d_{k_1+k_2-1}$ to select a permutation π from the list of 2^{k_2} permutations of $\mathcal{P}_m$.
- Compute the coset representative corresponding to the quadratic form:

$$Q = x_{\pi(0)}x_{\pi(1)} + x_{\pi(1)}x_{\pi(2)} + \cdots + x_{\pi(m-3)}x_{\pi(m-2)} + \sum_{i=0}^{m-2} a_i x_{\pi(i)} x_{\pi(m-1)} \tag{16}$$

by appropriately combining rows of the generator matrix of $\mathrm{RM}_2(2, m)$.

- Use bits $d_{k_1+k_2}, \ldots, d_{k_1+k_2+m}$ as information bits in an encoder for $\mathrm{RM}_2(1, m)$ to obtain a codeword of $\mathrm{RM}_2(1, m)$.
- Use modulo 2 addition to combine the coset representative obtained from Q and the codeword of $\mathrm{RM}_2(1, m)$ to obtain the final codeword.

B. Non-binary Codes with PMEPR at Most 4

We now apply similar ideas to develop OFDM codes over non-binary alphabets. Our analogue of Lemma 17 is:

Lemma 18: Let $m \geq 3$ and let $\mathcal{G}_m$ be the set of graphs

$$\{G(Q_{A,0}) : A = [a_0, a_1, \ldots, a_{m-2}], a_i, a_j \notin \{0, q/2\} \text{ for some } 0 \leq i \neq j < m-1\}.$$

Then $\mathcal{G}_m$ satisfies the condition of Lemma 16 for $k = 1$.

Proof: If $\pi : G(Q_{A,0}) \to G(Q_{B,0})$ is an isomorphism then π fixes vertex $m-1$ because π preserves the labels of edges incident with a vertex and the only vertex of $G(Q_{A,0})$ and of $G(Q_{B,0})$ with at least two edges not labelled $q/2$ is the vertex labelled $m-1$. □.

A simple counting argument shows that

$$|\mathcal{G}_m| = q^{m-1} - (qm - q - 2m + 4)2^{m-2}.$$

So we can obtain

$$\frac{m!}{2}\left[q^{m-1} - (qm - q - 2m + 4)2^{m-2}\right].$$

distinct graphs (and corresponding coset representatives) from the set $\mathcal{G}_m$ by applying the $m!/2$ distinct permutations from $\mathcal{P}_m$ to the vertex labels of graphs in $\mathcal{G}_m$. From a table of permutations in $\mathcal{P}_m$ we can derive (in a similar manner as in the binary case) q-ary OFDM codes which can be used to encode $\lfloor \log_2 m!/2 \rfloor + \lfloor \log_2 |\mathcal{G}_m| \rfloor + \lfloor (m+1) \log_2 q \rfloor$ information bits into q-ary codewords of length 2^m. For $q = 4$ (quaternary coding) and $m \geq 4$, the number of encoded bits is equal to $\lfloor \log_2 m! \rfloor + 4m - 2$, while for $q = 8$ (octary coding) and $m \geq 3$, the number of encoded bits is equal to $\lfloor \log_2 m! \rfloor + 6m - 2$. A table of parameters is given for small values of m and $q = 4, 8$ in Table II. The codes have minimum Hamming and Lee distance at least 2^{m-2} (from Theorem 4) and PMEPR of at most 4. Again, we note that while the number of encoded bits increases with m, the code rates still tend to zero.

By restricting to vectors $A = [a_0, a_1, \ldots, a_{m-2}]^T$ with $a_0, a_1 \notin \{0, q/2\}$, we obtain codes with slightly lower rate, but with a simple and direct encoding of information bits into vectors A. Consequently, there is no need to store a list of vectors with this modification.

Finally in this section, we outline how to obtain OFDM codes with minimum Lee distance equal to 2^{m-1} (instead of 2^{m-2} for the codes given above). From Theorem 4, we need only choose quadratic forms from $\mathrm{ZRM}_q(2, m)$ instead of $\mathrm{RM}_q(2, m)$. In other words, we consider quadratic forms having only even coefficients. In order that the forms be consistent with equation (13), we require that $q/2$ be even, so q must be divisible by 4. Then a particularly convenient way of obtaining forms is to use the encoding algorithm developed for $\mathrm{RM}_{q/2}(2, m)$ but to multiply by 2 all coefficients in the resulting forms. Of course, we can still take first order codewords from $\mathrm{RM}_q(1, m)$. For example, for $m \geq 8$, we obtain a quaternary, length 2^m code which encodes $\lfloor \log_2 m! \rfloor + 3m - 1$ information bits to codewords of $\mathrm{ZRM}_4(2, m)$, with efficient encoding similar to that for the binary encoder of Section V-A.

C. Binary Codes with PMEPR at most 2^{k+1}

In this section we sketch a way of specifying sets of graphs $\mathcal{G}_m$ satisfying the condition of Lemma 16 for general k and for $q = 2$. The specification can be extended to general q in a number of ways.

We define $S_t = 2^t - \binom{t}{3} - \binom{t}{2} - t - 1$.

Lemma 19: Suppose $m \geq k + 4$ and suppose $S_{m-k} \geq k$. Let $\mathcal{G}_m$ be the set of graphs $G(Q_{A,C})$ for which

- $A_0 < A_1 < \ldots < A_{k-1}$, where $A_j = \sum_{i=0}^{m-k-1} a_{ij} 2^i$,
- $\mathrm{wt}_{\mathrm{H}}([a_{0j}, a_{1j}, \ldots, a_{(m-k-1)j}]) \geq 4$ for each $0 \leq j < k$,
- $c_{ij} = 1$ for each $0 \leq i < j < k$.

Then $\mathcal{G}_m$ satisfies the condition of Lemma 16 and $|\mathcal{G}_m| = \binom{S_{m-k}}{k}$.

Proof: Let G_1 and G_2 be any pair of graphs in the set $\mathcal{G}_m$. Then every vertex labelled $0, 1, \ldots, m-k-1$ of both G_1 and G_2 has degree at most $k+2$, while every vertex labelled $m-k, \ldots, m-1$ has degree at least $k+3$. Then any isomorphism from G_1 to G_2 must induce a permutation of vertices $m-k, \ldots, m-1$. The number of graphs in $\mathcal{G}_m$ is equal to the number of k-subsets of the set of binary vectors of length $m-k$ and Hamming weight at least 4, a set of size S_{m-k}. □

When $m - k$ is large relative to k, the number of graphs identified by the above lemma is approximately equal to $2^{(m-k)k}/k!$. Applying permutations from the set $\mathcal{P}_m$, we obtain approximately $(m!/2) \cdot 2^{(m-k)k}/k!$ distinct graphs and quadratic forms. Codes enjoying efficient encoding algorithms formed large subsets of these quadratic forms can be derived in a similar manner as in Section V-A, but we omit the details. A table of code parameters for small values of m and $k = 2$ is given in Table III. It is evident that for moderate values of m, a modest increase in rate can be achieved over the codes in Table I, at the cost of increasing the PMEPR of the codes from 4 to 8.

VI. Lower Bounds on PMEPR

In this section, we develop lower bounds on PMEPR for cosets of $\mathrm{RM}_2(1, m)$ in $\mathrm{RM}_2(2, m)$, showing that the bound provided by Corollary 13 is tight in many cases. Our approach generalises some of the ideas in [5].

Our main theoretical tool is the weight distribution of second order cosets of $\mathrm{RM}_2(1, m)$ [24, Chapter 15].

Let Q be a quadratic form in variables $x_0, x_1, \ldots, x_{m-1}$:

$$Q(x_0, x_1, \ldots, x_{m-1}) = \sum_{0 \le i < j < m} q_{ij} x_i x_j, \qquad q_{ij} \in \mathbb{Z}_2.$$

We identify with Q an upper-triangular matrix U whose (i, j) entry is equal to q_{ij} for $0 \le i < j < m$. We then write $\mathbf{x} = [x_0, x_1, \ldots, x_{m-1}]$ and have:

$$Q(x_0, x_1, \ldots, x_{m-1}) = \mathbf{x} U \mathbf{x}^T$$

Notice that $B = U + U^T$ is the incidence matrix of the graph $G(Q)$. We define the *rank* of the quadratic form Q to be the rank of the matrix B (where the rank computation is carried out over $\mathbb{F}_2$). It is a consequence of Dickson's theorem ([24, p. 438, Theorem 4]) that the rank of Q is even. Moreover, if the rank of Q equals $2h$ and $D_{m,2h}$ denotes the $m \times m$ matrix which is zero except on the two diagonals immediately above and below the main diagonal, and there has $1010 \ldots 100 \ldots 0$ with h ones, then there exists an invertible matrix R such that $RBR^T = D_{m,2h}$.

Result 20: [24, Theorem 5, p. 441] Let Q be a quadratic form of rank $2h$ in m variables. Then the weight distribution of the coset $Q + \mathrm{RM}_2(1, m)$ is as follows:

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}

Following [5], we let $\mathbf{f}$ be an arbitrary codeword of the coset $Q + \mathrm{RM}_2(1, m)$ and consider the OFDM signal $S(\mathbf{f})(t)$ at time $t = 0$. From (1),

$$\begin{aligned} S(\mathbf{f})(0) &= \sum_{j=0}^{2^m-1} (-1)^{f_j} \\ &= 2^m - 2 \cdot \mathrm{wt}_{\mathrm{H}}(\mathbf{f}) \end{aligned}$$

Now as $\mathbf{f}$ varies over the coset, the spectrum of values taken on $\mathrm{wt}_{\mathrm{H}}(\mathbf{f})$ gives the weight distribution of $Q + \mathrm{RM}_2(1, m)$. By Result 20, at least 2^{2h+1} codewords have Hamming weight $2^{m-1} \pm 2^{m-h-1}$ and for any one of these codewords $\mathbf{f}$,

$$P(\mathbf{f})(0) = |S(\mathbf{f})(0)|^2 = 2^{2m-2h} = 2^m \cdot 2^{m-2h}$$

so that the PMEPR of the coset is at least 2^{m-2h}.

Thus a lower bound on PMEPR for $Q + \mathrm{RM}_2(1, m)$ can be derived from the rank of the form Q. This approach also gives lower bounds on PMEPR for the more general cosets $Q + \mathrm{RM}_q(1, m)$ when all the coefficients q_{ij} are equal to either 0 or $q/2$.

A simple application of this method yields a result already obtained in [5], showing that the bound on PMEPR for a coset of $\mathrm{RM}_2(2, m)$ of the type considered in [9], [10] and Corollary 11 is tight when m is odd:

Theorem 21: Suppose m is odd and let

$$Q(x_0, x_1, \ldots, x_{m-1}) = \sum_{i=0}^{m-2} x_{\pi(i)} x_{\pi(i+1)}$$

where π is a permutation of $\{0, 1, \ldots, m-1\}$. Then the PMEPR of the coset $Q + \mathrm{RM}_2(1, m)$ is equal to 2.

Proof: Since m is odd, the maximum possible rank of Q is $2h = m - 1$. Then $m - 2h = 1$ and we see that the PMEPR of the coset is at least 2. From Corollary 11, it is at most 2.□

A. Lower Bounds on PMEPR when $k=1$

Next we apply the rank method to the cosets of $\mathrm{RM}_2(1,m)$ considered in Section V-A. In the notation of that section, we consider the quadratic form Q obtained by applying a permutation π to the indices of the variables in $Q_{A,0}=\sum_{i=0}^{m-3}x_ix_{i+1}+\sum_{i=0}^{m-2}a_ix_ix_{m-1}$. The resulting matrix B can be transformed by a rank-preserving permutation of rows and columns (derived from π^{-1}) to the matrix

$$B'=\begin{bmatrix} Z_{m-1} & A \\ A^T & 0 \end{bmatrix}$$

where Z_{m-1} is the $(m-1)\times(m-1)$ matrix having zeros everywhere except on the two diagonals immediately above and below the main diagonal, where it equals 1. When m is even, applying a sequence of coupled row and column operations reduces this matrix to the form:

$$\begin{bmatrix} D_{m-1,m-2} & E \\ E^T & 0 \end{bmatrix}$$

where $E=[e_0,e_1,\dots,e_{m-2}]^T$ and

$$e_i=\begin{cases} \sum_{\ell=0}^{i/2}a_{2\ell} & \text{if } i \text{ is even} \\ a_i & \text{if } i \text{ is odd.}\end{cases}$$

It is now apparent that B has rank $m-2$ if $\sum_{i=0}^{(m-2)/2}a_{2i}=0$ and rank m if $\sum_{i=0}^{(m-2)/2}a_{2i}=1$. Thus, if an even number of the coefficients $a_0,a_2,\dots,a_{m-2}$ are non-zero, then the PMEPR of the coset $Q+\mathrm{RM}_2(1,m)$ is equal to at least 4. That the PMEPR is equal to exactly 4 in this case follows from Corollary 13. In the case where Q has rank m, we obtain a trivial lower bound of 1 on the PMEPR of the coset.

Example 22: We take $m=4$ and consider the quadratic form $Q=x_0x_1+x_0x_2+x_0x_3+x_1x_2+x_2x_3$ of Figure 1. We can take $k=1$ in Corollary 13, so the PMEPR of the coset $Q+\mathrm{RM}_2(1,4)$ is at most 4. The above argument predicts that the rank of Q is 2 and that the PMEPR of $Q+\mathrm{RM}_2(1,4)$ is exactly 4.

When m is odd, a similar sequence of row and column operations reveals that Q has rank equal to $m-1$, and we obtain a lower bound of 2 for the PMEPR of the coset $Q+RM(1,m)$. This should be compared with the upper bound of 4 predicted by Corollary 13.

B. Lower Bounds on PMEPR for General Second Order Cosets

We apply a generalisation of the above argument to a general quadratic form Q of the type considered in Lemma 14. We recall that Q can be obtained by applying a permutation π to the indices of variables in the form $Q_{A,C}$ of equation (13). In this case, the matrix $B=U+U^T$ can be transformed (using the permutation π^{-1} applied to rows and columns) to:

$$B'=\begin{bmatrix} Z_{m-k} & A \\ A^T & C+C^T \end{bmatrix}$$

where Z_{m-k} is the $(m-k)\times(m-k)$ matrix having zeros everywhere except on the two diagonals immediately above and below the main diagonal, where it equals 1. We analyse the rank of B'.

Suppose first of all that $m-k$ is odd. Then a sequence of coupled row and column operations reduces B' to the matrix:

$$\begin{bmatrix} D_{m-k,m-k-1} & E \\ E^T & C+C^T \end{bmatrix}$$

where $E=(e_{ij})$, $0\le i<m-k, 0\le j<k$ and

$$e_{ij}=\begin{cases} \sum_{\ell=0}^{i/2}a_{(2\ell)j} & \text{if } i \text{ is even} \\ a_{ij} & \text{if } i \text{ is odd.}\end{cases}$$

A further sequence of row and column operations reduce this matrix to the form:

$$\left[\begin{array}{cc|c} D_{m-k,m-k-1} & & 0_{k\times(m-k-2)} \\ & & \mathbf{v} \\ \hline 0_{(m-k-2)\times k} & \mathbf{v}^T & C+C^T \end{array}\right]$$

where $\mathbf{v} = (\sum_{\ell=0}^{(m-k-1)/2} a_{(2\ell)0}, \ldots, \sum_{\ell=0}^{(m-k-1)/2} a_{(2\ell)(k-1)})$. From this it is apparent that the form Q is of rank $m-k-1$ if and only if $\mathbf{v}=0$ and $C=0$ (the all-zero matrix). In this case, we obtain a lower bound of 2^{k+1} on the PMEPR of the coset $Q+\mathrm{RM}_2(1,m)$ and Corollary 13 is tight. We have:

Theorem 23: Suppose $m-k$ is odd, π is a permutation of $\{0,1,\ldots,m-1\}$,

$$Q = \sum_{i=0}^{m-k-2} x_{\pi(i)}x_{\pi(i+1)} + \sum_{i=0}^{m-k-1}\sum_{j=0}^{k-1} a_{ij}x_{\pi(i)}x_{\pi(m-k+j)}$$

and

$$\sum_{\ell=0}^{(m-k-1)/2} a_{(2\ell)j} = 0, \qquad 0 \le j < k.$$

Then the PMEPR of the coset $Q+\mathrm{RM}_2(1,m)$ is equal to 2^{k+1}.

In all other cases, the form Q has rank greater than $m-k-1$ and we cannot prove that the bound of Corollary 13 is tight by this approach. When $m-k$ is even, a similar sequence of reductions reveals that Q has rank at least $m-k$, and the largest lower bound on PMEPR that we can obtain by this approach is 2^k, less than the upper bound of 2^{k+1} predicted by Corollary 13.

In summary, for certain special quadratic forms Q, our rank-based approach can be used to show that Corollary 13 gives the exact value of PMEPR for the coset $Q+\mathrm{RM}_2(1,m)$.

VII. Conclusions and Open Problems

In this paper, we have shown how Golay complementary sets of polyphase sequences can be obtained from cosets of $\mathrm{RM}_q(1,m)$, the generalised first order Reed-Muller code. As a corollary, we obtained an upper bound on PMEPR for second order cosets of this code which depends only on a parameter of the graph associated with the coset.

We have used the graph theoretical approach and our bound on PMEPR to extend the range of coding options for practical applications of OFDM. The codes enjoy high minimum distances, good rates (at least for small numbers of carriers) and have efficient encoding and decoding algorithms.

We close with a discussion of open problems suggested by this work.

Recall that Corollary 13 gave the 'correct power of 2' bound on all but three second order cosets of $\mathrm{RM}_2(1,4)$. The three recalcitrant cosets are those with forms

$$Q_1 = x_0x_1 + x_2x_3, \quad Q_2 = x_0x_2 + x_1x_3, \quad Q_3 = x_0x_3 + x_1x_2,$$

and all have PMEPR less than 4. Interestingly, the corollary also gives the *exact* value of PMEPR for every coset of $\mathrm{RM}_4(1,4)$ in $\mathrm{ZRM}_4(1,m)$, except the cosets identified by $2Q_1, 2Q_2$ and $2Q_3$. In both cases, these cosets have isomorphic graphs with the property that deleting a single vertex leads to a graph consisting of an edge (i.e. a Hamiltonian path on two vertices) and a degree zero vertex. Other examples based on 5 vertices have lead us to prove, using an extension of our techniques, an improved version of Theorem 12:

Theorem 24: Suppose $Q:\{0,1\}^m \to \mathbb{Z}_q$ is a quadratic form in variables $x_0, x_1, \ldots, x_{m-1}$. Suppose that $G(Q)$ contains a set of k distinct vertices labelled $j_0, j_1, \ldots, j_{k-1}$ with the property that deleting those k vertices and all their edges results in a path on $m-k-1$ vertices and a single vertex of degree zero. Suppose further that all edges in the original graph between the degree zero vertex and the k deleted vertices are labelled

$q/2$. Let a be the label of either end vertex in the path (or either vertex of the graph when $k = m-2$). Then for any choice of $g', g_i \in \mathbb{Z}_q$,

$$\left\{ Q + \sum_{i=0}^{m-1} g_i x_i + g' + \frac{q}{2}\left(\sum_{\alpha=0}^{k-1} d_\alpha x_{j_\alpha} + d x_a \right) : d, d_\alpha \in \{0,1\} \right\}$$

is a Golay complementary set of size 2^{k+1}.

The improved theorem gives the correct power of 2 PMEPR bound for the cosets identified by Q_1, Q_2 and Q_3, but there are still quadratic forms in 5 variables where it does not. One example is the form

$$x_0x_1 + x_0x_4 + x_1x_4 + x_2x_4 + x_3x_4$$

where the corresponding coset has PMEPR equal to 3.449, but the improved theorem gives a bound of only 8. Notice that deleting the single vertex labelled 4 gives a graph with a single edge and two degree 0 vertices: so it is tempting to conjecture that a more general form of our theorem holds, in which deletion of k vertices to produce a Hamiltonian path and any number of degree 0 vertices still gives Golay complementary sets of size 2^{k+1}. But Stinchcombe [35] has given examples of graphs on 6 and more vertices where the PMEPR is too high for such a theorem to be true in general. What is the strongest possible generalisation of Theorem 12?

We have proved a lower bound on the PMEPR of second order cosets of $\mathrm{RM}_2(1,m)$ that depends on the rank of the quadratic form Q defining the coset. We used this as a tool to prove the tightness of Corollary 13 in certain cases. The bound also shows that Theorem 12 is sometimes best possible, in the sense that certain sequences cannot lie in Golay complementary sets of smaller size than those constructed in the theorem. So the bound is useful for establishing optimal results on complementary sets, as well as results on PMEPR of OFDM codes formed from cosets of $\mathrm{RM}_2(1,m)$. But we have already seen that the rank approach does not (and indeed cannot) always give tight results. This can be for one or more of the following reasons:

- because the actual PMEPR of a coset $Q + \mathrm{RM}_2(1,m)$ is not an exact power of 2 (for example, the cosets $\sum_{i=0}^{m-2} x_{\pi(i)}x_{\pi(i+1)}$ yielding length 2^m Golay complementary pairs appear to be of this type when m is even).
- because, as we have already discussed in this section, Theorem 12 and Corollary 13 are not best possible for many quadratic forms Q.
- because the rank approach is never strong enough (for example, when $m-k$ is even, or if C is non-zero in the analysis of Section VI-B).

Does examining instantaneous envelope power functions at times $t \neq 0$ help in some of these cases? It is well worth pointing out that in the example cited in the first case above, the corresponding quaternary cosets $2\sum_{i=0}^{m-2} x_{\pi(i)}x_{\pi(i+1)} + \mathrm{RM}_4(1,m) \in \mathrm{ZRM}_4(2,m)$ *do* have PMEPR exactly 2. A proof of this fact was given in [5], by constructing codewords whose power at $t=0$ is exactly 2^{m+1}. Indeed [10, Table II] shows that, at least for $m=4$, moving to quaternary versions $2Q + \mathrm{RM}_4(1,m)$ of binary cosets $Q + \mathrm{RM}_2(1,m)$ 'regularises' the PMEPR behaviour of cosets to be exact powers of two. Is there an analogue of our rank approach applicable to the non-binary case, and in particular the quaternary case, which can be used to prove tight lower bounds on PMEPRs of cosets in situations where our binary approach fails to do so? Such an approach may come from a better understanding of the Lee weight distribution of second order cosets of $\mathrm{RM}_q(1,m)$.

We have indicated how Theorem 12 and Corollary 13 explain much of the PMEPR behaviour of second order cosets of $RM_q(1,m)$ and how improvements in our techniques might explain more. But it was observed in [10] that there are 48 cosets of $\mathrm{RM}_8(1,4)$ in $\mathrm{ZRM}_8(2,4)$ having PMEPR exactly equal to 3. The work in our paper cannot explain this behaviour, because we have only constructed Golay complementary sets of size 2^{k+1}, while the PMEPR value suggests that the codewords of these 48 cosets might lie in triples with special correlation properties. But Golay triples cannot exist over $\mathbb{Z}_8$, essentially because no sum of three 8-th roots of unity can equal 0. Nieswand and Wagner [28] have provided a partial explanation by exhibiting, for each $m > 2$, a total of $2 \cdot m!$ cosets of $\mathrm{RM}_8(1,m)$ in $\mathrm{ZRM}_8(2,m)$ each of which contains a codeword $\mathbf{a}$ whose envelope power $P(\mathbf{a})(t)$ satisfies $P(\mathbf{a})(0) = 3 \cdot 2^m$. In the cases $m=3$ and $m=4$ the $2 \cdot m!$ cosets they have identified are precisely those whose maximum PMEPR is exactly 3. What other regularities appear in the PMEPRs of cosets as we move to higher alphabets, and how can they be explained in general?

Acknowledgements

I am grateful to Jonathan Jedwab and James Davis for bringing to my attention the problems addressed in this paper and for encouraging me in the initial stages of my work. I am particularly grateful to Jonathan for many hours of helpful discussion. My thanks also go to Alan Jones and Tim Wilkinson for providing the engineering motivation for this work and for patiently explaining practical aspects of OFDM systems.

References

[1] M. Alard and R. Lasalle. Principles of modulation and channel coding for digital broadcasting for mobile receivers. *EBU Review*, 224: 47–69, Aug. 1987.

[2] J.A.C. Bingham. Multicarrier modulation for data transmission: an idea whose time has come. *IEEE Commun. Magazine*, 28(1): 5–14, May 1990.

[3] S. Boyd. Multitone signals with low crest factor. *IEEE Trans. Circuits and Systems*, CAS-33: 1018–1022, 1986.

[4] S.Z. Budišin. New complementary pairs of sequences. *Elec. Lett.*, 26(13):881–883, June 1990.

[5] M.W. Cammarano and M. Walker. Integer maxima in power envelopes of Golay codewords. Technical report, University of Richmond, VA, USA, 1997.

[6] P.S. Chow, J.M. Cioffi, and J.A.C. Bingham. DMT-based ADSL: concept, architecture, and performance. In *IEE Colloquium on 'High Speed Access Technology and Services, Including Video-on-Demand'*, pages 3/1–6, Oct. 1994.

[7] L.J. Cimini, Jr. Analysis and simulation of a digital mobile channel using orthogonal frequency division multiplexing. *IEEE Trans. Commun.*, 33:665–675, July 1985.

[8] J.H. Conway and N.J.A. Sloane. Soft decoding techniques for codes and lattices, including the Golay code and the Leech lattice. *IEEE Trans. Inform. Theory*, IT-32: 41–50, 1986.

[9] 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.*, 33: 267–268, 1997.

[10] J.A. Davis and J. Jedwab. Peak-to-mean power control in OFDM, Golay complementary sequences and Reed-Muller codes. *IEEE Trans. Inform. Theory*, to appear.

[11] P. Delsarte, J. Goethals, and F.J. MacWilliams. On generalized Reed-Muller codes and their relatives. *Information and Control*, 16: 403–442, 1974.

[12] P. Fan and M. Darnell. *Sequence design for communications applications.* John Wiley and Sons, New York, 1996.

[13] M. Friese. Multicarrier modulation with low peak-to-mean average power ratio. *Elec. Lett.*, 32: 713–714, 1996.

[14] M.J.E. Golay. Multislit spectroscopy. *J. Opt. Soc. Amer.*, 39: 437–444, 1949.

[15] M.J.E. Golay. Static multislit spectroscopy and its application to the panoramic display of infrared spectra. *J. Opt. Soc. Amer.*, 41: 468–472, 1951.

[16] M.J.E. Golay. Complementary series. *IRE Trans. Inform. Theory*, IT-7: 82–87, 1961.

[17] A.J. Grant and R.D.J. van Nee. Efficient maximum-likelihood decoding of q-ary modulated Reed-Muller codes. *IEEE Commun. Lett.*, 2(5):134–136, May 1998.

[18] 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*, IT-40: 301–319, 1994.

[19] T.F. Ho and V.K. Wei. Synthesis of low-crest waveforms for multicarrier CDMA systems. In *IEEE Globecomm 1995*, pages 131–135, 1995.

[20] 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*, pages 904–908, Atlanta, April–May 1996.

[21] 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.*, 30: 2098–2099, 1994.

[22] T. Kasami, S. Lin, and W. Peterson. New generalizations of Reed-Muller codes, Part I: primitive codes. *IEEE Trans. Inform. Theory*, IT-14: 189–199, 1968.

[23] X. Li and L.J. Cimini, Jr. Effects of clipping and filtering on the performance of OFDM. *IEEE Commun. Lett.*, 2: 131–133, May 1998.

[24] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes (2nd edition).* North Holland, Amsterdam, 1986.

[25] S.H. Müller, R.W. Bäuml, R.F.H. Fischer, and J.B. Huber. OFDM with reduced peak-to-average power ratio by multiple signal representation. *Annales des Télécommunications*, 52(1–2): 58–67, 1997.

[26] S.H. Müller and J.B. Huber. A comparison of peak power reduction schemes for OFDM. In *IEEE Globecom'97*, Phoenix, Arizona, Nov. 1997.

[27] 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*, 7: 24–38, 1989.

[28] K.M. Nieswand and K.N. Wagner. Octary codewords with power envelopes of $3 * 2^m$. Technical report, University of Richmond, VA, USA, 1998.

[29] H. Ochiai and H. Imai. Block coding scheme based on complementary sequences for multicarrier signals. *IEICE Trans. Fundamentals*, pages 2136–2143, Nov. 1997.

[30] K.G. Paterson and A.E. Jones. Efficient decoding algorithms for generalised Reed-Muller codes. *Submitted*, 1998.

[31] K.G. Paterson and V. Tarokh. On the existence and construction of good codes with low peak-to-average power ratios. *Submitted*, 1999.

[32] B.M. Popović. Synthesis of power efficient multitone signals with flat amplitude sprectrum. *IEEE Trans. Commun.*, 39: 1031–1033, 1991.

[33] S. Shepherd, J. Orriss, and S. Barton. Asymptotic limits in peak envelope power reduction by redundant coding in orthogonal frequency-division multiplex modulation. *IEEE Trans. Commun.*, 46: 5–10, 1998.

[34] R. Sivaswamy. Multiphase complementary codes. *IEEE Trans. Inform. Theory*, IT-24(5):546–552, Sept. 1978.

[35] T. Stinchcombe. Personal communication.

[36] V. Tarokh and H. Jafarkhani. On reducing the peak to average power ratio in multicarrier communications. *Submitted*, 1998.

[37] C.-C. Tseng. Signal multiplexing in surface-wave delay lines using orthogonal pairs of Golay's complementary sequences. *IEEE Trans. Sonics and Ultrasonics*, SU-18: 103–107, 1971.

[38] C.-C. Tseng and C.L. Liu. Complementary sets of sequences. *IEEE Trans. Inform. Theory*, IT-18(5): 644–652, Sept. 1972.

[39] J.H. van Lint. *Introduction to Coding Theory (2nd edition)*. Springer-Verlag, Berlin, 1992.

[40] R.D.J. van Nee. OFDM codes for peak-to-average power reduction and error correction. In *IEEE Globecom 1996*, pages 740–744, London, Nov. 1996.

[41] G.R. Welti. Quaternary codes for pulsed radar. *IRE Trans. Inform. Theory*, IT-6: 400–408, June 1960.

[42] 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*, pages 825–829, Chicago, July 1995.

[43] D. Wulich. Reduction of peak-to-mean ratio of multicarrier modulation using cyclic coding. *Elec. Lett.*, 32(5): 432–433, Feb. 1996.

m	$k_1 = \lfloor \log_2 \lvert\mathcal{G}_m\rvert \rfloor$	$k_2 = \lfloor \log_2 \lvert\mathcal{P}_m\rvert \rfloor$	Encoded bits	Code rate
5	0	5	11	0.344
6	2	8	17	0.266
7	4	11	23	0.180
8	6	14	29	0.113
9	7	17	34	0.066
10	8	20	39	0.038

TABLE I

Number of encoded bits and code rate for binary OFDM codes with PMEPR at most 4.

m	Quaternary			Octary		
	$\lfloor \log_2 \lvert \mathcal{G}_m \rvert \rfloor$	Encoded bits	Code rate	$\lfloor \log_2 \lvert \mathcal{G}_m \rvert \rfloor$	Encoded bits	Code rate
3	2	11	0.688	5	18	0.750
4	5	18	0.563	8	26	0.542
5	7	24	0.375	11	34	0.354
6	9	31	0.242	14	43	0.219
7	11	38	0.148	17	52	0.135
8	13	45	0.088	20	61	0.079
9	15	52	0.051	23	70	0.046
10	17	59	0.029	26	79	0.026

TABLE II

Number of encoded bits and code rates for quaternary and octary OFDM codes with PMEPR at most 4.

m	$k_1 = \lfloor \log_2 \lvert \mathcal{G}_m \rvert \rfloor$	$k_2 = \lfloor \log_2 \lvert \mathcal{P}_m \rvert \rfloor$	Encoded bits	Code rate
7	3	11	22	0.172
8	7	14	30	0.117
9	10	17	37	0.072
10	13	20	44	0.043

TABLE III

NUMBER OF ENCODED BITS AND CODE RATES FOR BINARY OFDM CODE WITH PMEPR AT MOST 8.

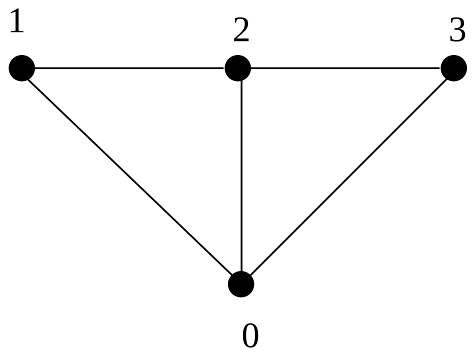

Fig. 1. The graph of the quadratic form $x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_2x_3$.

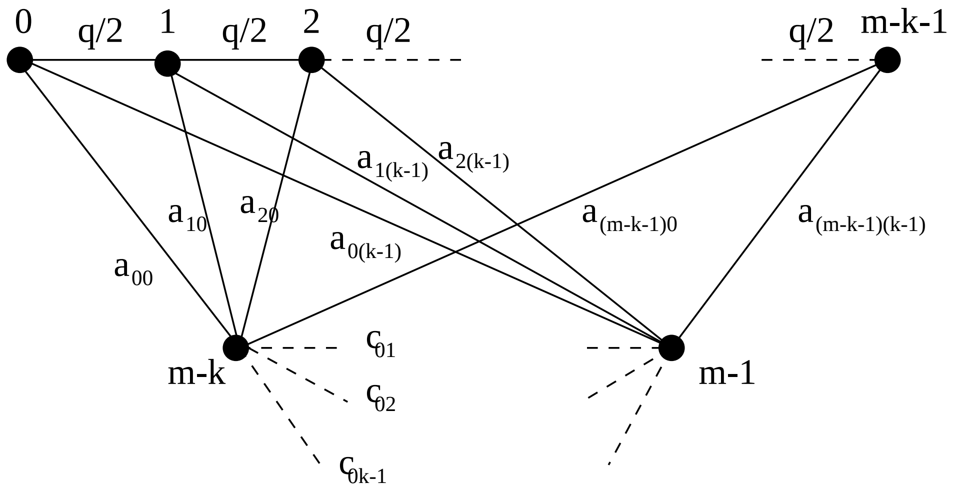

Fig. 2. The graph of the quadratic form $Q_{A,C}$