Codes, Correlations and Power Control in OFDM

James A. Davis*
Department of Mathematics and Computer Science,
University of Richmond, Virginia 23173, U.S.A.

Jonathan Jedwab and Kenneth G. Paterson
Hewlett-Packard Laboratories,
Filton Road, Stoke Gifford, Bristol BS34 8QZ, U.K.

Abstract

Practical communications engineering is continuously producing problems of interest to the coding theory community. A recent example is the power-control problem in Orthogonal Frequency Division Multiplexing (OFDM). We report recent work which gives a mathematical framework for generating solutions to this notorious problem that are suited to low-cost wireless applications. The key result is a connection between Golay complementary sequences and Reed-Muller codes. The former are almost ideal for OFDM transmissions because they have a very low peak-to-mean envelope power ratio (PMEPR), while the latter have efficient encoding and decoding algorithms and good error correction capability. This result is then generalised in two ways. Firstly we study polyphase Golay sequences, motivating the introduction of non-binary generalisations of the Reed-Muller codes. Secondly we consider Golay complementary sets, where the results can be presented most naturally in the language of graph theory. The practical impact is a flexible family of OFDM codes which combine low PMEPR with good error correction capability. However, the interaction between theory and practice is a two-way process: the application motivates further study of a fertile interplay between coding theory, graph theory and sequence design. We include a list of open problems which we hope will stimulate further research in this area.

Keywords

power; envelope; OFDM; Reed-Muller; code; Golay; complementary; sequence; pair; set

*This author thanks Hewlett-Packard for their generous support during the time of this research.

1 Introduction

Orthogonal frequency division multiplexing (OFDM) is a method of transmitting data simultaneously over multiple equally-spaced carrier frequencies, using Fourier transform processing for modulation and demodulation [1]. The method has been proposed or adopted for many types of radio systems such as wireless Local Area Networks [2] and digital audio and digital video broadcasting [3]. OFDM offers many well-documented advantages for multicarrier transmission at high data rates, particularly in mobile applications.

The principal difficulty with OFDM is that when the sinusoidal signals of the n carriers add mostly constructively the peak envelope power is as much as n times the mean envelope power. If the peak envelope power is subject to a design or regulatory limit then this has the effect of reducing the mean envelope power allowed under OFDM relative to that allowed under constant envelope modulation. This reduces the effective range of the OFDM transmissions and is particularly acute in mobile applications where battery power is a constraint. Moreover, to prevent signal distortions and spectral growth due to non-linearities inherent in electronic components, power amplifiers must be operated below their compression point where power is converted most efficiently. This results in more expensive and inefficiently used components.

In this paper we survey a method of controlling the PMEPR of OFDM signals which, in its basic form, allows transmission across the carriers of only those bi-phase sequences belonging to a Golay complementary pair. A recently recognised connection between such sequences and classical binary Reed-Muller codes guarantees the method to have good error correction properties and allows efficient encoding and decoding. A first extension to polyphase sequences involves generalising the Reed-Muller codes to non-binary alphabets, while a second extension to Golay sets has a natural graph theoretical interpretation. For low-cost mobile wireless applications, for which the number of carriers is typically 16 or 32, the method offers practical code rates.

As well as providing a range of solutions to the power-control problem, the work in this paper highlights a new and natural application area for algebraic coding theory, motivates the further study of some recently introduced families of codes [4] and solves a longstanding open problem about Golay complementary sets. It also shows that solving practical problems can lead to theoretical insights concerning the interactions between coding theory, graph theory and sequence design.

The paper is organised as follows.

Section 2 gives an overview of OFDM and Section 3 introduces Golay complementary sequences and sets and motivates their study via the OFDM power-control problem. In Sections 4 and 5 we introduce generalised Boolean functions and use them to describe certain classes of Golay complementary pairs and, more generally, sets. Section 6 shows that in the binary case, these Golay pairs and sets occur in cosets of the first-order Reed-Muller code within the second-order Reed-Muller code. This connection between Golay sequences and sets and Reed-Muller codes is a key result leading to practical and flexible OFDM codes. For the non-binary cases, we require two new linear codes over the ring $\mathbb{Z}_{2h}$ as generalisations of the Reed-Muller code and demonstrate a corresponding connection with the non-binary Golay sequences and sets previously determined. We give the minimum Hamming and Lee distance of these new codes as a measure of their error correction capability. Section 7 sketches how to turn the theoretical results on Golay complementary sequences and sets into practical OFDM codes. We demonstrate by example how the trade-offs between standard code parameters (rate and minimum distance) and PMEPR can be achieved in a flexible manner. In Section 8 we briefly outline a number of approaches to efficient decoding of the generalised Reed-Muller codes. In the final section we present some conclusions and open problems.

This survey draws heavily on references [5] and [6], which contain full details and proofs, as well as an account of prior and independent work on power control in OFDM using Golay complementary sequences. For further background on classical coding theory, see [7] or [8].

2 OFDM Transmission

We begin by describing the signals in an OFDM system and introducing some associated terminology.

An n-carrier OFDM signal is composed by adding together n equally spaced, phase-shifted sinusoidal carriers. Information is carried in the phase shift applied to each carrier. If H distinct, equally-spaced phase shifts are used, then we say that the OFDM system uses *H-ary phase-shift keying* or *H-PSK modulation*. With carrier frequencies $f_0 + j\Delta f, (0 \le j < n)$, the OFDM signal may be represented as the real part of the complex-valued function:

$$S_a(t) = \sum_{j=0}^{n-1} \omega^{a_j} e^{2\pi i (f_0 + j\Delta f)t}, \tag{1}$$

where the information-bearing sequence $a = (a_0, a_1, \ldots, a_{n-1})$, $a_j \in \mathbb{Z}_H$, is called an *OFDM codeword* and $\omega = e^{2\pi i/H}$ is a complex H-th root of unity. This signal is transmitted for a length of time equal to $1/\Delta f$, called the *symbol period*.

In a practical OFDM system, H will be a power of 2. For $H = 2$, we have binary OFDM codewords and *binary* or *BPSK* modulation. For $H = 4$, we have quaternary codewords and *quaternary* or *QPSK* modulation. Often n is also a power of 2, to ease signal processing, because then a sampled version of the signal can be computed using fast Fourier transform (FFT) techniques.

The instantaneous envelope power of the signal $|S_a(t)|$ is defined to be the function $P_a(t) = |S_a(t)|^2$. The envelope power is an upper bound for the actual power $\mathrm{Re}(S_a(t))^2$ of the OFDM signal. The average value of this envelope power function can be shown to equal n and so the peak-to-mean envelope power ratio (PMEPR) of the signal is defined to be

$$\frac{1}{n} \cdot \sup_t P_a(t).$$

We also refer to the PMEPR of the corresponding OFDM codeword a. The PMEPR of any codeword a is at most n and this upper bound is attained by the word $a = (0, 0, \ldots, 0)$, which can occur in an uncoded OFDM system.

3 Golay Complementary Sequences and Sets in OFDM

Definition 3.1 *Let $a = (a_0, a_1, \ldots, a_{n-1})$ and $b = (b_0, b_1, \ldots, b_{n-1})$, where $a_i, b_i \in \mathbb{Z}_H$. The* aperiodic autocorrelation of a at displacement u *is $C_a(u) = \sum_i \omega^{a_i - a_{i+u}}$, where the summation is understood to be over only those integer values for which both i and $i + u$ lie within $\{0, 1, \ldots, n-1\}$ and where $\omega = e^{2\pi i/H}$. The sequences a and b are called a* Golay complementary pair over $\mathbb{Z}_H$ of length n *if $C_a(u) + C_b(u) = 0$ for each $u \neq 0$. Any sequence which is a member of a Golay complementary pair is called a* Golay sequence.

We are interested in using Golay sequences as OFDM codewords because the resulting OFDM signals have PMEPR of at most 2, a substantial and practically very useful reduction from the maximum value of n. This result is due to Popović [9] who generalised earlier work of Boyd [10]:

Theorem 3.2 *The PMEPR of any Golay sequence is at most* 2.

Proof: It is an easy exercise to show that

$$\begin{aligned} P_a(t) &= \sum_{u=1-n}^{n-1} C_a(u) e^{2\pi i u \Delta f t} \\ &= C_a(0) + 2 \cdot \mathrm{Re} \sum_{\ell=1}^{n-1} C_a(u) e^{2\pi i u \Delta f t}. \end{aligned}$$

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

$$P_a(t) + P_b(t) = C_a(0) + C_b(0) = 2n.$$

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

Golay complementary pairs over $\mathbb{Z}_2$ were introduced by Golay [11], [12] in connection with infrared multislit spectrometry and have since found application in fields such as optical time domain reflectometry [13] and acoustic surface-wave encoding [14]. They are known to exist for all lengths $n = 2^\alpha 10^\beta 26^\gamma$, where $\alpha, \beta, \gamma \geq 0$ [15], but do not exist for length n having any prime factor congruent to 3 modulo 4 [16]. For a survey of previous results on non-binary Golay complementary pairs, see [17, Chapter 13].

As a generalisation of Golay complementary pairs, Golay complementary sets were introduced in [18]:

Definition 3.3 *For* $1 \leq j \leq N$, *let* $a^j = (a_0^j, a_1^j, \ldots, a_{n-1}^j)$ *where* $a_i^j \in \mathbb{Z}_H$. *Let* $\mathcal{A} = \{a^1, a^2, \ldots, a^N\}$ *The set* $\mathcal{A}$ *is called a* Golay complementary set over $\mathbb{Z}_H$ of size N *if*

$$\sum_{j=1}^{N} C_{a^j}(u) = 0, \quad u \neq 0.$$

Clearly, a Golay complementary set of size 2 is a Golay complementary pair. A survey of previous work on these sets and their applications can also be found in [17, Chapter 13].

As with Golay sequences, our motivation for studying Golay complementary sets is that their sequences can have low PMEPR. We have the following straightforward generalisation of Theorem 3.2.

Theorem 3.4 *The PMEPR of any sequence from a Golay complementary set of size N is at most N.*

4 Golay Sequences from Boolean Functions

Henceforth we impose the restriction $n = 2^m$. We will shortly give an explicit form for a large class of Golay complementary pairs over $\mathbb{Z}_{2h}$ of length 2^m, and deduce the form of a set of Golay sequences. We first require some notation.

A *Boolean function* is a function f from $\mathbb{Z}_2^m = \{(x_1, x_2, \ldots, x_m) \mid x_i \in \{0, 1\}\}$ to $\mathbb{Z}_2$. We regard each 0-1 variable x_i as itself being a Boolean function $f_i(x_1, x_2, \ldots, x_m) = x_i$ and consider the 2^m monomials

$$1,\, x_1, x_2, \ldots, x_m,\, x_1x_2, x_1x_3, \ldots, x_{m-1}x_m,\, \ldots,\, x_1x_2\cdots x_m. \tag{2}$$

Any Boolean function f can be uniquely expressed as a linear combination over $\mathbb{Z}_2$ of these monomials, where the coefficient of each monomial belongs to $\mathbb{Z}_2$ [8]. We specify a sequence $\mathbf{f}$ of length 2^m corresponding to f by listing the values taken by $f(x_1, x_2, \ldots, x_m)$ as $(x_1, x_2, \ldots, x_m)$ ranges over all its 2^m values in lexicographic order. In other words, if $(i_1, i_2, \ldots, i_m)$ is the binary representation of the integer i then the ith element of $\mathbf{f}$ (numbering the leftmost element as 0) is $f(i_1, i_2, \ldots, i_m)$. For example, for $m = 3$ we have

$$\mathbf{f} = (f(0,0,0), f(0,0,1), f(0,1,0), f(0,1,1), f(1,0,0), f(1,0,1), f(1,1,0), f(1,1,1))$$

and so $\mathbf{1} = (11111111)$, $\mathbf{x_1} = (00001111)$, $\mathbf{x_2} = (00110011)$, $\mathbf{x_3} = (01010101)$, and

$$\mathbf{x_1x_2} + \mathbf{x_2x_3} = (00010010).$$

We define a *generalised Boolean function* to be a function f from $\mathbb{Z}_2^m$ to $\mathbb{Z}_{2h}$, where $h \geq 1$. It is straightforward to show that any such function can be uniquely expressed as a linear combination over $\mathbb{Z}_{2h}$ of the monomials (2), where the coefficient of each monomial belongs to $\mathbb{Z}_{2h}$. As above, we specify a sequence $\mathbf{f}$ of length 2^m corresponding to the generalised Boolean function f. For example, for $h = 2$ and $m = 3$ we have $3\mathbf{x_1} = (00003333)$, $2\mathbf{x_1x_2x_3} = (00000002)$, and $\mathbf{x_1x_2} + 3\mathbf{x_2x_3} + 2\cdot\mathbf{1} = (22212232)$. (Technically, for such expressions to be valid we must embed the range space $\mathbb{Z}_2^m$ of the monomials (2) in $\mathbb{Z}_{2h}^m$.) Henceforth we shall drop the distinction between a generalised Boolean function and its corresponding sequence, and use the notation f to refer to both.

With this notation we are now ready to describe some Golay complementary pairs over $\mathbb{Z}_{2h}$ of length 2^m.

Theorem 4.1 *The sequences*

$$a = h\sum_{k=1}^{m-1} x_{\pi(k)}x_{\pi(k+1)} + \sum_{k=1}^{m} c_kx_k + c \tag{3}$$

and

$$b = a + hx_{\pi(1)} \tag{4}$$

are a Golay complementary pair over $\mathbb{Z}_{2h}$ of length 2^m, for any permutation π of the symbols $\{1, 2, \ldots, m\}$ and for any $c, c_k \in \mathbb{Z}_{2h}$.

Proof: The case $m = 1$ is easily checked by hand, so assume $m \geq 2$ and fix $u \neq 0$. By Definition 3.1, $C_a(u) + C_b(u)$ is the sum over i of terms $\omega^{a_i - a_{i+u}} + \omega^{b_i - b_{i+u}}$, where ω is a primitive $2h$-th root of unity. For a given integer i, set $j = i + u$ and let $(i_1, i_2, \ldots, i_m)$ and $(j_1, j_2, \ldots, j_m)$ be the binary representation of i and j respectively. The sequence element a_i is given by $a(i_1, i_2, \ldots, i_m)$, as discussed above.

Case 1: $j_{\pi(1)} \neq i_{\pi(1)}$. From (4), over $\mathbb{Z}_{2h}$ we have $a_i - a_j - b_i + b_j = h(j_{\pi(1)} - i_{\pi(1)}) = h$, so $\omega^{a_i - a_j}/\omega^{b_i - b_j} = \omega^h = -1$. Therefore $\omega^{a_i - a_j} + \omega^{b_i - b_j} = 0$.

Case 2: $j_{\pi(1)} = i_{\pi(1)}$. Since $j \neq i$, we can define v to be the smallest integer for which $i_{\pi(v)} \neq j_{\pi(v)}$. Let i' be the integer whose binary representation $(i_1, i_2, \ldots, 1 - i_{\pi(v-1)}, \ldots, i_m)$

differs from that of i only in position $\pi(v-1)$, and similarly let j' have binary representation $(j_1, j_2, \ldots, 1-j_{\pi(v-1)}, \ldots, j_m)$. By assumption $i_{\pi(v-1)} = j_{\pi(v-1)}$ and so $j' = i' + u$. We have therefore defined an invertible map from the ordered pair (i, j) to (i', j'), and both pairs contribute to $C_a(u) + C_b(u)$. Now substitution for i' in (3) gives $a_{i'} = a_i + hi_{\pi(v-2)} + hi_{\pi(v)} + c_{\pi(v-1)} - 2c_{\pi(v-1)} i_{\pi(v-1)}$ (unless $v = 2$, in which case we just delete terms involving $\pi(v-2)$ here and in what follows). Therefore $a_i - a_j - a_{i'} + a_{j'} = h(j_{\pi(v-2)} - i_{\pi(v-2)}) + h(j_{\pi(v)} - i_{\pi(v)}) - 2c_{\pi(v-1)}(j_{\pi(v-1)} - i_{\pi(v-1)}) = h$ by the definition of v. Then (4) implies that $b_i - b_j - b_{i'} + b_{j'} = a_i - a_j - a_{i'} + a_{j'} = h$. Arguing as in Case 1, we obtain $\omega^{a_i - a_j} + \omega^{a_{i'} - a_{j'}} = 0$ and $\omega^{b_i - b_j} + \omega^{b_{i'} - b_{j'}} = 0$. Therefore $(\omega^{a_i - a_j} + \omega^{b_i - b_j}) + (\omega^{a_{i'} - a_{j'}} + \omega^{b_{i'} - b_{j'}}) = 0$.

Combining these cases we see that $C_a(u) + C_b(u)$ comprises zero contributions (as in Case 1), and contributions which sum to zero in pairs (as in Case 2). Therefore $a(x_1, x_2, \ldots, x_m)$ and $b(x_1, x_2, \ldots, x_m)$ are a Golay complementary pair, by Definition 3.1. $\square$

Corollary 4.2 *For any permutation π of the symbols $\{1, 2, \ldots, m\}$ and for any $c, c_k \in \mathbb{Z}_{2h}$,*

$$a(x_1, x_2, \ldots, x_m) = h \sum_{k=1}^{m-1} x_{\pi(k)} x_{\pi(k+1)} + \sum_{k=1}^{m} c_k x_k + c$$

is a Golay sequence over $\mathbb{Z}_{2h}$ of length 2^m.

Corollary 4.2 explicitly determines $(2h)^{m+1} \cdot m!/2$ Golay sequences over $\mathbb{Z}_{2h}$ of length 2^m (using the factor $m!/2$ rather than $m!$ because the expression $\sum_{k=1}^{m-1} x_{\pi(k)} x_{\pi(k+1)}$ is invariant under the mapping $\pi \mapsto \pi'$, where $\pi'(k) = \pi(m+1-k)$). Exhaustive computations in the cases $h = 1$, $m \leq 6$ [19] and $h = 2$, $m \leq 4$, have not revealed any Golay sequences that are not accounted for by Corollary 4.2.

For a description of the relationship between Corollary 4.2 and previous work on Golay sequences, including Golay's original papers [20, 21], see [5, 6].

Theorem 4.1 can be used to identify sets of Golay complementary pairs:

Corollary 4.3 *Let $f = h \sum_{k=1}^{m-1} x_{\pi(k)} x_{\pi(k+1)} + \sum_{k=1}^{m} c_k x_k$ where π is a permutation of the symbols $\{1, 2, \ldots, m\}$ and $c_k \in \mathbb{Z}_{2h}$. Then any sequence in the set*

$$A = \{f + c,\ f + h(x_{\pi(1)} + x_{\pi(m)}) + c \mid c \in \mathbb{Z}_{2h}\} \tag{5}$$

forms a Golay complementary pair over $\mathbb{Z}_{2h}$ of length 2^m with any sequence in the set

$$B = \{f + hx_{\pi(1)} + c',\ f + hx_{\pi(m)} + c' \mid c' \in \mathbb{Z}_{2h}\}. \tag{6}$$

A careful count shows that this corollary explicitly identifies $(2h)^{m+2} \cdot m!/2$ Golay complementary pairs $\{a, b\}$ over $\mathbb{Z}_{2h}$ of length 2^m. However, the true number of Golay pairs can be larger than this because in some cases $C_A(u) = C_{A'}(u)$, for all u, for two distinct sets A, A' of the form (5). For an example of this phenomenon, see [5].

Note that we do not obtain any more Golay *sequences* from the above corollary than are already given in Corollary 4.2.

5 Golay Complementary Sets from Boolean Functions

We generalise the results of the last section on Golay complementary pairs to Golay complementary sets of size $2^{\ell+1}$. We begin by introducing some more notation.

Let $Q : \mathbb{Z}_2^m \to \mathbb{Z}_{2h}$ be defined by

$$Q(x_1, \ldots, x_m) = \sum_{1 \le j < k \le m} q_{jk} x_i x_j$$

where $q_{jk} \in \mathbb{Z}_{2h}$, so that Q is a generalised Boolean function in m variables of non-linear order 2. We say that Q is a *quadratic form* in m variables. We identify a labelled graph $G(Q)$ on m vertices with Q as follows. We label the vertices of $G(Q)$ by $1, 2, \ldots, m$ and join vertices j and k by an edge labelled q_{jk} if $q_{jk} \neq 0$. In the case $q = 2$, every edge is labelled 1 and by convention we will omit edge-labels in this case.

A graph G of the type defined above is said to be a *path* if either $m = 1$ (in which case the graph contains a single vertex and no edges), or $m \ge 2$ and G has exactly $m - 1$ edges all labelled h which form a Hamiltonian path in G. The set of path graphs on $m \ge 2$ vertices corresponds to the set of quadratic forms of the type:

$$h \sum_{k=1}^{m-1} x_{\pi(k)} x_{\pi(k+1)},$$

where π is a permutation of $\{1, 2, \ldots, m\}$ (and to the zero form when $m = 1$). These are the quadratic forms appearing in Theorem 4.1.

With the above definitions in hand, we are now ready to give a theorem explicitly constructing (in terms of generalised Boolean functions) size $2^{\ell+1}$ Golay complementary sets of length 2^m sequences over $\mathbb{Z}_{2h}$.

Theorem 5.1 *Suppose $Q : \mathbb{Z}_2^m \to \mathbb{Z}_{2h}$ is a quadratic form in m variables. Suppose further that $G(Q)$ contains a set of ℓ distinct vertices labelled $x_{j_1}, \ldots, x_{j_\ell}$ with the property that deleting those ℓ vertices and all their edges results in a path graph (necessarily on $m - \ell$ vertices). Let t be the label of either vertex of degree 1 in this path graph. Then for any choice of $c, c_k \in \mathbb{Z}_{2h}$,*

$$\{Q + \sum_{k=1}^{m} c_k x_k + c + h(\sum_{k=1}^{\ell} d_k x_{j_k} + d x_t) \mid d_k, d \in \mathbb{Z}_2\},$$

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

For a recursive proof of the theorem, see [6]. This theorem provides a partial answer to a problem posed in [18]: *Obtain direct construction procedures for complementary sets with given parameters, namely, the number of sequences in the set and their lengths.*

Example 5.2 *Let $2h = 2$, $m = 4$ and*

$$Q(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_3x_4.$$

The graph $G(Q)$ is shown in Figure 1. We see that deleting the vertex labelled 1 results in a path graph on vertices 2, 3 and 4. Applying Theorem 5.1 with $\ell = 1$, we get, for each choice

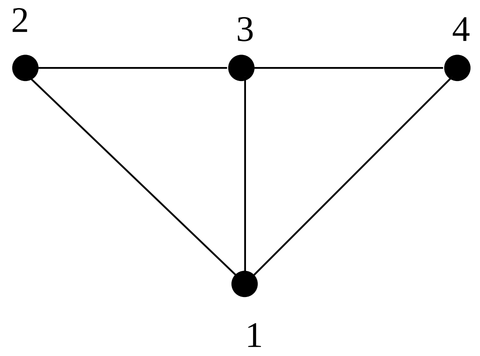

Figure 1: The graph of the quadratic form $x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_3x_4$.

of $c, c_1, c_2, c_3, c_4 \in \mathbb{Z}_2$, the following Golay complementary set of size 4:

$$\begin{array}{ll}\{ & Q + \sum_{k=1}^4 c_k x_k + c, \\ & Q + \sum_{k=1}^4 c_k x_k + c + x_1, \\ & Q + \sum_{k=1}^4 c_k x_k + c + x_1 + x_2, \\ & Q + \sum_{k=1}^4 c_k x_k + c + x_2 \qquad \}\end{array}$$

We are now able to give an explicit form (in terms of generalised Boolean functions and graphs) for a large class of sequences over $\mathbb{Z}_{2h}$ of length 2^m that lie in Golay complementary sets of size $2^{\ell+1}$.

Corollary 5.3 *Suppose $0 \leq \ell < m$, π is a permutation of $\{1, 2, \ldots, m\}$ and*

$$\begin{aligned} Q &= h \sum_{k=1}^{m-\ell-1} x_{\pi(k)} x_{\pi(k+1)} + \sum_{j=1}^{\ell} \sum_{k=1}^{m-\ell} a_{jk} x_{\pi(m-\ell+j)} x_{\pi(k)} \\ &\quad + Q'(x_{\pi(m-\ell+1)}, \ldots, x_{\pi(m)}). \end{aligned}$$

where $a_{jk} \in \mathbb{Z}_{2h}$ $(1 \leq j \leq \ell,\ 1 \leq k \leq m - \ell)$ and Q' is an arbitrary quadratic form in ℓ variables. Then

$$a(x_1, x_2, \ldots, x_m) = Q + \sum_{k=1}^{m} c_k x_k + c$$

lies in a Golay complementary set of size $2^{\ell+1}$ for any choice of $c, c_k \in \mathbb{Z}_{2h}$.

Proof: It is easy to show that the graph $G(Q)$ has the property that deleting the ℓ vertices labelled $\pi(m - \ell + 1), \ldots, \pi(m)$ results in a path in which all edges are labelled by h. The corollary follows from Theorem 5.1. □

Notice that the special case $\ell = 0$ of the preceding theorem and corollary recovers Theorem 4.1 and Corollary 4.2 on Golay complementary pairs of sequences. An analogue of Corollary 4.3 can also be proved.

Corollary 5.3 explicitly determines large numbers of OFDM codewords with PMEPR at most $2^{\ell+1}$. We do not have a simple formula for these numbers because the set of permutations under which the quadratic forms Q are invariant is not so straightforward to compute as in Corollary 4.2. However, [6] shows how to use graph theoretical concepts to generate and count quadratic forms of the type appearing in Corollary 5.3 that are distinct under a set of permutations of size $m!/2$. This is useful in constructing OFDM codes [6].

6 Reed-Muller Codes

The rth order binary Reed-Muller code $\mathrm{RM}(r,m)$ of length 2^m is generated by the monomials in the Boolean functions x_i of degree at most r [8]. This allows us to restate the binary cases $h=1$ of Corollary 4.2 and Corollary 5.3 as:

Corollary 6.1 *Each of the $m!/2$ cosets of $\mathrm{RM}(1,m)$ in $\mathrm{RM}(2,m)$ having a coset representative of the form $\sum_{k=1}^{m-1} x_{\pi(k)}x_{\pi(k+1)}$, where π is a permutation of the symbols $\{1,2,\ldots,m\}$, comprises 2^{m+1} binary Golay sequences of length 2^m.*

Corollary 6.2 *Each coset of $\mathrm{RM}(1,m)$ in $\mathrm{RM}(2,m)$ having a coset representative of the form $Q+\mathrm{RM}(1,m)$, where Q is as specified in Corollary 5.3, comprises 2^{m+1} binary sequences of length 2^m that lie in Golay complementary sets of size $2^{\ell+1}$.*

We wish to make analogous statements to Corollaries 6.1 and 6.2 for the non-binary cases $h>1$ of Corollaries 4.2 and 5.3.

To do this, we follow the landmark paper [4] and define a *linear code over $\mathbb{Z}_H$ of length n* to be a subset of $\mathbb{Z}_H^n$ such that the sum of any two codewords is a codeword. [4] demonstrates that defining linear codes in this way, over rings that are not fields, preserves many of the properties of classical codes even though not every element of the code alphabet has a multiplicative inverse. In particular such a code can be specified in terms of a generator matrix such that the code consists of all distinct linear combinations over $\mathbb{Z}_H$ of the rows of the matrix. We now define two new linear codes over $\mathbb{Z}_{2h}$ of length 2^m in terms of the generalised Boolean functions x_i described in Section 3.

Definition 6.3 *For $h\ge 1$ and $0\le r\le m$, the rth order linear code $\mathrm{RM}_{2h}(r,m)$ over $\mathbb{Z}_{2h}$ of length 2^m is generated by the monomials in the x_i of degree at most r.*

Definition 6.4 *For $h>1$ and $0\le r\le m+1$, the rth order linear code $\mathrm{ZRM}_{2h}(r,m)$ over $\mathbb{Z}_{2h}$ of length 2^m is generated by the monomials in the x_i of degree at most $r-1$ together with 2 times the monomials in the x_i of degree r (with the convention that the monomials of degree -1 and $m+1$ are equal to zero).*

The code $\mathrm{RM}_{2h}(r,m)$ generalises the binary Reed-Muller code $\mathrm{RM}(r,m)$ from the alphabet $\mathbb{Z}_2$ (the case $h=1$) to the alphabet $\mathbb{Z}_{2h}$. Likewise the code $\mathrm{ZRM}_{2h}(r,m)$ generalises the quaternary Reed-Muller code $\mathrm{ZRM}(r,m)$ defined in [4] from the alphabet $\mathbb{Z}_4$ (the case $h=2$) to the alphabet $\mathbb{Z}_{2h}$. In both cases the formal generator matrix is unchanged as h varies, but the alphabet over which it is interpreted changes. The number of monomials in the x_i of degree r is $\binom{m}{r}$, so $\mathrm{RM}_{2h}(r,m)$ contains $(2h)^{\sum_{i=0}^{r}\binom{m}{i}}$ codewords and $\mathrm{ZRM}_{2h}(r,m)$ contains $(2h)^{\sum_{i=0}^{r-1}\binom{m}{i}}.h^{\binom{m}{r}}$ codewords. Note these generalisations of the Reed-Muller code are distinct from the Generalised Reed-Muller code $\mathrm{GRM}(r,m)$ [22], which is defined over a field, and the quaternary Reed-Muller code $\mathrm{QRM}(r,m)$ [4], which generalises the quaternary representation of the Kerdock code.

We can measure the error correction capability of $\mathrm{RM}_{2h}(1,m)$ and $\mathrm{ZRM}_{2h}(2,m)$ in terms of their minimum Hamming distance and also their minimum Lee distance over $\mathbb{Z}_{2h}$ [22]. If the transmission channel renders all $2h-1$ possible errors for a given codeword position equally likely then the traditional Hamming distance metric is an appropriate measure. However if errors involving a transition between adjacent values in $\mathbb{Z}_{2h}$ are much more likely than other errors in a given position then the Lee distance metric is more appropriate. We consider both metrics to be useful measures of error correction capability for OFDM transmission and find:

Theorem 6.5 *The following hold for $0 \le r \le m$:*

	$\mathrm{RM}_{2h}(r,m)$ $(h \ge 1)$	$\mathrm{ZRM}_{2h}(r,m)$ $(h > 1)$
minimum Hamming distance	2^{m-r}	2^{m-r}
minimum Lee distance	2^{m-r}	2^{m-r+1}

We can restate Corollary 4.2 in terms of these generalised Reed-Muller codes as:

Corollary 6.6 *For h even, each of the $m!/2$ cosets of $\mathrm{RM}_{2h}(1,m)$ in $\mathrm{ZRM}_{2h}(2,m)$ having a coset representative of the form $h\sum_{k=1}^{m-1} x_{\pi(k)}x_{\pi(k+1)}$, where π is a permutation of the symbols $\{1,2,\dots,m\}$, comprises $(2h)^{m+1}$ Golay sequences over $\mathbb{Z}_{2h}$ of length 2^m.*

The restriction to h even in the above corollary is needed to ensure that the cosets do lie in $\mathrm{ZRM}_{2h}(2,m)$, a code with minimum Lee distance equal to 2^{m-1}. For h odd, they lie in $\mathrm{RM}_{2h}(2,m)$.

We can also restate Corollary 5.3 in a similar way. We have two different forms of the restatement, depending on whether the coset representatives Q have coefficients which are all even (in which case the coset lies in $\mathrm{ZRM}_{2h}(2,m)$) or are unrestricted (in which case the coset lies in $\mathrm{RM}_{2h}(2,m)$). We see that more cosets are available if we move from the code $\mathrm{ZRM}_{2h}(2,m)$ to the code $\mathrm{RM}_{2h}(2,m)$, but this is at the cost of a decreased minimum Lee distance.

Corollary 6.7 *Each coset of $\mathrm{RM}_{2h}(1,m)$ in $\mathrm{ZRM}_{2h}(2,m)$ (or in $\mathrm{RM}_{2h}(1,m)$) having a coset representative of the form*

$$Q = h\sum_{k=1}^{m-\ell-1} x_{\pi(k)}x_{\pi(k+1)} + \sum_{j=1}^{\ell}\sum_{k=1}^{m-\ell} a_{jk}x_{\pi(m-\ell+j)}x_{\pi(k)} + Q'(x_{\pi(m-\ell+1)},\dots,x_{\pi(m)}).$$

where $0 \le \ell \le m$, $a_{jk} \in \mathbb{Z}_{2h}$ $(1 \le j \le \ell,\ 1 \le k \le m-\ell)$, Q' is an arbitrary quadratic form in ℓ variables and where π is a permutation of the symbols $\{1,2,\dots,m\}$, comprises $(2h)^{m+1}$ sequences over $\mathbb{Z}_{2h}$ of length 2^m that lie in Golay complementary sets of size $2^{\ell+1}$.

In summary, we see that large numbers of $2h$-ary OFDM codewords with low PMEPR are available in cosets of the code $\mathrm{RM}_{2h}(1,m)$. These cosets are contained in either the code $\mathrm{ZRM}_{2h}(2,m)$ or the code $\mathrm{RM}_{2h}(2,m)$, each of which has useful error correction capability. It is this fortuitous combination of PMEPR and coding properties which enables us to find good solutions to the OFDM power-control problem.

7 OFDM Codes

In this section we sketch how the theory developed above can be used to construct OFDM codes. Full details can be found in [5, 6]. We concentrate on codes in which the alphabet size $2h$ is equal to 2^t for $t = 1, 2, 3$. We also focus on codes with $n = 16$ or $n = 32$ carriers. These parameter choices are the most important for low-cost applications of OFDM (such as mobile wireless applications).

In contrast to classical coding theory, where the two parameters of fundamental importance are rate and (normalised) minimum distance, we have a third parameter, the PMEPR of the code. We define this to be the maximum of the PMEPRs of all the codewords in the code. We also define the *rate* of a length n OFDM code $\mathcal{C}$ over $\mathbb{Z}_{2^t}$ to be $\log_2 |\mathcal{C}|/(nt)$. The denominator here expresses the maximum number of bits that can be transmitted per OFDM symbol using uncoded 2^t-PSK modulation on n carriers, while the numerator is equal to the number of information bits encoded by $\mathcal{C}$.

We are interested in examining the possible trade-offs between rate, minimum distance and PMEPR for codes that are formed from unions of cosets of the code $\mathrm{RM}_{2^t}(1, m)$ inside either $\mathrm{ZRM}_{2^t}(2, m)$ or $\mathrm{RM}_{2^t}(2, m)$. An immediate consequence of this coset structure is that the codes enjoy efficient encoding algorithms. In outline, information bits are partly used to specify a codeword of the first order code $\mathrm{RM}_{2^t}(1, m)$ via a linear combination of the rows of the appropriate generator matrix, and partly to select a coset representative from a stored list of representatives. As an alternative to storing such lists, [6] reports a number of techniques which directly use information bits to specify coset representatives. For implementation convenience we always use $2^{w'}$ cosets of $\mathrm{RM}_{2^t}(1, m)$ for some integer w', and so $w' + t(m+1)$ information bits will be encoded in each OFDM codeword.

7.1 Binary Coding Options

As a simple illustration of the kinds of coding options available, we consider the case of $n = 16$ carriers. By taking a single 'Golay coset' identified by Corollary 6.1 in the case $m = 4$, we get a binary, length 16 code with rate 0.31, minimum Hamming distance 8 and a PMEPR of 2. Using instead 8 of the 12 'Golay cosets', we obtain a code still having a PMEPR of 2, but with an increased rate of 0.50 and decreased minimum Hamming distance of 4. A compromise option can be obtained using four out of the six cosets identified by Corollary 6.1 that lie in the Kerdock code of length 16 [7]. These six cosets have representatives:

$$\begin{gathered}
x_1x_2 + x_2x_4 + x_3x_4, \\
x_1x_3 + x_2x_3 + x_2x_4, \\
x_1x_4 + x_3x_4 + x_2x_3, \\
x_1x_2 + x_1x_3 + x_3x_4, \\
x_2x_4 + x_1x_4 + x_1x_3, \\
x_2x_3 + x_1x_2 + x_1x_4.
\end{gathered}$$

The resulting code has rate 0.44 and minimum Hamming distance 6. A fourth binary option can be obtained by working with 32 cosets identified by Corollary 6.2. The resulting code trades an increased code rate of 0.62 for an increased PMEPR of 4, but still has minimum Hamming distance of 4. Further coding options can be obtained by interleaving and concatenating of shorter codes and by moving from 16 to 32 carriers.

7.2 Quaternary and Octary Coding Options

We can also derive a variety of quaternary and octary OFDM codes using Corollaries 6.6 and 6.7 to identify variable numbers of cosets, again trading-off code rate, minimum distance and PMEPR.

As one example, we note that if $m \geq 4$ is even and the set of cosets $\{Q + \mathrm{RM}(1, m)\}$ is a binary Kerdock code of length 2^m, then the minimum Hamming distance of the code $\{hQ + \mathrm{RM}_{2h}(1, m)\}$ over $\mathbb{Z}_{2h}$ is equal to $2^{m-1} - 2^{(m-2)/2}$. For $m = 4$ and $h = 2$, we obtain a quaternary, length 16 OFDM code with rate 0.38, minimum Hamming distance 6, minimum Lee distance 8 and PMEPR of 2.

As another example, peculiar to the octary case, we note the existence of 48 cosets of $\mathrm{RM}_8(1, 4)$ in $\mathrm{ZRM}_8(2, 4)$ having PMEPR of 3 [5]. These 48 cosets were found by ranking all 4096 cosets of $\mathrm{RM}_8(1, 4)$ in $\mathrm{ZRM}_8(1, 4)$ in order of increasing PMEPR (the PMEPR of each coset being computed by evaluating the PMEPR of each of the 32768 codewords in each coset). For the beginnings of a theoretical explanation for the existence of these cosets, see [23]. These cosets can be used to obtain a length 16 OFDM code with rate 0.42, minimum Hamming distance 4, minimum Lee distance 8 and PMEPR of 3.

We have one further set of options in the quaternary and octary cases: we can trade-off Lee distance against rate by moving from cosets chosen from $\mathrm{ZRM}_4(2, m)$ to cosets chosen from the larger set $\mathrm{RM}_4(2, m)$. As just one example, Corollary 6.7 identifies 32 cosets of $\mathrm{RM}_4(1, 4)$ in $\mathrm{ZRM}_4(2, 4)$, but 512 cosets of $\mathrm{RM}_4(1, 4)$ in $\mathrm{RM}_4(2, 4)$, all these cosets having PMEPR at most 4.

8 Decoding Algorithms

In this section we outline decoding algorithms for codes of the type described in Section 7.

One possible first step in obtaining a decoding algorithm for such a code is to apply an appropriate generalisation of the supercode decoding method [24]. This method applies to codes that are the union of cosets of a binary code C; the basic idea is subtract in turn each possible coset representative from the received codeword and to decode the result as a codeword of C, the best decoding result over all cosets determining the coset representative.

Applying the supercode method reduces our decoding problem to that of finding an efficient decoding algorithm for $\mathrm{RM}_{2h}(1, m)$. We report on two distinct approaches to this problem. The first approach, reported in [25], is a natural generalisation of the fast Hadamard transform (FHT) algorithm for decoding the binary first-order Reed-Muller code $\mathrm{RM}(1, m)$. It is a maximum-likelihood soft-decision algorithm that works in the Euclidean domain: it operates on the complex vector y obtained by applying an inverse fast Fourier transform to the sampled, received signal. This signal is in turn a noise-corrupted version of the transmitted signal modelled by the real part of (1). The second approach, developed in [5], works in the 'coding' domain: it has as input a vector containing just the phase information in the components of y. It results in a decoder for $\mathrm{RM}_{2^t}(1, m)$ with respect to both Hamming and Lee distance and uses t real-number FHTs and some additional computation.

Both of these approaches are adequate when the number of cosets in the code is small, since the total complexity is just the number of cosets times the complexity of the first-order decoder. But several of the codes from [5, 6] described in Section 7 involve from tens to thousands of cosets, and new decoding methods are called for. We refer the interested reader to [26] for such a method and an in-depth comparison of the many decoding strategies available.

8.1 A Maximum Likelihood Algorithm

In [25], Grant and van Nee show how to generalise the standard FHT decoding algorithm for the binary code $\mathrm{RM}(1,m)$ [8] to the codes $\mathrm{RM}_{2h}(1,m)$. Let y denotes the length 2^m received codeword (with coefficients that are complex numbers). A maximum likelihood estimate of the original codeword can be inferred from the entry of maximum modulus in the vector Y where

$$Y = (H_m)^T y$$

and the entries of H_m are determined from

$$H_m[a,b] = \omega^{a^T \cdot b}, \quad a \in \mathbb{Z}_2^m,\ b \in \mathbb{Z}_{2h}^m,\ \omega = e^{2\pi i/2h}.$$

A fast algorithm for computing this matrix product can be derived from the decomposition:

$$H_m = \prod_{i=1}^{m} I_{2^{m-i}} \otimes H_1 \otimes I_{(2h)^{i-1}}$$

where I_p denotes the $p \times p$ identity matrix, $\otimes$ denotes a Kronecker product and

$$H_1 = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{2h-1} \end{bmatrix}.$$

While this algorithm always yields an estimate of the transmitted codeword which is closest in Euclidean distance to the received codeword (in other words, it is a maximum likelihood decoding algorithm), it is computationally intensive, requiring approximately 2^{mt} additions and multiplications of complex numbers to perform one decoding in $\mathrm{RM}_{2^t}(1,m)$. The complex multiplications can be replaced by manipulations of real and imaginary parts in the quaternary case and an exact analysis of the algorithm's complexity may be found in [25].

8.2 Iterative Algorithms

Algorithm 5.3 of [5] gives a method which iteratively decodes in $\mathrm{RM}_{2^t}(1,m)$. In outline, the algorithm makes use of the fact that the modulo 2 reduction of the received word, whose components are regarded as symbols from $\mathbb{Z}_{2^t}$, can be regarded as a word in $\mathrm{RM}_2(1,m)$ with the addition of some noise and hence decoded using the standard FHT technique. The modulo 2 reduction of the coefficients used in encoding the transmitted word can then be determined. These coefficients are used as information bits in a modulo 2^t encoding process and the resulting codeword subtracted from the received word. The new word can then be regarded modulo 4 as twice a word in $\mathrm{RM}_2(1,m)$ plus noise. So the FHT can be applied to this word and the modulo 4 part of the transmitted word deduced. Iterating this process t times, all the modulo 2^k reductions of the codeword for $k = 1, 2, \ldots, t$ can be determined and from these the original transmitted codeword reconstructed.

It can be shown that this algorithm acts as a decoder for $\mathrm{RM}_{2^t}(1,m)$ with respect to both Hamming and Lee distance: it always corrects errors of Hamming or Lee weight less than the limit $d/2 = 2^{m-2}$ guaranteed by the minimum Hamming or Lee distance $d = 2^{m-1}$ of the code. In fact the class of errors which can always be corrected by the algorithm includes many whose Hamming or Lee weight greatly exceeds this limit.

The algorithm can be easily adapted for use in soft-decision as well as hard-decision decoding. It is scalable in the sense that the decoder for $\mathrm{RM}_{2^{t+1}}(1,m)$ can be obtained directly from the decoder for $\mathrm{RM}_{2^t}(1,m)$ by including one additional iteration. The complexity of the soft-decision version of the algorithm for $\mathrm{RM}_{2^t}(1,m)$ is approximately $tm2^m$ real additions and multiplications. This can be a substantial saving over the maximum-likelihood algorithm of [25].

It is also shown in [5, Algorithm 5.6] how to interleave the t decoding steps used to decode $\mathrm{RM}_{2^t}(1,m)$ with the supercode decoding part to obtain an algorithm for decoding arbitrary unions of cosets of $\mathrm{RM}_{2^t}(1,m)$ that is potentially much efficient than a straightforward application of the supercode approach.

9 Conclusions and Open Problems

We have presented recent theoretical work highlighting the connection between generalised Reed-Muller codes and Golay complementary pairs and sets of sequences. This work leads to a flexible range of OFDM codes enjoying efficient encoding and decoding and tightly controlled PMEPR. We gave an outline of recent work on encoding methods and decoding algorithms for these codes.

We hope that the combination of algebraic coding theory, graph theory and practical application will encourage other researchers to consider other approaches to the power-control coding problem for OFDM. To this end, we close with a short list of what we consider to be the most important problems arising out of this work.

- Corollary 4.2 identifies a large number of Golay sequences of length 2^m over $\mathbb{Z}_{2h}$. We have reported some numerical evidence that this corollary accounts for all the Golay sequences with these parameters. Is this the case?

- Similarly, Corollary 5.1 identifies large numbers of Golay complementary quadruples contained in second-order cosets of $\mathrm{RM}_{2h}(1,m)$. It is certainly not the case that all length 2^m quadruples must be contained in $\mathrm{RM}_{2h}(2,m)$. Is there a simple description, not necessarily in terms of generalised Boolean functions, of all quadruples of length 2^m?

- As we observed in Section 7, there are 48 cosets of $\mathrm{RM}_8(1,4)$ in $\mathrm{ZRM}_8(2,4)$ having PMEPR of exactly 3. This suggests that the words of these cosets might lie in triples with special correlation properties. These triples cannot be Golay complementary sets however (such sets must be of even size over $\mathbb{Z}_8$). Find a theoretical explanation for this 'fine structure' behaviour of the PMEPR of second-order cosets.

- Corollary 5.1 can be used to show that every second-order coset of $\mathrm{RM}_{2h}(1,m)$ can be partitioned into Golay complementary sets of certain sizes. However, cosets can sometimes be partitioned into smaller sets [6]. In terms of PMEPR, Corollary 5.1 is not always best possible. Find a generalisation which is.

- In this direction, finding lower bounds on the PMEPR of cosets may be helpful. An elementary approach to this problem was introduced in [27] and shows that, for m odd and $h = 1$, or m even and $h = 2$, the PMEPR of any 'Golay coset' of $\mathrm{RM}_{2h}(1,m)$ is exactly 2. This approach was generalised in [6] to obtain a lower bound on PMEPR of a second order coset Q of $\mathrm{RM}(1,m)$ in terms of the rank of the quadratic form Q. The bound can be used to show the optimality of Corollary 5.1 in certain cases. Finding stronger and more generally applicable lower bounds would be of great interest.

- We have noted that exactly 6 of the cosets of RM$(1,4)$ making up the length 16 Nordstrom-Robinson/Kerdock code are of the type appearing in Corollary 6.1. This yielded a series of attractive OFDM coding options. For general even m, the size of the intersection of a Kerdock set of quadratic forms [7, page 54–55] with the set of quadratic forms in Corollary 6.1 is at most $\binom{m}{2}$. This can be shown as follows: the differences of quadratic forms in such an intersection must be non-singular, and therefore the corresponding symplectic matrices must have distinct first rows; but the quadratic forms of Corollary 6.1 give rise to a set of symplectic matrices with just $\binom{m}{2}$ different first rows. The bound is attained for $m = 4$. Is it attained for other values of m? This question can be generalised to consider the intersections of (m, d)-sets and the Delsarte-Goethals codes $\mathcal{DG}(m, d)$ [8, Chapters 15.5 and 21.8] with the sets of quadratic forms arising in the binary case of Corollary 5.3.

Acknowledgements

We would like to thank the organisers of the Bad Windsheim Workshop for organising an excellent meeting and for their tolerance concerning deadlines.

References

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

[2] M. Aldinger. Multicarrier COFDM scheme in high bitrate radio local area networks. In *5th IEEE Int. Symp. on Personal, Indoor and Mobile Radio Commun., The Hague*, pages 969–973, Sept 1994.

[3] P. Shelswell. The COFDM modulation system: the heart of digital audio broadcasting. *Elec. Commun. Eng. J.*, pages 127–136, June 1995.

[4] 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*, **40**:301–319, 1994.

[5] J.A. Davis and J. Jedwab. Peak-to-mean power control in OFDM, Golay complementary sequences and Reed-Muller codes. Technical Report HPL-97-158, Hewlett-Packard Labs., Bristol, Dec 1997.

[6] K.G. Paterson. Generalised Reed-Muller codes and power control in OFDM modulation. Technical Report HPL-98-57, Hewlett-Packard Labs., Bristol, March 1998.

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

[8] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland, Amsterdam, 1986.

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

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

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

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

[13] M. Nazarathy, S.A. Newton, R.P. Giffard, D.S. Moberly, F. Sischka, W.R. Trutna, Jr., and S. Foster. Real-time long range complementary correlation optical time domain reflectometer. *IEEE J. Lightwave Technology*, **7**:24–38, 1989.

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

[15] R.J. Turyn. Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings. *J. Combin. Theory (A)*, **16**:313–333, 1974.

[16] S. Eliahou, M. Kervaire, and B. Saffari. A new restriction on the lengths of Golay complementary sequences. *J. Combin. Theory (A)*, **55**:49–59, 1990.

[17] P. Fan and M. Darnell. *Sequence Design for Communications Applications.* Communications Systems, Techniques and Applications. Research Studies Press, Taunton, 1996.

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

[19] T. Stinchcombe. Personal communication.

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

[21] M.J.E. Golay. Sieves for low autocorrelation binary sequences. *IEEE Trans. Inform. Theory*, **IT-23**:43–51, 1977.

[22] W.W. Peterson and E.J. Weldon, Jr. *Error-Correcting Codes.* MIT Press, Cambridge, 2nd edition, 1972.

[23] K.M. Nieswand and K.N. Wagner. Octary codewords with power envelopes of $3 * 2^m$. Preprint, University of Richmond, 1998.

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

[25] A. Grant and R.D.J. van Nee. Efficient maximum-likelihood decoding of Q-ary modulated Reed-Muller codes. *IEEE Comm. Lett.*, **2**:134–136, 1998.

[26] K.G. Paterson and A.E. Jones. Efficient decoding algorithms for generalised Reed-Muller codes. Technical report, Hewlett-Packard Labs., Bristol, Nov. 1998.

[27] M.W. Cammarano and M.L. Walker. Integer maxima in power envelopes of Golay codewords. Preprint, University of Richmond, 1997.