1999

Codes, Correlations and Power Control in OFDM

James A. Davis
University of Richmond, jdavis@richmond.edu

Jonathan Jedwab

Kenneth G. Paterson

Recommended Citation

Davis, James A., Jonathan Jedwab, and Kenneth G. Paterson. "Codes, Correlations and Power Control in OFDM." In *Difference Sets, Sequences and Their Correlation Properties*, edited by A. Pott, V. Kumaran, Tor Helleseth, and Dieter Jungnickel, 113-32. Nato Science Series C. Netherlands: Springer, 1999.

CODES, CORRELATIONS AND POWER CONTROL IN OFDM

JAMES A. DAVIS
Department of Mathematics and Computer Science
University of Richmond, Virginia 23173, U.S.A.
email: jdavis@richmond.edu

AND

JONATHAN JEDWAB AND KENNETH G. PATERSON
Hewlett-Packard Laboratories
Filton Road, Stoke Gifford, Bristol BS34 8QZ, U.K.
email: jij@hplb.hpl.hp.com,
kp@hplb.hpl.hp.com

Abstract. Practical communications engineering is continually 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.

A. Pott et al. (eds.), Difference Sets, Sequences and their Correlation Properties, 113–132.

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 (Cimini (1985)). The method has been proposed or adopted for many types of radio systems such as wireless local area networks (Aldinger (1994)) and digital audio and digital video broadcasting (Shelswell (1995)). 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 which would be 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 binary 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 correcting 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 described in this paper highlights a new and natural application area for algebraic coding theory, motivates the further study of some families of codes recently introduced by Hammons, Kumar, Calderbank, Sloane and Solé (1994) and solves a longstanding open problem about Golay complementary sets. It also shows that solving practical problems can lead to theoretical insights, in this case 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 in order to 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 material contained in Davis and Jedwab (1999) and Paterson (1999). These references contain full details and proofs as well as an account of prior and independent work on Golay complementary sequences, and on power control in OFDM using these sequences. For further background on classical coding theory, see van Lint (1992) or MacWilliams and Sloane (1986).

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 n carrier frequencies $f_0 + j\Delta f$, $0 \leq j < n$, 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, during the symbol period when the OFDM codeword a is transmitted, is defined to be

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

We also refer to the PMEPR of the 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

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 $C_a(u) = \sum_j \omega^{a_j - a_{j+u}}$, where the summation is understood to be over only those integer values for which both j and $j + u$ 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* $\mathbb{Z}_H$ 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*. (The definition of a Golay polynomial pair over the multiplicative group $\{\pm 1\}$, used for example by Eliahou, Kervaire and Saffari (1990), can easily be seen to be equivalent to the definition given here for a Golay complementary pair over $\{0, 1\}$.)

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 (1991) who generalised earlier work of Boyd (1986):

Theorem 3.1. *The PMEPR of any Golay sequence is at most* 2.

Proof. It is straightforward to show that

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

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 (1949, 1951) in connection with infrared multislit spectrometry and have since found application in fields such as optical time domain reflectometry (Nazarathy, Newton, Giffard, Moberly, Sischka, Trutna, and Foster (1989)) and acoustic surface-wave encoding (Tseng (1971)). They are known to exist for all lengths $n = 2^\alpha 10^\beta 26^\gamma$, where $\alpha, \beta, \gamma \geq 0$ (Turyn (1974)), but do not exist for length n having any prime factor congruent to 3 modulo 4 (Eliahou, Kervaire and Saffari (1990)). For a survey of previous results on non-binary Golay complementary pairs, see Chapter 13 of Fan and Darnell (1996).

Golay complementary sets were introduced by Tseng and Liu (1972) as a generalisation of Golay complementary pairs. 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

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

Clearly, a Golay complementary set of size 2 is a Golay complementary pair. A survey of previous work on these sets and their applications can also be found in Chapter 13 of Fan and Darnell (1996).

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 3.1.

Theorem 3.2. *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 $\mathbb{Z}_2$ (MacWilliams and Sloane (1986)). 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 i-th 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

$$\begin{aligned}\mathbf{f} &= (f(0,0,0), f(0,0,1), f(0,1,0), f(0,1,1),\\ &\quad f(1,0,0), f(1,0,1), f(1,1,0), f(1,1,1))\end{aligned}$$

and so

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

and

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

see also Wolfmann (1999) in this volume. 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*

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

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 our definition of Golay complementary sequences, $C_a(u) + C_b(u)$ 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

$$a_i - a_j - b_i + b_j = h(j_{\pi(1)} - i_{\pi(1)}) = h, \quad \text{so} \quad \omega^{a_i - a_j}/\omega^{b_i - b_j} = \omega^h = -1.$$

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 and 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. □

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 $h = 1$, $m \leq 6$ and $h = 2$, $m \leq 4$ by T. Stinchcombe (personal communication) have shown that, for these parameters, Corollary 4.2 accounts for all Golay sequences.

Theorem 4.1 can be used to identify sets of Golay complementary pairs (noting that the addition of a constant $d \in \mathbb{Z}_{2h}$ to a sequence over $\mathbb{Z}_{2h}$ does not change the aperiodic autocorrelations of the sequence):

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

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

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 Davis and Jedwab (1999).

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

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

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 $h = 1$, 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 $m \geq 2$ and G has exactly $m-1$ edges all labelled h which form a Hamiltonian path. The set of path graphs on m vertices corresponds to the set of quadratic forms of the type

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

when $m \geq 2$, where π is a permutation of $\{1, 2, \ldots, m\}$ (and corresponds 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 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 $j_1, \ldots, j_\ell$ with the property that deleting those ℓ vertices and all their edges results in a path graph (necessarily on $m - \ell$ vertices). Let t be the label of either vertex of degree 1 in this path graph. Then for any choice of $c, c_k \in \mathbb{Z}_{2h}$,*

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

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

Theorem 5.1, which was proved recursively by Paterson (1999), provides a partial answer to a problem posed by Tseng and Liu (1972):

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

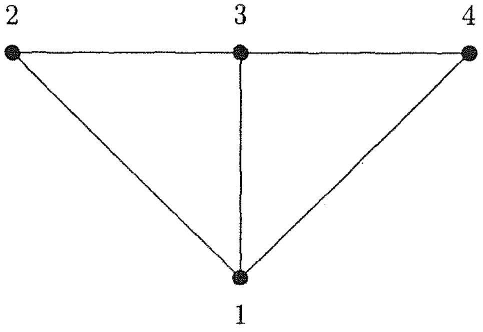

Figure 1. The graph of the quadratic form $x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_3x_4$.

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

$$\begin{aligned}\{ \quad & Q + \textstyle\sum_{k=1}^4 c_kx_k + c, \\ & Q + \textstyle\sum_{k=1}^4 c_kx_k + c + x_1, \\ & Q + \textstyle\sum_{k=1}^4 c_kx_k + c + x_2, \\ & Q + \textstyle\sum_{k=1}^4 c_kx_k + c + x_1 + x_2 \quad \}.\end{aligned}$$

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 5.2. *Suppose* $0 \le \ell < m$ *and let* π *be a permutation of* $\{1, 2, \ldots, m\}$ *Let*

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

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

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

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 $\pi(m-\ell+1), \dots, \pi(m)$ 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 5.2 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, Paterson (1999) shows how to use graph theoretical concepts to generate and count quadratic forms of the type appearing in Corollary 5.2 that are distinct under a set of permutations of size $m!/2$. This is useful in constructing OFDM codes.

6. Reed-Muller Codes

The r-th 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, see MacWilliams and Sloane (1986) or Wolfmann (1999). This allows us to restate the binary case $h = 1$ of Corollaries 4.2 and 5.2 as follows:

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 $\{1,2,\dots,m\}$, 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* 5.2, *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 5.2.

To do this, we follow the landmark paper of Hammons, Kumar, Calderbank, Sloane and Solé (1994) 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. 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.

For $h \geq 1$ and $0 \leq r \leq m$, the r-th 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.

For $h > 1$ and $0 \leq r \leq m+1$, the r-th 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 two 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 by Hammons, Kumar, Calderbank, Sloane and Solé (1994) 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 $(2h)^{\sum_{i=0}^{r-1}\binom{m}{i}} \cdot h^{\binom{m}{r}}$ codewords. Note that these generalisations of the Reed-Muller code are distinct from the "generalised Reed-Muller code $\mathrm{GRM}(r,m)$" (see Peterson and Weldon (1972), for instance) which is defined over a field, and from the quaternary Reed-Muller code $\mathrm{QRM}(r,m)$ (see Hammons, Kumar, Calderbank, Sloane and Solé (1994)) which generalises the quaternary representation of the Kerdock code.

We can measure the error correction capability of $\mathrm{RM}_{2h}(r,m)$ and $\mathrm{ZRM}_{2h}(r,m)$ in terms of their minimum Hamming distance and also their minimum Lee distance over $\mathbb{Z}_{2h}$ (see Peterson and Weldon (1972) for a definition). 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 obtain the following theorem:

Theorem 6.3. *Table 1 shows the minimum distances for the codes* $\mathrm{RM}_{2h}(r,m)$ *and* $\mathrm{ZRM}_{2h}(r,m)$ *for* $0 \leq r \leq m$.

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

Corollary 6.4. *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*

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

TABLE 1. Minimum distances of generalisations of Reed-Muller codes

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

where π is a permutation of the symbols $\{1,2,\ldots,m\}$, 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 lie in $\mathrm{ZRM}_{2h}(2,m)$, a code whose minimum Lee distance is 2^{m-1}. For h odd, the cosets lie in the code $\mathrm{RM}_{2h}(2,m)$, which has a smaller minimum Lee distance of 2^{m-2}.

We can also restate Corollary 5.2 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 6.5. *Each coset of $\mathrm{RM}_{2h}(1,m)$ in $\mathrm{ZRM}_{2h}(2,m)$ or in $\mathrm{RM}_{2h}(2,m)$ having a coset representative of the form*

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

where $0 \leq \ell \leq m$, $a_{jk} \in \mathbb{Z}_{2h}$ $(1 \leq j \leq \ell,\ 1 \leq k \leq m-\ell)$, Q' is an arbitrary quadratic form in ℓ variables and where π is a permutation of the symbols $\{1,2,\ldots,m\}$, 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. We concentrate on codes in which the alphabet size $2h$ is equal to 2^t for $t = 1, 2, 3$ and for which the number of carriers $n = 2^m$ is 16 or 32. 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. For example, information bits can be used partly 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. 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 with binary modulation. 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 at most 2. Using instead 8 of the 12 "Golay cosets", we obtain a code still having a PMEPR of at most 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 (see van Lint (1992)). These six cosets have representatives

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

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 concatenation 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 6.4 and 6.5 to identify variable numbers of cosets, again trading-off code rate, minimum distance and PMEPR.

As an 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 $\{2^{t-1}Q + \mathrm{RM}_{2^t}(1,m)\}$ over $\mathbb{Z}_{2^t}$ is equal to $2^{m-1} - 2^{(m-2)/2}$. For $m = 4$ and $t = 2$, we obtain a quaternary, length 16 OFDM code with rate 0.38, minimum Hamming distance 6, minimum Lee distance 8 and PMEPR of at most 2.

As another example, peculiar to the octary case, Davis and Jedwab (1999) noted the existence of 48 cosets of $\mathrm{RM}_8(1,4)$ in $\mathrm{ZRM}_8(2,4)$ having PMEPR of exactly 3 and Nieswand and Wagner (1998) gave a partial explanation for their existence. We can use these cosets to obtain a length 16 OFDM code with rate 0.42, minimum Hamming distance 4, minimum Lee distance 8 and PMEPR of 3.

There is a further set of options in the quaternary and octary cases: we can trade-off Lee distance against rate by moving from cosets chosen from $\mathrm{ZRM}_{2^t}(2,m)$ to cosets chosen from the larger set $\mathrm{RM}_{2^t}(2,m)$ (for $t = 2$ and 3 respectively). For example, Corollary 6.5 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 of which have PMEPR of at most 4.

8. Decoding Algorithms

In this section we outline decoding algorithms for codes of the type described in Section 7, all of which are the union of cosets of the linear code $\mathrm{RM}_{2h}(1,m)$.

One possible first step in obtaining a decoding algorithm for such a code is to apply an appropriate generalisation of the supercode decoding method, as described by Conway and Sloane (1986) for binary codes. The basic idea is to subtract in turn each possible coset representative from the received codeword and to decode the result as a codeword of $\mathrm{RM}_{2h}(1,m)$, the best decoding result over all cosets determining the coset representative.

Applying the supercode method in this way reduces the decoding problem to that of finding an efficient decoding algorithm for $\mathrm{RM}_{2h}(1,m)$. We outline two distinct approaches to this problem. The first approach, described in Section 8.1, 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, described in Section 8.2, 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 requiring 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 some of the codes described in Section 7 involve hundred or even thousands of cosets, and new decoding methods are clearly called for. Paterson and Jones (1998) describe such a method and give a detailed comparison of the many decoding strategies available.

8.1. A MAXIMUM LIKELIHOOD ALGORITHM

Grant and van Nee (1998) generalise the standard FHT decoding algorithm for the binary code $\mathrm{RM}(1,m)$ (see MacWilliams and Sloane (1986)) to the codes $\mathrm{RM}_{2h}(1,m)$. Let y denote 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 $\mathrm{RM}_{2^t}(1,m)$. In the quaternary case, the complex multiplications can be replaced by manipulations of real and imaginary parts.

8.2. AN ITERATIVE ALGORITHM

Davis and Jedwab (1999) give an iterative algorithm for decoding $\mathrm{RM}_{2^t}(1,m)$. The algorithm makes use of the fact that the componentwise 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 (suitably modified) 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.

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 significantly exceeds this limit.

The complexity of the algorithm for decoding $\mathrm{RM}_{2^t}(1,m)$ is approximately $tm2^m$ real additions. Furthermore the t decoding steps used to decode $\mathrm{RM}_{2^t}(1,m)$ can be interleaved with the supercode decoding method to obtain an algorithm for decoding arbitrary unions of cosets of $\mathrm{RM}_{2^t}(1,m)$ that can be much more efficient than a straightforward application of the supercode approach. The algorithm can easily be adapted for use in soft-decision as well as hard-decision decoding.

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 have given 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 described here will encourage further research. To this end, we close with what we consider to be some of the most interesting problems arising from 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 accounts for all the Golay sequences with these parameters. Is this the case?
- The case $\ell = 1$ of Corollary 6.5 identifies large numbers of Golay complementary quadruples contained in second-order cosets of $\mathrm{RM}_{2h}(1,m)$. But not all such quadruples occur in second-order cosets of $\mathrm{RM}_{2h}(1,m)$. Is there a simple description, not necessarily in terms of generalised Boolean functions, of all Golay complementary quadruples of length 2^m?
- As noted in Section 7, there are 48 cosets of $\mathrm{RM}_8(1,4)$ in the code $\mathrm{ZRM}_8(2,4)$ having PMEPR of exactly 3. This suggests that the words of these cosets might lie in triples with special correlation properties. (However these triples cannot be Golay complementary sets because such sets must be of even size over $\mathbb{Z}_8$). Explain this phenomenon, possibly building on the work of Nieswand and Wagner (1998).
- Corollary 6.5 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, since cosets can sometimes be partitioned into smaller sets (see Paterson (1999)), Corollary 6.5 does not always give an optimal result in terms of PMEPR. Find a generalisation which does.

- Cammarano and Walker (1997) and Paterson (1999) have identified circumstances in which Corollary 6.5 gives an optimal result by finding *lower* bounds on the PMEPR of second-order cosets of $\mathrm{RM}_{2h}(1,m)$. Find stronger or more widely applicable lower bounds.
- We noted in Section 7.1 that exactly 6 of the cosets of $\mathrm{RM}(1,4)$ making up the Kerdock code of length 16 are of the type appearing in Corollary 6.1. This yields a series of attractive OFDM coding options. For general even m, the size of the intersection of a Kerdock set of quadratic forms (see pp. 54–55 of van Lint (1992)) 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 $\mathcal{DG}(m,d)$ (see Chapters 15.5 and 21.8 of MacWilliams and Sloane (1986)) with the set of quadratic forms arising in the binary case of Corollary 5.2.

Acknowledgements

The first author thanks Hewlett-Packard for generous support during the time of this research.

References

Aldinger, M. (1994) Multicarrier COFDM scheme in high bitrate radio local area networks, in *5th IEEE Int. Symp. on Personal, Indoor and Mobile Radio Commun., The Hague*, pp.969–973.

Boyd, S. (1986) Multitone signals with low crest factor, *IEEE Trans. Circuits and Systems* **CAS-33**, 1018–1022.

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

Cammarano, M.W. and Walker, M.L. (1997) Integer maxima in power envelopes of Golay codewords, Technical Report TR-99-02, Dept. Math. Comp. Science, University of Richmond.

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

Davis, J.A. and Jedwab, J. (1999) Peak-to-mean power control in OFDM, Golay complementary sequences and Reed–Muller codes, *IEEE Trans. Inform. Theory*, to appear.

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

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

Golay, M.J.E. (1949) Multislit spectroscopy, *J. Opt. Soc. Amer.* **39**, 437–444.

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

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

Hammons, Jr., A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A. and Solé, P. (1994) The $\mathbb{Z}_4$–linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory* **40**, 301–319.

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

MacWilliams, F.J. and Sloane, N.J.A. (1986) *The Theory of Error–Correcting Codes*, North–Holland, Amsterdam.

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

Nieswand, K.M. and Wagner, K.N. (1998) Octary codewords with power envelopes of $3 * 2^m$, Technical Report TR-99-03, Dept. Math. Comp. Science, University of Richmond.

Paterson, K.G. (1999) Generalised Reed–Muller codes and power control in OFDM modulation, *IEEE Trans. Inform. Theory*, to appear.

Paterson, K.G. and Jones, A.E. (1998) Efficient decoding algorithms for generalised Reed-Muller codes, Technical Report HPL-98-195, Hewlett–Packard Labs., Bristol.

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

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

Shelswell, P. (1995) The COFDM modulation system: the heart of digital audio broadcasting, *Elec. Commun. Eng. J.*, June volume, 127–136.

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

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

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

J. Wolfmann (1999), Bent functions and coding theory, this volume.