2-13-1997

Peak-to-mean power control and error correction for OFDM transmission using Golay sequences and Reed-Muller codes

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

J Jedwab

Follow this and additional works at: [http://scholarship.richmond.edu/mathcs-faculty-publications](http://scholarship.richmond.edu/mathcs-faculty-publications)  
Part of the [Computer Sciences Commons](http://scholarship.richmond.edu/mathcs-faculty-publications), and the [Mathematics Commons](http://scholarship.richmond.edu/mathcs-faculty-publications)

**Recommended Citation**


This Article is brought to you for free and open access by the Math and Computer Science at UR Scholarship Repository. It has been accepted for inclusion in Math and Computer Science Faculty Publications by an authorized administrator of UR Scholarship Repository. For more information, please contact scholarshiprepository@richmond.edu.
Peak-to-mean power control and error correction for OFDM transmission using Golay sequences and Reed-Muller codes

J.A. Davis and J. Jedwab

Indexing terms: Frequency division multiplexing, Golay codes, Reed-Muller codes, Power control, Error correction

A coding scheme for OFDM transmission is proposed, exploiting a previously unrecognised connection between pairs of Golay complementary sequences and second-order Reed-Muller codes. The scheme solves the notorious problem of power control in OFDM systems by maintaining a peak-to-mean envelope power ratio of at most 3dB while allowing simple encoding and decoding at high code rates for binary, quaternary or higher-phase modulation schemes.

Introduction: Orthogonal frequency division multiplexing (OFDM) modulation schemes offer many advantages for multicarrier transmission at high data rates over time dispersive channels [1], particularly in mobile applications. The principal difficulty with such schemes is the need to control the peak-to-mean envelope power ratio (PMEPR) [2]. Any practical scheme must also allow good error correction, ease of encoding and decoding, and a high code rate.

The scheme of [2, 3] uses block coding to transmit across the N carriers only those binary sequences with small aperiodic autocorrelations is zero for all \( u \neq 0 \), and a pair of sequences is a Golay complementary pair if the sum of their aperiodic autocorrelations is zero for all \( u > 0 \). We shall call any sequence which is a member of a Golay complementary pair a Golay sequence. There are at least \( 2^m \) binary Golay sequences of length \( 2^m \) [6, 7]. These sequences are potentially available for OFDM transmission, as mentioned in [3], but hitherto it has not been apparent that they possess sufficient intrinsic structure to form a practical coding scheme. Indeed most authors have contrasted the analysis of aperiodic sequence properties, for which constrained computer search is often the best known method [8], with that of periodic sequence properties, for which powerful algebraic methods such as group theory and character theory are available [9].

For background on coding theory, the reader should refer to [10, 11].

Second-order Reed-Muller codes: We consider \( 0 \)-1 binary sequences of length \( 2^m \). Let \( x_i \) be the all-ones sequence. For \( i = 1, 2, ..., m \) let \( x_i \) be \( 2^m \) concatenated copies of the sequence comprising \( 2^{m-1} \) 0's followed by \( 2^{m-1} \) 1's. Then \( x_0, x_1, ..., x_m \) form the rows of a generator matrix for the first-order Reed-Muller code \( RM(1, m) \), and these sequences together with the componentwise products \( x_i x_j \) for \( 1 \leq i < j \leq m \) form the rows of a generator matrix for the second-order Reed-Muller code \( RM(2, m) \). Our central result is:

**Theorem 1**: The codeword \( \sum_{i=0}^{m-1} x_{i}(\pi) x_{i-(\pi)} + \sum_{N=0}^{m} c,N x_N \) is a binary Golay sequence of length \( 2^m \) for any permutation \( \pi \) of \( \{1, 2, ..., m\} \) and for any coefficients \( c, \in \{0,1\} \).

This shows how the \( 2^m \) binary Golay sequences given by Golay’s recursive and interleaving constructions [6] can be explicitly represented as \( 2^m \) distinct cosets of \( RM(1, m) \), each containing \( 2^m \) coset codewords.

The code consisting of all sequences identified in Theorem 1 is a subcode of \( RM(2, m) \) and therefore has a minimum distance of at least \( 2^m \). We can encode \( \log_2(m!^2) \) data bits as the choice of coset representative (for example, using a look-up table), and a further \( m+1 \) data bits directly as the \( c_N \). Received codewords can be efficiently decoded using standard hardware or software decoders for \( RM(2, m) \) (for example using majority-logic decoding [11]), recovering the coset representative from the coefficients of the terms \( x_N \).

**Corollary 1**: \( \log_2(m!^2) + m+1 \) data bits can be encoded as \( 2^m \) code bits such that all codewords have a PMEPR of at most \( 2^m \), and belong to \( RM(2, m) \).

For example, for \( m = 3 \) there are three choices of coset representative, namely \( x_1 x_2 x_3, x_1 x_3 x_2, x_2 x_1 x_3 \). Intermediate verification is often the best known method [8], with that of periodic sequence properties, for which powerful algebraic methods such as group theory and character theory are available [9].

The coding scheme of corollary 1 uses only Golay sequences to ensure the PMEPR is at most \( 2^m \). We can improve the code rate without unduly increasing the PMEPR by instead ordering the \( 2^m \) codewords according to the value of one data bit and add this coset representative to the encoded value \( \sum_N c_N x_N \) of four further data bits \((c_0, c_1, c_2, c_3)\) to produce an 8-bit transmitted code word.

Although certain aspects of Theorem 1 might, with hindsight and after careful consideration, be recognised in examples given in [7, 12], the connection with Reed-Muller codes and the consequent advantages for a practical coding scheme have not previously been noted.

The scheme of corollary 1 uses only Golay sequences to ensure the PMEPR is at most \( 2^m \). We can improve the code rate without unduly increasing the PMEPR by instead ordering the \( 2^m \) codewords according to the value of one data bit and add this coset representative to the encoded value \( \sum_N c_N x_N \) of four further data bits \((c_0, c_1, c_2, c_3)\) to produce an 8-bit transmitted code word.

Although certain aspects of Theorem 1 might, with hindsight and after careful consideration, be recognised in examples given in [7, 12], the connection with Reed-Muller codes and the consequent advantages for a practical coding scheme have not previously been noted.

The coding scheme of corollary 1 uses only Golay sequences to ensure the PMEPR is at most \( 2^m \). We can improve the code rate without unduly increasing the PMEPR by instead ordering the \( 2^m \) codewords according to the value of one data bit and add this coset representative to the encoded value \( \sum_N c_N x_N \) of four further data bits \((c_0, c_1, c_2, c_3)\) to produce an 8-bit transmitted code word.

Although certain aspects of Theorem 1 might, with hindsight and after careful consideration, be recognised in examples given in [7, 12], the connection with Reed-Muller codes and the consequent advantages for a practical coding scheme have not previously been noted.

The coding scheme of corollary 1 uses only Golay sequences to ensure the PMEPR is at most \( 2^m \). We can improve the code rate without unduly increasing the PMEPR by instead ordering the \( 2^m \) codewords according to the value of one data bit and add this coset representative to the encoded value \( \sum_N c_N x_N \) of four further data bits \((c_0, c_1, c_2, c_3)\) to produce an 8-bit transmitted code word.

Although certain aspects of Theorem 1 might, with hindsight and after careful consideration, be recognised in examples given in [7, 12], the connection with Reed-Muller codes and the consequent advantages for a practical coding scheme have not previously been noted.
Polyphase sequences: Theorem 1 generalises naturally to polyphase sequences:

Theorem 2: The codeword \(2^m \sum_{i=0}^{m-1} x_i \rho_i + \sum_{i=m}^{2m-1} c_i \rho_i\) is a 2-phase Golay sequence of length \(2^m\) for any permutation \(\pi\) of \(\{1, 2, \ldots, m\}\) and for any coefficients \(c_i \in \{0, 1, 2, 1\}\).

This explicitly determines \(2^m \rho_m / 2\) 2-phase Golay sequences and so provides a polyphase coding scheme analogous to Corollary 1. In the quaternary case \(2^2 = 4\) these sequences occur as \(\rho_m / 2\) cosets of \(ZRM(1,m)\) in \(ZRM(2,m)\), each containing \(4^m\) codewords (see [13] for the definition of the quaternary Reed-Muller code under which \(ZRM(2,m)\) maps to \(\mathbb{Z}_{RM}(1,m)\)). Received quaternary codewords can be efficiently decoded in the binary domain by applying the Gray map, under which \(ZRM(2,m)\) maps to \(RM(2m+1,13)\). For higher phases \(2^2 = 8, 16, \ldots\), Theorem 2 indicates an appropriate definition for the corresponding first-order and second-order Reed-Muller code. For all values of \(2^n\), theorem 2 provides a coding scheme in which \(\log_2 (m!/2)^{1+m+1}\) data symbols can be encoded as \(2^n\) code symbols such that all codewords have a PMEPR of at most 2 and have a minimum Hamming distance of at least \(2^m/2\).

We can find similar variations on this scheme as described for the binary case, for example the code rate can be increased while maintaining the minimum Hamming distance.

A very recent paper [14] reports the independent investigation of the use of Golay sequences in OFDM schemes. Translated into the language of the present paper, [14] essentially identifies a subset of the polyphase Golay sequences of theorem 2 involving \(m\) of the \(m!/2\) coset representatives and arbitrary \(c_i\), noting that when only one coset representative is used the minimum Hamming distance between codewords is \(2^m - 1\). However, [14] does not make the connection with first- or second-order Reed-Muller codes and in particular does not propose the use of efficient decoding techniques for Reed-Muller codes. [14] also does not determine the minimum Hamming distance when more than one coset representative is used (except in the case \(m = 3\)).

Conclusion: We have outlined a coding scheme in which the main criteria for a practical OFDM transmission system are simultaneously satisfied. Details of the results announced here will be provided in a forthcoming paper, including proofs of the claimed theorems 1 and 2, how to combine the identified Golay sequences into Golay complementary pairs, details of the decoding algorithms, and comparison of implementation options according to choice of code rate, PMEPR, minimum Hamming distance and number of phases.

Acknowledgments: We are grateful to T. Wilkinson and J. Jones for helpful discussions that led to this research. J.A. Davis thanks Hewlett-Packard for generous hospitality and support during his sabbatical year 1995–6.

© IEE 1997

12 December 1996

J.A. Davis (Department of Mathematics and Computer Science, University of Richmond, Virginia 23173, USA)

J. Jedwab (Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol BS12 6QZ, United Kingdom)

References


