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

Recommended Citation
Davis, James A., and J. Jedwab. "Peak-to-mean Power Control and Error Correction for OFDM Transmission Using Golay Sequences and Reed-Muller Codes." *Electronics Letters* 33, no. 4 (February 13, 1997): 267-68. doi:10.1049/el:19970205.

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 signalling together with good error correction.

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 PMEPR. However, this entails an exhaustive search to identify the best sequences, requires large look-up tables for encoding and decoding, and leaves the problem of error correction unresolved. The scheme of [4] instead takes the transmitted codewords from a coset of a linear error-correcting code, choosing the coset representative or 'mask vector' by computationally intensive search in order to reduce the PMEPR. In this way the error correction properties are assured but the appropriate choice of linear code and coset representative for optimal PMEPR remains an open problem.

The PMEPR of a binary or polyphase sequence of length N can be as large as N, but if the sequence is constrained to be a member of a Golay complementary pair then its PMEPR is at most 2, as recognised in [5]. (The aperiodic autocorrelation function of a sequence $(a_1, a_2, \ldots a_N)$ for which $a_i \in \{0, 1, \ldots, M-1\}$ is $C(u) = \Sigma_{i=1}^{N-u}\exp(2\pi j(a_i-a_{i+u})/M)$ for $u \geq 0$, 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 $2^m m!$ binary Golay sequences of length 2^m [6, 7]. These sequences are potentially suitable 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_0 be the all-ones sequence. For $i = 1, 2, \ldots, m$ let x_i be 2^{i-1} concatenated copies of the sequence comprising 2^{m-i} 0's followed by 2^{m-i} 1's. Then $x_0, x_1, \ldots, x_m$ 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 $\Sigma_{i=1}^{m-1} x_{\pi(i)} x_{\pi(i+1)} + \Sigma_{i=0}^{m} c_i x_i$ is a binary Golay sequence of length 2^m for any permutation π of $\{1,2, \ldots, m\}$ and for any coefficients $c_i \in \{0,1\}$.

This shows how the $2^m m!$ binary Golay sequences given by Golay's recursive and interleaving constructions [6] can be explicitly represented as $m!/2$ distinct cosets ol RM(1, m), each containing 2^{m+1} 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-2}, We can encode $\lfloor \log_2(m!/2) \rfloor$ 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_i. 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 $x_i x_j$.

Corollary 1: $\lfloor \log_2(m!/2) \rfloor + m + 1$ data bits can be encoded as 2^m code bits such that all codewords have a PMEPR of at most 2, have a minimum distance of at least 2^{m-2}, and belong to RM(2, m).

For example, for $m = 3$ there are three choices of coset representative, namely $x_1x_2+x_2x_3 = 00010010$, $x_1x_3+x_2x_3 = 00010100$ and $x_1x_2+x_1x_3 = 00000110$. We select one of two coset representatives (say the first two) according to the value of one data bit and add this coset representative to the encoded value $\Sigma_i c_i x_i$ of four further data bits (c_1,c_2,c_3,c_4) to produce an 8-bit transmitted codeword.

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. We can improve the code rate without unduly increasing the PMEPR by instead ordering the $2^{m(m-1)/2}$ coset representatives of RM(1, m) within RM(2, m), in increasing order of maximum PMEPR over the coset, and then selecting coset representatives from the ordered list. For example, by allowing any coset representative from the first half of the ordered list we can encode up to $m(m+1)/2$ data bits while retaining a minimum distance of 2^{m-2}. In the case of length 16 codewords, this increases the number of data bits from 8 to 10 while retaining a mimmum distance of 4 by using 32 rather than 8 coset representatives, and yet the maximum PMEPR only increases from 2 to 4 (whereas it would be 16 if any transmitted sequence were allowed).

Alternatively, we can increase the minimum distance in corollary 1 in exchange for a small reduction in code rate by choosing a subset of the $m!/2$ coset representatives for Golay sequences identified in theorem 1. All such coding schemes retain a PMEPR of at most 2. The extreme version is to use just one coset representative so that the code is a single coset of RM(1, m) with a minimum distance of 2^{m-1}, encoding $m+1$ data bits (and taking advantage of special decoding algorithms for RM(1, m) [11]). Intermediate versions can also be found. For example, in the case of length 16 codewords we can increase the minimum distance from 4 to 6 by reducing the number of data bits from 8 to 7.

Polyphase sequences: Theorem 1 generalises naturally to polyphase sequences:

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

This explicitly determines $2^{l(m+1)} \cdot m!/2$ 2^l-phase Golay sequences and so provides a polyphase coding scheme analogous to Corollary 1. In the quaternary case $2^l = 4$ these sequences occur as $m!/2$ cosets of ZRM($1,m$) in ZRM($2,m$), each containing 4^{m+1} codewords (see [13] for the definition of the quaternary Reed-Muller code ZRM(r, 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($2,m+1$) [13]. For higher phases 2^l = 8, 16, ..., Theorem 2 indicates an appropriate definition for the corresponding first-order and second-order Reed-Muller code. For all values of 2^l, theorem 2 provides a coding scheme in which $\lfloor \log_{2^l}(m!/2) \rfloor + m + 1$ data symbols can be encoded as 2^m 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 A. 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.

12 December 1996
Electronics Letters Online No: 19970205

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

1 BINGHAM, J.A.C.: 'Multicarrier modulation for data transmission: an idea whose time has come', *IEEE Commun. Mag.*, 1990, **28**, pp. 5–14

2 JONES, A.E., WILKINSON, T.A., and BARTON, S.K.: 'Block coding scheme for reduction of peak to mean envelope power ratio of multicarrier transmission scheme', *Electron. Lett.*, 1994, **30**, pp. 2098–2099

3 WILKINSON, T A., and JONES, A.E.: 'Minimisation of the peak to mean envelope power ratio of multicarrier transmission schemes by block coding'. Proc. IEEE 45th Veh. Technol. Conf., Chicago, July 1995, pp. 825–829

4 JONES, A.E., and WILKINSON, T.A.: 'Combined coding for error control and increased robustness to system nonlinearities in OFDM'. Proc. IEEE 46th Veh. Technol. Conf., Atlanta, April–May 1996, pp. 904–908

5 POPOVIC, B.M.: 'Synthesis of power efficient multitone signals with flat amplitude spectrum', *IEEE Trans. Commun.*, 1991, **39**, pp. 1031–1033

6 GOLAY, M.J.E.: 'Complementary series', *IRE Trans. Inf. Theory*, 1961, **7**, pp. 82–87

7 GOLAY, M.J.E.: 'Sieves for low autocorrelation binary sequences', *IEEE Trans. Inf. Theory*, 1977, **23**, pp. 43–51

8 GOLAY, M.J.E., and HARRIS, D.B.: 'A new search for skewsymmetric binary sequences with optimal merit factors', *IEEE Trans. Inf. Theory*, 1990, **36**, pp. 1163–1166

9 POTT, A.: 'Finite geometry and character theory'. Lecture Notes in Mathematics 1601, (Springer-Verlag, Berlin 1995)

10 VAN LINT, J.H.: 'Introduction to coding theory'. (Springer-Verlag, Berlin 1992), 2nd Edn.

11 MacWILLIAMS, F.J., and SLOANE, N.J.A.: 'The theory of error-correcting codes' (North-Holland, Amsterdam 1986)

12 BUDISIN, S.Z.: 'New complementary pairs of sequences', *Electron. Lett.*, 1990, **26**, pp. 881–883

13 HAMMONS, A.R., KUMAR, P.V., CALDERBANK, A.R., SLOANE, N.J.A., and SOLE, P.: 'The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes', *IEEE Trans. Inf. Theory*, 1994, **40**, pp. 301–319

14 VAN NEE, R.D.J.: 'OFDM codes for peak-to-average power reduction and error correction'. Proc. IEEE Globecom, London, November 1996, pp. 740–744