Bounds on the PMEPR of Translates of Binary Codes

Kai-Uwe Schmidt

26 July 2010 (revised 23 September 2010)

.

Abstract

The use of error-correcting codes for tight control of the peak-to-mean envelope power ratio (PMEPR) in orthogonal frequency-division multiplexing (OFDM) transmission is considered. A well-known approach for the construction of such codes is to take a code that is good in the classical coding-theoretic sense and to choose a translate of this code that minimizes the PMEPR. A fundamental problem is to determine the minimum PMEPR over all translates of a given code. Motivated by a recent lower bound for this minimum, an existence result is presented here. Roughly speaking, given a code $\mathcal{C}$ of sufficiently large length n, there exists a translate of $\mathcal{C}$ with PMEPR at most $k\log(|\mathcal{C}|n^{1+\epsilon})$ for all $\epsilon > 0$ and for some k independent of n. This result is then used to show that for $n \geq 32$ there is a translate of the lengthened dual of a binary primitive t-error-correcting BCH code with PMEPR at most $8(t+2)\log n$.

Keywords

code, dual BCH code, orthogonal frequency-division multiplexing (OFDM), peak-to-mean envelope power ratio (PMEPR), translate

1 Introduction

Orthogonal frequency-division multiplexing (OFDM) is a key concept in the development of wired and wireless communications systems in the past decade. It provides excellent ability to cope with multipath propagation and fast-moving environment. On the other hand, a principal drawback of OFDM is the typically high peak-to-mean envelope power ratio (PMEPR) of uncoded OFDM signals. That is, the peak transmit power can be many times the average transmit power.

In order to ensure a distortionless transmission, all components in the transmission chain must be linear across a wide range of signal levels. This results in power inefficiency, which is particularly severe in mobile applications, where battery lifetime is a major concern. On the other hand,

Kai-Uwe Schmidt is with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC V5A 1S6, Canada. He is supported by Deutsche Forschungsgemeinschaft (German Research Foundation) under Research Fellowship SCHM 2609/1-1. Email: kuschmidt@sfu.ca

nonlinearities in the transmission chain can lead to a loss of orthogonality among the carriers and to out-of-band radiation. The former has the effect of degrading the total system performance and the latter is subject to strong regulations.

In this letter, we consider biphase modulation of the OFDM subcarriers. Let $F = \mathrm{GF}(2)$ be the finite field containing two elements. For any word $c \in F^n$, write $c = (c_0, c_1, \ldots, c_{n-1})$. Given $c \in F^n$, the OFDM modulator outputs the complex baseband signal

$$S_c(\theta) = \sum_{j=0}^{n-1} (-1)^{c_j} e^{\sqrt{-1}2\pi j\theta} \quad \text{for } 0 \le \theta < 1.$$

The *PMEPR of this signal* (or of the modulating word c) is given by

$$\mathrm{PMEPR}(c) := \frac{1}{n} \sup_{0 \le \theta < 1} |S_c(\theta)|^2.$$

By a (binary) *code of length* n we mean a nonempty subset of F^n. Given a code $\mathcal{C}$, the *PMEPR of* $\mathcal{C}$ is defined to be

$$\mathrm{PMEPR}(\mathcal{C}) := \max_{c \in \mathcal{C}} \mathrm{PMEPR}(c).$$

Note that each linear code of length n has PMEPR equal to n, which is caused by the existence of the all-zero word in the code.

The general objective is to construct codes of a given length n having high rate, large minimum Hamming distance, and small PMEPR. Explicit code constructions with small PMEPR are scarce; we refer to [1] for a good overview. In this letter, we analyze a simple approach by Jones and Wilkinson [2] to construct codes with given minimum Hamming distance and small PMEPR. This method will be described next. Given $s \in F^n$, a *translate* of a code $\mathcal{C}$ of length n is defined to be

$$s + \mathcal{C} := \{s + c : c \in \mathcal{C}\}.$$

If $\mathcal{C}$ is linear, then a translate of $\mathcal{C}$ is a *coset* of $\mathcal{C}$, and there are exactly $2^n/|\mathcal{C}|$ such cosets. Note that the rate and the minimum Hamming distance of each translate of a code $\mathcal{C}$ equal those of the original code. The idea of [2] is to take a known code and to choose a translate of this code with reduced PMEPR. Compared to many other approaches to construct codes with small PMEPR, the advantage of this method is that encoding and decoding is standard (by choosing an appropriate original code).

The following existence result was obtained by Litsyn and Wunder [3, Thm. 15]. Given a code $\mathcal{C}$ of length n, there exists an $s \in F^n$ such that, for all real λ, the proportion of codewords in $s + \mathcal{C}$ with PMEPR at least λ is at most the proportion of codewords in F^n with PMEPR at least λ. However, this does not ensure the existence of translates with PMEPR significantly less than its worst-case value, namely n.

Ideally, given a code $\mathcal{C}$ of length n, we would like to find a translate of $\mathcal{C}$ with minimum PMEPR. However, except for small n, the computation of a translate with minimum PMEPR is a difficult problem in combinatorial optimization. A feasible solution is currently unknown, although suboptimal algorithms have been proposed in the literature [2], [4], [5]. In order to asses the outcome of such an algorithm, it is of importance to have information about the minimum PMEPR over all translates of the input code $\mathcal{C}$. In [6] the author proved a lower bound for this minimum. This bound depends on the *covering radius* of $\mathcal{C}$, which is defined to be

$$\rho(\mathcal{C}) := \max_{s \in F^n} \min_{c \in \mathcal{C}} d(s, c),$$

where $d(s, c)$ is the Hamming distance between s and c.

Proposition 1 ([6, Thm. 2]). *Let $\mathcal{C}$ be a code of length n, and suppose that $\rho(\mathcal{C}) \leq \frac{n}{2}$. Then, for each $s \in F^n$, we have*

$$\mathrm{PMEPR}(s + \mathcal{C}) \geq \frac{1}{n} \left(n - 2\rho(\mathcal{C})\right)^2 .$$

This bound was derived in [6] as part of a more general result that holds for nonbinary translates of $\mathcal{C}$. The result was used in [6] to show that for many families of codes it is impossible to reduce the PMEPR significantly by taking translates of them. For example, every translate of a linear code $\mathcal{C}$ of length n with rate $R \geq \frac{1}{2}$ must have PMEPR at least $4n(R - \frac{1}{2})^2$, which depends linearly on n.

On the other hand, [6] exhibits code families for which Proposition 1 imposes very weak restrictions on the PMEPR of its translates, among them are the duals of the binary primitive BCH codes. This motivates further investigation of the minimum PMEPR over all their translates.

The main result of this letter, to be proved in Section 2, is roughly speaking the following. Given a code $\mathcal{C}$ of length n, then for sufficiently large n there is a translate of $\mathcal{C}$ having PMEPR at most $k \log(|\mathcal{C}| n^{1+\epsilon})$ for all $\epsilon > 0$ and some k independent of n. We then apply this result in Section 3 to the lengthened duals of binary primitive t-error-correcting BCH codes to show that for $n \geq 32$ there is a translate of such a code with PMEPR at most $8(t + 2) \log n$. This answers a question raised by Paterson and Tarokh [7].

2 Main Result

We begin with a standard result from probability theory, known as Hoeffding's inequality.

Lemma 2 ([8, Thm. 2]). *Let $X_0, X_1, \ldots, X_{n-1}$ be independent random variables satisfying $\mathbb{E}(X_j) = 0$ and $|X_j| \leq 1$ for all j satisfying $0 \leq j < n$. Then, for all real $\lambda \geq 0$,*

$$\Pr\left(\left(\sum_{j=0}^{n-1} X_j \right)^2 \geq \lambda \right) \leq 2\, e^{-\frac{\lambda}{2n}} .$$

We shall also need the following lemma that allows us to compute an upper bound for the PMEPR of a codeword $c \in F^n$ from N equi-spaced samples of its associated signal, whenever $N > n$.

Lemma 3 ([1, Thm. 4.8]). *Let $K > 1$ be such that Kn is integer. Then, for each $c \in F^n$, we have*

$$\mathrm{PMEPR}(c) \leq \frac{1}{\left(\cos \frac{\pi}{2K}\right)^2} \, \frac{1}{n} \max_{0 \leq \ell < Kn} \left| S_c\left(\tfrac{\ell}{Kn}\right) \right|^2 .$$

Our main result is the following.

Theorem 4. *Let $\mathcal{C}$ be a code of length n. Let $K > 1$ be such that Kn is integer, and let $\epsilon > 0$ be real. Then there exists $s \in F^n$ such that*

$$\mathrm{PMEPR}(s + \mathcal{C}) \leq \frac{4}{\left(\cos \frac{\pi}{2K}\right)^2} \log\left(|\mathcal{C}|\, n^{1+\epsilon}\right) \tag{1}$$

for each $n \geq n_0$, where n_0 is the smallest integer n that satisfies

$$\frac{4K}{n^\epsilon} < 1 - \frac{1}{2^n}. \tag{2}$$

Proof. We regard s to be drawn randomly from the sample space F^n, whose 2^n elements each occur with the same probability $\frac{1}{2^n}$. Write

$$a(n) := 4n \log(|\mathcal{C}|\, n^{1+\epsilon}), \tag{3}$$

let $c \in F^n$, and let θ be real. Then

$$\begin{aligned}\Pr\Big(\big|S_{s+c}(\theta)\big|^2 \geq a(n)\Big) \leq{}& \Pr\Big(\big(\Re[S_{s+c}(\theta)]\big)^2 \geq \tfrac{1}{2}a(n)\Big) \\ &+ \Pr\Big(\big(\Im[S_{s+c}(\theta)]\big)^2 \geq \tfrac{1}{2}a(n)\Big),\end{aligned} \tag{4}$$

where $\Re[z]$ and $\Im[z]$ denote the real and the imaginary part of $z \in \mathbb{C}$, respectively. Writing $s = (s_0, s_1, \ldots, s_{n-1})$ and $c = (c_0, c_1, \ldots, c_{n-1})$, we have

$$\begin{aligned}\Re(S_{s+c}(\theta)) &= \sum_{j=0}^{n-1} (-1)^{s_j + c_j} \cos(2\pi j\theta) \\ \Im(S_{s+c}(\theta)) &= \sum_{j=0}^{n-1} (-1)^{s_j + c_j} \sin(2\pi j\theta).\end{aligned}$$

We can therefore use Lemma 2 to bound the probabilities on the right-hand side of (4). This gives

$$\Pr\Big(\big|S_{s+c}(\theta)\big|^2 \geq a(n)\Big) \leq 4\, e^{-\frac{a(n)}{4n}}.$$

Now by a crude estimate,

$$\begin{aligned}&\Pr\Big(\max_{c\in\mathcal{C}} \max_{0\leq\ell<Kn} \big|S_{s+c}(\tfrac{\ell}{Kn})\big|^2 \geq a(n)\Big) \\ &\quad\leq \sum_{c\in\mathcal{C}} \sum_{\ell=0}^{Kn-1} \Pr\Big(\big|S_{s+c}(\tfrac{\ell}{Kn})\big|^2 \geq a(n)\Big) \\ &\quad\leq 4Kn|\mathcal{C}|\, e^{-\frac{a(n)}{4n}}.\end{aligned}$$

Using the definition (3) of $a(n)$, this is equivalent to

$$\Pr\Big(\max_{c\in\mathcal{C}} \max_{0\leq\ell<Kn} \big|S_{s+c}(\tfrac{\ell}{Kn})\big|^2 \geq 4n \log(|\mathcal{C}|\, n^{1+\epsilon})\Big) \leq \frac{4K}{n^\epsilon}. \tag{5}$$

The assumption (2) implies that this probability is strictly less than $1 - \frac{1}{2^n}$, so there must be at least one $s \in F^n$ for which

$$\max_{c\in\mathcal{C}} \max_{0\leq\ell<Kn} \big|S_{s+c}(\tfrac{\ell}{Kn})\big|^2 \leq 4n \log(|\mathcal{C}|\, n^{1+\epsilon}). \tag{6}$$

The theorem follows from Lemma 3. □

We remark that, since the probability in (5) tends to zero as $n \to \infty$, the proof of the theorem shows in fact that the conclusion of the theorem holds for almost all s, that is, for all s in F^n except a fraction of F^n that tends to zero as $n \to \infty$.

We also note that the constant in (1) can be improved. In (4), we have estimated the magnitude of $S_{s+c}(\theta)$ by inspecting the magnitudes of the real and imaginary parts of $S_{s+c}(\theta)$. This approach can be generalized by projecting $S_{s+c}(\theta)$ onto more than two lines through the origin in the complex plane, leading to a slightly better constant (see [1, Sec. 4.5] for details).

3 Application to Lengthened Duals of BCH Codes

In this section we apply our results to the lengthened dual of the binary primitive t-error-correcting BCH code.

Let $m \geq 2$ be integer. For $1 \leq 2t-1 \leq 2^{\lfloor m/2 \rfloor}$, let $\mathcal{C}_t^-$ be the dual of the binary primitive t-error-correcting BCH code of length $2^m - 1$. It is well known [9, p. 281] that $\mathcal{C}_t^-$ is a linear code of length $2^m - 1$, dimension mt, and minimum Hamming distance at least $2^{m-1} - (t-1)2^{m/2}$.

By lengthening $\mathcal{C}_t^-$, we obtain the code $\mathcal{C}_t$, which is a linear code of length $n = 2^m$, dimension $mt + 1$, and minimum Hamming distance at least $2^{m-1} - (t-1)2^{m/2}$. Letting α be a primitive element in $\mathrm{GF}(2^m)$, a generator matrix for $\mathcal{C}_t$ is given by

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 0 & 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(n-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 1 & \alpha^{2j-1} & \alpha^{(2j-1)2} & \cdots & \alpha^{(2j-1)(n-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 1 & \alpha^{2t-1} & \alpha^{(2t-1)2} & \cdots & \alpha^{(2t-1)(n-1)} \end{pmatrix}, \tag{7}$$

where, as usual, an element $\beta \in \mathrm{GF}(2^m)$ is replaced by its corresponding vector of size $m \times 1$ containing the coordinates of β relative to a fixed basis for $\mathrm{GF}(2^m)$ over $\mathrm{GF}(2)$. Note that a generator matrix for $\mathcal{C}_t^-$ is obtained from (7) by deleting the first row and the first column.

Paterson and Tarokh [7, Cor. 18] proved that every nonconstant codeword of $\mathcal{C}_t$ has PMEPR at most

$$(2t-1)^2 \left(\tfrac{2}{\pi} \log n + \tfrac{2}{\pi} \log 2 + 3\right)^2, \tag{8}$$

and noted [7, p. 1985] that, by taking translates of $\mathcal{C}_t$, it may be possible to obtain a significant reduction of the PMEPR. In what follows we analyze the PMEPR of translates of $\mathcal{C}_t$.

We first discuss the lower bound given in Proposition 1. It is known [10] that the covering radius of $\mathcal{C}_t^-$ is bounded above by

$$\rho(\mathcal{C}_t^-) \leq 2^{m-1} - 1 - \left(\sqrt{t} - \sqrt[6]{t}\right)\sqrt{2^m - t - 2}.$$

It is readily verified that $\rho(\mathcal{C}_t) \leq \rho(\mathcal{C}_t^-) + 1$, which gives

$$\rho(\mathcal{C}_t) \leq \frac{n}{2} - \left(\sqrt{t} - \sqrt[6]{t}\right)\sqrt{n - t - 2}.$$

We then find from Proposition 1 that for all $s \in F^n$ we have

$$\mathrm{PMEPR}(s + \mathcal{C}_t) \geq 4\left(\sqrt{t} - \sqrt[6]{t}\right)^2 \frac{n - t - 2}{n}.$$

This bound is asymptotically independent of n. Noting that $|\mathcal{C}_t| = 2n^t$, application of Theorem 4 with $K = 2$ and $\epsilon = \frac{3}{4}$ gives the following existence result.

Corollary 5. *Let $\mathcal{C}_t$ be the code of length $n = 2^m$ as defined above. Then there exists $s \in F^n$ such that*

$$\mathrm{PMEPR}(s + \mathcal{C}_t) \leq 8(t+2)\log n \tag{9}$$

for each $m \geq 5$.

The leading constant in (9) can be clearly improved, especially for large m. The essential point is that the PMEPR of translates of $\mathcal{C}_t$ can be $O(\log n)$ as $n \to \infty$, whereas (8) asserts that the PMEPR of the nonconstant codewords of $\mathcal{C}_t$ is $O((\log n)^2)$ as $n \to \infty$. Moreover, by the remark after Theorem 4, a translate $s + \mathcal{C}_t$ will satisfy (9) almost surely for large n.

4 Discussion

We have shown that for sufficiently large n there exists a translate of a code $\mathcal{C}$ of length n whose PMEPR is roughly logarithmic in $|\mathcal{C}|n$. For many codes however (including for our example) there is still a large gap between the lower bound, given in Proposition 1, and the existence result, given in Theorem 4. It is known that the lower bound is best possible in certain nontrivial cases. One example is $\mathcal{C}_1$, which is the first-order Reed–Muller code. By assuming a particular ordering of the coordinates of $\mathcal{C}_1$, Davis and Jedwab [11] exhibited cosets of $\mathcal{C}_1$ with PMEPR at most 2. Proposition 1 implies [6, Cor. 8] that this is best possible at least for $m \in \{3, 5, 7\}$. This does however not mean that the upper bound in Theorem 4 can be significantly improved. Notice that the bounds in Proposition 1 and Theorem 4 hold uniformly for all codes obtained by permuting the n coordinates of a given code of length n, and it might be possible that the minimum PMEPR over all translates of a code strongly depends on the ordering of its coordinates. We leave potential improvements of the upper and lower bounds on the minimum PMEPR over all translates of a given code as a challenging open problem.

References

[1] S. Litsyn, *Peak power control in multicarrier communications.* Cambridge University Press, 2007.

[2] A. E. Jones and T. A. Wilkinson, "Combined coding for error control and increased robustness to system nonlinearities in OFDM," *Proc. of IEEE 46th Vehicular Technology Conf. (VTC), Atlanta, GA*, pp. 904–908, Apr. 1996.

[3] S. Litsyn and G. Wunder, "Generalized bounds on the crest-factor distribution of OFDM signals with applications to code design," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 992–1006, Mar. 2006.

[4] V. Tarokh and H. Jafarkhani, "On the computation and reduction of the peak-to-average power ratio in multicarrier communications," *IEEE Trans. Commun.*, vol. 48, no. 1, pp. 37–44, Jan. 2000.

[5] G. Wunder and H. Boche, "A baseband model for computing the PAPR in OFDM systems," *Proc. of 4th Int. Conf. Source and Channel Coding, Berlin, Germany*, pp. 273–280, Jan. 2002.

[6] K.-U. Schmidt, "On the peak-to-mean envelope power ratio of phase-shifted binary codes," *IEEE Trans. Commun.*, vol. 56, no. 11, pp. 1816–1823, Nov. 2008.

[7] K. G. Paterson and V. Tarokh, "On the existence and construction of good codes with low peak-to-average power ratios," *IEEE Trans. Inf. Theory*, vol. 46, no. 6, pp. 1974–1987, Sep. 2000.

[8] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *J. Amer. Stat. Assoc.*, vol. 58, no. 301, pp. 13–30, Mar. 1963.

[9] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.

[10] A. A. Tietäväinen, "An upper bound on the covering radius as a function of the dual distance," *IEEE Trans. Inf. Theory*, vol. 36, no. 6, pp. 1472–1474, Nov. 1990.

[11] J. A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed–Muller codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2397–2417, Nov. 1999.