Bounds on Envelope Power of Trace Codes for OFDM

Kenneth G. Paterson
Extended Enterprise Laboratory
HP Laboratories Bristol
HPL-98-176
October, 1998

OFDM, multicarrier, modulation, power, PMEPR, simplex code, dual BCH code, exponential sums, Lagrange interpolation, Galois rings

Bounds for exponential sums over finite fields and Galois rings are combined with Lagrange interpolation to obtain bounds on the peak-to-mean envelope power ratio (PMEPR) of a variety of OFDM coding schemes obtained from trace codes. This class of codes includes the binary simplex code, duals of binary, primitive BCH codes and a variety of their $\mathbb{Z}_{2^e}$- analogues.

Internal Accession Date Only

Bounds on Envelope Power of Trace Codes for OFDM

Kenneth G. Paterson,
Hewlett-Packard Laboratories,
Filton Road, Stoke-Gifford,
Bristol BS12 6QZ, U.K.

Abstract

Bounds for exponential sums over finite fields and Galois rings are combined with Lagrange interpolation to obtain bounds on the peak-to-mean envelope power ratio (PMEPR) of a variety of OFDM coding schemes obtained from trace codes. This class of codes includes the binary simplex code, duals of binary, primitive BCH codes and a variety of their $\mathbb{Z}_{2^e}$-analogues.

Keywords

OFDM; multicarrier; modulation; power; PMEPR; simplex code; dual BCH code; exponential sums; Lagrange interpolation; Galois rings.

I. Introduction

Orthogonal Frequency Division Multiplexing (OFDM) is a multicarrier modulation technique with the potential to allow reliable transmission at high rates over highly time dispersive channels at low signal-to-noise ratios [4]. When combined with powerful error-correction codes, the technique is well suited to the harsh, non-Gaussian, multi-path noise environment inherent in mobile radio applications. OFDM has been proposed for use in wireless LANs [2], ADSL wire-line modems [5] and digital audio and video broadcasting [1].

A q-phase n-carrier OFDM signal with carrier frequencies $f_0 + j\Delta f, (0 \leq j < n)$ may be represented as the real part of the complex-valued function:

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

where the data-bearing sequence $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$, $a_j \in \mathbb{Z}_q$, is called an OFDM codeword and $\omega = e^{2\pi i/q}$ is a complex q-th root of unity. In a practical OFDM system, q will be a power of 2. The instantaneous envelope power of the OFDM signal is defined to be the function $P(\mathbf{a})(t) = |S(\mathbf{a})(t)|^2$. This function bounds the actual transmit power of the OFDM signal $\Re(S_{\mathbf{a}}(t))$ and it is easily shown to have average value equal to n. The peak-to-mean envelope power ratio (PMEPR) of the OFDM signal (and the codeword $\mathbf{a}$) is defined to be $\frac{1}{n}\max_t P(\mathbf{a})(t)$. Notice that the maximum PMEPR over all length n OFDM codewords $\mathbf{a}$ is equal to n, the number of carriers (this maximum is attained by the all-zero word at $t = 0$, for example).

The major barrier to the widespread acceptance of OFDM is the high PMEPR of uncoded OFDM signals. If the peak transmit power is limited, either by regulatory or application constraints, this has the effect of reducing the mean power allowed under OFDM relative to that under constant power modulation techniques. This in turn reduces the range of OFDM transmissions. Moreover, to prevent spectral growth of the OFDM signal in the form of intermodulation amongst subcarriers and out-of-band radiation, either highly linear power amplifiers must be used, or non-linear amplifiers with a higher nominal power rating must operated inefficiently in their linear region (i.e. with a large input

back-off). Either option leads to the use of more expensive components than are needed with other modulation techniques.

A number of approaches have been proposed to deal with this power control problem [7], [11], [18], [23], [34]. A simple idea introduced in [14] and developed further in [33] is to select for transmission those codewords which minimise or reduce the PMEPR. A more sophisticated approach adopted in [13] is to use codewords drawn from an additive offset of a linear code $\mathcal{C}$. The idea is to choose $\mathcal{C}$ for its error-correcting properties and the offset to reduce the PMEPR of the resulting coded OFDM transmissions. This approach enjoys the twin benefits of power control and error-correction and is simple to implement in practice, but requires extensive calculation to find good codes and offsets. In [6], Davis and Jedwab developed a powerful theory which yields a class of codes enjoying very tight power control, large minimum distance and possessing efficient soft-decision decoding algorithms. These codes are formed from unions of cosets of the classical Reed-Muller codes and new generalisations of them, and as such can be regarded as falling in the general framework of the work in [13]. Special cases of these codes were also given in [24], [32] and the underlying theory was further developed in [26]. Very recently, Tarokh and Jafarkhani [31] have developed an efficient computational method for finding offsets to be used in conjunction with codes for OFDM. This approach has the potential to allow substantial reductions in PEMPR to be achieved for a wide class of codes but gives no concrete guarantees about the size of achievable reductions.

Given the above, it is of obvious interest to find bounds on PMEPR for other classes of good error-correcting codes. In this paper we develop such bounds for *trace codes*, whose codewords can be roughly characterised as having a representation as the trace of a polynomial function evaluated on a subset of a finite field or Galois ring. This class includes duals of primitive BCH codes [21, Chapter 9] and their $\mathbb{Z}_{2^e}$-analogues [9], [16]. Our approach is as follows. Firstly we show how bounding the PMEPR of OFDM codes is related to a classical problem in analysis of finding complex polynomials that are small in absolute value everywhere on the unit circle. Then we show how Lagrange interpolation allows us to translate a bound on the absolute values of a polynomial at the roots of unity into a (weaker) bound that is valid on the whole unit circle. This method was suggested to us by P. Borwein. Finally, we show how *hybrid character sums* over Galois fields and rings can be used get suitable bounds at the roots of unity for polynomials corresponding to trace codes.

As a sample of the kind of result we can get using this approach, we prove:

Theorem 1: Let $\mathcal{C}$ be the dual of a binary, primitive t-error-correcting BCH code of length $n = 2^m - 1$. Then any non-zero codeword of $\mathcal{C}$ has PMEPR at most $(2t-1)^2(\frac{2}{\pi}\log 2n + 2)^2$.

Note that the bound above applies directly to the code $\mathcal{C}$ rather than to an offset (or coset) of the code. It may be possible to obtain significant reductions in PMEPR by using such offsets, and we leave the determination of good offsets as a difficult open problem. Note also that, in common with the other bounds we obtain, the bound in Theorem 1 is unlikely to be tight. We will mention some methods that might be used to improve our bounds.

Finally, we note that similar techniques can be used to obtain bounds for codes over alphabets of size p^e, p an odd prime. These codes are of less immediate practical relevance for OFDM however.

II. PMEPR and Polynomials on the Unit Circle

Consider a q-ary OFDM codeword $\mathbf{a} = [a_0, a_1, \ldots, a_{n-1}]$. We associate with $\mathbf{a}$ the unimodular polynomial $a(z) = \omega^{a_0} + \omega^{a_1} z + \cdots + \omega^{a_{n-1}} z^{n-1}$ where $\omega = e^{2\pi i/q}$. Now for $\beta \in \mathbb{R}$, we have:

$$\begin{aligned} |S(\mathbf{a})(\beta/\Delta f)| &= |e^{2\pi i f_0 \beta/\Delta f}| \cdot \left| \sum_{j=0}^{n-1} \omega^{a_j} e^{2\pi i \beta j} \right| \\ &= \left| \sum_{j=0}^{n-1} \omega^{a_j} (e^{2\pi i \beta})^j \right| \\ &= \left| a(e^{2\pi i \beta}) \right|. \end{aligned}$$

Hence the maximum value of $|S(\mathbf{a})(t)|$, $t \in \mathbb{R}$, is given by the maximum absolute value of the polynomial $a(z)$ on the unit circle, $\{z : |z| = 1\}$. So the PMEPR of the OFDM codeword $\mathbf{a}$ can be obtained by studying the behaviour of the corresponding polynomial on the unit circle and a 'good' codeword corresponds to a unimodular polynomial that remains small in absolute value on the unit circle.

Such polynomials are of interest in analysis [27], and in the design of filters [8]. It is shown in [8] that, with probability 1 as $n \to \infty$, the maximum absolute value of a polynomial with random coefficients from $\{+1, -1\}$ is $(1 + o(1))(n \log n)^{1/2}$. This means that for sufficiently large n, a random OFDM codeword will almost certainly have PMEPR close to $\log n$ in value. This should be compared to the worst case value of n over all codewords and the bound in Theorem 1 of $O((\log n)^2)$ for a restricted class of codewords. A related but harder analytic question concerns the existence of so-called sequences $\{p_n(z)\}$ of ultra-flat polynomials. These are unimodular polynomials satisfying $\deg p_n = n - 1$ and

$$\lim_{n \to \infty} \frac{\max_{|z|=1} |p_n(z)|}{\min_{|z|=1} |p_n(z)|} = 1.$$

These polynomials are not simply small on the unit circle, but remain uniformly close in absolute value to $\sqrt{n}$. See [25], [20], [15], [3] for motivating problems and subsequent work on ultra-flat polynomials. Polynomials that are 'close' to ultra-flat might be interesting for OFDM applications, since the corresponding signals have close to constant envelope power in the time-domain and thus are less susceptible to spectral growth through distortions introduced by non-linear amplification. Unfortunately, current proofs of existence of ultra-flat polynomials are non-constructive, and the only result on flat polynomials with coefficients that are q-th roots of unity [3] requires (after correcting an arithmetical error in the paper) a value of q around 2500.

III. Lagrange Interpolation

Let $a(z) : \mathbb{C} \to \mathbb{C}$ be a degree $n - 1$ polynomial, and let $\zeta = e^{2\pi i/n}$ be a complex n-th root of unity. Lagrange interpolation allows us to express $a(z)$ in terms of its values at the powers of ζ (generally, at any n distinct points):

$$a(z) = \sum_{\ell=0}^{n-1} \rho_\ell(z) a(\zeta^\ell), \qquad z \in \mathbb{C}$$

where

$$\rho_\ell(z) = \prod_{0 \le k < n, k \ne \ell} \frac{z - \zeta^k}{\zeta^\ell - \zeta^k}$$

It follows that we can bound $|a(z)|$ on the unit circle as:

$$\max_{|z|=1} |a(z)| \leq \max_{|z|=1} \sum_{\ell=0}^{n-1} |\rho_\ell(z)| \cdot \max_{0 \leq \ell < n} |a(\zeta^\ell)|. \tag{1}$$

For polynomials $a(z)$ obtained from the codes that we study, it turns out that the $a(\zeta^\ell)$ can be expressed as hybrid exponential sums over Galois fields and rings. Good bounds for these sums are readily available in the literature and are quoted in Section IV below. So to obtain a bound on $\max_{|z|=1} |a(z)|$ for our $a(z)$, we need to bound $\max_{|z|=1} \sum_{\ell=0}^{n-1} |\rho_\ell(z)|$ in (1). Such a result is provided by:

Lemma 2: We have:

$$\max_{|z|=1} \sum_{\ell=0}^{n-1} |\rho_\ell(z)| \leq \frac{2}{\pi} \log 2n + 2$$

Proof: Let $|z| = 1$. It is then easy to show that $\rho_\ell(z) = \rho_{\ell+a}(\zeta^a z)$ for any integer a, where $\ell + a$ is computed modulo n. Hence

$$\sum_{\ell=0}^{n-1} |\rho_\ell(z)| = \sum_{\ell=0}^{n-1} |\rho_{\ell+a}(\zeta^a z)| = \sum_{\ell=0}^{n-1} |\rho_\ell(\zeta^a z)|.$$

and so we can assume that $\arg z \in [-\pi/n, \pi/n)$.

Let $g_\ell(z) = \prod_{0 \leq k < n, k \neq \ell} z - \zeta^k$. Thus

$$\rho_\ell(z) = \frac{g_\ell(z)}{g_\ell(\zeta^\ell)}.$$

It is not hard to show that $|g_\ell(\zeta^\ell)| = n$ and so

$$\sum_{\ell=0}^{n-1} |\rho_\ell(z)| = \frac{1}{n}|g_0(z)| + \frac{1}{n} \sum_{\ell=1}^{n-1} |g_\ell(z)|.$$

Now g_0 is a polynomial of degree $n-1$ with coefficients that are of absolute value 1 (in fact, $g_0(z) = \sum_{k=0}^{n-1} z^k$). So $|g_0(z)| \leq n$ and

$$\sum_{\ell=0}^{n-1} |\rho_\ell(z)| \leq 1 + \frac{1}{n} \sum_{\ell=1}^{n-1} |g_\ell(z)|.$$

For $z \neq \zeta^\ell$, we have:

$$g_\ell(z) = \prod_{0 \leq k < n, k \neq \ell} z - \zeta^k = \frac{z^n - 1}{z - \zeta^\ell}$$

so

$$|g_\ell(z)| = \frac{|z^n - 1|}{|z - \zeta^\ell|} \leq \frac{2}{|z - \zeta^\ell|}.$$

Geometrical considerations show that for $\arg z \in [0, \pi/n)$,

$$|z - \zeta^\ell| \geq \begin{cases} 2\sin(\frac{2\pi(\ell-1/2)}{2n}) & \text{for } \arg \zeta^\ell \in [2\pi/n, \pi] \\ \end{cases}$$

with a similar pair of bounds when $\arg z \in [-\pi/n, 0)$. For $\arg z \in [\pi/n, \pi/n)$, we conclude that:

$$\sum_{\ell=0}^{n-1} |\rho_\ell(z)| \leq 1 + \frac{1}{n} \sum_{\ell=1}^{n-1} \frac{1}{\sin(\frac{\pi\ell}{2n})}.$$

Using the approximation $\sin x > \frac{2}{\pi}x$ for $x \in (0, \pi/2)$, we can easily bound this last sum by $\log n$. In the following slightly more delicate analysis, derived by following [28] and correcting a computational error, we improve this bound to $\frac{2}{\pi}\log 2n + 1$. This will prove the lemma. Since $\mathrm{cosec}(x)$ is decreasing on $[0, \pi/2]$, we have:

$$\begin{aligned}
\frac{1}{n}\sum_{\ell=1}^{n-1} \frac{1}{\sin(\frac{\pi\ell}{2n})} &\leq \frac{1}{n} \cdot \frac{1}{\sin(\frac{\pi}{2n})} + \frac{1}{n}\int_1^n \mathrm{cosec}(\frac{\pi x}{2n}) dx \\
&< 1 + \frac{2}{\pi}\left(-\log\tan(\frac{\pi}{4n})\right) \\
&< 1 + \frac{2}{\pi}\left(-\log\sin(\frac{\pi}{4n})\right) \\
&< 1 + \frac{2}{\pi}\log 2n
\end{aligned}$$

where we have used the inequality $\sin x > \frac{2}{\pi}x$ for $x \in (0, \pi/2)$ and elementary properties of the log and trigonometric functions. □

IV. Exponential Sums Over Galois Fields and Rings

We introduce exponential sums for Galois fields of characteristic 2 and for Galois rings of characteristic 2^k. Much of what we say can be generalised to fields and rings of arbitrary odd characteristic p^k, but since our motivation is to obtain bounds on the power of q-PSK modulated OFDM signals where q is a power of 2, we do not give the details here.

A. Bounds for exponential sums over Galois fields

For each $b \in \mathbb{F}_{2^m}$, define a map ψ_b from $\mathbb{F}_{2^m}$ to the set $\{1, -1\}$ by writing

$$\psi_b(x) = (-1)^{\mathrm{tr}_1^m(bx)}, \quad x \in \mathbb{F}_{2^m}$$

where tr_1^m denotes the trace function for $\mathbb{F}_{2^m}$ The maps ψ_b are called the *additive characters* of $\mathbb{F}_{2^m}$. The map ψ_0 is called the *trivial* additive character. For $b \neq 0$,

$$\sum_{x \in \mathbb{F}_{2^m}} \psi_b(x) = 0.$$

Now let $n = 2^m - 1$ and let $\zeta = \exp(2\pi i/n)$ be a complex n-th root of unity. Let α be a primitive element in $\mathbb{F}_{2^m}$. For each integer ℓ with $0 \leq \ell < 2^m - 1$, we define a map χ_ℓ from $\mathbb{F}_{2^m}^*$ to the set of powers of ζ by writing

$$\chi_\ell(\alpha^i) = \zeta^{\ell i}, \quad 0 \leq i < 2^m - 1.$$

The maps χ_ℓ are called the *multiplicative characters* of $\mathbb{F}_{2^m}$. The map χ_0 is called the *trivial* multiplicative character.

Before stating the bounds on exponential sums, we need a technical definition.

Definition 3: Let $f(x) \in \mathbb{F}_{2^m}[x]$ and suppose f is not expressible in the form $g(x)^2 + g(x) + b$ where $g(x) \in \mathbb{F}_{2^m}[x]$ and $b \in \mathbb{F}_{2^m}$. Then we say that f is *non-degenerate*. A sufficient condition for f to be non-degenerate is that f has odd degree

Result 4: [21, p.281, Theorem 19] Let ψ be a non-trivial additive character of $\mathbb{F}_{2^m}$ and let $f(x) \in \mathbb{F}_{2^m}[x]$ be of degree r. Suppose f is non-degenerate. Then:

$$\left| \sum_{x \in \mathbb{F}_{2^m}} \psi(f(x)) \right| \leq (r-1)2^{m/2}.$$

Result 5: [29, page 45, Theorem 2Gi)] Let ψ be a non-trivial additive character of $\mathbb{F}_{2^m}$. Let χ be a non-trivial multiplicative character of $\mathbb{F}_{2^m}$ of order d with $d|(2^m-1)$. Let $f(x) \in \mathbb{F}_{2^m}[x]$ have degree r, where r is odd. Suppose $g(x) \in \mathbb{F}_{2^m}[x]$ has s distinct roots and that $\gcd(d, \deg g) = 1$. Then

$$\left| \sum_{x \in \mathbb{F}_{2^m}^*} \psi(f(x))\chi(g(x)) \right| \leq (r+s-1)2^{m/2}.$$

B. Galois rings and bounds for exponential sums over Galois rings

We give a list of definitions for Galois rings of characteristic 2^e and quote the results on exponential sums over these rings that we need. For more background, see [16].

In what follows, $R_{e,m}$ denotes the Galois ring of characteristic 2^e and degree m (see [16], [30] for further details). This ring contains 2^{em} elements, has characteristic 2^e and can be shown to be isomorphic to the factor ring $\mathbb{Z}_{2^e}[x]/(f(x))$ where f is a *monic basic irreducible* of degree m.

The units $R_{e,m}^*$ in $R_{e,m}$ contain a cyclic subgroup $\mathcal{T}_{e,m}^*$ of order $2^m - 1$. We let β denote a generator of this set. We write

$$\mathcal{T}_{e,m} = \mathcal{T}_{e,m}^* \cup \{0\} = \{\beta^j, 0 \leq j < 2^m - 1\} \cup \{0\}.$$

and call $\mathcal{T}_{e,m}$ the *Teichmuller set* in $R_{e,m}$.

It can be shown that every element $x \in R_{e,m}$ has a 2-adic expansion:

$$x = x_0 + 2x_1 + \cdots + 2^{e-1}x_{e-1}, \quad x_j \in \mathcal{T}_{e,m}.$$

We define the *Frobenius automorphism* σ on $R_{e,m}$ by

$$\sigma(x) = x_0^2 + 2x_1^2 + \cdots + 2^{e-1}x_{e-1}^2$$

and, by analogy with the finite fields case, the absolute trace function Tr_1^m on $R_{e,m}$ by

$$\mathrm{Tr}_1^m(x) = \sum_{j=0}^{m-1} \sigma^j(x).$$

We also define characters for the ring $R_{e,m}$. For odd b with $1 \leq b \leq 2^e - 1$, let $\psi_b : R_{e,m} \to \mathbb{C}$ denote the *additive character* of $R_{e,m}$ defined by:

$$\psi_b(x) = e^{\frac{2\pi i b}{2^e}\mathrm{Tr}_1^m(x)}, \quad x \in R_{e,m}$$

and for each integer ℓ with $0 \leq \ell < 2^m - 1$, let $\chi_\ell : R_{e,m}^* \to \mathbb{C}$ denote the *multiplicative character* defined by:

$$\chi_\ell(x) = e^{\frac{2\pi i \ell}{2^m-1}j}, \quad x \in R_{e,m}^*$$

where $x = \beta^j \bmod 2$ with $0 \leq j < 2^m - 1$. (The modulo 2 reduction map is a homomorphism which,

primitive element $\alpha \in \mathbb{F}_{2^m}$. So for any $x \in R_{e,m}^*$ we have $x \bmod 2 = \alpha^j$ for some $0 \le j < 2^m - 1$ and then $x = \beta^j \bmod 2$).

We call ψ_0 and χ_0 the *trivial* characters for the Galois ring.

Definition 6: Let $f(x) \in R_{e,m}[x]$ and suppose f is not expressible in the form

$$\sigma(g(x)) - g(x) + b$$

for any $g(x) \in R_{e,m}[x]$ and any $b \in R_{e,m}$. Here $\sigma(\sum_j g_j x^j) = \sum_j \sigma(g_j) x^{2j}$. Then we say that f is *non-degenerate.*

An easily verified condition for f of degree at least 1 to be non-degenerate is that f contains no terms of even degree. For completeness, we include a proof of this fact. Suppose $f = \sigma(g) - g + b$ for some $g(x) \in R_{e,m}[x]$ and some $b \in R_{e,m}$. Suppose g has degree $d \ge 1$ and write $g(x) = \sum_{j=0}^{d} g_j x^j$. Notice that $\sigma(g_d) \ne 0$, so $\sigma(g)$ has a term $\sigma(g_d)x^{2d}$ of degree $2d$. Since g has degree only d, the polynomial $\sigma(g) - g + b$ also contains the non-zero term $\sigma(g_d)x^{2d}$. But f contains no terms of even degree. The only remaining case is where g has degree $d = 0$. But then so does $f = \sigma(g) - g + b$ — a contradiction.

Now let f be a polynomial with 2-adic expansion:

$$f(x) = F_0[x] + 2F_1[x] + \cdots 2^{e-1}F_{e-1}[x], \quad F_i[x] \in \mathcal{T}_{e,m}[x]$$

Then we define the *weighted degree* of f to be

$$D_f = \max\{2^{e-1}d_0, 2^{e-2}d_1, \ldots, d_{e-1}\}$$

where d_j is the degree of F_j.

Result 7: [16, Theorem 1] Let ψ be a non-trivial additive character of $R_{e,m}$. Let $f(x) \in R_{e,m}[x]$ be non-degenerate and of weighted degree D_f. Then

$$\left| \sum_{x \in \mathcal{T}_{e,m}} \psi(f(x)) \right| \le (D_f - 1)2^{m/2}.$$

Result 8: [30, Theorem 2] Let ψ be a non-trivial additive character of $R_{e,m}$. Let $f(x) \in R_{e,m}[x]$ be non-degenerate and of weighted degree D_f. Let χ be a non-trivial multiplicative character of $R_{e,m}$. Then

$$\left| \sum_{x \in \mathcal{T}_{e,m}^*} \psi(f(x))\chi(x) \right| \le D_f 2^{m/2}.$$

V. Bounds on PMEPR for Code Families

A. Duals of Binary, Primitive BCH Codes

Let $f \in \mathbb{F}_{2^m}[x]$ be a polynomial and let $\alpha \in \mathbb{F}_{2^m}$ be a primitive element. With f we associate a length $n = 2^m - 1$ binary vector $\mathbf{a}_f$ whose components are

$$(a_f)_j = \mathrm{tr}_1^m(f(\alpha^j)), \quad 0 \le j < 2^m - 1$$

and a degree $n - 1$ polynomial with $\{+1, -1\}$ coefficients $a_f(z) = \sum_{j=0}^{n-1} (-1)^{(a_f)_j} z^j$. Let $t \ge 1$. Then we define $\mathcal{C}$ to be the dual of the binary, primitive t-error correcting BCH code. That is, we take for $\mathcal{C}$ the set:

$$\{\mathbf{a}_f : f(x) = f_1 x + f_3 x^3 + \cdots f_{2t-1} x^{2t-1} \in \mathbb{F}_{2^m}[x]\}.$$

It is well known that, for $2t-1 < 2^{\lceil m/2 \rceil}+1$, $\mathcal{C}$ is a linear code of dimension mt with minimum distance at least $2^{m-1}-(t-1)2^{m/2}$. This last fact can be proved using an application of Result 4 — see [21, Theorem 18, p. 280] for details. This bound on minimum distance can be improved in certain cases [22].

With this definition, we now prove Theorem 1.

Proof: (of Theorem 1).

Let $\mathbf{a}_f$ be a non-zero word of $\mathcal{C}$. This word is obtained from a non-zero, non-degenerate polynomial $f(x) = \sum_{j=1}^{t} f_{2j-1}x^{2j-1} \in \mathbb{F}_{2^m}[x]$ and we are interested in bounding the quantity

$$\max_{|z|=1} |a_f(z)|.$$

Let $\zeta = e^{2\pi i/n}$. Then for $0 \leq \ell < n$,

$$\begin{aligned} |a_f(\zeta^\ell)| &= \left| \sum_{j=0}^{n-1} (-1)^{(a_f)_j} (\zeta^\ell)^j \right| \\ &= \left| \sum_{j=0}^{n-1} (-1)^{\mathrm{tr}_1^m(f(\alpha^j))} \zeta^{\ell j} \right| \\ &= \left| \sum_{x \in \mathbb{F}_{2^m}^*} \psi_1(f(x)) \chi_\ell(x) \right|. \end{aligned}$$

For $\ell = 0$, the expression above reduces to $|\sum_{x\in\mathbb{F}_{2^m}^*} \psi_1(f(x))|$ which can be bounded above by $(2t-2)2^{m/2}+1$, using Result 4.

For $\ell \neq 0$, χ_ℓ is a non-trivial multiplicative character and Result 5 with $r = 2t-1$ and $s = 1$ yields

$$|a_f(\zeta^\ell)| \leq (2t-1)2^{m/2}.$$

Thus $\max_{0\leq\ell<n} |a_f(\zeta^\ell)| \leq (2t-1)2^{m/2}$. The theorem now follows from (2) and Lemma 1. □

A number of notes on Theorem 1 are in order.

First of all, we observe that the bound on PMEPR is crucially dependent on the ordering of the components of the code $\mathcal{C}$. This is in contrast to the usual situation in coding theory where arbitrary permutations of coordinates do not alter the minimum distance of a code.

Secondly, we examine in more detail the case $t = 1$ of the theorem. Here the code is the simplex code with parameters $[2^m-1, m, 2^{m-1}]$. All the non-zero codewords are cyclic shifts of the sequence with terms $\mathrm{tr}_1^m(\alpha^j)$, which is an m-sequence (maximal length shift register sequence). These sequences were proposed for use in OFDM in [19]. Unfortunately, as was pointed out in [12], the calculation of the power properties of m-sequences in [19] is incorrect. Our theorem provides a bound of order $(\log n)^2$ on the PMEPR of m-sequences.

We note that in the special case of $t = 2$, the dual BCH code consists of the sequences of a Gold set and their cyclic shifts. We also point out that the following result of Lahtonen can be used to obtain a bound with leading term $\frac{36}{\pi^2}(\log n)^2$ on the PMEPR of the sequences of the small Kasami set and their cyclic shifts:

Result 9: [17] Let $m = 2s$ and $T = 2^s+1$. Let χ be a non-trivial multiplicative character of $\mathbb{F}_{2^m}$. Suppose that either $\sigma \neq 0$ or $\mathrm{tr}_s^m\lambda \neq 0$ (or both). Then

$$\left| \sum_{x\in\mathbb{F}_{2^m}^*} (-1)^{\mathrm{tr}_1^m(\sigma x+\lambda x^T)} \chi(x) \right| \leq 3\cdot 2^{m/2}+2^{m/4}.$$

Finally, we note that similar (but slightly weaker) bounds on PMEPR can be derived for the duals

B. The quaternary codes $\mathcal{K}^-$ and $\mathcal{DG}_t^-$

Let $f \in R_{e,m}[x]$ be a polynomial and let $\beta \in R_{e,m}$ be a generator for $\mathcal{T}_{e,m}^*$. With f we associate a length $n = 2^m - 1$ vector $\mathbf{a}_f$ whose components from $\mathbb{Z}_{2^e}$ are:

$$(a_f)_j = \mathrm{Tr}_1^m(f(\beta^j)), \quad 0 \le j < 2^m - 1.$$

We also associate with f a degree $n-1$ polynomial with coefficients that are 2^e-th roots of unity

$$a_f(z) = \sum_{j=0}^{n-1} \omega^{(a_f)_j} z^j, \quad \omega = e^{2\pi i/2^e}.$$

Taking $e = 2$, we can now introduce two families of quaternary code. We define the code $\mathcal{K}^-$ to be the following set of $\mathbb{Z}_4$-valued vectors of length $n = 2^m - 1$:

$$\mathcal{K}^- = \{\mathbf{a}_f : f(x) = b_0 x, b_0 \in R_{2,m}\}.$$

For $1 \le t \le (m-1)/2$, we define the code $\mathcal{DG}_t^-$ to be the following set of $\mathbb{Z}_4$-valued vectors of length $n = 2^m - 1$:

$$\mathcal{DG}_t^- = \{\mathbf{a}_f : f(x) = b_0 x + 2\sum_{j=1}^{t} b_j x^{1+2^j}, b_0 \in R_{2,m}, b_j \in \mathcal{T}_{2,m}\}.$$

The minimum Lee distances of the codes $\mathcal{K}^-$ and $\mathcal{DG}_t^-$ can be bounded below by $2^m - 2^{m/2}$ and $2^m - 2^{t+\frac{m}{2}}$ respectively, using Result 7 and the fact that non-zero codewords of the codes are obtained from polynomials having weighted degrees 2 and $2^t + 1$. These bounds on minimum distances can be improved for m odd [10] to obtain the codes' true minimum Lee distances of $2^m - 2^{\frac{m-1}{2}}$ and $2^m - 2^{r+\frac{m-1}{2}}$ respectively. The code $\mathcal{K}^-$ contains 2^{2m} quaternary words and the code $\mathcal{DG}_t^-$ contains 2^{2m+tm} quaternary words.

All these codes can be extended to length 2^m by adding a coordinate corresponding to $a_f(0)$, and the ranks can then be increased by 1 by adding modulo 4 to every codeword multiples of the all-1 codeword. Applying both these steps gives codes $\mathcal{K}$ and $\mathcal{DG}_t$ whose images under Gray map when m is odd are the well-known Kerdock and Delsarte-Goethals codes [9].

We have:

Theorem 10: Any non-zero codeword of $\mathcal{K}^-$ has PMEPR at most $4(\frac{2}{\pi}\log 2n + 2)^2$. Any non-zero codeword of $\mathcal{DG}_t^-$ has PMEPR at most $(2^t+1)^2(\frac{2}{\pi}\log 2n + 2)^2$.

Proof: We treat both types of code $\mathcal{K}^-$ and $\mathcal{DG}_t^-$ together. Suppose $t \ge 0$. Let $f(x) = b_0 x + 2\sum_{j=1}^{t} b_j x^{1+2^j}$ where $b_0 \in R_{2,m}$, $b_j \in \mathcal{T}_{2,m}$ for $1 \le j \le t$ and the sum over j is empty when $t = 0$. Suppose further that the b_j are not all zero. Then f is a non-degenerate polynomial of weighted degree 2^t+1 which, for $t = 0$, corresponds to a non-zero codeword of $\mathcal{K}^-$ and for $t > 0$, to a non-zero codeword of $\mathcal{DG}_t^-$.

Now for $0 \le \ell < n$,

$$\begin{aligned} |a_f(\zeta^\ell)| &= \left|\sum_{j=0}^{n-1} \omega^{(a_f)_j} (\zeta^\ell)^j\right| \\ &= \left|\sum_{x \in \mathcal{T}_{2,m}^*} \psi_1(f(x))\chi_\ell(x)\right| \end{aligned}$$

where ψ_1 and χ_ℓ are respectively additive and multiplicative characters for $R_{2,m}$. For $\ell = 0$, the expression above reduces to $|\sum_{x \in \mathcal{T}^*_{2,m}} \psi_1(f(x))|$ which can be bounded above by $2^t \cdot 2^{m/2} + 1$, using Result 7. For $\ell \neq 0$, χ_ℓ is a non-trivial multiplicative character and Result 8 yields

$$|a_f(\zeta^\ell)| \leq (2^t + 1) \cdot 2^{m/2}, \quad 1 \leq \ell < n.$$

Thus $\max_{0 \leq \ell < n} |a_f(\zeta^\ell)| \leq (2^t + 1) \cdot 2^{m/2}$. The theorem now follows from (2) and Lemma 1. □

C. Weighted Degree Trace Codes

We now introduce our final family of non-binary codes, the weighted degree trace codes. For odd D with $1 \leq D < 2^{\lceil m/2 \rceil} + 1$, define

$$\mathcal{C}_D^- = \{\mathbf{a}_f : f \in R_{e,m}[x], f = \sum_{j=0}^{D-1/2} f_{2j+1} x^{2j+1}, D_f \leq D\}.$$

Thus $\mathcal{C}_D^-$ is a 2^e-ary code of length $n = 2^m - 1$ obtained from a set of non-degenerate polynomials of weighted degree at most D. The code is linear over $\mathbb{Z}_{2^e}$. It can be shown, using 2-adic expansions and simple counting, that $|\mathcal{C}_D^-| = 2^{(D - \lfloor D/4 \rfloor)m}$ when $e = 2$ and that $|\mathcal{C}_D^-| = 2^{(D+1-wt_H(D+1 \bmod 2^e) - \lfloor D+1/2^e \rfloor)m}$ when $e > 2$. Result 8 can be applied to show that the minimum Lee distance of $\mathcal{C}_D^-$ is at least $2^m - (D-1)2^{m/2}$ when $e = 2$. This bound can be improved in certain cases [10]. For $e > 2$, Result 8 can be used to lower-bound the minimum Euclidean distance of the code. Finally, the following theorem can be proved using an almost identical argument to that used in the proof of Theorem 10:

Theorem 11: Any non-zero codeword of $\mathcal{C}_D^-$ has PMEPR at most $D^2(\frac{2}{\pi} \log 2n + 2)^2$.

The code family $\mathcal{C}_{2t-1}^-$ is the natural 2^e-ary analogue of the family of duals of t-error-correcting BCH codes studied in Section V-A. The bounds on PMEPR in Theorems 1 and 11 are identical for these two families.

D. Improved Bounds and Open Problems

We suggest a number of ways in which the bounds of Theorems 1, 10 and 11 might be improved and a number of open questions.

Firstly, the factor of order $(\log n)^2$ in each bound arises from our use of Lagrange interpolation, in particular the bound in Lemma 2. The constant $2/\pi$ here, obtained using Sarwate's improvement of the Vinogradov method in [28], can be further improved slightly using methods also in [28]. However, it seems plausible that this bound could be lowered from $O(\log n)$ to $O((\log n)^{1/2})$. Such an improvement would not be surprising in view of the $(\log n)^{1/2}$ factor in the result of [8] on the expected maximum absolute value of random polynomials on the unit circle. Such an improvement may come from a more careful analysis of the sum in Lemma 2.

On the other hand, codes containing large numbers of sequences with a constant bound on PMEPR (i.e. a bound that is independent of n) have recently been exhibited in [6]. These codes are constructed from cosets of (generalised) first-order Reed-Muller codes. It is known that the Reed-Muller codes have very poor PMEPR themselves, but the results of [6] show that their cosets can have PMEPR as low as 2. So it is possible to do substantially better than our exponential sum bounds indicate (albeit for other families of codes) by working with cosets of linear codes. We ask: can further reductions in PMEPR be achieved by considering cosets of the trace codes studied in this paper? From the results of [8], it can be shown that any sequence of length n binary codes whose PMEPR is independent of n must have rate tending to zero as $n \to \infty$. In fact the rate is already at most $O((\log n)^{-4})$ for a code whose PMEPR is roughly $\log n$. Can the trade-off between rate, PMEPR and minimum distance be further quantified?

We also mention that in practical OFDM systems, n, the number of carriers, is usually a power

and de-modulator. However our results are applicable only to codes of length $2^m - 1$ (or divisors of this length if we consider non-primitive versions of the trace codes), so in practice we would need to perform oversampling in the modulator. We are forced to consider lengths $2^m - 1$ because the hybrid expontential sums that we use to bound the power of OFDM transmissions involve multiplicative characters of $\mathbb{F}_{2^m}$ and $R_{e,m}$. Bounding the PMEPR for the length 2^m extensions of trace codes is left as an important open problem.

Finally, we note that the techniques developed in this paper apply to any code whose discrete Fourier transform (DFT) is uniformly small. This is because the values at the roots of unity of the polynomial $a(z)$ associated with a codeword $\mathbf{a}$ are just the coefficients of the discrete Fourier transform of $\mathbf{a}$. Lemma 2 allows us to extend a bound on these coefficients to a somewhat weaker bound that holds on the entire unit circle, and we used exponential sums to bound the DFTs of trace codes. Which other families of classical error-correcting codes have small DFTs?

REFERENCES

[1] M. Alard and R. Lasalle. Principles of modulation and channel coding for digital broadcasting for mobile receivers. *EBU Review*, 224: 47–69, Aug. 1987.

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

[3] J. Beck. Flat polynomials on the unit circle — Note on a problem of Littlewood. *Bull. London Math. Soc.*, 23: 269–277, 1991.

[4] J.A.C. Bingham. Multicarrier modulation for data transmission: an idea whose time has come. *IEEE Commun. Magazine*, 28(1): 5–14, May 1990.

[5] P.S. Chow, J.M. Cioffi, and J.A.C. Bingham. DMT-based ADSL: concept, architecture, and performance. In *IEE Colloquium on 'High Speed Access Technology and Services, Including Video-on-Demand'*, pages 3/1–6, Oct. 1994.

[6] J.A. Davis and J. Jedwab. Peak-to-mean power control in OFDM, Golay complementary sequences and Reed-Muller codes. *Submitted*, 1997.

[7] M. Friese. Multicarrier modulation with low peak-to-mean average power ratio. *Elec. Lett.*, 32: 713–714, 1996.

[8] A. Gersho, B. Gopinath, and A.M. Odlyzko. Coefficient inaccuracy in transversal filtering. *Bell System Tech. Journal*, 58: 2301–2316, 1979.

[9] 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*, IT-40: 301–319, 1994.

[10] T. Helleseth, P.V. Kumar, O. Moreno, and A.G. Shanbag. Improved estimates via exponential sums for the minimum distance of $\mathbf{Z}_4$-linear trace codes. *IEEE Trans. Inform. Theory*, IT-42(4): 1212–1216, July 1996.

[11] T.F. Ho and V.K. Wei. Synthesis of low-crest waveforms for multicarrier CDMA systems. In *IEEE Globecomm 1995*, pages 131–135, 1995.

[12] J. Jedwab. Comment: M-sequences for OFDM peak-to-average power ratio reduction and error correction. *Elec. Lett.*, 33(15): 1293–1294, July 1997.

[13] A.E. Jones and T.A. Wilkinson. Combined coding for error control and increased robustness to system nonlinearities in OFDM. In *IEEE 46th Vehicular Technology Conference*, pages 904–908, Atlanta, April–May 1996.

[14] A.E. Jones, T.A. Wilkinson, and S.K. Barton. Block coding scheme for reduction of peak to mean envelope power ratio of multicarrier transmission schemes. *Elec. Lett.*, 30: 2098–2099, 1994.

[15] J.-P. Kahane. Sur les polynômes à coefficients unimodulaires. *Bull. London Math. Soc.*, 12: 321–342, 1980.

[16] P.V. Kumar, T. Helleseth, and A.R. Calderbank. An upper bound for Weil exponential sums over Galois rings and applications. *IEEE Trans. Inform. Theory*, IT-41(2): 456–468, March 1995.

[17] J. Lahtonen. On the odd and aperiodic correlation properties of the Kasami sequences. *IEEE Trans. Inform. Theory*, IT-41(5): 1506–1508, Sept. 1995.

[18] X. Li and L.J. Cimini, Jr. Effects of clipping and filtering on the performance of OFDM. In *IEEE 47th Vehicular Technology Conference*, pages 1634–1638, Phoenix, May 1997.

[19] X. Li and J.A. Ritcey. M-sequences for OFDM peak-to-average power ratio reduction and error correction. *Elec. Lett.*, 33(7): 554–555, March 1997.

[20] J.E. Littlewood. On polynomials $\sum^n \pm z^m, \sum^n e^{\alpha_m i} z^m, z = e^{\theta i}$. *J. London Math. Soc.*, 41: 367–376, 1966.

[21] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes (2nd edition).* North Holland, Amsterdam, 1986.

[22] O. Moreno and C.J. Moreno. The MacWilliams-Sloane conjecture on the tightness of the Carlitz-Uchiyama bound and the weights of duals of BCH codes. *IEEE Trans. Inform. Theory*, IT-40(6): 1894–1907, Nov. 1994.

[23] S.H. Müller, R.W. Bäuml, R.F.H. Fischer, and J.B. Huber. OFDM with reduced peak-to-average power ratio by multiple signal representation. *Annales des Télécommunications*, 52(1–2): 58–67, 1997.

[24] H. Ochiai and H. Imai. Block coding scheme based on complementary sequences for multicarrier signals. *IEICE Trans. Fundamentals*, pages 2136–2143, Nov. 1997.

[25] P. Erdös. Some unsolved problems. *Michigan Math J.*, 4: 291–300, 1957.

[26] K.G. Paterson. Generalised Reed-Muller codes and power control in OFDM. *Submitted*, 1998.

[27] R. Salem and A. Zygmund. Some properties of trigonometric series whose terms have random signs. *Acta Math.*, 91: 245–301, 1954.

[28] D.V. Sarwate. An upper bound on the aperiodic autocorrelation function for a maximal-length sequence. *IEEE Trans. Inform. Theory*, IT-30(4): 685–687, July 1984.
[29] W. Schmidt. *Equations Over Finite Fields — An Elementary Approach.* Springer, Berlin, 1976.
[30] A.G. Shanbag, P.V. Kumar, and T. Helleseth. Upper bound for a hybrid sum over Galois rings with applications to aperiodic correlation for some q-ary sequences. *IEEE Trans. Inform. Theory*, IT-42: 250–254, 1996.
[31] V. Tarokh and H. Jafarkhani. On reducing the peak to average power ratio in multicarrier communications. *Submitted*, 1998.
[32] R.D.J. van Nee. OFDM codes for peak-to-average power reduction and error correction. In *IEEE Globecom 1996*, pages 740–744, London, Nov. 1996.
[33] T.A. Wilkinson and A.E. Jones. Minimisation of the peak to mean envelope power ratio of multicarrier transmission schemes by block coding. In *IEEE 45th Vehicular Technology Conference*, pages 825–829, Chicago, July 1995.
[34] D. Wulich. Reduction of peak-to-mean ratio of multicarrier modulation using cyclic coding. *Elec. Lett.*, 32(5): 432–433, Feb. 1996.