HEWLETT PACKARD

On the Existence and Construction of Good Codes with Low Peak-to-Average Power Ratios

Kenneth Paterson, Vahid Tarokh*
Extended Enterprise Laboratory
HP Laboratories Bristol
HPL-1999-51
April, 1999

OFDM, multicarrier, power, PAPR, PMPR, PMEPR, bounds, Varshamov, Gilbert, simplex code, dual BCH code, Kerdock code, Delsarte-Goethals code, exponential sum, Lagrange interpolation, finite field, Galois ring

The first lower bound on the peak-to-average power ratio (PAPR) of a constant energy code of a given length n, minimum Euclidean distance and rate is established. Conversely, using a non-constructive Varshamov-Gilbert style argument yields a lower bound on the achievable rate of a code of a given length, minimum Euclidean distance and maximum PAPR. The derivation of these bounds relies on a geometrical analysis of the PAPR of such a code. Further analysis shows that there exist asymptotically good codes whose PAPR is at most 8 log n. These bounds motivate the explicit construction of error-correcting codes with low PAPR. Bounds for exponential sums over Galois fields and rings are applied to obtain an upper bound of order $(\log n)^2$ on the PAPRs of a constructive class of codes the trace codes. This class includes the binary simplex code, duals of binary, primitive BCH codes and a variety of their non-binary analogues. Some open problems are identified.

Internal Accession Date Only
*AT & T Labs - Research , 180 Park Avenue, Florham Park, NJ

On the Existence and Construction of Good Codes with Low Peak-to-Average Power Ratios

Kenneth G. Paterson, *Member, IEEE*, and Vahid Tarokh, *Member, IEEE*

Abstract

The first lower bound on the peak-to-average power ratio (PAPR) of a constant energy code of a given length n, minimum Euclidean distance and rate is established. Conversely, using a non-constructive Varshamov-Gilbert style argument yields a lower bound on the achievable rate of a code of a given length, minimum Euclidean distance and maximum PAPR. The derivation of these bounds relies on a geometrical analysis of the PAPR of such a code. Further analysis shows that there exist asymptotically good codes whose PAPR is at most $8 \log n$. These bounds motivate the explicit construction of error-correcting codes with low PAPR. Bounds for exponential sums over Galois fields and rings are applied to obtain an upper bound of order $(\log n)^2$ on the PAPRs of a constructive class of codes, the trace codes. This class includes the binary simplex code, duals of binary, primitive BCH codes and a variety of their non-binary analogues. Some open problems are identified.

Keywords

OFDM; multicarrier; power; PAPR; PMPR; PMEPR; bounds; Varshamov; Gilbert; simplex code; dual BCH code; Kerdock code; Delsarte-Goethals code; exponential sum; Lagrange interpolation; finite field; Galois ring.

I. Introduction

Multicarrier communications is a technique with a long history [3], [5], [6], [11], [35], [36], [37], [44], [47] that has recently seen rising popularity in wireless and wireline applications [1], [4], [7], [8]. This revitalisation of the technique, also known as orthogonal frequency division multiplexing (OFDM) or discrete multi-tone (DMT), is mainly due to the advancing capabilities of digital signal processors. International standards making use of OFDM for wireless LANs are currently being established by IEEE 802.11 and ETSI BRAN committees. For wireless applications, an OFDM-based system can be of interest because it provides a greater immunity to impulse noise and fast fades and eliminates the need for equalisers, while efficient hardware implementations can be realised using FFT techniques.

A major barrier to the widespread acceptance of OFDM is the high peak-to-average power ratio (PAPR) of uncoded OFDM signals. If the peak transmit power is limited, either by regulatory or application constraints, this has the effect of reducing the average 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, the transmit amplifier must be operated in its linear region (i.e. with a large input back-off), where the conversion from DC to RF power is inefficient. This may have a deleterious effect on battery lifetime in mobile applications. In many low-cost applications the drawbacks of high PAPR outweigh all the potential benefits of OFDM systems.

A number of approaches have been proposed to deal with this power control problem [12], [17], [24], [28], [31], [46]. A simple idea introduced in [19] and developed further in [45] is to select for transmission those codewords which minimise or reduce the PMEPR. A more sophisticated approach adopted in [20] 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 PAPR 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. Very recently, [43] introduced a geometrical approach to the offset selection problem. This approach leads to a computationally efficient algorithm making use of a maximum-likelihood decoder for the underlying code to find good offsets. As an example, the

K.G. Paterson is with Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol BS34 8QZ, U.K.
V. Tarokh is with AT& T Labs – Research, 180 Park Avenue, Florham Park, New Jersey 07932, USA.

algorithm was used to obtain a reduction of 4.5 dB in the PAPR of the rate 1/2 BPSK code proposed in the ETSI BRAN Hiperlan-II standardisation committee.

Another strand of work on codes with reduced PAPR can be found in the papers [9], [10], [30], [29], [32]. In [10], Davis and Jedwab developed a powerful theory which yields a class of codes enjoying PAPR as low as 2, large minimum distance and possessing efficient soft-decision decoding algorithms [14], [33]. These codes are formed from unions of cosets of the classical Reed-Muller codes and new generalisations of them. Special cases of these codes were also given in [30], [29] and the underlying theory was further developed in [32]. While these block codes reduce PAPR, they also result in reduced transmission rates, severely so for large numbers of carriers.

Given the above raft of theoretical and practical work on the reduced PAPR coding for OFDM systems, it is of obvious importance to investigate the fundamental trade-offs between rate R, minimum Euclidean distance d and PAPR of a code. It is worth noting that until now, researchers have assumed that the redundancy introduced by considering only codewords having low PAPR can be exploited to perform error correction [42]. We establish in this paper that this assumption is false by proving in Theorem 5 a general lower bound on PAPR as a function of n, R and d. We also provide in Theorem 7 a non-constructive Varshamov-Gilbert style lower bound on the rate of a code, given n, d and the maximum tolerable PAPR. Further analysis of this bound shows that asymptotically good sequences of codes exist with PAPR growth of order only $8 \log n$.

Our two bounds bounds may be interpreted as placing limits on the achievable region of triples (R, d, PAPR) for codes. They motivate us to find explicit constructions for error-correcting codes having low PAPR. In the second part of the paper, we will describe a class of codes, the trace codes, which includes as sub-classes the well-known binary simplex code, the duals of binary, primitive BCH codes and a variety of their $\mathbb{Z}_{2^e}$-analogues. None of these sub-classes yields asymptotically good sequences of codes, but we will demonstrate how their PAPRs can be bounded by $O((\log n)^2)$.

The novel theoretical insight of [43] is a geometrical interpretation of the PAPR of a code $\mathcal{C}$. Using this insight allows us to translate of the problem of constructing constant energy codes with low PAPR to the problem of packing codewords on a complex sphere subject to the constraint that the minimum distance of the code and the union of two specific curves on the sphere is maximised. This re-formulation allows us to extend classical sphere-packing arguments to prove both our lower bound on PAPR and our Varshamov-Gilbert style bound. The reader primarily interested in these results should consult Sections II – V. The results on the PAPR of trace codes are proved by combining a bound from Lagrange interpolation with a novel application of bounds for hybrid character sums over Galois fields and rings. The reader more interested in this topic is directed to Sections II, VI and VII.

The organisation of the paper is as follows.

In Section II, we introduce the communication model, formulate the PAPR problem that we study and establish our notation. In Section III, we will prove a lower bound on the PAPR of any length n, constant energy code $\mathcal{C}$ containing $|\mathcal{C}|$ codewords, having minimum Euclidean distance d and rate $R = \log_2(|\mathcal{C}|)/n$. In Section IV, we prove our existence result establishing a lower bound on the rate of a length n, constant energy code having minimum Euclidean distance d and a given maximum PAPR. We study the asymptotic behaviour of this bound in Section V. Then in Section VI, we provide some necessary background on exponential sums. This is used in Section VII to prove upper bounds on the PAPRs of trace codes. We make some conclusions and suggestions for future work in Section VIII.

II. The communication model

Figure 1 shows a block diagram of an OFDM system. At each time $t = 0, \mathcal{T}, 2\mathcal{T}, \ldots$ blocks B_t of k bits arrive at the encoder. These k bits are encoded as a vector $\mathbf{c}$ of n constellation symbols from a constellation $\mathcal{Q} \subset \mathbb{C}$. The admissible sequences are called codewords, and the ensemble of all possible codewords is a code $\mathcal{C}$ of rate $R = k/n$. We denote the minimum Euclidean distance of the code $\mathcal{C}$ by d.

The vector $\mathbf{c}$ of n constellation symbols are provided to the input of a discrete Fourier transform (DFT) by

a serial to parallel block, producing a sequence of symbols $C_0, C_1, \ldots, C_{n-1}$, where

$$C_l = \sum_{i=0}^{n-1} c_i \exp(\frac{-2\pi j\ il}{n}), \tag{1}$$

for $l = 0, 1, 2, \ldots, n-1$. Here $j = \sqrt{-1}$.

This sequence is the input to the RF chain which produces the transmitted signal. This signal at time t is modelled by the real part of the complex envelope:

$$S_{\mathbf{c}}(t) = \left(\sum_{i=0}^{n-1} c_i \exp(-2\pi j(f_0 + if_s)t) \right) \tag{2}$$

for $0 \leq t \leq \frac{1}{f_s}$, where f_0 is the carrier frequency and f_s is the bandwidth of each tone. The relation between the quantities f_s and $\mathcal{T}$ depends on whether a guard time is assigned, or a cyclic prefix is used and these details have no bearing upon the bounds derived in this paper. However, we note that $f_s = 1/\mathcal{T}$ is commonly assumed in an ideal situation.

The receiver receives the signal $\Re(S_{\mathbf{c}}(t))$ perturbed by noise and performs the inverse operations: the RF chain at the receiver down-converts, processes the received data and obtains estimates of the parameters $C_\ell, \ell = 0, 1, \ldots, n-1$. The receiver then applies an IDFT on these estimates and generates estimates of $c_0, c_1, \ldots, c_{n-1}$. The receiver then extracts the block B_T of input bits by applying a suitable error correction algorithm.

For any codeword $\mathbf{c}$, the instantaneous power of the corresponding transmitted signal $\Re(S_{\mathbf{c}}(t))$ is equal to $(\Re S_{\mathbf{c}}(t))^2$. This power is less than or equal to the function $|S_{\mathbf{c}}(t)|^2$, called the *envelope power* of the OFDM signal.

The average value of the envelope power is exactly equal to $\|\mathbf{c}\|^2$ while, for $f_0 >> f_s$, the average power of the actual OFDM signal is approximately equal to $\frac{1}{2}\|\mathbf{c}\|^2$. We define PAPR($\mathbf{c}$), the peak-to-average power ratio of the OFDM signal, to be the ratio of the peak power of $\Re(S_{\mathbf{c}}(t))$ to $\|\mathbf{c}\|^2$, the average envelope power. We write $\zeta = f_0/f_s$, and note that in a typical OFDM application, we have $\zeta >> 1$ (for example, in the ETSI BRAN standard, $f_0 = 5 \times 10^9$ and $f_s \simeq 300 \times 10^3$). Then we have

$$\mathrm{PAPR}(\mathbf{c}) = \max_{0 \leq t \leq 1} \frac{\left| \Re\left(\sum_{i=0}^{n-1} c_i \exp(-2\pi j(\zeta + i)t) \right) \right|^2}{\|\mathbf{c}\|^2}. \tag{3}$$

Note that in the literature, PAPR is often referred to as peak-to-mean power ratio (PMPR). Notice also that

$$\mathrm{PAPR}(\mathbf{c}) \leq \max_{0 \leq t \leq 1} \frac{|S_{\mathbf{c}}(t)|^2}{\|\mathbf{c}\|^2}.$$

The function on the right of the above inequality is called the peak-to-mean envelope power ratio (PMEPR) of the codeword or OFDM signal. We denote it by PMEPR($\mathbf{c}$). It is often more convenient to work with PMEPR than PAPR. It is straightforward to show that if

$$c(z) = c_0 + c_1 z + \cdots + c_{n-1} z^{n-1}$$

denotes the degree $n-1$ polynomial whose coefficients are derived from $\mathbf{c}$, then

$$\mathrm{PMEPR}(\mathbf{c}) = \frac{1}{\|\mathbf{c}\|^2} \max_{|z|=1} |c(z)|^2.$$

So the PMEPR of a codeword is related to the maximum squared absolute value of the corresponding polynomial on the unit circle. This observation will be useful in the sequel.

For a code $\mathcal{C}$, we define

$$\mathrm{PAPR}(\mathcal{C}) = \max_{\mathbf{c} \in \mathcal{C}} (\mathrm{PAPR}(\mathbf{c}))$$

and refer to it as the peak-to-average power ratio (PAPR) of $\mathcal{C}$.

We will assume throughout the remainder of this paper that all the codewords in our codes have average envelope power $\|\mathbf{c}\|^2$ equal to n (we say that the codes have constant energy). This assumption certainly holds for any constellation in which each symbol has absolute value 1, for example any PSK constellation.

We next state the main problem studied in this paper.

Statement of The Problem: What is the achievable region of triples $(R, d, \mathrm{PAPR}(\mathcal{C}))$ for a length n code $\mathcal{C}$?

Since this statement includes as a special case the most basic open problem in coding theory (to classify the achievable region of pairs (R, d) with unrestricted PAPR), we cannot hope for a complete solution to the problem. Instead, we establish bounds on $\mathrm{PAPR}(\mathcal{C})$ given (R, d), and attempt to construct codes coming close to the bounds.

III. A lower bound on the PAPR of codes

In this section, we establish a lower bound on the PAPR of a constant energy code of length n, rate R and Euclidean distance d.

Let $\mathcal{C}$ denote such a code. Then the codewords $\mathbf{c}$ of $\mathcal{C}$ are points on the n-dimensional complex sphere of radius $\sqrt{n}$. We define the curve Ω by

$$\Omega = \{\omega(t, \zeta), 0 \leq t < 1\}.$$

where

$$\omega(t, \zeta) = (\exp(2\pi j \zeta t), \exp(2\pi j(\zeta + 1)t), \ldots, \exp(2\pi j(\zeta + n - 1)t)) \in \mathbb{C}^n$$

This curve lies on the same sphere as the codewords of $\mathcal{C}$. We define the curve $-\Omega$ to consist of all the points $\{-\omega(t, \zeta), 0 \leq t < 1\}$. Then $-\Omega$ is the antipodal image of Ω.

We now will prove a simple, albeit fundamental, result which provides us with the key to establishing bounds on the PAPR of codes. This result gives a geometric interpretation to the PAPR of a code, showing that the closer a codeword to the curve $\Omega \cup -\Omega$, the larger its PAPR.

Lemma 1: Let $\mathcal{C}$ denote a code of length n, rate R and Euclidean distance d. Let d_* denote the minimum Euclidean distance between the codewords of $\mathcal{C}$ and the points of $\Omega \cup -\Omega$. Then $d_* \leq \sqrt{2n}$ and

$$\mathrm{PAPR}(\mathcal{C}) \geq n(1 - \delta)^2$$

where $\delta = d_*^2/2n$.

Proof: We first prove that $d_* \leq \sqrt{2n}$. To this end, let $\mathbf{c}$ denote an arbitrary codeword of $\mathcal{C}$. Then for any $0 \leq t < 1$, $\omega(t, \zeta)$ and $-\omega(t, \zeta)$ are antipodal points on the n-dimensional complex sphere of radius $\sqrt{n}$. It follows that

$$\|\omega(t, \zeta) - \mathbf{c}\|^2 + \| - \omega(t, \zeta) - \mathbf{c}\|^2 = 4n, \tag{4}$$

which means that either $\|\omega(t, \zeta) - \mathbf{c}\| \leq \sqrt{2n}$ or $\| - \omega(t, \zeta) - \mathbf{c}\| \leq \sqrt{2n}$. It follows that $d_* \leq \sqrt{2n}$.

One of the following two cases can occur:

- Case 1: In this case, there exists $\mathbf{c} \in \mathcal{C}$ and $0 \leq t_* < 1$ such that $\|\mathbf{c} - \omega(t_*, \zeta)\| \leq d_*$. Then

$$\begin{aligned} 2\Re\left(\sum_{i=0}^{n-1} c_i \exp(-2\pi j(\zeta + i)t_*)\right) &= \|\mathbf{c}\|^2 + \|\omega(t_*, \zeta)\|^2 - \|\mathbf{c} - \omega(t_*, \zeta)\|^2 \\ &= 2n - \|\mathbf{c} - \omega(t_*, \zeta)\|^2 \\ &\geq 2n - d_*^2. \end{aligned}$$

We recall from equation (3) that

$$\mathrm{PAPR}(\mathbf{c}) = \max_{0 \leq t \leq 1} \frac{\left|\Re\left(\sum_{i=0}^{n-1} c_i \exp(-2\pi j(\zeta + i)t)\right)\right|^2}{\|\mathbf{c}\|^2}.$$

Thus

$$\mathrm{P}APR(\mathbf{c}) \geq \frac{1}{n}\left|\Re\left(\sum_{i=0}^{n-1} c_i \exp(-2\pi j t_*(\zeta+i))\right)\right|^2 \geq \frac{1}{n}(n-d_*^2/2)^2 = n(1-\delta)^2.$$

We conclude that PAPR($\mathcal{C}$) is at least $n(1-\delta)^2$.

- Case 2: In this case, there exists $\mathbf{c} \in \mathcal{C}$ and $0 \leq t_* < 1$ such that $\|\mathbf{c} - [-\omega(t_*, \zeta)]\| \leq d_*$. Thus

$$\begin{aligned} -2\Re\left(\sum_{i=0}^{n-1} c_i \exp(-2\pi j(\zeta+i)t_*)\right) &= 2n - \|\mathbf{c} + \omega(t_*,\zeta)\|^2 \\ &\geq 2n - d_*^2. \end{aligned}$$

Thus

$$PAPR(\mathbf{c}) \geq \frac{1}{n}\left|-\Re\left(\sum_{i=0}^{n-1} c_i \exp(-2\pi j t_*(\zeta+i))\right)\right|^2 \geq \frac{1}{n}(n-d_*^2/2)^2 = n(1-\delta)^2.$$

Thus in this case the peak-to-average power ratio of $\mathcal{C}$ is at least $n(1-\delta)^2$ as well. □

For any subset S of the n-dimensional complex sphere of radius $\sqrt{n}$ and any $r \geq 0$, we define $H(S,r)$ to be the surface consisting of all those points of the sphere which are within distance r of S. We let $A(S,r)$ denote the area of $H(S,r)$. So for any point $\mathbf{x}$ on the sphere, $H(\mathbf{x},r)$ is a spherical cap. It is well-known that (see for instance [41]):

$$A(r) := A(\mathbf{x},r) = \frac{2\pi^{n-\frac{1}{2}} n^{n-\frac{1}{2}}}{(n-\frac{3}{2})!}\int_0^{2\arcsin(r/2\sqrt{n})} \sin^{2n-2}\theta d\theta. \tag{5}$$

We can now prove the following Lemma.

Lemma 2: Let $\mathcal{C}$ be a code of length n, rate R and Euclidean distance d. Suppose that for some d_* with $\frac{d}{2} \leq d_* \leq \sqrt{2n}$:

$$A(\Omega \cup -\Omega, d_* - \frac{d}{2}) + 2^{nR} A(\frac{d}{2}) \geq \frac{2\pi^n n^{n-\frac{1}{2}}}{(n-1)!}. \tag{6}$$

Then PAPR($\mathcal{C}$) $\geq n(1-\delta)^2$ where $\delta = d_*^2/2n$.

Proof: The spherical caps $H(\mathbf{c}, \frac{d}{2})$, $\mathbf{c} \in \mathcal{C}$ and the surface $H(\Omega \cup -\Omega, d_* - \frac{d}{2})$ must meet or overlap since the sum of their areas is at least that of the area of the n-dimensional complex sphere (given by the right side of inequality (6)). Therefore the minimum distance of $\mathcal{C}$ from the points of the curve $\Omega \cup -\Omega$ is at most d_*. We can now apply Lemma 1. □

We have an explicit expression for the term $2^{nR}A(d/2)$ occurring in the inequality (6). To make the inequality into a usable one, we need to obtain a good lower bound on $A(\Omega \cup -\Omega, d_* - \frac{d}{2})$. Clearly, the curve Ω twists around the sphere many times since ζ is assumed to be large. To obtain our lower bound we will restrict our attention to almost one complete rotation of the curve Ω around the complex sphere. Let $\tilde{\Omega} = \{\omega(t,\zeta) : 0 \leq t < \frac{1}{\zeta}\}$. Clearly, $H(\tilde{\Omega} \cup -\tilde{\Omega}, r) \subseteq H(\Omega \cup -\Omega, r)$ and $A(\tilde{\Omega} \cup -\tilde{\Omega}, r) \leq A(\Omega \cup -\Omega, r)$ for any $r \geq 0$.

We need the following technical result.

Lemma 3: Let $\mathcal{D}$ be the curve on the n-dimensional complex sphere of radius $\sqrt{n}$ given by the set of points

$$\mathcal{D} = \{(\exp(2\pi j\zeta t), \exp(2\pi j\zeta t), \ldots, \exp(2\pi j\zeta t)), 0 \leq t < \frac{1}{\zeta}\}.$$

Notice that replacing each complex coordinate by a pair of real and imaginary coordinates allows us to think of $\mathcal{D}$ as a circle in the plane of the points $(0,1,0,1,\ldots,0,1)$ and $(1,0,1,0,\ldots,1,0)$. Let

$$r_* = r - \frac{2\pi n^{\frac{3}{2}}}{\sqrt{3}\zeta},$$

Then provided that $r_* \geq 0$, we have

$$H(\mathcal{D}, r_*) \subseteq H(\tilde{\Omega} \cup -\tilde{\Omega}, r). \tag{7}$$

Proof: Let $\mathbf{x} \in H(\mathcal{D}, r_*)$. We aim to show that $\mathbf{x} \in H(\tilde{\Omega} \cup -\tilde{\Omega}, r)$. Now there exists $0 \leq t_* < \frac{1}{\zeta}$ such that $\|\mathbf{x} - \mathbf{y}\| \leq r_*$, where

$$\mathbf{y} = (\exp(2\pi j \zeta t_*), \exp(2\pi j \zeta t_*), \ldots, \exp(2\pi j \zeta t_*)).$$

Consider the point $\omega(t_*, \zeta)$ on $H(\tilde{\Omega})$. We have:

$$\begin{aligned}
\|\omega(t_*,\zeta) - \mathbf{y}\|^2 &= \|\omega(t_*,\zeta)\|^2 + \|\mathbf{y}\|^2 - 2\Re(\omega(t_*,\zeta) \cdot \bar{\mathbf{y}}) \\
&= 2n - 2\sum_{i=0}^{n-1} \cos(2\pi i t_*) \\
&= \begin{cases} (2n-1) - \frac{\sin((2n-1)\pi t_*)}{\sin(\pi t_*)} & \text{if } t_* \neq 0 \\ 0 & \text{if } t_* = 0 \end{cases}
\end{aligned}$$

We now recall the inequalities

$$x - \frac{x^3}{6} \leq \sin x \leq x, \quad x \geq 0 \tag{8}$$

Using these inequalities we have, for $t_* \neq 0$,

$$\begin{aligned}
\|\omega(t_*,\zeta) - \mathbf{y}\|^2 &= (2n-1) - \frac{\sin((2n-1)\pi t_*)}{\sin(\pi t_*)} \\
&\leq (2n-1) - \frac{(2n-1)\pi t_* - \frac{[(2n-1)\pi t_*]^3}{6}}{\pi t_*} \\
&= \frac{(2n-1)^3 [\pi t_*]^2}{6} \\
&\leq \frac{4\pi^2 n^3}{3\zeta^2}.
\end{aligned}$$

It follows that

$$\|\omega(t_*,\zeta) - \mathbf{y}\| \leq \frac{2\pi n^{\frac{3}{2}}}{\sqrt{3}\zeta}$$

and so

$$\|\mathbf{x} - \omega(t_*,\zeta)\| \leq \|\mathbf{x} - \mathbf{y}\| + \|\mathbf{y} - \omega(t_*,\zeta)\| \leq r_* + \frac{2\pi n^{\frac{3}{2}}}{\sqrt{3}\zeta} = r.$$

Hence $\mathbf{x} \in H(\tilde{\Omega} \cup -\tilde{\Omega}, r)$. □

Lemma 4: For any $r_* \geq 0$, we have

$$A(\mathcal{D}, r_*) \geq \max\left\{1, \lfloor \frac{\pi}{\arcsin(r_*/\sqrt{n})} \rfloor\right\} \cdot \frac{2\pi^{n-\frac{1}{2}} n^{n-\frac{1}{2}}}{(n-\frac{3}{2})!} \int_0^{2\arcsin(r_*/2\sqrt{n})} \sin^{2n-2}\theta d\theta$$

where we define $\lfloor \frac{\pi}{\arcsin(r_*/\sqrt{n})} \rfloor = 0$ for $r_* \geq \sqrt{n}$.

Proof: Let $\ell = \max\{1, \lfloor \frac{\pi}{\arcsin(r_*/\sqrt{n})} \rfloor\}$ when $0 \leq r_* \leq \sqrt{n}$ and $\ell = 1$ otherwise. Consider any ℓ points $\mathbf{x}_i$, $0 \leq i < \ell$ on the curve $\mathcal{D}$ having circular angular distance $2\arcsin(r_*/\sqrt{n})$ from one another. Then the spherical caps $H(\mathbf{x}_i, r_*)$ do not overlap. Each of these caps is also contained in $H(\mathcal{D}, r_*)$. The lemma follows on using the formula for $A(r_*)$ given in (5). □

We are now ready to give an effective formulation of Lemma 2.

Theorem 5: Let $\mathcal{C}$ denote a code of length n, rate R and Euclidean distance d. Let d_* denote any value of x that is greater than $\frac{d}{2} + \frac{2\pi n^{\frac{3}{2}}}{\sqrt{3}\zeta}$ for which the inequality:

$$\max\{1, \lfloor \frac{\pi}{\theta_2(x)} \rfloor\} \cdot \int_0^{2\theta_1(x)} \sin^{2n-2}\theta d\theta + 2^{nR} \int_0^{2\arcsin(d/4\sqrt{n})} \sin^{2n-2}\theta d\theta \geq \frac{\sqrt{\pi}(n-\frac{3}{2})!}{(n-1)!} \tag{9}$$

is satisfied. Here

$$\theta_1(x) = \arcsin((x - \frac{d}{2} - \frac{2\pi n^{\frac{3}{2}}}{\sqrt{3}\zeta})/2\sqrt{n}), \tag{10}$$

$$\theta_2(x) = \arcsin((x - \frac{d}{2} - \frac{2\pi n^{\frac{3}{2}}}{\sqrt{3}\zeta})/\sqrt{n}) \tag{11}$$

Suppose further that $d_* \leq \sqrt{2n}$. Then $\mathrm{PAPR}(\mathcal{C}) \geq n(1-\delta)^2$ where $\delta = d_*^2/2n$.

Proof: We firstly establish that inequality (9) always has solutions. Notice that on rescaling the inequality throughout by a factor of $\frac{2\pi^{n-\frac{1}{2}} n^{n-\frac{1}{2}}}{(n-\frac{3}{2})!}$, the right side becomes equal to the area of the n-dimensional complex sphere of radius $\sqrt{n}$, while the first term on the left side is lower bounded by the area of a single spherical cap of radius $x - \frac{d}{2} - \frac{2\pi n^{\frac{3}{2}}}{\sqrt{3}\zeta}$. Putting $x = \frac{d}{2} + \frac{2\pi n^{\frac{3}{2}}}{\sqrt{3}\zeta}$ makes this area equal to zero, while putting $x = 2\sqrt{n} + \frac{d}{2} + \frac{2\pi n^{\frac{3}{2}}}{\sqrt{3}\zeta}$ ensures that the cap encompasses the whole sphere. The second term on the left side becomes equal to $2^{nR}A(\frac{d}{2})$ after rescaling, and is non-negative. It follows that the inequality is satisfied for at least some values of x that are greater than or equal to $\frac{d}{2} + \frac{2\pi n^{\frac{3}{2}}}{\sqrt{3}\zeta}$. We let d_* denote any such value.

From Lemma 3, we know that

$$A(\Omega \cup -\Omega, d_* - \frac{d}{2}) \geq A(\tilde{\Omega} \cup -\tilde{\Omega}, d_* - \frac{d}{2}) \geq A(\mathcal{D}, d_* - \frac{d}{2} - \frac{2\pi n^{\frac{3}{2}}}{\sqrt{3}\zeta}).$$

while from Lemma 4, we know that

$$A(\mathcal{D}, d_* - \frac{d}{2} - \frac{2\pi n^{\frac{3}{2}}}{\sqrt{3}\zeta}) \geq \max\{1, \lfloor \frac{\pi}{\theta_2(d_*)} \rfloor\} \cdot \frac{2\pi^{n-\frac{1}{2}} n^{n-\frac{1}{2}}}{(n-\frac{3}{2})!} \int_0^{2\theta_1(d_*)} \sin^{2n-2}\theta d\theta$$

where we again define $\lfloor \frac{\pi}{\theta_2(d_*)} \rfloor$ to equal 0 when the arcsin function in θ_2 is undefined. So from the inequality (9) which holds for $x = d_*$, we obtain the inequality:

$$A(\Omega \cup -\Omega, d_* - \frac{d}{2}) + 2^{nR} A(\frac{d}{2}) \geq \frac{2\pi^n n^{n-\frac{1}{2}}}{(n-1)!}.$$

The theorem now follows from Lemma 2. □

The above bound is somewhat computationally unwieldy except perhaps for relatively small values of n. However, it does prove that there is a trade-off between the parameters rate, minimum Euclidean distance and PAPR of a code. It shows in a strict sense that redundancy introduced by considering only those codewords with low PAPR cannot all be exploited to provide error correction. Informally, this is because the words of low PAPR are restricted to lie in a certain region of the sphere, and this region shrinks as the PAPR decreases. Theorem 5 makes this numerically explicit.

It seems difficult to perform an asymptotic analysis of the bound that might establish a region of pairs of rate and minimum Euclidean distance beyond which the PAPR of a code must grow faster than a certain function. This difficulty can be partially explained from the existence results that we establish in the next section: we postpone further discussion of the strength of our lower bound until then.

IV. On the existence of codes with a given minimum distance and PAPR

In this section, we assume that d and d_* are given and prove the existence of codes of length n, minimum distance at least d and peak-to-average power ratio at most d_*. Our tool is a Varshamov-Gilbert type of argument. We require a technical lemma whose proof can be found in the appendix.

Lemma 6: Let $c(z)$ be a polynomial of degree $n-1$ over $\mathbb{C}$. Let $W = \lceil 2\pi(n-1) \rceil$. Then

$$\max_{|z|=1} |c(z)| \leq 2 \cdot \max_{0 \leq k < W} |c(\exp(-2\pi jk/W))| .$$

Theorem 7: Let d and d_* be given and let 2^{nR} be the largest integer for which

$$4\lceil 2\pi(n-1) \rceil A(d_*) + 2^{nR} A(d) \leq \frac{2n^{n-\frac{1}{2}}\pi^n}{(n-1)!}$$

holds. Then there exists a code $\mathcal{C}$ of rate R with minimum Euclidean distance at least d and peak-to-average power ratio at most $8n(1-\delta)^2$ where $\delta = d_*^2/2n$.

Proof: Let $W = \lceil 2\pi(n-1) \rceil$. We define the vectors

$$\mathbf{v}_k = (1, \exp(2\pi jk/W), \exp(2\pi j 2k/W), \ldots, \exp(2\pi j(W-1)k/W)), \quad 0 \leq k < W,$$

and

$$\mathbf{v}_{k+W} = -\mathbf{v}_k, \quad 0 \leq k < W.$$

Consider the spherical caps $I(\mathbf{v}_k, d_*)$, $I(j\mathbf{v}_k, d_*)$, $k = 0, 1, \ldots, 2W-1$ on the n-dimensional complex sphere of radius $\sqrt{n}$. Suppose that the sum of the areas of these caps is less than the area of this sphere. Then we can choose a point $\mathbf{c}_0$ on the sphere which is not in the union of these caps.

Inductively, let us assume that the codewords $\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{\ell-1}$ ($\ell \geq 1$) are chosen. Then we consider the spherical caps $H(\mathbf{v}_k, d_*)$, $H(j\mathbf{v}_k, d_*)$, $k = 0, 1, \ldots, 2W-1$ and $H(\mathbf{c}_i, d)$, $i = 0, 1, \ldots, \ell-1$. If the sum of areas of these caps is less than the area of the n-dimensional complex sphere of radius $\sqrt{n}$, then we can choose a codeword $\mathbf{c}_\ell$ which is not in the union of the caps. It is easy to see that this process can be repeated as long as

$$4\lceil 2\pi(n-1) \rceil A(d_*) + (\ell+1) A(d) \leq \frac{2n^{n-\frac{1}{2}}\pi^n}{(n-1)!}.$$

At the end of the induction process, we have chosen points $\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{2^{nR}-1}$. We define the code $\mathcal{C}$ to consist of these points. Clearly this code has minimum distance at least d by virtue of the manner in which the codewords were chosen. Furthermore, the distance between any codeword $\mathbf{c}$ and any of $\mathbf{v}_k$, $j\mathbf{v}_k$ ($0 \leq k < 2W-1$) is at least d_*. We thus have

$$\begin{aligned}
\|\mathbf{c} - \mathbf{v}_k\| &\geq d_*, \quad 0 \leq k < W, \\
\|\mathbf{c} + \mathbf{v}_k\| &\geq d_*, \quad 0 \leq k < W, \\
\|\mathbf{c} - j\mathbf{v}_k\| &\geq d_*, \quad 0 \leq k < W, \\
\|\mathbf{c} + j\mathbf{v}_k\| &\geq d_*, \quad 0 \leq k < W.
\end{aligned}$$

which together imply that:

$$\begin{aligned}
2\left| \Re\left(\sum_{i=0}^{n-1} c_i \exp(-2\pi jki/W) \right) \right| &\leq 2n - d_*^2, \quad 0 \leq k < W, \\
2\left| \Im\left(\sum_{i=0}^{n-1} c_i \exp(-2\pi jki/W) \right) \right| &\leq 2n - d_*^2, \quad 0 \leq k < W.
\end{aligned}$$

Writing $c(z) = \sum_{i=0}^{n-1} c_i z^i$, these can be written as

$$2\,|\Re\left(c(\exp(-2\pi jk/W))\right)| \leq 2n - d_*^2, \quad 0 \leq k < W,$$
$$2\,|\Im\left(c(\exp(-2\pi jk/W))\right)| \leq 2n - d_*^2, \quad 0 \leq k < W.$$

We deduce that

$$|c(\exp(-2\pi jk/W))| \leq \sqrt{2}(n - \frac{d_*^2}{2}), \quad 0 \leq k < W.$$

Applying Lemma 6, we conclude that for all z with $|z| = 1$,

$$|c(z)| \leq 2\sqrt{2}(n - \frac{d_*^2}{2}).$$

Thus

$$\mathrm{PAPR}(\mathbf{c}) \leq \mathrm{PMEPR}(\mathbf{c}) = \frac{1}{n} \max_{|z|=1} |c(z)|^2 \leq 8n(1-\delta)^2$$

where $\delta = d_*^2/2n$. This completes the proof. □

V. Asymptotic interpretation of the Varshamov-Gilbert lower bound

In this Section, we analyze the asymptotics of the bound established in Theorem 7.

An Inequality of Shannon: For our analysis, we will need to estimate the area of a spherical cap. For a completely different purpose, it transpires that Shannon has considered the function $A(r)$ and asymptotic approximations to it. Indeed, he establishes [41, p. 292] that, for $\theta_1 < \frac{\pi}{2}$

$$\frac{\sin^{2n-1}\theta_1}{\cos\theta_1}(1 - \frac{1}{2n}\tan^2\theta_1) \leq (2n-1)\int_0^{\theta_1} \sin^{2n-2}\theta d\theta \leq \frac{\sin^{2n-1}\theta_1}{\cos\theta_1} \tag{12}$$

This means in particular that

$$0 \leq \int_0^{\theta_1} \sin^{2n-2}\theta d\theta \leq \frac{\sin^{2n-1}\theta_1}{(2n-1)\cos\theta_1}. \tag{13}$$

for any $n \geq 2$ and $0 \leq \theta_1 < \frac{\pi}{2}$.

We can now prove an existence result showing that asymptotically good codes with low peak-to-average power ratio exist. Our result is summarised in the following result.

Theorem 8: Let $R \geq 0$, $\epsilon > 0$, and $\Delta \geq 0$ be such that

$$2^R\sqrt{2\Delta(1 - \frac{\Delta}{2})} < 1.$$

Then for all sufficiently large n, there exists a code $\mathcal{C}$ of length n, rate R and minimum distance $d = \sqrt{2\Delta n}$ having peak-to-average power ratio of at most $8\log n$.

Proof: Write $\delta = 1 - \sqrt{\frac{\log n}{n}}$. By Theorem 7, provided that

$$4\lceil 2\pi(n-1)\rceil A(\sqrt{2\delta n}) + 2^{nR}A(\sqrt{2\Delta n}) \leq \frac{2n^{n-\frac{1}{2}}\pi^n}{(n-1)!},$$

then there exists a code $\mathcal{C}$ of rate R with minimum Euclidean distance at least d and peak-to-average power ratio at most $8n(1-\delta)^2 = 8\log n$. We thus have to prove that the above inequality holds for all sufficiently large n.

We replace the expression for $A(r)$ given in equation (5) in the above inequality. After simple manipulations, we observe that it suffices to prove that the inequality

$$4\lceil 2\pi(n-1)\rceil \int_0^{2\arcsin(\sqrt{2\delta}/2)} \sin^{2n-2}\theta d\theta + 2^{nR}\int_0^{2\arcsin(\sqrt{2\Delta}/2)} \sin^{2n-2}\theta d\theta \leq \frac{2\sqrt{\pi}(n-\frac{3}{2})!}{(n-1)!} \tag{14}$$

holds for all sufficiently large n. We now use the above inequality of Shannon. After further computations, and using the Wallis product identity to observe that for large n,

$$\frac{(n-\frac{3}{2})!}{(n-1)!} \approx \frac{2}{\sqrt{n}},$$

it can be shown that it suffices to prove that the inequality

$$4\pi\sqrt{n}\frac{2n-2}{(2n-1)}\frac{\sin^{2n-1}(\theta_1)}{\cos(\theta_1)} + \frac{\sqrt{n}}{(2n-1)}2^{nR}\frac{\sin^{2n-1}(\theta_2)}{\cos(\theta_2)} \leq 2\sqrt{\pi} \tag{15}$$

holds asymptotically, where

$$\theta_1 = 2\arcsin(\sqrt{2\delta}/2),$$
$$\theta_2 = 2\arcsin(\sqrt{2\Delta}/2).$$

Because $2^R\sin(\theta_2) = 2^R\sqrt{2\Delta(1-\frac{\Delta}{2})} < 1$, we see that

$$\lim_{n\to\infty}\frac{\sqrt{n}}{(2n-1)}2^{nR}\frac{\sin^{2n-1}(\theta_2)}{\cos(\theta_2)} = 0.$$

It is also easy to show that $\sin(\theta_1) = \sqrt{2\delta(1-\frac{\delta}{2})} < 1$. It follows that $\sin(\theta_1) = \sqrt{1-\frac{\log n}{n}}$. Thus $\sin^2(\theta_1) = 1-\frac{\log n}{n}$ and $\cos(\theta_1) = \sqrt{\frac{\log n}{n}}$. Then we have

$$4\pi\sqrt{n}\frac{2n-2}{(2n-1)}\frac{\sin^{2n-1}(\theta_1)}{\cos(\theta_1)} = \frac{4\pi n}{\sqrt{\log n}}\frac{2n-2}{(2n-1)}(1-\frac{\log n}{n})^{(n-0.5)}$$

But $n(1-\frac{\log n}{n})^n \to 1$ as $n\to\infty$ and so

$$\lim_{n\to\infty} 4\pi\sqrt{n}\frac{2n-2}{(2n-1)}\frac{\sin^{2n-1}(\theta_1)}{\cos(\theta_1)} = 0.$$

Thus inequality (15) holds for all sufficiently large n and the result is proved. □

The above theorem establishes a region of pairs (R,Δ) in which asymptotically good sequences of codes with PAPR no greater than $8\log n$ are guaranteed to exist. In fact, a result of [13] can be used to show that for a BPSK constellation, a randomly chosen word almost certainly has PAPR $(1+o(1))\log n$. From this it can be shown that with probability 1, an asymptotically good BPSK code has PAPR growing as $O(\log n)$. This does not preclude the existence of individual BPSK codes with PAPR growth of lower order, however. We see that even though our result constructs constant energy codes rather than BPSK codes, it is consistent with the results of [13]. Moreover, we show that asymptotically good codes with low PAPR exist in a non-probablistic sense.

Our result can be further interpreted as saying that in a certain region of (R,Δ) pairs, considering asymptotically good code sequences does not have a catastrophic impact on PAPR. In fact, the restriction to (R,Δ) pairs satisfying $2^R\sqrt{2\Delta(1-\frac{\Delta}{2})} < 1$ is only used in the proof to establish the 'classical' part of the Varshamov-Gilbert bound, that the caps of an appropriate radius around code points can be packed onto the sphere, so that the code has a certain minimum Euclidean distance. The PAPR part of the result comes from examining

the asymptotic behaviour of the term $4\lceil 2\pi(n-1)\rceil A(\sqrt{2\delta n})$ with δ appropriately chosen so as to yield a PAPR of at most $8\log n$, and this analysis is independent of the pair (R,Δ) under consideration. So our geometric interpretation of PAPR allows us to examine the coding properties and the PAPR properties of a code in a common framework, and allows us to separate their contributions to packing bounds. This observation, and the fact that (at least in the BPSK case) the PAPR of a code is almost certainly $O(\log n)$, partly explains why we have been unable to perform an analysis of Theorem 5 for sequences of codes that are asymptotically good in the usual coding-theoretic sense. Indeed, the PAPR growth of any sequence of asymptotically good codes satisfying a Euclidean analogue of the Varshamov-Gilbert bound need be no more than of order $\log n$. This suggests that the lower bound of Theorem 5 may have interesting implications for the region of achievable (R,Δ) pairs in the case where PAPR is restricted to have growth strictly less than $O(\log n)$. We have not attempted such an analysis.

VI. Explicit construction of codes with low PAPR from exponential sums

We have seen in the previous section that asymptotically good sequences of constant energy codes with PAPR of order $\log n$ exist. In this section and the next, we give explicit constructions for three families of codes whose PAPRs we can bound as $O((\log n)^2)$. Unfortunately, none of the families yields asymptotically good sequences of codes. In our defence, we note that setting aside any PAPR constraint, even the explicit construction of asymptotically good codes is a notoriously difficult problem.

The families we consider are length 2^m, 2^e-PSK codes and are derived from special cases of what we call *lengthened trace codes*. The lengthened trace codes are linear over $\mathbb{Z}_{2^e}$ and their codewords can be roughly characterised as having a representation as the trace of a polynomial function evaluated on a finite field ($e=1$) or Galois ring ($e>1$). Our first family is derived from the set of lengthened duals of binary, primitive BCH codes [26, Chapter 9]. The other two families are derived from $\mathbb{Z}_{2^e}$-analogues of the first and were introduced in [15], [21]. Loosely speaking, for each integer $t\geq 1$, we construct a set of BPSK codes of length $n=2^m$, rate $t\log n$ and minimum squared Euclidean distance $\simeq 2n-4(t-1)\sqrt{n}$ which have PAPR bounded by $O((t\log n)^2)$. The parameters of the other two families can be similarly stated.

Our approach to bounding the PAPRs of these codes is as follows. We recall that the PAPR of a codeword $\mathbf{c}$ is bounded by

$$\mathrm{PAPR}(\mathbf{c}) \leq \mathrm{PMEPR}(\mathbf{c}) = \frac{1}{\|\mathbf{c}\|^2}\max_{|z|=1}|c(z)|^2.$$

where $c(z)=c_0+c_1z+\cdots+c_{n-1}z^{n-1}$ denotes the degree $n-1$ polynomial whose coefficients are derived from $\mathbf{c}$. We show how Lagrange interpolation allows us to translate a bound on the absolute values of a degree $n-1$ polynomial at the n-th roots of unity into a (weaker) bound that is valid on the whole unit circle. This method was suggested to us by P. Borwein. Then we show how *hybrid character sums* over Galois fields and rings can be used get bounds on $|c(z)|$ at the roots of unity for polynomials $c(z)$ corresponding to the 2^e-PSK versions of codewords $\mathbf{c}$ of the length 2^m-1 trace codes. Finally, we use these results to obtain bounds on PMEPR for the 2^e-PSK versions of non-constant codewords of the lengthened trace codes (obtained from the original trace codes by adding a constant codeword and an overall parity check). We note that similar techniques can be used to obtain bounds for length p^m codes over p^e-PSK constellations, p an odd prime. These codes are of less immediate practical relevance for OFDM however.

A. Lagrange interpolation

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

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

where

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

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

$$\max_{|z|=1} |c(z)| \le \max_{|z|=1} \sum_{\ell=0}^{n-1} |\rho_\ell(z)| \cdot \max_{0 \le \ell < n} |c(\nu^\ell)|. \tag{16}$$

For our purposes, we need to bound $\max_{|z|=1} \sum_{\ell=0}^{n-1} |\rho_\ell(z)|$ in (16). Such a result is provided by the following Lemma, whose proof is given in the appendix:

Lemma 9: We have:

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

B. Background on exponential sums over Galois fields and rings

We quote the bounds for exponential sums over Galois fields of characteristic 2 that we need, give some background on Galois rings of characteristic 2^k and report the analogous bounds for exponential sums over Galois rings. Further reading on finite fields may be found in [23] and on Galois rings in [21].

In what follows, $\mathbb{F}_{2^m}$ denotes the Galois (finite) field with 2^m elements. 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.

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

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

The maps χ_ℓ are called the *multiplicative characters* of $\mathbb{F}_{2^m}$. The map χ_0 is called the *trivial* multiplicative character. We define the *order* of a multiplicative character χ to be the least positive integer d such that $\chi^d = \chi_0$.

Definition 10: 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.

We now state the required bounds on exponential sums.

Result 11: [26, 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:

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

Result 12: [39, 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

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

Now we turn our attention to Galois rings. In what follows, $R_{e,m}$ denotes the Galois ring of characteristic 2^e and degree m. 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

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

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:

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

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

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

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

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

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

$$\chi_\ell(x) = \nu^{\ell i}, \quad x \in R^*_{e,m}$$

where $\nu = \exp(2\pi j/(2^m - 1))$ and $x = \beta^i \bmod 2$ with $0 \le i < 2^m - 1$. (The modulo 2 reduction map is a homomorphism which, when applied to $R^*_{e,m}$, yields the non-zero elements of $\mathbb{F}_{2^m}$. The image of β under this map is a primitive element $\alpha \in \mathbb{F}_{2^m}$. So for any $x \in R^*_{e,m}$ we have $x \bmod 2 = \alpha^i$ for some $0 \le i < 2^m - 1$ and then $x = \beta^i \bmod 2$).

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

Definition 13: 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 $\sigma(\sum_i g_i x^i) = \sum_i \sigma(g_i)x^{2i}$. 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 $g(x) = \sum_{i=0}^d g_i x^i$. 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_i is the degree of F_i.

We have the following results bounding exponential sums over Galois rings.

Result 14: [21, 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

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

Result 15: [40, 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

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

VII. On the PAPRs of trace codes

We are now ready to introduce the three distinct classes of trace code that we consider and to derive our bounds on their PAPRs.

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 $n = 2^m - 1$, $\{+1, -1\}$-valued vector $\mathbf{c}_f$ whose components are

$$(c_f)_i = (-1)^{\mathrm{tr}_1^m(f(\alpha^i))}, \quad 0 \leq i < 2^m - 1$$

and the corresponding degree $n-1$ polynomial with $\{+1, -1\}$-valued coefficients $c_f(z) = \sum_{i=0}^{n-1} (c_f)_i z^i$. Let $t \geq 1$. Then we define $\mathcal{C}_t^-$ to be the set:

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

It is clear that $\mathcal{C}_t^-$ is derived from a binary code by mapping the binary alphabet into a BPSK constellation. The underlying binary code is in this case the dual of the binary, primitive t-error correcting BCH code. It is well known that, for $2t - 1 < 2^{\lceil m/2 \rceil} + 1$, this code 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 11 — see [26, Theorem 18, p. 280] for details. This bound on minimum distance can be improved in certain cases [27].

With this definition, we now prove:

Theorem 16: Let $\mathcal{C}_t^-$ be as defined above. Then any non-constant codeword of $\mathcal{C}_t^-$ has PMEPR at most

$$\frac{2^m}{2^m - 1}(2t-1)^2 \left(\frac{2 \log 2}{\pi}(m+1) + 2 \right)^2.$$

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

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

As before, let $\nu = \exp(2\pi j/n)$ where $n = 2^m - 1$. Then for $0 \leq \ell < n$,

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

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 11.

For $\ell \neq 0$, χ_ℓ is a non-trivial multiplicative character and Result 12 with $r = 2t-1$ and $s = 1$ yields

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

Thus $\max_{0\leq\ell<n} |c_f(\nu^\ell)| \leq (2t-1)2^{m/2}$. Applying inequality (16) and Lemma 9, we obtain

$$\max_{|z|=1} |c_f(z)| \leq (2t-1)2^{m/2}(\frac{2}{\pi}\log(2(2^m-1))+2) \tag{17}$$

and hence

$$\text{PMEPR}(\mathbf{c}_f) = \frac{1}{2^m-1}\max_{|z|=1}|c_f(z)|^2 \leq \frac{2^m}{2^m-1}\cdot(2t-1)^2(\frac{2}{\pi}\log(2(2^m-1))+2)^2$$

from which the theorem follows. □

A number of notes on Theorem 16 are in order.

We firstly examine in more detail the case $t = 1$ of the theorem. Here $\mathcal{C}_t^-$ is derived from the binary simplex code with parameters $[2^m-1, m, 2^{m-1}]$. All the non-zero codewords in this code are cyclic shifts of the sequence with terms $\text{tr}_1^m(\alpha^i)$, which is an m-sequence (maximal length shift register sequence). These sequences were proposed for use in OFDM in [25]. Unfortunately, as was pointed out in [18], the calculation of the power properties of m-sequences in [25] is incorrect. Our theorem provides to our knowledge the first bound on the PMEPR of m sequences. The bound is of order $(\log n)^2$ where n is the sequence length.

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 17: [22] 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 $\text{tr}_s^m\lambda \neq 0$ (or both). Then

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

We also note that similar (but slightly weaker) bounds on PMEPR can be derived for the duals of non-primitive BCH codes too.

Finally, we show how Theorem 16 can be adapted to handle the BPSK codes $\mathcal{C}_t$ obtained from lengthened versions of the dual BCH codes. Here $\mathcal{C}_t$ is obtained by adding to the dual BCH code the complements of all codewords and then an overall parity check. This produces a code of length 2^m whose dimension is one greater than that of original code and whose minimum distance is the same. In the case $t = 1$, this code is equivalent to the binary first-order Reed-Muller code $RM(1, m)$. Notice that the polynomials $d(z)$ corresponding to codewords of $\mathcal{C}_t$ can be written as $d(z) = c' + zc(z)$ where $c' \in \mathbb{C}$ satisfies $|c'| = 1$ and where $c(z)$ is a polynomial corresponding to a codeword of $\mathcal{C}_t^-$. Hence $\max_{|z|=1}|d(z)| \leq 1+\max_{|z|=1}|c(z)|$ and it is easy, using inequality (17), to prove:

Corollary 18: Let $\mathcal{C}_t$ be obtained by lengthening $\mathcal{C}_t^-$. Then any non-constant codeword of $\mathcal{C}_t$ has PMEPR at most $(2t-1)^2\left(\frac{2\log 2}{\pi}(m+1)+3\right)^2$.

B. The 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 $\mathbf{c}_f$ whose components are:

$$(c_f)_i = \omega^{\text{Tr}_1^m(f(\beta^i))}, \quad 0 \leq i < 2^m-1.$$

where $\omega = \exp(2\pi j/2^e)$ is a 2^e-th root of unity, and a degree $n-1$ polynomial

$$c_f(z) = \sum_{i=0}^{n-1} (c_f)_i z^i.$$

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

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

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

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

The code $\mathcal{K}^-$ contains 2^{2m} words and the code $\mathcal{DG}_t^-$ contains 2^{2m+tm} words. The minimum Lee distances of the quaternary codes underlying $\mathcal{K}^-$ 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 14 and the fact that non-zero codewords of the codes are obtained from non-degenerate polynomials having weighted degrees 2 and $2^t + 1$. These bounds on minimum distances can be improved for m odd [16] to obtain the quaternary codes' true minimum Lee distances of $2^m - 2^{\frac{m-1}{2}}$ and $2^m - 2^{r+\frac{m-1}{2}}$ respectively. Of course, bounds on the minimum Euclidean distances of the QPSK codes can be obtained directly from Result 14.

The underlying quaternary codes can be lengthened by adding a coordinate corresponding to $f(0)$ (an overall parity check) and then adding modulo 4 to every codeword multiples of the all-one codeword. This yields quaternary codes whose QPSK versions we denote by $\mathcal{K}$ and $\mathcal{DG}_t$. When m is odd, the images under the Gray map of the lengthened quaternary codes are the well-known Kerdock and Delsarte-Goethals codes [15].

We have:

Theorem 19: Any non-constant codeword of $\mathcal{K}^-$ has PMEPR at most

$$4\frac{2^m}{2^m-1}\left(\frac{2\log 2}{\pi}(m+1)+2\right)^2$$

and any non-constant codeword of $\mathcal{DG}_t^-$ has PMEPR at most

$$\frac{2^m}{2^m-1}(2^t+1)^2\left(\frac{2\log 2}{\pi}(m+1)+2\right)^2.$$

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

Let $\nu = \exp(2\pi j/n)$ where $n = 2^m - 1$. Then for $0 \le \ell < n$,

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

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 14. For $\ell \ne 0$, χ_ℓ is a non-trivial multiplicative character and Result 15 yields

$$|c_f(\nu^\ell)| \le (2^t+1)\cdot 2^{m/2}, \quad 1 \le \ell < n.$$

Thus $\max_{0\le\ell<n}|c_f(\nu^\ell)| \le (2^t+1)\cdot 2^{m/2}$. Applying inequality (16) and Lemma 9, we obtain

$$\max_{|z|=1}|c_f(z)| \le (2^t+1)2^{m/2}(\frac{2}{\pi}\log(2(2^m-1))+2)$$

and hence

$$\mathrm{PMEPR}(\mathbf{c}_f) = \frac{1}{2^m-1}\max_{|z|=1}|c_f(z)|^2 \le \frac{2^m}{2^m-1}\cdot(2^t+1)^2(\frac{2}{\pi}\log(2(2^m-1))+2)^2$$

from which the theorem follows. □

We also have the following corollary, whose proof is similar to that of Corollary 18

Corollary 20: Any non-constant codeword of $\mathcal{K}$ has PMEPR at most $4\left(\frac{2\log 2}{\pi}(m+1)+3\right)^2$. Any non-constant codeword of $\mathcal{DG}_t$ has PMEPR at most $(2^t+1)^2\left(\frac{2\log 2}{\pi}(m+1)+3\right)^2$.

C. Weighted degree trace codes

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

$$\mathcal{C}_t^- = \{\mathbf{c}_f : f \in R_{e,m}[x], f = \sum_{j=0}^{t-1} f_{2j+1}x^{2j+1}, D_f \le 2t-1\}.$$

Thus $\mathcal{C}_t^-$ is a code of length $n = 2^m-1$ obtained from a set of non-degenerate polynomials of weighted degree at most $2t-1$. The underlying 2^e-ary code is linear over $\mathbb{Z}_{2^e}$ and when $e=1$, coincides with the dual of the t-error correcting BCH code introduced in Section VII-A.

It can be shown, using 2-adic expansions and simple counting, that $|\mathcal{C}_t^-| = 2^{(D-\lfloor D/4\rfloor)m}$ when $e=2$ and that $|\mathcal{C}_t^-| = 2^{(D+1-wt_H(D+1 \bmod 2^e)-\lfloor D+1/2^e\rfloor)m}$ when $e>2$. Here $d=2t-1$. Result 15 can be applied to show that the minimum Lee distance of the 2^e-ary version of $\mathcal{C}_t^-$ is at least $2^m-(2t-2)2^{m/2}$ when $e=2$. This bound can be improved in certain cases [16]. For $e>2$, Result 15 can be used to lower-bound the minimum Euclidean distance of the code. The following theorem can be proved using an almost identical argument to that used in the proof of Theorem 19:

Theorem 21: Any non-constant codeword of $\mathcal{C}_t^-$ has PMEPR at most

$$\frac{2^m}{2^m-1}(2t-1)^2\left(\frac{2\log 2}{\pi}(m+1)+2\right)^2.$$

Notice that the bounds on PMEPR in Theorem 16 for the dual BCH codes and in Theorem 21 for the weighted degree trace codes are identical.

The codes $\mathcal{C}_t^-$ can also be lengthened to produce codes $\mathcal{C}_t$ and the following corollary is now easily established:

Corollary 22: Any non-constant codeword of $\mathcal{C}_t$ has PMEPR at most

$$(2t-1)^2\left(\frac{2\log 2}{\pi}(m+1)+3\right)^2.$$

VIII. Conclusions and open problems

In this paper, we established the first lower bound on the PAPR of a code $\mathcal{C}$ defined over a unit energy signal constellation as a function of its rate, distance and length. The bound suggests that a reduction in the peak-to-average power ratio (reducing the cost of power amplifiers in a multicarrier communications) can be penalised by a decrease in rate and/or distance. We also established a lower bound on the achievable rate of a code given its distance and peak-to-average power ratio. These bounds are related to a generalisation of the classical sphere packing to the case where the points to be packed on the surface of a sphere are required to be further than a threshold from some curves. The practical significance of the peak-to-average power ratio problem motivates the further study of this *generalised packing problem.*

We have not provided an asymptotic analysis of our lower bound. It is conceivable that an analysis of this bound involving PAPR growth of order less than $O(\log n)$ would yield non-trivial restrictions on the achievable region of (R, Δ) pairs for asymptotically good sequences of codes (where we now allow $\zeta = \zeta_n$ to depend explicitly on n and assume that $\lim_{n\to\infty} n^{\frac{3}{2}}/\zeta_n = 0$). For example,is there a least restrictive condition that must be put on PAPR growth in order to show that any sequence of codes either has R or Δ tending to zero?

In the other direction, the existence of asymptotically good sequences of codes with PAPR growth strictly less than order $\log n$ is not ruled out by the results of [13] or by our results. But finding such sequences of codes requires a deeper understanding of the words with low PAPR, or if even they exist at all in sufficient numbers. We note that the Reed-Muller based codes presented in [10], [32] have constant PAPR, but do not yield asymptotically good codes (since their rates tend rapidly to zero).

We have concentrated in this paper on constant energy codes, and as a special case, signal constellations such as PSK which have constant absolute values. Indeed our bound in Theorem 5 applies directly to constant energy codes, and our existence result in Theorem 7 also constructs constant energy codes. It may be possible to obtain improved bounds by considering the more restrictive class of PSK codes, c.f. [34]. Also, in practice, non-constant constellations are of interest, for example the 16-QAM and 64-QAM constellations. It would be of interest to extend our theory to handle such constellations.

Motivated by our Varshamov-Gilbert style existence theorem, we attempted to construct families of codes with low PAPR. We used bounds for exponential sums over Galois fields and rings to establish PMEPR (and hence PAPR) bounds for trace codes, in particular for three families of length 2^m codes: the extended duals of primitive, binary BCH codes, the $\mathbb{Z}_4$-analogues of the Kerdock and Delsarte-Goethals codes, and the extended weighted degree trace codes. None of these codes families yields asymptotically good sequences of codes.

The bounds that we have developed on the PMEPRs of trace codes apply directly to the codes themselves rather than to offsets (or cosets) of the codes [20], [43]. It may be possible to obtain significant reductions in PMEPR by using such offsets, and we leave the analytical determination of good offsets for trace codes as a difficult open problem.

In fact, the PMEPR bounds in Corollaries 18, 20 and 22 are unlikely to be tight. The factor of order $(\log n)^2$ in each bound arises from our use of Lagrange interpolation, in particular the bound in Lemma 9. On the other hand, the exponential sum bounds predict that at n discrete times over a symbol period (corresponding to the n-th roots of unity), the instantaneous-to-average powers of the codewords of the trace codes are actually of *constant* order (i.e. independent of n). So it seems plausible that the order of magnitude in each of our bounds could be lowered from $O((\log n)^2)$ to, say, $O(\log n)$. Such an improvement would not be inconsistent with the results of [13] on the expected maximum absolute value of *random* polynomials on the unit circle and may come from a more careful analysis of the sum in Lemma 9, or by using entirely new techniques.

We also note that the techniques developed in Sections VI and VII of 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 $c(z)$ associated with a codeword $\mathbf{c}$ are just the coefficients of the discrete Fourier transform of $\mathbf{c}$. Lemma 9 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. We ask: which other families of classical error-correcting codes have small DFTs?

IX. Acknowledgement

The authors wish to thank Dr. A.R. Calderbank, Dr. H. Jafarkhani and Dr. J. Jedwab for valuable comments and suggestions.

Appendix

In this appendix, we prove Lemmas 6 and 9.

Our proof of Lemma 6 is obtained by correcting an argument of Beck [2]. We require an additional classical result from complex analysis known as Bernstein's inequality.

Lemma 23: Let $c(z)$ be a polynomial of degree $n-1$ over $\mathbb{C}$. Then

$$\max_{|z|=1} |c'(z)| \leq (n-1) \cdot \max_{|z|=1} |c(z)|.$$

Writing $z = \exp(2\pi j\beta)$, we can restate the above lemma as:

$$\max_{0\leq\beta<1} |c'(\exp(2\pi j\beta))| \leq 2\pi(n-1) \cdot \max_{0\leq\beta<1} |c(\exp(2\pi j\beta))|.$$

Proof: (of Lemma 6) Recall that $W = \lceil 2\pi(n-1) \rceil$. Suppose $M = \max_{|z|=1} |c(z)|$ is attained at $z = \exp(2\pi j\beta)$ where $0 \leq \beta < 1$. Then for some i with $0 \leq i < W$, we have

$$\left| \beta - \frac{-i}{W} \right| \leq \frac{1}{2W}$$

and then

$$\begin{aligned}
|M - |c(\exp(-2\pi ji/W))|\,| &= |\,|c(\exp(2\pi j\beta))| - |c(\exp(-2\pi ji/W))|\,| \\
&\leq |c(\exp(2\pi j\beta)) - c(\exp(-2\pi ji/W))| \\
&= \left| \int_{-i/W}^{\beta} c'(\exp(2\pi j\theta)) d\theta \right| \\
&\leq \int_{-i/W}^{\beta} |c'(\exp(2\pi j\theta))| d\theta \\
&\leq \left| \beta - \frac{-i}{W} \right| \max_{0\leq\theta<1} |c'(\exp(2\pi j\theta))| \\
&\leq \frac{1}{2W} \cdot 2\pi(n-1) \max_{0\leq\theta<1} |c(\exp(2\pi j\theta))| \\
&= \frac{\pi(n-1)M}{W}.
\end{aligned}$$

Hence

$$M \leq \frac{1}{1 - \frac{\pi(n-1)}{W}} \cdot |c(\exp(-2\pi ji/W))| \leq 2 \max_{0\leq k<W} |c(\exp(-2\pi jk/W))|$$

and the proof is complete. □

Proof: (of Lemma 9) Let $|z| = 1$. It is then easy to show that $\rho_\ell(z) = \rho_{\ell+a}(\nu^a z)$ for any integer a, where $\ell + a$ is computed modulo n. Hence

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

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

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

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

It is not hard to show that $|g_\ell(\nu^\ell)| = n$ 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 $z \neq \nu^\ell$, we have:

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

so

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

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

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

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 [38] 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. □

References

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

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

[3] P. A. Bello, "Selective fading limitations of the Kathryn modem and some system design considerations," *IEEE Trans. Commun. Technol.*, vol. 13, pp. 320–333, Sept. 1965.

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

[5] R. W. Chang, "Synthesis of band-limited orthogonal signals for multichannel data transmission," *Bell Syst. Tech. J.*, vol. 45, pp. 1775–1796, Dec. 1966.

[6] R. W. Chang and R. A. Gibbey, " A theoretical study of performance of an orthogonal multiplexing data transmission scheme," *IEEE Trans. Commun. Technol.,* vol. 16, pp. 529–540, Aug. 1968.

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

[8] L. J. Cimini, Jr., "Analysis and simulation of a digital mobile channel using orthogonal frequency division multiplexing," *IEEE Trans. Commun.*, vol. 33, pp. 665–675, July 1985.

[9] J. A. Davis and J. Jedwab, "Peak-to-mean power control and error correction for OFDM transmission using Golay sequences and Reed-Muller codes," *Elec. Lett.*, vol. 33, pp. 267–268, 1997.

[10] J. A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences and Reed-Muller codes," *IEEE Trans. Inform. Theory*, to appear.

[11] M. L. Doelz, E. T. Heald and D. L. Martin, "Binary data transmission techniques for linear systems," *Proc. IRE,* vol. 45, pp. 656–661, May 1957.

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

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

[14] A.J. Grant and R.D.J. van Nee, "Efficient maximum-likelihood decoding of Q-ary modulated Reed-M-uller codes," *IEEE Comm. Lett.*, vol. 2, pp. 134–136, 1998.

[15] 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*, vol. 40, pp. 301–319, 1994.

[16] T. Helleseth, P.V. Kumar, O. Moreno and A.G. Shanbag, "Improved estimates via exponential sums for the minimum distance of $\mathbb{Z}_4$-linear trace codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1212–1216, 1996.

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

[18] J. Jedwab, "Comment: M-sequences for OFDM peak-to-average power ratio reduction and error correction," *Elec. Lett.*, vol. 33, pp. 1293–1294, 1997.

[19] 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, *Elect. Lett.*, vol. 30, pp. 2098–2099, 1994.

[20] A. E. Jones and T. A. Wilkinson, "Combined coding error control and increased robustness to system nonlinearities in OFDM," *Proc. IEEE 46th Vehicular Technology Conference*, pp. 904–908, Atlanta, 1996.

[21] 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*, vol. 41, pp. 456–468, 1995.

[22] J. Lahtonen, "On the odd and aperiodic correlation properties of the Kasami sequences," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1506–1508, 1995.

[23] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, Vol. 20 (2nd Edition), Cambridge University Press, 1997.

[24] X. Li and L. J. Cimini, Jr., "Effects of clipping and filtering on the performance of OFDM," *Proc. IEEE 47th Vehicular Technology Conference*, pp. 1634–1638, Phoenix, 1997.

[25] X. Li and J.A. Ritcey, "M-sequences for OFDM peak-to-average power ratio reduction and error correction," *Elec. Lett.*, vol. 33, pp. 554-555, 1997.

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

[27] 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*, vol. 40, pp. 1894–1907, 1994.

[28] 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*, vol. 52, pp. 58–67, 1997.

[29] R.D.J. van Nee, "OFDM codes for peak-to-average power reduction and error correction," *Proc. IEEE Globecom 1996*, pp. 740–744, London, 1996.

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

[31] R. O'Neill and L. B. Lopes, "Envelope variations and spectral splatter in clipped multicarrier signals," *Proc. PIMRC'95*, pp. 71–75, Sept. 1995.

[32] K. G. Paterson, "Generalised Reed-Muller codes and power control in OFDM modulation," *IEEE Trans. Inform. Theory*, submitted.

[33] K. G. Paterson and A.E. Jones, "Efficient decoding algorithms for generalised Reed-Muller codes," *IEEE Trans. Comm.*, submitted.

[34] P. Piret, "Bounds for codes over the unit circle," IEEE Trans. Inform. Theory, vol. 32, pp. 760–767, 1986.

[35] G. C. Porter, "Error distribution and diversity performance of a frequency-differential PSK HF modem," *IEEE Trans. Commun. Technol.*, vol. 16, pp. 567–575, 1968.

[36] B. R. Saltzberg, "Performance of an efficient data transmission system," *IEEE Trans. Commun. Technol.*, vol. 15, pp. 805–813, 1967.

[37] J. Salz and S. B. Weinstein, "Fourier transform communication system," *Proc. ACM Symp. Probl. Optimiz. Data Commun. Syst.*, pp. 99–128, Pine Mountain, GA, Oct. 1969.

[38] D.V. Sarwate, "An upper bound on the aperiodic autocorrelation function for a maximal-length sequence," *IEEE Trans. Inform. Theory*, vol. 30, pp. 685–687, 1984.

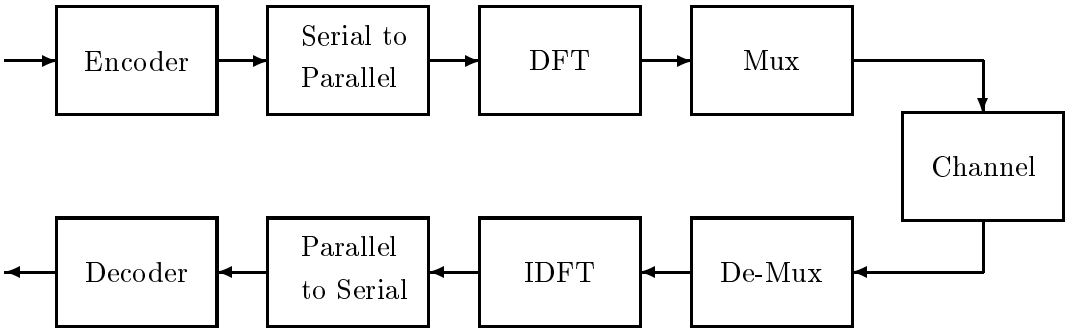

Fig. 1. OFDM Block Diagram.

[39] W. Schmidt, *Equations over finite fields — An elementary approach*, Springer, Berlin, 1976.

[40] 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*, vol. 42, pp. 250–254, 1996.

[41] C.E. Shannon, "Probability of Error for Optimal Codes in a Gaussian Channel," *Claude Shannon Collected Papers*, IEEE Press, pp. 279-324, 1993.

[42] S. Shepherd, J. Orriss and S. Barton, "Asymptotic limits in peak envelope power reduction by redundant coding in orthogonal frequency-division multiplex modulation," *IEEE Trans. Comm.*, vol. 46, pp. 5–10, 1998.

[43] V. Tarokh and H. Jafarkhani, "On Reducing the Peak to Average Power Ratio in Multicarrier Communications," *IEEE Trans. Comm.*, submitted.

[44] S. B. Weinstein and P. M. Ebert, "Data transmission by frequency-division multiplexing using the discrete Fourier transform," *IEEE Trans. Commun. Technol.*, vol. 19, pp. 628–634, 1971.

[45] T. A. Wilkinson and A. E. Jones, "Minimisation of the peak to mean envelope power ratio of multicarrier transmission schemes by block coding," *Proc. IEEE 45th Vehicular Technology Conference*, pp. 825–829, Chicago, July 1995.

[46] D. Wulich, "Reduction of peak-to-mean ratio of multicarrier modulation using cyclic coding," *Elec. Lett.*, vol. 32, pp. 432–433, 1996.

[47] M. S. Zimmerman and A. L. Kirsch, "The AN/GSC-10 (KATHRYN) variable rate data modem for HF radio," *IEEE Trans. Commun. Technol.*, vol. 15, pp. 197–205, 1967.