Low Correlation, High Nonlinearity Sequences for multi-code CDMA

Patrick Solé* Dmitrii Zinoviev†

Abstract

Families of binary low correlation sequences with high nonlinearity (in relation with their Walsh Hadamard transform) are constructed by using the most significant bit of linear recurrence sequences over the ring $\mathbb{Z}_{2^l}$, for $l \geq 3$. The engineering motivation is the design of a multicode CDMA scheme with a control of low peak to average power ratio (PAPR). Proof techniques combine Galois Ring theory (local Weil bound) with spectral analysis over the additive group of $\mathbb{Z}_{2^l}$. New estimates on the size of weighted degree trace codes are derived. The parameters of the sequences families constructed are shown to lie above a modified Varshamov-Gilbert bound.

Keywords: CDMA, Correlation, Galois Rings, MSB, Nonlinearity, PAPR, Trace codes

1 Introduction

In a recent paper [8] a communication model for multi-code CDMA was introduced where the Peak to Average Power Ratio (PAPR) of a binary word c of length $n = 2^m$ is computed as

$$PAPR(c) = \frac{(n - 2d_*(c))^2}{n},$$

where $d_*(c)$ is the distance of c to the first order Reed–Müller code $RM(1, m)$, a quantity called *nonlinearity* in the cryptographic community [1]. (This situation should not be confused with codes for OFDM where the crucial quantity to control is the DFT like in

*CNRS-I3S, ESSI, Route des Colles, 06 903 Sophia Antipolis, France, ps@essi.fr.

†CNRS-I3S, ESSI, Route des Colles, 06 903 Sophia Antipolis, France, zinoviev@essi.fr and Institute for Problems of Information Transmission, Russian Academy of Sciences, Bol'shoi Karetnyi, 19, GSP-4, Moscow, 101447, Russia,dzinov@iitp.ru.

e.g. [9]). In that communication model words that are evaluations of bent functions have $PAPR = 1$. Similarly, almost bent functions [1] correspond to $PAPR = 2$. A natural question, then, is to construct binary codes that are both good for the Hamming distance and the codewords of which have low largest $PAPR$.

In this correspondence, we construct families of binary low correlation sequences with high nonlinearity, or, equivalently, binary codes with high minimum Hamming distance and low largest PAPR. In [8] the constructions are for short lengths and small PAPR. In constrast, in the present work, we are providing large infinite families of length 2^m of PAPR arbitrary but parametrized by an integer l, thus achieving more design flexibility. Further, the parameters of the sequence families constructed are shown to lie strictly above the generalized Varshamov-Gilbert bound of [8, Lemma 2]. The technique employed uses the most significant bit (MSB) of some linear recurrence sequence over the ring $\mathbb{Z}_{2^l}$, for $l \geq 4$. The linear recurrence is chosen, like in [10], in such a way as to optimize the use of the local Weil bound. Like in [5] a Fourier transform on the additive group of the ring is used to derive correlation estimates of the binary sequences from character sum estimates on the ring sequences they are derived from. At a technical level an estimate of the size of weighted degree trace codes is derived (Lemma 4.1) that corrects some estimates in [9].

The note is organized as follows. Section II is dedicated to definitions and notation. Section III explains the spectral approach and the character sum bound employed. Section IV studies the fine detail of the polynomials over the ring extension, that are used to define the sequences in Section V. Section VI and VII contain the bounds on, respectively, the nonlinearity and the correlation. In Section VIII, for concreteness, the special case of $l = 3$ and polynomials whose weighted degree is at most three is considered. Section IX recapitulates the parameters of the sequence families constructed in the previous section. The final section (Section X) checks the statement about the generalized Varshamov-Gilbert bound of [8, Lemma 2].

2 Preliminaries

Let $R = GR(2^l, m)$ denote the Galois ring of characteristic 2^l with 2^{lm} elements. Let ξ be an element in $GR(2^l, m)$ that generates the Teichmüller set $\mathcal{T}$ of $GR(2^l, m)$. Specifically, let $\mathcal{T} = \{0, 1, \xi, \xi^2, \ldots, \xi^{2^m-2}\}$ and $\mathcal{T}^* = \{1, \xi, \xi^2, \ldots, \xi^{2^m-2}\}$. We use the *convention* that $\xi^\infty = 0$.

The 2-adic expansion of $x \in GR(2^l, m)$ is given by

$$x \;=\; x_0 + 2x_1 + \cdots + 2^{l-1}x_{l-1},$$

where $x_0, x_1, \ldots, x_{l-1} \in \mathcal{T}$. The Frobenius operator F is defined for such an x as

$$F(x_0 + 2x_1 + \cdots + 2^{l-1}x_{l-1}) \;=\; x_0^2 + 2x_1^2 + \cdots + 2^{l-1}x_{l-1}^2,$$

and the trace Tr, from $GR(2^l, m)$ downto $\mathbb{Z}_{2^l}$, as

$$\mathrm{Tr} \ := \ \sum_{j=0}^{m-1} F^j.$$

We also define another trace tr from $\mathbb{F}_{2^m}$ downto $\mathbb{F}_2$ as

$$\mathrm{tr}(x) := \sum_{j=0}^{m-1} x^{2^j}.$$

Throughout this note, we let $n = 2^m$ and $R^* = R \backslash 2R$. Let $\mathrm{MSB} : \mathbb{Z}_{2^l}^n \to \mathbb{Z}_2^n$ be the most-significant-bit map, i.e.,

$$\mathrm{MSB}(x_0 + 2x_1 + \ldots + 2^{l-1}x_{l-1}) \ = \ x_{l-1}.$$

3 DFT and the local Weil bound

We assume henceforth in the whole paper that $l \geq 4$. Let l be a positive integer and $\omega = e^{2\pi i/2^l}$ be a primitive 2^l-th root of 1 in $\mathbb{C}$. Let ψ_k be the additive character of $\mathbb{Z}_{2^l}$ such that

$$\psi_k(x) \ = \ \omega^{kx}.$$

Let $\mu : \mathbb{Z}_{2^l} \to \{\pm 1\}$ be the be the mapping $\mu(t) = (-1)^c$, where c is the most significant bit of $t \in \mathbb{Z}_{2^l}$,i.e. it maps $0, 1, ..., 2^{l-1} - 1$ to $+1$ and $2^{l-1}, 2^{l-1} + 1, ..., 2^l - 1$ to -1. Our goal is to express this map as a linear combination of characters. Recall the Fourier transformation formula on $\mathbb{Z}_{2^l}$:

$$\mu \ = \ \sum_{j=0}^{2^l-1} \mu_j \psi_j, \ \text{where } \mu_j \ = \ \frac{1}{2^l} \sum_{x=0}^{2^l-1} \mu(x)\psi_j(-x). \tag{1}$$

For all β in the ring $R := \ GR(2^l, m)$, we denote by Ψ_β the character

$$\Psi_\beta : R \to \mathbb{C}^*, x \mapsto \omega^{\mathrm{Tr}(\beta x)}.$$

Note that for the defined above ψ_k and Ψ_β, we have:

$$\psi_k(\mathrm{Tr}(\beta x)) \ = \ \Psi_{\beta k}(x). \tag{2}$$

Let $f(X)$ denote a polynomial in $R[X]$ and let

$$f(x) \ = \ F_0(x) + 2F_1(x) + \ldots + 2^{l-1}F_{l-1}(x)$$

denote its 2-adic expansion. Let d_i be the degree in x of F_i. Let χ be an arbitrary additive character of R, and set D_f to be the *weighted degree* of f, defined as

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

With the above notation, we have (under mild technical conditions) the bound

$$|\sum_{x\in\mathcal{T}} \chi(f(x))| \leq (D_f - 1)2^{m/2}. \tag{3}$$

See [4] for details. We will need the following property of the weighted degree:

Lemma 3.1 *Let $f(x) \in R[x]$ and $\alpha \in R^* = R\backslash 2R$ is a unit of R and let $g(x) = f(\alpha x) \in R[x]$. Then*

$$D_g \;=\; D_f,$$

where D_f, D_g are respectively the weighted degrees of the polynomials $f(x)$ and $g(x)$.

Proof. Due to the linearity, we can assume that $f(x)$ is of the form $2^i F(x)$, where $F(x) \in \mathcal{T}$ is of degree d. Thus

$$F(x) \;=\; c_0 + c_1 x + \ldots + c_d x^d,$$

where $c_j \in \mathcal{T}$, $j = 0, 1, \ldots, d$ and the weighted degree D_f of f is equal to $2^{l-1-i}d$. Suppose that

$$\alpha^k \;=\; \sum_{j=0}^{l-1} \alpha_{jk} 2^j.$$

Substituting αx into $F(x)$, and using the above expansion we obtain that $F(\alpha x)$ equals

$$\sum_{k=0}^{d} c_k \alpha^k x^k \;=\; \sum_{k=0}^{d} c_k \Big(\sum_{j=0}^{l-1} \alpha_{jk}\Big) x^k.$$

Changing the order of summation, this is

$$\sum_{j=0}^{l-1} 2^j \sum_{k=0}^{d} \alpha_{jk} x^k \;=\; \sum_{j=0}^{l-1} 2^j F_j(x),$$

where $F_j(x)$ are polynomials in $\mathcal{T}[x]$ of degree at most d. Since α is a unit and $\alpha_{0k} \neq 0$ $(k = 0, \ldots d)$, the polynomial

$$F_0(x) \;=\; \sum_{k=0}^{d} \alpha_{0k} c_k x^k,$$

is of degree d. Thus the weighted degree of $f(\alpha x)$ equals $2^{l-1-i}d$. $\square$

4 Polynomials over the Galois ring $GR(2^l, m)$.

Recall that $R = GR(2^l, m)$. A polynomial

$$f(x) \;=\; \sum_{j=0}^{d} c_j x^j \in R[x]$$

is called **canonical** if $c_j = 0$ for all even j.

Given an integer $D \geq 4$, define

$$S_D \;=\; \{f(x) \in R[x] \mid D_f \leq D, f \text{ is canonical}\},$$

where D_f is the weighted degree of f. Observe that S_D is an $GR(2^l, m)-$module. The main result of this section is:

Lemma 4.1 *For any integer $D \geq 4$, we have:*

$$|S_D| \;=\; 2^{(D-\lfloor D/2^l \rfloor)m},$$

where $\lfloor x \rfloor$ is the largest integer $\leq x$.

Proof. By definition of the weighted degree, we have

$$\max\{d_0 2^{l-1}, d_1 2^{l-2}, \ldots, d_{l-1}\} \leq D,$$

and in particular:

$$d_0 2^{l-1} \leq D,\; d_1 2^{l-2} \leq D,\; \ldots,\; d_{l-1} \leq D.$$

Since d_{l-1} is odd, it follows that:

$$d_{l-1} \leq D_{l-1} \;=\; 2\left\lfloor \frac{D-1}{2} \right\rfloor + 1.$$

Similarly, for any $0 \leq j \leq l-1$, we have that d_j:

$$d_j \leq D_j \;=\; 2\left\lfloor \frac{D - 2^{l-j-1}}{2^{l-j}} \right\rfloor + 1.$$

Thus for the fixed set of $l-1$ odd numbers D_0, $D_1, \ldots,$ D_{l-1}, we have:

$$|\{f(x) \in R[x] |\, d_j \leq D_j, j = 0, 1, \ldots, l-1, f \text{ is canonical}\}| \;=\; 2^{m\left(\frac{D_0+1}{2} + \frac{D_1+1}{2} + \ldots + \frac{D_{l-1}+1}{2}\right)}.$$

Furthermore, we obtain

$$\frac{D_0+1}{2} + \frac{D_1+1}{2} + \ldots + \frac{D_{l-1}+1}{2} \;=\; \sum_{j=0}^{l-1} \left\lfloor \frac{D - 2^{l-j-1}}{2^{l-j}} \right\rfloor + l - 1. \tag{4}$$

Since for any real x and integer k we have that $\lfloor x + k \rfloor \;=\; \lfloor x \rfloor + k$, the right hand side of (4) is equal to

$$\sum_{j=0}^{l-1} \left\lfloor \frac{D + 2^{l-j-1}}{2^{l-j}} \right\rfloor \;=\; \sum_{j=0}^{l-1} \left\lfloor \frac{D + 2^j}{2^{j+1}} \right\rfloor.$$

There exist integer numbers r, and k such that $D = 2^l k + r$, where $0 \leq r \leq 2^l - 1$. Thus the above expression is equal to:

$$(2^l - 1)k + \sum_{j=0}^{l-1} \left\lfloor \frac{r + 2^j}{2^{j+1}} \right\rfloor . \tag{5}$$

Next, we will prove by induction that:

$$\sum_{j=0}^{l-1} \left\lfloor \frac{r + 2^j}{2^{j+1}} \right\rfloor \;=\; r. \tag{6}$$

Indeed, the case $l = 2$, can be verified directly. Now suppose (6) holds for all $l \leq L$. Consider the case $l = L + 1$. When $0 \leq r \leq 2^L - 1$, we have that

$$\left\lfloor \frac{r + 2^L}{2^{L+1}} \right\rfloor \;=\; 0,$$

and (6) holds by the induction hypothesis. When $2^L \leq r \leq 2^{L+1} - 1$, we can write that $r = 2^L + r'$, where $0 \leq r' \leq 2^L - 1$ and observing that the term (corresponding to $j = L$)

$$\left\lfloor \frac{2^L + r' + 2^L}{2^{L+1}} \right\rfloor \;=\; 1,$$

the left hand side of (6) is equal to

$$\sum_{j=0}^{L-1} \left\lfloor \frac{2^L + r' + 2^j}{2^{j+1}} \right\rfloor + 1 \;=\; 1 + \sum_{j=0}^{L-1} 2^{L-j-1} + \sum_{j=0}^{L-1} \left\lfloor \frac{r' + 2^j}{2^{j+1}} \right\rfloor .$$

Note that

$$\sum_{j=0}^{L-1} 2^{L-j-1} \;=\; 1 + 2 + \ldots + 2^{L-1} \;=\; 2^L - 1. \tag{7}$$

Moreover by induction hypothesis (for $l = L$):

$$\sum_{j=0}^{L-1} \left\lfloor \frac{r' + 2^j}{2^{j+1}} \right\rfloor \;=\; r'. \tag{8}$$

Thus (7) and (8) imply (6).

Note that $k = \lfloor D/2^l \rfloor$. So, applying (6), (5) is equal to:

$$(2^l - 1)k + r \;=\; 2^l k + r - k \;=\; D - \left\lfloor \frac{D}{2^l} \right\rfloor .$$

The Lemma follows. $\square$

5 Binary codes and sequences

Definition 5.1 *For any integer $D \geq 4$, let $C_l(m, D)$ denote the $\mathbb{Z}_{2^l}$-linear code of length n:*

$$C_l(m, D) \ = \ \{\mathbf{x} \ = \ (x_\infty, x_0, \ldots, x_{n-2}) \in \mathbb{Z}_{2^l}^n | \, x_j \ = \ Tr(f(\xi^j)), \ f \in S_D\}. \tag{9}$$

Define now the punctured at infinity version of $C_l(m, D)$.

Definition 5.2 *For any integer $D \geq 4$, let $C_l(m, D)^*$ denote the $\mathbb{Z}_{2^l}$-linear code of length $n-1$:*

$$C_l(m, D)^* \ = \ \{\mathbf{x} \ = \ (x_0, \ldots, x_{n-2}) \in \mathbb{Z}_{2^l}^{n-1} | \, x_j \ = \ Tr(f(\xi^j)), \ f \in S_D\}. \tag{10}$$

The following result is direct from the order of ξ and Lemma 4.1.

Lemma 5.3 *Let $C(l, m, D) = \mathrm{MSB}(C_l(m, D))$ be the image of $C_l(m, D)$ defined by (9) under the* MSB *map. Then $C(l, m, D)$ is a binary code of length n with $2^{(D-\lfloor D/2^l \rfloor)m}$ codewords. Further, its punctured at ∞ version $C(l, m, D)^*$ is shift-invariant.*

By this lemma, it makes sense to define the binary periodic sequences family $S(l, m, D)$ as the (periodized) image under the MSB map of $C_l(m, D)^*$, or, equivalently the sequences whose periods are the words of $C(l, m, D)^*$.

6 PAPR

We employ the same techniques and notations as in the preceding section. Observe first that the scalar product xy of $x, y \in \mathbb{F}_2^m$ can always be expressed – thanks to the existence of a self-dual basis of $\mathbb{F}_2^m$ over $\mathbb{F}_2$ – by means of the trace function:

$$x.y = tr(xy).$$

(We tacitly identify an element of $\mathbb{F}_{2^m}$ with its coordinate vector over the said basis.) Let $\widehat{c}(y)$ denote the Walsh-Hadamard Fourier coefficient of c_t in y, namely:

$$\widehat{c}(y) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{c(x)+tr(xy)}, \tag{11}$$

where $c(\xi^t) = c_t$, for $t \in \mathcal{T}$, is viewed as a Boolean function.

Theorem 6.1 *For all $c \in C(l, m, D)$ and all $y \in \mathbb{F}_2^m$, we have the bound*

$$|\widehat{c}(y)| \leq (2l \ln(2)/\pi + 1)(D-1)\sqrt{n}$$

Proof. For any $u \in R$ we write $\bar{u} \in \mathbb{F}_{2^m}$ for its mod 2 reduction. Then for any $u, v \in R$ we have that:

$$\mathrm{tr}(\bar{u}\bar{v}) \ = \ \mathrm{MSB}(2^{l-1}\mathrm{Tr}(uv)).$$

Consequently

$$\mathrm{MSB}(\mathrm{Tr}(f(x))) + \mathrm{MSB}(2^{l-1}\mathrm{Tr}(ux)) \ = \ \mathrm{MSB}(\mathrm{Tr}(f(x) + 2^{l-1}ux)).$$

Note that for any $u \in R$ the weighed degree of $2^{l-1}ux \in R[x]$ is ≤ 1. Thus if $f(x) \in S_D$ then the polynomial $f(x) + 2^{l-1}ux$ belongs to the linear space S_D. So, in (11) without lost of generality, we can drop the tr term. Recall that $\xi \in \mathcal{T}^*$ is a generator of the Teichmüller set. By definition of ψ_j and Ψ_α, (where $0 \neq q \in R$), for any $0 \leq j \leq 2^l - 1$, we have:

$$\psi_j(\mathrm{Tr}(x)) \ = \ \Psi_j(x).$$

As we have $c_t = \mathrm{MSB}(\mathrm{Tr}(f(\xi^t)))$, and by (1), we obtain that $(-1)^{c_t}$ is equal to:

$$\mu(\mathrm{Tr}(f(\xi^t))) \ = \ \sum_{j=0}^{2^l-1} \mu_j \psi_j(\mathrm{Tr}(f(\xi^t))) \ = \ \sum_{j=0}^{2^l-1} \mu_j \Psi_j(f(\xi^t))).$$

Changing the order of summation, we obtain that:

$$\sum_{t=\infty}^{n-2} (-1)^{c_t} \ = \ \sum_{j=0}^{2^l-1} \mu_j \sum_{x \in \mathcal{T}} \Psi_j(f(x)). \tag{12}$$

Applying (3), the absolute value of the Right Hand Side of (12) can be estimated from above by:

$$((D_f - 1)\sqrt{2^m} + 1) \sum_{j=0}^{2^l-1} |\mu_j|. \tag{13}$$

Recall Corollary 7.4 of [5] which states that for $l \geq 4$ the following estimate holds:

$$\sum_{j=0}^{2^l-1} |\mu_j| \ < \ \frac{2l\ln(2)}{\pi} + 1.$$

Thus (13) can be estimated from above by:

$$(2l\ln(2)/\pi + 1)(D_f - 1)\sqrt{2^m}.$$

The result follows. □

This translates immediately in terms of PAPR.

Corollary 6.2 *For all $c \in C(l, m, D)$, we have, for large n, the bound*

$$PAPR \leq 0.195l^2(D-1)^2(1 + o(1)).$$

Proof. Follows immediately, by the well-known connection between Walsh-Hadamard transform and distance to the Reed Muller code of the first order [6, 8]. □

7 Minimum Distance

Theorem 7.1 *With notation as above, and for all phase shifts τ, in the range $0 < \tau < 2^m - 1$, let ($n = 2^m$)*

$$\Theta(\tau) = \sum_{t=0}^{n-2} (-1)^{c_t} (-1)^{c'_{t+\tau}},$$

where $c_t = \mathrm{MSB}(\mathit{Tr}(f_1(\xi^t)))$ and $c'_t = \mathrm{MSB}(\mathit{Tr}(f_2(\xi^t)))$. We then have the bound ($l \geq 4$):

$$|\Theta(\tau)| \leq \left(\frac{2l}{\pi}\ln(2) + 1\right)^2 [1 + (D-1)\sqrt{2^m}],$$

where $D = max\{D_{f_1}, D_{f_2}\}$.

Proof. As we have $c_t = \mathrm{MSB}(\mathrm{Tr}(f_1(\xi^t)))$, where t ranges between 0 and $n-2$ and by (1), we obtain that $(-1)^{c_t}$ is equal to:

$$\mu(\mathrm{Tr}(f_1(\xi^t))) \;=\; \sum_{j=0}^{2^l-1} \mu_j \psi_j(\mathrm{Tr}(f_1(\xi^t))) \;=\; \sum_{j=0}^{2^l-1} \mu_j \Psi_j(f_1(\xi^t))).$$

Changing the order of summation, we obtain that:

$$\Theta(\tau) = \sum_{j_1=0}^{2^l-1} \sum_{j_2=0}^{2^l-1} \mu_{j_1}\mu_{j_2} \sum_{t=0}^{n-2} \Psi_{j_1}(f_1(\xi^t))\Psi_{j_2}(f_2(\xi^{t+\tau})). \tag{14}$$

By definition of Ψ, we have:

$$\Psi_{j_1}(f_1(\xi^t))\Psi_{j_2}(f_2(\xi^{t+\tau})) \;=\; \Psi(g(\xi^t)),$$

where $g(x) = j_1 f_1(x) + j_2 f_2(x\xi^\tau)$. Note that if $f(x) \in S_D$ then $f(x\xi^\tau) \in S_D$ since, by Lemma 3.1 the change of variables $x \to x\xi^\tau$ does not increase the weighted degree. Moreover S_D is an R-linear space. Thus the polynomial $g(x)$ belongs to S_D along with f_1 and f_2. Applying (3), we obtain:

$$\Big|\sum_{t=0}^{n-2} \Psi_{j_1}(f_1(\xi^t))\Psi_{j_2}(f_2(\xi^{t+\tau}))\Big| \;=\; \Big|\sum_{x\in\mathcal{T}^*} \Psi(g(x))\Big| \;\leq\; 1 + (D-1)\sqrt{2^m}. \tag{15}$$

Recall the Corollary 14 of [5] which states that for $l \geq 4$ the following estimate holds:

$$\sum_{j_1=0}^{2^l-1}\sum_{j_2=0}^{2^l-1} |\mu_{j_1}\mu_{j_2}| \;=\; \Big(\sum_{j=0}^{2^l-1} |\mu_j|\Big)^2 \;\leq\; \left(\frac{2l\ln(2)}{\pi} + 1\right)^2. \tag{16}$$

Combining (15) with (16) the result follows. □

Using the standard connection between crosscorrelation and Hamming distance of binary sequences we obtain the following.

Corollary 7.2 *The binary code $C(l, m, D)$ of length 2^m has minimum distance*

$$\geq 2^{m-1} - \frac{1}{2}(0.44l + 1)^2 (D-1) 2^{m/2}.$$

8 The case $l = 3$ and $D = 3$

In this section we consider in details the case $l = 3$ and $D = 3$. Let $R = GR(8, m)$. Following Section IV, define

$$S_3 \ = \ \{f(x) \in R[x] \mid D_f \leq 3, f \text{ is canonical}\},$$

where D_f is the weighted degree of f. Let

$$f(x) \ = \ F_0(x) + 2F_1(x) + 4F_2(x)$$

be the 2-adic expansion of f and d_i be the degree in x of F_i. Then

$$D_f \ = \ \max\{4d_0, 2d_1, d_2\} \ \leq \ 3$$

implies $d_0 = 0$, $d_1 \leq 1$, and $d_2 \leq 3$. Thus $f(x) = 2F_1(x) + 4F_2(x)$, where

$$F_1(x) = c_0 x, \ F_2(x) = c_1 x + c_2 x^3, \ c_0, c_1, c_2 \in \mathcal{T}.$$

As $|\mathcal{T}| = 2^m$, we obtain that S_3 has 2^{3m} elements.

Recall Lemma 2 of [5]:

$$\sum_{i=0}^{7} |\mu_i| \ = \ (2 + \sqrt{2}). \tag{17}$$

Thus we obtain the estimate on PAPR. The estimate on the minimum distance follows from:

$$\sum_{i=0}^{7}\sum_{j=0}^{7} |\mu_i \mu_j| \ = \ \Big(\sum_{j=0}^{7} |\mu_j|\Big)^2 \ = \ (2 + \sqrt{2})^2.$$

To summarize, for $m \geq 10$, the binary code $C(3, m, 3)$ has the following parameters:

- length $n = 2^m$
- size $|C(3, m, 3)| \ = \ n^3$
- PAPR at most $\leq 46.6(1 + o(1))$.
- minimum Hamming distance at least

$$\geq \frac{n}{2} - (2 + \sqrt{2})^2\sqrt{n}.$$

For instance, in case of $m = 10$, we get the estimate

- length $n = 1024$
- size $|C(3, 10, 3)| \ = \ 2^30$
- PAPR at most ≤ 46.7.
- minimum Hamming distance at least

$$\geq 139.$$

9 Conclusion

In this note we constructed a distance invariant binary code $C(l, m, D)$ with the following parameters

- length $n = 2^m$
- size $|C(l, m, D)| \ = \ 2^{(D-\lfloor D/2^l \rfloor)m}$
- PAPR at most $0.195l^2(D-1)^2$
- minimum Hamming distance d at least $\geq 2^{m-1} - \frac{1}{2}(0.44l+1)^2(D-1)2^{m/2}$

Equivalently we constructed a family $S(l, m, D)$ of binary periodic sequences of

- period $n - 1 = 2^m - 1$
- size $|S_D| \sim 2^{(D-\lfloor D/2^l \rfloor)m}/(n-1)$
- PAPR at most $0.195l^2(D-1)^2$
- periodic correlation at most $(0.44l+1)^2[1 + (D-1)2^{m/2}]$

By comparison the explicit constructions in [8] are limited to a small PAPR (=1 or 2) and logarithmic family size. Here we allow an arbitrary PAPR but with many more sequences. It is shown in the Appendix that these parameters, in a suitable range, lie above the Gilbert-Varshamov-style bound of [8, Lemma 2].

10 Appendix: a Gilbert-Varshamov-style bound

For any $0 \leq r \leq n$, set

$$H(r) \ = \ \sum_{k=0}^{r} \binom{n}{k},$$

i.e. the number of words in a Hamming sphere of dimension n and radius r. Let

$$H_2(x) = -x \log_2(x) - (1-x)\log_2(1-x).$$

Lemma 7, Ch.10, §11 of [6] asserts that for any $0 < \mu < 1/2$ the following estimate holds

$$\frac{2^{nH_2(\mu)}}{\sqrt{8n\mu(1-\mu)}} \leq H(\mu n) \leq 2^{nH_2(\mu)}. \tag{18}$$

The goal of this section is to verify that for the certain choice of parameters l, m and D the code $C = C(l, m, D)$ satisfies

$$2nH(d_* - 1) + 2^{(D-\lfloor D/2^l \rfloor)m} H(d-1) \ \geq \ 2^n,$$

where $d_* = \min\{d_*(c) \ : \ c \in C\}$. In fact, we want to show that

$$2^{(D-\lfloor D/2^l \rfloor)m} H(d-1) \ \geq \ 2^n, \tag{19}$$

where recall that

$$d \geq \frac{n}{2}\left(1 - \frac{(0.44l+1)^2(D-1)}{2\sqrt{n}}\right).$$

Using the Taylor expansion of ln, we have that for any $|\delta| < 1$

$$H_2\left(\frac{1}{2}(1-\delta)\right) \ = \ 1 - \frac{1}{\ln 2}\sum_{k=1}^{\infty}\frac{\delta^{2k}}{2k(2k-1)}.$$

Taking into account that $|\delta| < 1$ and

$$\sum_{k=2}^{\infty}\frac{1}{2k(2k-1)} \ = \ \frac{1}{3\cdot 4} + \frac{1}{5\cdot 6} + \ldots \ < \ \frac{1}{3},$$

we obtain

$$H_2\left(\frac{1}{2}(1-\delta)\right) \ > \ 1 - \frac{\delta^2}{2\ln 2} - \frac{\delta^4}{3\ln 2}. \tag{20}$$

Thus, using (18) and (20), we obtain

$$H(d-1) \ \geq \ H\left(\frac{n}{2}(1-\delta)\right) \ \geq \ \frac{2^{nH_2(\frac{1}{2}(1-\delta))}}{\sqrt{2n(1-\delta^2)}} \ \geq \ \frac{2^{n(1-\delta^2/(2\ln 2)-\delta^4/(3\ln 2))}}{\sqrt{2n}}, \tag{21}$$

where

$$\delta \ = \ \frac{(0.44l+1)^2(D-1)}{2\sqrt{n}}.$$

Taking the logarithms of (19) and applying (21), we arrive at

$$D(1-2^{-l})m - \frac{n\delta^2}{2\ln 2} - \frac{n\delta^4}{3\ln 2} - \frac{\ln(2n)}{2} \geq 0.$$

We recall that $n = 2^m$ and rewrite this inequality

$$D(1-2^{-l})m \geq \frac{n\delta^2}{2\ln 2}\left(1 - \frac{2\delta^2}{3}\right) + \frac{(m+1)\ln(2)}{2}. \tag{22}$$

Assume that $l \geq 1$ and $D \geq 1$ are fixed integers, choose $m \geq 8$ so that $2m \geq l^4 D$. Then $\sqrt{n} = 2^{m/2} \geq 2m \geq l^2 D$ and

$$\delta \leq \frac{l^2 D}{2\sqrt{n}} \leq 0.5.$$

When $l \geq 2$ (m is at least 8 and $D \geq 1$), the right hand side of inequality (22) can be estimated from above by (we use that $1/(2\ln 2) < 0.73$ and $\delta < 0.45 l^2 D/\sqrt{n}$)

$$0.73n\delta^2 + 0.37m \ < \ 0.15l^4D^2 + 0.37Dm < 0.3Dm + 0.37Dm < 0.75Dm \leq D(1-2^{-l})m.$$

When $l = 1$ (m is at least 8 and $D \geq 4$), the right hand side of inequality (22) can be estimated from above by (we use that $1/(2\ln 2) < 0.73$ and $\delta < 1.04l^2D/\sqrt{n}$)

$$0.73n\delta^2 + 0.37m \ < \ 0.79l^4D^2 + 0.1Dm < 0.4Dm + 0.1Dm < 0.5Dm.$$

Thus inequality (22) is verified.

Acknowledgement: We thank the associate editor for helpful suggestions that greatly improved the material presentation.

References

[1] C. Carlet, P. Charpin et V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, Designs Codes and Cryptography **15**, p. 125-156 (1998)

[2] 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. IT-**40**, pp. 301–319, March 1994.

[3] T. Helleseth, P.V. Kumar, Sequences with low Correlation, in *Handbook of Coding theory,* vol. II, V.S. Pless, W.C. Huffman, eds, North Holland (1998), 1765–1853.

[4] 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. IT-**41**, pp. 456–468, May 1995. properties Hammons, Jr.,

[5] J. Lahtonen, S. Ling, P. Solé, D. Zinoviev, $\mathbb{Z}_8$-Kerdock codes and pseudo-random binary sequences, Journal of Complexity, Volume 20, Issues 2-3, April-June 2004, Pages 318-330.

[6] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland (1977).

[7] B.R. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York (1974).

[8] K. G. Paterson, On Codes with Low Peak-to-Average Power Ratio for Multi-Code CDMA, IEEE Trans. on Inform. Theory, vol.IT-**50**, pp. 550–559, March 2004.

[9] K. G. Paterson, V. Tarokh, On the existence and construction of good codes with low peak-to-average power ratios, IEEE Trans. on Inform. Theory, vol.IT-**46**, pp. 1974–1987, Sept. 2000.

[10] A. Shanbhag, P. V. Kumar and T. Helleseth, Improved Binary Codes and Sequence Families from $\mathbb{Z}_4$-Linear Codes, IEEE Trans. on Inform. Theory, vol.IT-**42**, pp. 1582-1586, Sep. 1996.