Z8-Kerdock codes and pseudorandom binary sequences

Lahtonen, Jyrki; Ling, San; Sole, Patrick; Zinoviev, Dmitrii

2003

Lahtonen, J., Ling, S., Solé, P., & Zinoviev, D. (2003). Z8-Kerdock codes and pseudorandom binary sequences. Journal of Complexity, 20(2-3), 318-330.

https://hdl.handle.net/10356/98360

https://doi.org/10.1016/j.jco.2003.08.014

$\mathbf{Z}_8$-Kerdock codes and pseudorandom binary sequences

Jyrki Lahtonen,[a] San Ling,[b,*] Patrick Solé,[c] and Dmitrii Zinoviev[d]

[a] *University of Turku, Department of Mathematics, FIN-20014 Turku, Finland*
[b] *Department of Mathematics, National University of Singapore, Singapore 117543, Republic of Singapore*
[c] *CNRS-I3S, ESSI, Route des Colles, 06 903 Sophia Antipolis, France*
[d] *CNRS-I3S, ESSI, Route des Colles, 06 903 Sophia Antipolis, France*

Abstract

The $\mathbb{Z}_8$-analogues of the Kerdock codes of length $n = 2^m$ were introduced by Carlet in 1998. We study the binary sequences of period $n - 1$ obtained from their cyclic version by using the most significant bit (MSB)-map. The relevant Boolean functions are of degree 4 in general. The linear span of these sequences has been known to be of the order of m^4. We will show that the crosscorrelation and nontrivial autocorrelation of this family are both upper bounded by a small multiple of $\sqrt{n}$. The nonlinearity of these sequences has a similar lower bound. A generalization of the above results to the alphabet $\mathbb{Z}_{2^l}, l \geqslant 4$ is sketched out.

Keywords: Generalized Kerdock code; Most significant bit map; Boolean functions; Correlation; Nonlinearity

1. Introduction

For signature sequences in a spread spectrum multiple-access communication system, it is desirable [9] to employ code-sequences having two kinds of

*Corresponding author.
E-mail addresses: lahtonen@utu.fi (J. Lahtonen), lings@math.nus.edu.sg (S. Ling), ps@essi.fr (P. Solé), zinoviev@essi.fr (D. Zinoviev).

pseudo-randomness properties:

- statistical: low non-central autocorrelation and low overall crosscorrelation
- cryptographical: large linear span, and high nonlinearity.

Many sequences in the literature meet the first requirement; some like the No sequences and the bent function sequences also enjoy a large linear span [4, Section 6.2]. However, the No sequence family (together with its generalizations) as well as the bent function sequences suffer from the fact that the families are relatively small—the cardinality of the family is approximately the square root of the length of the sequences.

In this article, we construct larger families of binary sequences of length $T = 2^m - 1$ with reasonable correlation properties and a linear span of the order $\mathcal{O}(m^4)$. Furthermore, the size of the family is approximately $T^2/4$. As the crosscorrelations and the nontrivial autocorrelations of our family are only bounded by $3(2+\sqrt{2})\sqrt{T+1}$, and the nonlinearity by $3\sqrt{2+\sqrt{2}}\sqrt{T+1}$, our families have somewhat worse correlation properties than the binary families constructed using the theory of Galois rings of characteristic 4 (cf. [4]). However, the linear span of these so-called $\mathbb{Z}_4$-linear families is only of the order $\mathcal{O}(m^2)$. Thus, our families might be an attractive alternative in an application where a larger family of sequences is required, and where higher linear span is desired even at the cost of slightly worse correlation properties.

The $\mathbb{Z}_8$-analogues of the Kerdock codes of length $n = 2^m$ were introduced by Carlet [2]. We study the binary sequences of period $n-1$ attached to its shortened and punctured version. The relevant Boolean functions are of degree 4 in general.

The above-mentioned bounds on the nonlinearity and correlation follow from the Galois Ring analogue of the Weil inequality [6] and some elementary character theory. As a by-product, we obtain a construction of quartic sequences with controlled nonlinearity. The linear span was known [5] to be of the order $\mathcal{O}(m^4)$. A key tool we shall use is the ability to express arbitrary complex valued functions defined on a finite abelian group G as linear combinations of characters of G, i.e., we perform discrete Fourier analysis on a finite abelian group. In retrospect this is a very natural generalization of one of the key ingredients in the successful applications of rings of characteristic 4, namely the fact that the Lee weight of an element $a \in \mathbb{Z}_4$ can be simply expressed by the equation

$$w_{\mathrm{Lee}}(a) = 1 - \mathrm{Re}\,(i^a) = \psi_0(a) - \frac{1}{2}\left(\psi(a) + \bar{\psi}(a)\right).$$

So we prefer to read the right-hand side of this equation as a linear combination of the principal character $\psi_0 : a \mapsto 1$, the character $\psi : a \mapsto i^a$, and its conjugate character $\bar{\psi}$. It is easy to write a similar expression for the MSB-map (really for any mapping by the inverse Fourier transform). In Section 4 we will carry out such an analysis of the most significant bit (MSB)-map of the group $\mathbb{Z}_8$ (see the next section for definitions and details). The last section in this article is devoted to the

generalization of Lemma 2 and Theorem 7 to the case of the alphabet $\mathbb{Z}_{2^l}$, where $l \geqslant 4$.

Another key ingredient in the success of $\mathbb{Z}_4$-based designs of families of sequences is the observation (originally due to A. Nechaev) that in addition to the cyclic group $\mathscr{T}^*$ of nonzero elements of the Teichmüller set, one may also use the larger group $\mathscr{T}^* \cup -\mathscr{T}^*$ that is also cyclic. Indeed, the Gray map $\mathbb{Z}_4 \to \mathbb{Z}_2^2$ is simply the concatenation of the MSB-map evaluated at an element *and* at its negative. The corresponding cyclic subgroup of the unit group of Galois rings of characteristic 8 could also be used to design families of sequences of twice the length. We have not fully pursued this line of research yet. Early results seem to indicate that one should not expect very exciting new sequence families to arise from this construction idea. Something comparable to the families introduced in this article will probably come out, though.

2. Definitions and notation

Let $GR(8,m)$ denote the Galois ring of characteristic 8 with 8^m elements. Let ξ be an element in $GR(8,m)$ so that $\xi^{2^m} = \xi$ and set the Teichmüller set of $GR(8,m)$ to be $\mathscr{T} = \{0, 1, \xi, \xi^2, \ldots, \xi^{2^m-2}\}$. The 2-adic expansion of $x \in GR(8,m)$ is given by

$$x = u + 2v + 4w,$$

where $u, v, w \in \mathscr{T}$. The Frobenius operator F is defined for such an x as

$$F(u + 2v + 4w) = u^2 + 2v^2 + 4w^2,$$

and the trace Tr, from $GR(8,m)$ down to $\mathbb{Z}_8$, as

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

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

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

Throughout this note, we let $n = 2^m$. We define first a cyclic code which is the analogue of the simplex code:

$$S_m = \{(Tr(\lambda\xi^t))_{t=0}^{n-2} \mid \lambda \in GR(8,m)\}.$$

Let $\mathscr{I} = \{\infty, 0, 1, \ldots, n-2\}$. We use the convention that $\xi^\infty = 0$. Define an extended (and augmented) cyclic code as follows:

$$\overline{S_m} = \{(Tr(\lambda\xi^t) + A)_{t \in \mathscr{I}} \mid \lambda \in GR(8,m),\ A \in \mathbb{Z}_8\}.$$

Let $MSB : \mathbb{Z}_8^n \to \mathbb{Z}_2^n$ be the most-significant-bit map, i.e.,

$$MSB(a + 2b + 4c) = c.$$

Define the binary code s_m as $s_m = MSB(S_m)$.

3. Boolean functions

The 2-adic representation of $Tr(\lambda\xi^t)$ is given by the following result of Carlet (cf. [2, Proposition 6]).

Theorem 1. *Let $\lambda = \xi^r + 2\xi^s + 4\xi^w \in GR(8, m)$. For $t \in \mathscr{I}$, write*

$$Tr(\lambda\xi^t) = a_t + 2b_t + 4c_t,$$

where $a_t, b_t, c_t \in \mathbb{F}_2$. Then, with $\theta \equiv \xi \bmod 2$,

$$a_t = tr(\theta^{r+t})$$

$$b_t = Q(\theta^{r+t}) + tr(\theta^{s+t})$$

$$c_t = R(\theta^{r+t}) + Q(\theta^{s+t}) + tr(\theta^{r+t} + \theta^{s+t})Q(\theta^{r+t}) + tr(\theta^{w+t}),$$

where

$$Q(x) = \sum_{0 \leqslant i < j \leqslant m-1} x^{2^i + 2^j}$$

and

$$R(x) = \sum_{0 \leqslant i_1 < i_2 < i_3 < i_4 \leqslant m-1} x^{2^{i_1} + 2^{i_2} + 2^{i_3} + 2^{i_4}} + \sum_{0 \leqslant i_1 < i_2 < i_3 \leqslant m-1} x^{2^{i_1} + 2^{i_2} + 2^{i_3}} (x^{2^{i_1}} + x^{2^{i_2}} + x^{2^{i_3}}).$$

4. Imbalance and autocorrelation properties

Let $\zeta = e^{2\pi i/8} = (1 + i)/\sqrt{2}$ be a primitive 8th root of 1 in $\mathbb{C}$. For $x, y, z, t \in \mathbb{Q}$, set

$$A = x + y + z + t,$$

$$Q_j = x + y\zeta^j + z\zeta^{2j} + t\zeta^{3j}, \text{for } j = 1, 3, 5, 7.$$

Let $\mu : \mathbb{Z}_8 \to \{\pm 1\}$ be the mapping $\mu(t) = (-1)^c$, where c is the most significant bit of $t \in \mathbb{Z}_8$. For all $j = 0, 1, \ldots, 7$ let $\psi_j : \mathbb{Z}_8 \to \mathbb{C}^*$ be the character

$$\psi_j(t) = \zeta^{jt}.$$

The following lemma should be viewed as discrete Fourier analysis of the MSB-mapping μ.

Lemma 2. *For the constants* $\mu_j = (1+\zeta^{-j}+\zeta^{-2j}+\zeta^{-3j})/4,\ j=1,3,5,7$ *we have*

$$\mu = \mu_1\psi_1 + \mu_3\psi_3 + \mu_5\psi_5 + \mu_7\psi_7.$$

Furthermore,

$$(|\mu_1| + |\mu_3| + |\mu_5| + |\mu_7|)^2 = 2+\sqrt{2}.$$

Proof. The expression for the μ_j's follows from Lemma 11 below by the identity $X^4-1=(X-1)(X^3+X^2+X+1)$, and the fact that $(\zeta^{-j})^4=-1$ for j odd. Since $\zeta=(1+i)/\sqrt{2}$, it follows that $\mu_1=(1-(1+\sqrt{2})i)/4=\overline{\mu_7}$ and $\mu_3=(1+(1-\sqrt{2})i)/4=\overline{\mu_5}$, from which

$$(|\mu_1| + |\mu_3| + |\mu_5| + |\mu_7|)^2 = 2+\sqrt{2}$$

can be easily deduced. □

We record the following consequence of this result for future use.

Lemma 3. *We have for all* $x,y,z,t\in\mathbb{Q}$

$$A = \mu_1 Q_1 + \mu_3 Q_3 + \mu_5 Q_5 + \mu_7 Q_7,$$

where $\mu_j, j=1,3,5,7$ *are the coefficients of the previous lemma.*

Proof. Writing

$$Q_j = x\psi_j(0) + y\psi_j(1) + z\psi_j(2) + t\psi_j(3),$$

we see that, by Lemma 2, we have

$$\sum_j \mu_j Q_j = x\mu(0) + y\mu(1) + z\mu(2) + t\mu(3),$$

which is A, by definition of μ. □

For all $\lambda\in GR(8,m)$ we denote by Ψ_λ the character

$$\Psi_\lambda : GR(8,m)\to\mathbb{C}^*,\quad x\mapsto\zeta^{Tr(\lambda x)}.$$

The following lemma follows from [6].

Lemma 4. *For all* $\lambda\in GR(8,m), \lambda\neq 0$, *we have*

$$\left|\sum_{x\in\mathcal{T}} \Psi_\lambda(x)\right| \leqslant 3\sqrt{2^m}.$$

Proof. We restate [6, Theorem 1] for the special Galois Ring of concern here. Let $f(X)$ denote a polynomial in $GR(8,m)[X]$ and let

$$f = F_0 + 2F_1 + 4F_2$$

denote its 2-adic expansion. Let n_i be the degree in X of F_i. Call χ an arbitrary additive character of $GR(8,m)$, and N the *weighted degree* of f, namely

$$N = \max(4n_0,\ 2n_1,\ n_2).$$

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

$$\left|\sum_{x\in\mathscr{T}} \chi(f(x))\right| \leqslant (N-1)2^{m/2}.$$

See [6] for details. The result follows upon considering a linear f, when $N = 4$. □

We now have the following results on, respectively, the imbalance and the autocorrelation function of the binary sequence $(c_t)_{t\in\mathbb{N}}$.

Theorem 5. *With notation as above, we have*

$$\left|\sum_{t\in\mathscr{I}} (-1)^{c_t}\right| \leqslant 3\sqrt{2+\sqrt{2}}\sqrt{2^m}.$$

Proof. Write $z_t = Tr(\lambda\xi^t)$. For $0\leqslant i\leqslant 7$, let n_i denote the number of t such that $z_t = i$. Then,

$$\sum_{t\in\mathscr{I}} (-1)^{c_t} = \sum_{i=0}^{3} (n_i - n_{i+4}),$$

while

$$\sum_{t\in\mathscr{I}} \zeta^{z_t} = \sum_{i=0}^{3} (n_i - n_{i+4})\zeta^i.$$

Using the notation above with $x = n_0 - n_4$, $y = n_1 - n_5$, $z = n_2 - n_6$, and $t = n_3 - n_7$ we get

$$Q_j = \sum_{t\in\mathscr{I}} \zeta^{jz_t}.$$

Going back to the definition of z_t, we get

$$Q_j = \sum_{t\in\mathscr{I}} \Psi_\lambda(j\xi^t),$$

and, after a change of variable

$$Q_j = \sum_{x\in\mathscr{T}} \Psi_\lambda(x).$$

By Lemma 4, $|Q_j| \leqslant 3\sqrt{2^m}$ for all $j = 1, 3, 5, 7$. Therefore, using Lemma 3 and the triangle inequality, we obtain

$$\left| \sum_{t \in \mathscr{I}} (-1)^{c_t} \right| \leqslant 3\sqrt{2+\sqrt{2}}\sqrt{2^m}. \qquad \square$$

Theorem 6. *With notation as above, and for all phase shifts* $\tau, 0 < \tau < 2^m - 1$, *let*

$$\Theta(\tau) = \sum_{t \in \mathscr{I}} (-1)^{c_t}(-1)^{c_{t+\tau}}.$$

We then have the bound

$$|\Theta(\tau)| \leqslant 3(2+\sqrt{2})\sqrt{2^m}.$$

Proof. Again let ξ be a generator of the Teichmüller set. As we have $c_t = MSB(Tr(\lambda\xi^t))$, Lemma 2 implies that

$$\Theta(\tau) = \sum_{j,j'} \mu_j \mu_{j'} \sum_{x \in \mathscr{T}} \Psi_{\lambda(j+j'\xi^\tau)}(x).$$

Here $j + j'\xi^\tau \neq 0$ as $\xi^\tau \notin \mathbb{Z}_8$, so the claim follows from the triangle inequality, Lemma 4 and Lemma 2, and the elementary identity

$$\sum_{j,j'} |\mu_j \mu_{j'}| = \left(\sum_j |\mu_j| \right)^2. \qquad \square$$

We remark that, using the technique of Theorem 6, it is also easy to bound the crosscorrelation function of two MSB-sequences (c_t) and (c'_t) respectively defined by the equations $c_t = MSB(Tr(\lambda_1\xi^t))$ and $c'_t = MSB(Tr(\lambda_2\xi^t))$. The argument in the above proof can be carried out provided that the parameters λ_1, λ_2 are chosen carefully. To be more precise, we must exclude the cases where $j\lambda_1 + j'\lambda_2\xi^\tau = 0$ for some odd $j, j' \in \mathbb{Z}_8$ and some phase-shift τ. For otherwise we cannot apply the bound of Lemma 4. As only the odd values of j, i.e., the units of the ring $\mathbb{Z}_8$, appear in the expansion of Lemma 2, the equation $j\lambda_1 + j'\lambda_2\xi^\tau = 0$ will never hold for any τ, when λ_1 and λ_2 belong to different cosets of the subgroup $\mathbb{Z}_8^* \times \mathscr{T}^*$ of the unit group of our ring $GR(8, m)$. We summarize this discussion in the following Theorem.

Theorem 7. *There exists a family of* $N_m := 2^{m-2}(2^m+1) \sim T^2/4$ *cyclically distinct binary sequences of period* $T = 2^m - 1$, *and auto- and crosscorrelation at most* $11\sqrt{T+1}$.

Proof. The order of the unit group of $GR(8, m)$ is $8^m - 2^m$. The order of $\mathbb{Z}_8^* \times \mathscr{T}^*$ is $4(2^m - 1)$. Observe that $3(2+\sqrt{2}) \simeq 10.24$. The period is determined in Section 6. $\square$

For the sake of comparison, the family $S(m,3)$ of [1,8] allocates as many sequences of period T with a correlation peak at most $2\sqrt{T}$. However, both the nonlinearity and the linear span of our sequences are fairly high as the next two sections show.

We further remark that we can also bound the incomplete sums of the types considered in the above two theorems, where we restrict the range of summation to a subinterval of the index set $\mathscr{I}$. To that end we would also need to invoke the Shanbhag–Kumar–Helleseth bound on hybrid sums. Such estimates are based on a method originally due to I.M. Vinogradow. We refer the reader to [7] for an account of this version of Vinogradow's method.

5. Nonlinearity

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 $\hat{c}(y)$ denote the Walsh–Hadamard Fourier coefficient of c_t in y, namely:

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

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

Theorem 8. *For all $c\in s_m$ and all $y\in\mathbb{F}_2^m$, we have the bound*

$$|\hat{c}(y)|\leqslant 3\sqrt{2+\sqrt{2}}\sqrt{n}.$$

Proof. It suffices to replace c by $c+tr(y\theta^t)$ and θ^w by $\theta^{w'}$ such that $\theta^{w'} = y+\theta^w$ to reduce to Theorem 5. □

For the sake of comparison, for even m, the bent sequences have a better nonlinearity (viz. $\sqrt{n}$). All known constructions of infinite families of bent functions are quadratic, as opposed to our quartic family of Boolean functions [3].

6. Period and linear span

The following result follows from [5, Theorem 7] by letting $k=2$.

Proposition 9. (Kumar–Helleseth). *The linear span of the binary sequence* $(c_t)_{t\in\mathbb{N}}$ *is at most* $\sum_{j=1}^{4}\binom{m}{j}$ *and at least* $\binom{m}{4}$.

The binary sequence $(c_t)_{t\in\mathbb{N}}$ has period 2^m-1.

Proposition 10. *The period of the binary sequence* $(c_t)_{t\in\mathbb{N}}$ *is* 2^m-1.

Proof. To determine the period, it suffices to show that the greatest common divisor of 2^m-1 with the exponents of x in $R(x)$ is equal to 1. Among these exponents are: $\alpha=2\cdot 2^{i_1}+2^{i_2}+2^{i_3}$, $\beta=2^{i_1}+2\cdot 2^{i_2}+2^{i_3}$, $\gamma=2^{i_1}+2^{i_2}+2\cdot 2^{i_3}$ and $\delta=2^{i_1}+2^{i_2}+2^{i_3}+2^{i_4}$. Since $4\delta-\alpha-\beta-\gamma=4\cdot 2^{i_4}=2^{i_4+2}$, the g.c.d. of these three exponents divides 2^{i_4+2}. Since 2^m-1 is odd, it follows that the period is 2^m-1. □

We remark that the above result on the period of the sequence (c_t) also follows immediately from our bound on its autocorrelation, Theorem 6, in those cases, where the length of the sequence exceeds $3(2+\sqrt{2})\sqrt{2^m}+1$, i.e., for all $m\geqslant 7$.

Note that the linear span is of the order of the fourth power of the logarithm of the period, which is better than the No sequences whose linear span is only logarithmic in the period [4, Section 6.2].

7. Generalization to $\mathbb{Z}_{2^l}$

Let l be a positive integer (without loss of generality, we assume that $l\geqslant 4$) and let $\zeta=e^{2\pi i/2^l}$ be a primitive 2^lth root of 1 in $\mathbb{C}$. Let ψ_k be the additive character of $\mathbb{Z}_{2^l}$ such that

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

Let $\mu:\mathbb{Z}_{2^l}\to\{\pm 1\}$ be the most significant bit map. It maps $0,1,\ldots,2^{l-1}-1$ to $+1$ and $2^{l-1},2^{l-1}+1,\ldots,2^l-1$ to -1. Our goal is to express this map as a linear combination of characters. Recall the Fourier transformation formula on $\mathbb{Z}_{2^l}$:

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

We need the following lemma:

Lemma 11. *We have that*:

$$\mu_j=\frac{2}{2^{l-1}}\frac{1}{1-\zeta^{-j}}, \tag{2}$$

where $j=1,3,\ldots,2^l-1$ *is odd, and* $\mu_j=0$ *when* $j=0,2,\ldots,2^l-2$ *is even.*

Proof. From the definition of ζ, it follows that $\psi_j(x \pm 2^{l-1}) = -\psi_j(x)$. The most significant bit function $\mu(x)$ satisfies $\mu(x + 2^{l-1}) = -\mu(x)$. Thus

$$\mu(x + 2^{l-1})\psi_j(-(x + 2^{l-1})) = \mu(x)\psi_j(-x)$$

and we have

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

Note that $\mu(x) = 1$ when $x = 0, 1, \ldots, 2^{l-1} - 1$. So we have

$$\mu_j = \frac{2}{2^l} \sum_{x=0}^{2^{l-1}-1} \zeta^{-jx} = \frac{1}{2^{l-1}} \frac{1 - (\zeta^{-j})^{2^{l-1}}}{1 - \zeta^{-j}}. \tag{3}$$

Since $\zeta^{\pm 2^l} = 1$ and $\zeta^{\pm 2^{l-1}} = -1$, we have

$$1 - (\zeta^{-j})^{2^{l-1}} = 1 - (-1)^j,$$

which is 2 when j is odd and zero when j is even. The Lemma follows. □

From this Lemma we obtain:

Corollary 12. *We have*:

$$|\mu_j| = |\mu_{2^l - j}| = \frac{1}{2^{l-1}} \frac{1}{\sin(\pi j / 2^l)}, \tag{4}$$

when $j = 1, 3, \ldots, 2^{l-1} - 1$ *is odd.*

Proof. Indeed, we have

$$|1 - \zeta^{\pm j}| = |\zeta^{\pm j/2}|\,|\zeta^{\mp j/2} - \zeta^{\pm j/2}| = 2 \sin\left(\frac{\pi j}{2^l}\right).$$

The corollary follows. □

The main result of this section is the following theorem:

Theorem 13. *Set* $q = 2^l$. *Then we have*:

$$\sum_{j=1}^{q-1} |\mu_j| < \frac{2}{\pi} \ln(\cot(\pi/(2q))) + \frac{4}{q \sin(\pi/q)}$$

$$\sum_{j=1}^{q-1} |\mu_j| > \frac{2}{\pi} \ln(\cot(\pi/(2q))) + \frac{2}{\pi} \ln(\tan(\pi/4 - \pi/(2q))).$$

Proof. Using Lemma 11 and Corollary 12, we have

$$\sum_{j=1}^{q-1} |\mu_j| = 2\sum_{j=1}^{q/2-1} |\mu_j| = \frac{4}{q}\sum_{k=0}^{q/4-1} \frac{1}{\sin(\pi(2k+1)/q)}. \tag{5}$$

Consider the following function:

$$f(x) = \frac{1}{\sin(\pi x/q)}.$$

This function is positive and decreasing on the interval $[1, q/2-1]$. Thus, for any $a, b \in [1, q/2-1]$ and $a<b$, we have

$$f(b)(b-a) < \int_a^b f(x)\,dx < f(a)(b-a).$$

We use it when b is $a+2$ and a runs over $1, 3, \ldots, q/2-3$. Taking the sum and dividing by 2, we obtain:

$$\frac{1}{2}\int_1^{q/2-1} f(x)\,dx + f(q/2-1) < \sum_{k=0}^{q/4-1} f(2k+1) < \frac{1}{2}\int_1^{q/2-1} f(x)\,dx + f(1).$$

Since $f(x)$ is positive on the interval $[1, q/2]$, we will drop the $f(q/2-1)$ term from the lower bound and integrate up to $q/2$ in the upper bound. Thus we obtain a weaker estimate

$$\frac{1}{2}\int_1^{q/2-1} f(x)\,dx < \sum_{k=0}^{q/4-1} f(2k+1) < \frac{1}{2}\int_1^{q/2} f(x)\,dx + f(1). \tag{6}$$

Recall that

$$\int \frac{dx}{\sin(x)} = \ln(\tan(x/2)) + const.$$

Using this formula, we obtain the following for the lower bound:

$$\frac{1}{2}\int_1^{q/2-1} \frac{dx}{\sin(\pi x/q)} = \frac{q}{2\pi}\int_{\pi/q}^{\pi/2-\pi/q} \frac{dt}{\sin(t)},$$

which is equal to the product of $q/(2\pi)$ and

$$\ln(\tan(\pi/4 - \pi/(2q))) - \ln(\tan(\pi/(2q))).$$

Similarly, for the upper bound we have:

$$\frac{1}{2}\int_1^{q/2} \frac{dx}{\sin(\pi x/q)} = -\frac{q}{2\pi}\ln(\tan(\pi/(2q))).$$

Recall that $\cot(t) = 1/\tan(t)$. Thus we can estimate the sum of (6) from above as:

$$\sum_{k=0}^{q/4-1} \frac{1}{\sin(\pi(2k+1)/q)} < \frac{q}{2\pi}\ln(\cot(\pi/(2q))) + \frac{1}{\sin(\pi/q)},$$

and from below as:

$$\frac{q}{2\pi}\ln(\cot(\pi/(2q))) + \frac{q}{2\pi}\ln(\tan(\pi/4 - \pi/(2q))).$$

Multiplying it by $4/q$, we obtain the estimate of (5). The Theorem follows. □

In particular, we obtain the following:

Corollary 14. *Let $q = 2^l$ where $l \geqslant 4$. Then*

$$\sum_{j=0}^{q-1} |\mu_j| < \frac{2}{\pi}\ln(q) + 1. \tag{7}$$

Proof. Recall that when $0 < x < \pi/4$, we have $\tan(x) > x$. Thus

$$\ln(\cot(x)) = -\ln(\tan(x)) < -\ln(x).$$

We apply this inequality when $x = \pi/(2q) \leqslant \pi/32$ to obtain:

$$\ln\left(\cot\left(\frac{\pi}{2q}\right)\right) < \ln(q) - \ln(\pi/2). \tag{8}$$

Furthermore since:

$$\frac{\pi}{q} > \sin\left(\frac{\pi}{q}\right) > \frac{\pi}{q}\left(1 - \frac{1}{6}\left(\frac{\pi}{q}\right)^2\right) > 0.993\,\frac{\pi}{q},$$

we have that

$$\frac{4}{\pi} < \frac{4}{q\sin(\pi/q)} < \frac{4}{0.993\pi} < 1.283.$$

Combining it with (8) multiplied by $2/\pi$, and using that

$$1.283 - \frac{2}{\pi}\ln\left(\frac{\pi}{2}\right) < 1,$$

we obtain the required estimate. □

We are now in a position to generalize Theorem 7 to higher l's. The proof is analogous and omitted.

Theorem 15. *There exists a family of*

$$N_{l,m} := 2^{m-l-1}\,\frac{2^{(l-1)m} - 1}{2^m - 1} \sim T^{l-1}/2^{l-1}$$

cyclically distinct binary sequences of period $T = 2^m - 1$, and auto- and cross-correlations at most $0.19l^2(2^{l-1} - 1)\sqrt{T+1}$.

8. Conclusion

In this work, from the $\mathbb{Z}_8$-Kerdock code, we have derived sequences of MSB type. Generalizing to other cyclic codes (e.g., Delsarte–Goethals) seems feasible. Our key tool was to express the MSB-function as a linear combination of characters of the group $\mathbb{Z}_8$. While the correlation performance of our sequences is lower than, e.g., the $S(m,3)$ family of [1,8], both the nonlinearity and the linear span are fairly high. We leave as an open problem to determine these two invariants for $l \geqslant 4$.

Acknowledgments

The research of San Ling is partially supported by NUS-ARF research Grant R-146-000-029-112 and DSTA research Grant R-394-000-011-422. This research was done while San Ling was visiting ESSI, Sophia Antipolis. The author thanks ESSI for its hospitality. Patrick Solé is grateful to NUS Math Dept. for its kind hospitality.

References

[1] A. Barg, On Small Families of Sequences with Low Periodic Correlation, Lecture Notes in Computer Science, Vol. 781, Springer, Berlin, 1994, pp. 154–158.
[2] C. Carlet, $\mathbb{Z}_{2^k}$-linear codes, IEEE Trans. Inform. Theory 44 (1998) 1543–1547.
[3] C. Carlet, P. Charpin, V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, Designs Codes Cryptography 15 (1998) 125–156.
[4] T. Helleseth, P.V. Kumar, Sequences with low Correlation, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding theory, Vol. II, North-Holland, Amsterdam, 1998, pp. 1765–1853.
[5] P.V. Kumar, T. Helleseth, An expansion of the coordinates of the trace function over Galois rings, Appl. Alg. Engr. Comm. Comp. 8 (1997) 353–361.
[6] P.V. Kumar, T. Helleseth, A.R. Calderbank, An upper bound for Weil exponential sums over Galois rings and applications, IEEE Trans. Inform. Theory 41 (1995) 456–468.
[7] J. Lahtonen, On the odd and the aperiodic correlation properties of the binary Kasami sequences, IEEE Trans. Inform. Theory 41 (1995) 1506–1508.
[8] A. Shanbhag, P.V. Kumar, T. Helleseth, Improved binary codes and sequence families from $\mathbb{Z}_4$-linear codes, IEEE Trans. Inform. Theory 42 (1996) 1582–1586.
[9] M.K. Simon, J.K. Omura, R.A. Scholtz, B.K. Levitt, Spread Spectrum Communication Vol. I, Computer Science Press, Rockville, MD, 1985.

Further reading

S. Boztas, R. Hammons, P.V. Kumar, 4-phase sequences with near-optimum correlation properties, IEEE Trans. Inform. Theory 38 (1992) 1101–1113.
A.R. Hammons Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Inform. Theory 40 (1994) 301–319.
S. Ling, P. Solé, Nonlinear p-ary sequences, Appl. Alg. Engr. Comm. Comp. 14 (2003) 117–125.
F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
D.A. Marcus, Number Fields, Springer Universitext, New York, 1977.
B.R. McDonald, Finite Rings with Identity, Marcel Dekker, New York, 1974.