Quasi-orthogonal cocycles, optimal sequences and a conjecture of Littlewood

J. A. Armario & D. L. Flannery

Journal of Algebraic Combinatorics
An International Journal

ISSN 0925-9899

J Algebr Comb
DOI 10.1007/s10801-020-00971-2

ONLINE FIRST

Springer

Journal of Algebraic Combinatorics
https://doi.org/10.1007/s10801-020-00971-2

Quasi-orthogonal cocycles, optimal sequences and a conjecture of Littlewood

J. A. Armario[1] · **D. L. Flannery**[2]

Received: 1 February 2020 / Accepted: 4 August 2020

Abstract

A quasi-orthogonal cocycle, defined over a group of order congruent to 2 modulo 4, is naturally analogous to an orthogonal cocycle (i.e., one defined over a group of order divisible by 4, and whose display matrix is Hadamard). Here we extend the theory of quasi-orthogonal cocycles in new directions, using equivalences with various optimal binary and quaternary sequences.

Keywords Cocycle · Quasi-orthogonal · Sequence · Array · Autocorrelation · Merit factor · Golay pairs · Butson Hadamard matrix · EW matrix

Mathematics Subject Classification 05B10 · 05B20 · 94A55

1 Introduction

The theory of quasi-orthogonal cocycles and associated combinatorial objects has been explored in recent papers [4–6]. The current paper makes further progress in understanding the significance of these cocycles.

Dedicated to Professor K. T. Arasu on the occasion of his 65th birthday.

✉ J. A. Armario
armario@us.es

D. L. Flannery
dane.flannery@nuigalway.ie

1 Departamento de Matemática Aplicada I, Universidad de Sevilla, Avda. Reina Mercedes s/n, 41012 Seville, Spain

2 School of Mathematics, Statistics and Applied Mathematics, National University of Ireland Galway, Galway H91TK33, Ireland

Published online: 19 August 2020

Specifically, we examine optimal binary and quaternary sequences for periodic, negaperiodic, and aperiodic autocorrelation, from the cocyclic point of view. We thereby obtain a sufficient condition (in terms of quasi-orthogonal cocycles over $\mathbb{Z}_{2m}$, m odd) for a conjecture of Littlewood about the asymptotic behavior of the merit factor of binary sequences. It is known that this problem is related to the L_4-norm of complex-valued polynomials with ± 1 coefficients on the unit circle. In addition, we establish: a characterization of binary periodic optimal sequences of length $2m$ via binary sequences of length m; a method for constructing an EW matrix (a kind of D-optimal matrix) from optimal quaternary sequences; a bijection between negaperiodic Golay pairs of binary sequences of length $2m$ and periodic Golay pairs of quaternary sequences of length m. Applying the latter bijection, we discover a new quaternary complex Hadamard matrix of order 70.

2 Cocycles

This section reviews some elementary 2-cohomology and other basic results. For groups G and U, where U is finite abelian, a map $\psi : G \times G \rightarrow U$ such that

$$\psi(g,h)\psi(gh,k) = \psi(g,hk)\psi(h,k) \quad \forall g,h,k \in G$$

is a *cocycle*. The group of these cocycles is denoted $Z^2(G,U)$. Given a map $\phi : G \rightarrow U$, the *coboundary* $\partial\phi \in Z^2(G,U)$ is defined by $\partial\phi(g,h) = \phi(g)^{-1}\phi(h)^{-1}\phi(gh)$. The coboundaries form a subgroup $B^2(G,U)$ of $Z^2(G,U)$. For convenience, our cocycles are normalized, i.e., $\psi(1,1) = 1$. Each cocyclic matrix $M_\psi = [\psi(g,h)]_{g,h\in G}$ over G usually has first row and column indexed by 1_G.

Lemma 1 [11, Lemma 6.6] *$M_\psi M_\psi^\top$ has (i,j)th entry*

$$\psi(g_i g_j^{-1}, g_j) \textstyle\sum_{g\in G} \psi(g_i g_j^{-1}, g).$$

Let $U = \langle -1 \rangle \cong \mathbb{Z}_2$. In this case, if M_ψ is a Hadamard matrix (so that $|G| = 2$ or $|G| \equiv 0 \mod 4$), then ψ is said to be *orthogonal*.

The *row excess* $RE(M)$ of a cocyclic $\{\pm 1\}$-matrix M indexed by G is the sum of the absolute values of all row sums, apart from the row indexed by 1_G. By Lemma 1, ψ is orthogonal precisely when $RE(M_\psi) = 0$.

Henceforth we are interested mainly in cocycles over G of just even order, i.e., $|G| = 4t + 2 > 2$.

Proposition 1 [4, Proposition 1] *Let $\psi \in Z^2(G,\mathbb{Z}_2)$.*

(i) *$RE(M_\psi) \geq 4t$, and $RE(M_\psi) \geq 8t + 2$ if $\psi \in B^2(G,\mathbb{Z}_2)$.*
(ii) *$RE(M_\psi) = 4t$ if and only if $n/2$ rows of M_ψ each sum to 0 and the remaining non-initial rows each have sum ± 2.*

(iii) *Let* $\psi \in B^2(G, \mathbb{Z}_2)$. *Then* $RE(M_\psi) = 8t + 2$ *if and only if every non-initial row sum of* M_ψ *is* ± 2.

By analogy with the definition of orthogonal cocycles, we call ψ *quasi-orthogonal* if $RE(M_\psi)$ is minimal: $RE(M_\psi) = 4t$ for $\psi \notin B^2(G, \mathbb{Z}_2)$, and $RE(M_\psi) = 8t + 2$ for $\psi \in B^2(G, \mathbb{Z}_2)$. The analogy between orthogonal and quasi-orthogonal cocycles was noticed originally in connection with the maximal determinant problem for square binary matrices (to be discussed below).

3 Optimal sequences, arrays, and matrices

Let $\mathbf{s} = (s_1, \ldots, s_r)$ where $s_i > 1$, and let G be the abelian group $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$. An $\mathbf{s}$-*array* is just a map $\phi : G \to C$ where $C = \{\pm 1\}$ or $\{\pm 1, \pm \mathrm{i}\}$. Of course, a sequence is an $\mathbf{s}$-array with $r = 1$.

Let w be a non-negative integer. The *periodic autocorrelation at shift* w of an array $\phi : G \to C$ is

$$R_\phi(w) = \sum_{g \in G} \phi(g)\overline{\phi(g + w)},$$

reading arguments modulo n; the overline denotes complex conjugate.

A sequence ϕ of length n such that $R_\phi(w) = 0$ for $0 < w < n$ is *perfect*. No perfect binary (resp., quaternary) sequences of length $n > 4$ (resp., $n > 16$) are known; see [2,16]. Consequently, we search for sequences with next best possible periodic autocorrelation (according to [3, p. 2940] and [15]). A binary sequence ϕ of length $n \equiv 2 \mod 4$ is an OBS (*optimal binary sequence*) if $|R_\phi(w)| = 2$ for all w, $0 < w < n$. A quaternary sequence ϕ of odd length n is an OQS (*optimal quaternary sequence*) if $R_\phi(w) \in \{\pm 1\}$ for all w, $0 < w < n$ ($R_\phi(w)$ is real by [6, Corollary 2]).

Let $|G| \equiv 2 \mod 4$. A binary array ϕ on G is an OBA (*optimal binary array*) if $|R_\phi(w)| = 2$ for all nonzero $w \in G$. When $G = \mathbb{Z}_2 \times \mathbb{Z}_m$, this definition coincides with the definition of OBS. The following two facts from [5,6] relate (normalized) optimal arrays and sequences to quasi-orthogonal cocycles (we remark that Result 1 is Proposition 1 (iii) combined with the identity $R_\phi(w) = \phi(w) \sum_{g \in G} \partial\phi(w, g)$).

Result 1 Let $|G| = 2m$, m odd. A binary $\mathbf{s}$-array ϕ on G is an OBA if and only if $\partial\phi$ is quasi-orthogonal.

Result 2 There exists an OQS of odd length m if and only if there exists a quasi-orthogonal cocycle over $\mathbb{Z}_2 \times \mathbb{Z}_m$ that is not a coboundary.

Result 1 leads to a new characterization of optimal binary sequences, which we give next. Result 2 will be applied to construction of EW matrices.

Theorem 1 *Let m be odd. A binary sequence $\phi = (\phi(0), \ldots, \phi(2m-1))$ is an OBS if and only if there exist binary sequences a, b each of length m such that*

$$\begin{aligned} |R_a(w) + R_b(w)| &= 2, \quad 1 \le w \le m-1, \\ |R_{a,b}(0)| &= 1, \\ |R_{a,b}(w) + R_{a,b}(m-w)| &= 2, \quad 1 \le w \le (m-1)/2, \end{aligned}$$

where $R_{a,b}(w) = \sum_{k=0}^{2m-1} a(k)b(k+w)$ is the periodic cross-correlation function.

Proof Define

$$a(j) = \begin{cases} \phi(j) & j \text{ even} \\ \phi(m+j) & j \text{ odd}, \end{cases} \qquad b(j) = \begin{cases} \phi(m+j) & j \text{ even} \\ \phi(j) & j \text{ odd}, \end{cases}$$

and $\varphi = \begin{bmatrix} a(0) & \cdots & a(m-1) \\ b(0) & \cdots & b(m-1) \end{bmatrix}$. We calculate that

$$R_\phi(w) = R_\varphi(w \bmod 2,\; w \bmod m).$$

Hence, ϕ is optimal if and only if the $(2, m)$-array φ is an OBA; which, by Result 1, is equivalent to $\partial\varphi \in B^2(\mathbb{Z}_2 \times \mathbb{Z}_m, \langle -1 \rangle)$ being quasi-orthogonal.

Let

$$M = \begin{bmatrix} A & B \\ B & A \end{bmatrix}$$

where A, B are the $m \times m$ back-circulant $\{\pm 1\}$-matrices with first rows $(a(0), \ldots, a(m-1))$ and $(b(0), \ldots, b(m-1))$, respectively. The normalization of M is $M_{\partial\varphi} = DMD$ for a diagonal matrix D. Thus, by Lemma 1, the entries of $MM^\top$ are row sums of $M_{\partial\varphi}$ up to sign. Proposition 1 then implies that $\partial\varphi$ is quasi-orthogonal if and only if

$$\mathrm{abs}(MM^\top) = 2mI + 2(J - I) \tag{1}$$

where J is the all 1s matrix, and $\mathrm{abs}(X)$ is obtained from X by taking the absolute value of each entry. Since A and B are back-circulant, they are symmetric, so from (1) we get

$$\mathrm{abs}(A^2 + B^2) = 2mI + 2(J - I) \tag{2}$$

$$\mathrm{abs}(AB + BA) = 2J. \tag{3}$$

By inspection, (2) is equivalent to $|R_a(w) + R_b(w)| = 2$ for $1 \le w \le m-1$, and (3) is equivalent to the remaining conditions in the statement of the theorem. $\square$

Example 1 If $\phi = (1, -1, 1, -1, 1, 1, -1, -1, 1, 1, 1, 1, 1, 1)$ then $R_\phi = (14, 2, 2, 2, 2, 2, 2, -2, 2, 2, 2, 2, 2, 2)$. Also $a = (1, 1, 1, 1, 1, 1, -1)$, $b = (-1, -1, 1, -1, 1, 1, 1)$, $R_a = (7, 3, 3, 3, 3, 3, 3)$, $R_b = (7, -1, -1, -1, -1, -1, -1)$, and $R_{a,b} = (-1, 3, 3, -1, 3, -1, -1)$.

For the rest of this section, 'determinant' of a matrix means the absolute value of its determinant.

Let M be a *D-optimal design of order* n: an $n \times n$ $\{\pm 1\}$-matrix with largest possible determinant at the given order. Hadamard famously proved that $\det M \leq n^{n/2}$. For orders $n \not\equiv 0 \mod 4$, more stringent bounds have been established. Let $n \equiv 2 \mod 4$; Ehlich [9] and independently Wojtas [17] proved that

$$\det M \leq (2n-2)(n-2)^{\frac{1}{2}n-1}.$$

This bound can be attained only if $n-1$ is the sum of two squares. A D-optimal design that attains the Ehlich–Wojtas bound is called an *EW matrix*. If a cocyclic matrix M_ψ is EW, then ψ is quasi-orthogonal [1]. Below, we go in the other direction, providing a construction of EW matrices from a type of OQS.

Theorem 2 *Suppose that there exists a quaternary sequence f of odd length m such that $R_f(w) = 1$ for all w, $0 < w < m$. Let C be the circulant matrix with first row $[f(0), f(1), \ldots, f(m-1)]$, and write $C = \frac{1-\mathrm{i}}{2}(A + \mathrm{i}B)$ where A, B are $\{\pm 1\}$-matrices of order m. Further, let*

$$M = \begin{bmatrix} A & B \\ -B & A \end{bmatrix}.$$

Then

$$MM^\top = \begin{bmatrix} L & 0 \\ 0 & L \end{bmatrix} \tag{4}$$

where $L = 2(m-1)I_m + 2J_m$, $A = \mathrm{Re}(C) - \mathrm{Im}(C)$, and $B = \mathrm{Re}(C) + \mathrm{Im}(C)$. Hence M is an EW matrix and $2m-1$ must be the sum of two squares.

Proof By the definitions,

$$MM^\top = \begin{bmatrix} AA^\top + BB^\top & -AB^\top + BA^\top \\ -BA^\top + AB^\top & AA^\top + BB^\top \end{bmatrix}$$

and

$$CC^* = \frac{1}{2}(AA^\top + BB^\top - \mathrm{i}AB^\top + \mathrm{i}BA^\top),$$

where $*$ denotes complex conjugate transpose. Also, $CC^* = (m-1)I + J$ because $R_f(w) = 1$ for $1 \leq w \leq m-1$. The result is now clear. $\square$

Example 2 Let $f_1 = (1, \mathrm{i}, 1)$ and $f_2 = (1, -1, 1, 1, 1)$. Then $R_{f_1} = (3, 1, 1)$, $R_{f_2} = (5, 1, 1, 1, 1)$, $A_1 = \begin{bmatrix} 1 & -1 & 1 \\ 1 & 1 & -1 \\ -1 & 1 & 1 \end{bmatrix}$, $B_1 = J_3$, and $A_2 = B_2 = \begin{bmatrix} 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 & 1 \end{bmatrix}$.

At first glance, Theorem 2 does not extend to OQS f such that $R_f(w)$ takes on values -1. But a Hadamard equivalent of the matrix M in that situation could satisfy (4). Note that, conversely, an EW matrix M certainly satisfies (4) up to equivalence.

4 Negaperiodic optimal sequences

Let $\phi = (\phi(0), \ldots, \phi(n-1))$ be a binary sequence, and denote the concatenation $\phi \mid -\phi$ by ϕ'. Then

$$NR_\phi(w) := \sum_{k=0}^{n-1} \phi(k)\phi'(k+w)$$

is the *negaperiodic autocorrelation of* ϕ *at shift* w. It is well known that

$$\max_{0<w<n} |NR_\phi(w)| \geq \begin{cases} 0 & n \text{ even} \\ 1 & n \text{ odd}. \end{cases}$$

Sequences ϕ such that $NR_\phi(w) = 0$ for $1 \leq w \leq n-1$ do not exist at lengths $n > 2$ [13, Result 4.8]. Hence, if n is even, then $|NR_\phi(w)| \geq 2$ for some w. A binary sequence ϕ of length $2m$ such that $NR_\phi(w) \in \{0, \pm 2\}$ for all w, $0 < w < 2m$, has *optimal negaperiodic autocorrelation*. In [6], we showed that there exists a binary sequence of length $2m \equiv 2 \mod 4$ with optimal negaperiodic autocorrelation if and only if there exists a quasi-orthogonal cocycle over $\mathbb{Z}_2 \times \mathbb{Z}_m$ that is not a coboundary.

A pair ϕ_1, ϕ_2 of binary (resp., quaternary) sequences, each of length n, such that $NR_{\phi_1}(w) + NR_{\phi_2}(w) = 0$ (resp., $R_{\phi_1}(w) + R_{\phi_2}(w) = 0$) for $1 \leq w \leq n-1$ is a *negaperiodic Golay pair* (NGP) (resp., *quaternary periodic Golay pair*).

An $n \times n$ matrix H with entries in $\{\pm 1, \pm \mathrm{i}\}$ is a *quaternary complex Hadamard matrix* or *Butson Hadamard matrix* (denoted $BH(n, 4)$) if $HH^* = nI$. We discuss how to construct $BH(n, 4)$ from negaperiodic Golay pairs. In particular, we construct a $BH(70, 4)$ that seems to be new. Previously there were two known inequivalent $BH(70, 4)$, one due to Djokovic [7] and the other due to Egan [8].

Lemma 2 *Let m be odd. There is a bijection between the set of negaperiodic Golay pairs of length $2m$ (denoted $PUGP(2m, 2, 1)$ in [8]) and the set of periodic Golay pairs of quaternary sequences of length m ($PUGP(m, 4, 0)$ in [8]).*

Proof Let φ be a binary sequence of length $2m$, and (per [6, Lemma 1]) let ϕ be the $(2, m)$-array associated to φ, defined as follows. For $m \equiv 1 \mod 4$:

$$\phi(a,k) = \begin{cases} \varphi(k+am) & k \equiv 0 \mod 4 \\ (-1)^{1-a}\varphi(k+(1-a)m) & k \equiv 1 \mod 4 \\ -\varphi(k+am) & k \equiv 2 \mod 4 \\ (-1)^{a}\varphi(k+(1-a)m) & k \equiv 3 \mod 4 \end{cases}$$

and for $m \equiv 3 \mod 4$:

$$\phi(a,k) = \begin{cases} (-1)^{a}\varphi(k+am) & k \equiv 0 \mod 4 \\ \varphi(k+(1-a)m) & k \equiv 1 \mod 4 \\ (-1)^{1-a}\varphi(k+am) & k \equiv 2 \mod 4 \\ -\varphi(k+(1-a)m) & k \equiv 3 \mod 4. \end{cases}$$

Furthermore (per [6, Remark 1]), let f be the associated quaternary sequence of length m defined by

$$f(k) = \frac{1-\mathrm{i}}{2}(\phi(0,k) + \mathrm{i}\phi(1,k)),$$
$$\phi(a,k) = \begin{cases} \mathrm{Re}(f(k)) - \mathrm{Im}(f(k)) & \text{if } a = 0 \\ \mathrm{Re}(f(k)) + \mathrm{Im}(f(k)) & \text{if } a = 1. \end{cases}$$

By routine computation, (φ_1, φ_2) is an NGP$(2m)$ if and only if (f_1, f_2) is a periodic Golay pair of quaternary sequences of length m. □

Example 3

$$f_1 = (1, \mathrm{i}, \mathrm{i}, -\mathrm{i}, 1, 1, -\mathrm{i}, 1, -1, -1, -\mathrm{i}, -\mathrm{i}, -1, -\mathrm{i}, -\mathrm{i}, \mathrm{i}, \mathrm{i}, 1,$$
$$-\mathrm{i}, -\mathrm{i}, -\mathrm{i}, \mathrm{i}, -\mathrm{i}, 1, -1, 1, 1, 1, -\mathrm{i}, -1, -1, 1, 1, \mathrm{i}, 1)$$

and

$$f_2 = (1, \mathrm{i}, -1, -\mathrm{i}, -\mathrm{i}, 1, \mathrm{i}, -1, \mathrm{i}, 1, -\mathrm{i}, \mathrm{i}, -\mathrm{i}, 1, -\mathrm{i}, -\mathrm{i}, 1, -\mathrm{i}, \mathrm{i}, 1, \mathrm{i},$$
$$-\mathrm{i}, \mathrm{i}, -1, \mathrm{i}, -\mathrm{i}, -1, -\mathrm{i}, -\mathrm{i}, -1, -\mathrm{i}, \mathrm{i}, -\mathrm{i}, -1, \mathrm{i})$$

is the quaternary periodic Golay pair as in Lemma 2 associated to the NGP of length 70 in [12, p. 662].

The following is a special case of [8, Theorem 3.2].

Theorem 3 *Let* (f_1, f_2) *be a quaternary periodic Golay pair of odd length* m. *Then*

$$H = \begin{bmatrix} A & B \\ -B^* & A^* \end{bmatrix}$$

is a $BH(2m, 4)$, *where* A *and* B *are circulant matrices with first rows* $[f_1(0), \ldots, f_1(m-1)]$ *and* $[f_2(0), \ldots, f_2(m-1)]$, *respectively.*

Corollary 1 *Theorem 3 and Example 3 furnish a new* $BH(70, 4)$.

Our method of constructing $BH(70, 4)$ is similar to the one in [8]; Egan uses a bijection between $PUGP(m, 4, 1)$ and $PUGP(2m, 2, 1)$.

We point out that

$$PUGP(2m, 2, 0) \neq PUGP(2m, 2, 1)$$

and

$$GP(2m) = PUGP(2m, 2, 0) \cap PUGP(2m, 2, 1),$$

where $GP(2m)$ denotes the set of binary (aperiodic) Golay pairs of length $2m$. Egan [8, Theorem 2.2] proved that

$$GP(m, 4) = \cap_{k=0}^{3} PUGP(m, 4, k)$$

where $GP(m, 4)$ denotes the set of quaternary (aperiodic) Golay pairs. Thus, $GP(m, 4) = \cap_{k=1}^{3} PUGP(m, 4, k)$.

5 Aperiodic optimal sequences

The *aperiodic autocorrelation* at shift w of a binary sequence ϕ of length n is

$$C_\phi(w) = \sum_{0 \le k < n-w} \phi(k)\phi(k+w).$$

We observe that

$$R_\phi(w) = C_\phi(w) + C_\phi(n-w), \quad NR_\phi(w) = C_\phi(w) - C_\phi(n-w). \tag{5}$$

Typically, sequences with good aperiodic autocorrelation are identified among sequences with good periodic autocorrelation. By (5), it might be advisable to search also among the sequences with good negaperiodic autocorrelation as a first step. We show how this task reduces yet again to the existence problem for quasi-orthogonal cocycles.

Lemma 3 *Let ϕ be a binary sequence of length $2m$. Define $\mu \in Z^2(\mathbb{Z}_{2m}, \langle -1 \rangle) \setminus B^2(\mathbb{Z}_{2m}, \langle -1 \rangle)$ by $\mu(j,k) = (-1)^{\lfloor (j+k)/2m \rfloor}$, and put $\psi = \mu \partial \phi$. Then*

$$NR_\phi(w) = \phi(0)\phi(w)\psi(n-w, w) \sum_{j=0}^{2m-1} \psi(n-w, j) \quad \forall w,\ 0 < w < 2m.$$

Proof If A is the $2m \times 2m$ nega-back-circulant $\{\pm 1\}$-matrix with first row $[\phi(0), \dots, \phi(2m-1)]$, then $[AA^\top]_{1,j} = NR_\phi(j-1)$. We normalize $B = A \circ M_\mu$ to obtain the coboundary matrix $M_{\partial\phi}$, i.e., $M_{\partial\phi} = DBD$ where D is the diagonal matrix with $[D]_{j,j} = \phi(j-1)$ and $\circ$ denotes Hadamard (componentwise) product. Since $M_\psi = M_{\partial\phi} \circ M_\mu = D(B \circ M_\mu)D = DAD$, we have $AA^\top = DM_\psi M_\psi^\top D$, so

$$NR_\phi(j-1) = \phi(0)\phi(j-1)[M_\psi M_\psi^\top]_{1,j}.$$

By Lemma 1, we are done. □

Corollary 2 *Let m be odd. Then $\phi = (\phi(0), \dots, \phi(2m-1)) \in \{\pm 1\}^{2m}$ is optimal negaperiodic if and only if the cocycle $\mu\partial\phi$ is quasi-orthogonal.*

Proof This follows from Proposition 1 and Lemma 3. □

The final topic that we consider concerns the *merit factor* of a binary sequence ϕ of length n:

$$F(\phi) = \frac{n^2}{2\sum_{0<w<n} |C_\phi(w)|^2}.$$

The growth rate of the optimal merit factor, as sequence length increases, is related to a classical conjecture of Littlewood [14] about the asymptotic behavior of norms of polynomials on the unit circle. We bound $F(\phi)$ relying on the existence of quasi-orthogonal coboundaries and non-coboundary cocycles over $\mathbb{Z}_{2m}$, m odd.

Proposition 2 *Suppose that ϕ is an OBS of length $n \equiv 2 \mod 4$, and let μ be as in Lemma 3. If $\mu\partial\phi$ is quasi-orthogonal, then $C_\phi(w) \in \{0, \pm 1, \pm 2\}$, with $|C_\phi(w)| = 1$ for $n/2$ different values w. Hence*

$$\frac{n^2}{5n-8} \le F(\phi) \le n. \tag{6}$$

Proof Each non-initial row sum of $M_{\partial\phi}$ is ± 2 by Result 1. On the other hand, if $\psi = \mu\partial\phi$ is quasi-orthogonal, then M_ψ has $\frac{n}{2}$ rows summing to zero, and $\frac{n-2}{2}$ rows summing to ± 2 (Proposition 1). Therefore, (5) and Lemma 3 yield that

$$\begin{aligned} C_\phi(w) + C_\phi(n-w) &= \pm 2 \\ C_\phi(w) - C_\phi(n-w) &= \ \ 0 \end{aligned}$$

for $n/2$ values w, and

$$C_\phi(w) + C_\phi(n-w) = \pm 2$$
$$C_\phi(w) - C_\phi(n-w) = \pm 2$$

otherwise. The conclusion follows. □

Example 4 If $\phi = (1, -1, 1, -1, 1, 1, -1, -1, 1, 1, 1, 1, 1, 1)$ then $C_\phi = (14, 1, 2, 1, 2, 1, 0, -1, 2, 1, 0, 1, 0, 1)$, $R_\phi = (14, 2, 2, 2, 2, 2, 2, -2, 2, 2, 2, 2, 2, 2)$, and $F(\phi) = 5.15789\ldots$

Define $\beta(n)$ to be the maximum of $F(\phi)$ as ϕ ranges over the set of all binary sequences of length n.

Conjecture 1 (Littlewood [14]) $\limsup_{n\to\infty} \beta(n) = \infty$.

Corollary 3 *If there exists an infinite family of sequences ϕ satisfying the hypotheses of Proposition 2, then Conjecture 1 is true.*

Golay [10] made an opposing conjecture about $\beta(n)$, as follows.

Conjecture 2 $\limsup_{n\to\infty} \beta(n) = 12.32\ldots$

This second conjecture appears to have a stronger foundation. So we suspect that there does not exist an infinite family of quasi-orthogonal coboundaries $\partial\phi$ over $\mathbb{Z}_2 \times \mathbb{Z}_m$ with $\mu\partial\phi$ quasi-orthogonal too.

Experimental evidence is sparse. After carrying out exhaustive computer searches up to $m = 13$, apart from $m = 11$ we always found ϕ such that $\partial\phi$ and $\mu\partial\phi$ are quasi-orthogonal. For $23 \leq m \leq 30$, such cocycles do not exist: the optimal merit factor is known, and it is smaller than the lower bound in (6).

Acknowledgements The first author thanks Kristeen Cheng for reading the manuscript. We are also grateful to Ronan Egan for advice. This research was partially supported by project FQM-016 funded by JJAA (Spain).

References

1. Álvarez, V., Armario, J.A., Frau, M.D., Gudiel, F.: The maximal determinant of cocyclic $(-1, 1)$-matrices over D_{2t}. Linear Algebra Appl. **436**(4), 858–873 (2012)
2. Arasu, K.T., de Launey, W., Ma, S.L.: On circulant complex Hadamard matrices. Des. Codes Cryptogr. **25**(2), 123–142 (2002)
3. Arasu, K.T., Ding, C., Helleseth, T., Kumar, P.V., Martinsen, H.: Almost difference sets and their sequences with optimal autocorrelation. IEEE Trans. Inform. Theory **47**(7), 2934–2943 (2001)
4. Armario, J.A., Flannery, D.L.: On quasi-orthogonal cocycles. J. Combin. Des. **26**(8), 401–411 (2018)
5. Armario, J.A., Flannery, D.L.: Generalized binary arrays from quasi-orthogonal cocycles. Des. Codes Cryptogr. **87**(10), 2405–2417 (2019)
6. Armario, J.A., Flannery, D.L.: Almost supplementary difference sets and quaternary sequences with optimal autocorrelation. Cryptogr. Commun. **12**, 757–768 (2020)

7. Djoković, D.Z.: Good matrices of order 33, 35 and 127 exist. J. Combin. Math. Combin. Comput. **14**, 145–152 (1993)
8. Egan, R.: Phased unitary Golay pairs, Butson Hadamard matrices and a conjecture of Ito's. Des. Codes Cryptogr. **87**(1), 67–74 (2019)
9. Ehlich, H.: Determiantenabschätzungen für binäre Matrizen. Math. Z. **83**, 123–132 (1964)
10. Golay, M.J.E.: The merit factor of long low autocorrelation binary sequences. IEEE Trans. Inf. Theory **28**(3), 543–549 (1982)
11. Horadam, K.J.: Hadamard Matrices and Their Applications. Princeton University Press, Princeton (2007)
12. Ito, N.: On Hadamard groups IV. J. Algebra **234**, 651–663 (2000)
13. Jedwab, J.: Generalized perfect arrays and Menon difference sets. Des. Codes Cryptogr. **2**(1), 19–68 (1992)
14. Littlewood, J.E.: On polynomials $\sum^n \pm z^m,\ \sum^n e^{\alpha_m i} z^m,\ z = e^{\theta i}$. J. Lond. Math. Soc. **41**(1), 367–376 (1966)
15. Lüke, H.D., Schotten, H.D., Hadinejad-Mahram, H.: Binary and quadriphase sequences with optimal autocorrelation properties: a survey. IEEE Trans. Inform. Theory **49**(12), 3271–3282 (2003)
16. Schmidt, B.: Towards Ryser's conjecture. In: Casacuberta, C., Miró-Roig, R.M., Verdera, J., Xambó-Descamps, S. (eds.) European Congress of Mathematics. Progress in Mathematics vol 201, pp. 533–541. Birkhäuser, Basel (2001)
17. Wojtas, W.: On Hadamard's inequality for the determinants of order non-divisible by 4. Colloq. Math. **12**, 73–83 (1964)