Almost supplementary difference sets and quaternary sequences with optimal autocorrelation

J. A. Armario and D. L. Flannery

[1] Departamento de Matemática Aplicada I, Universidad de Sevilla, Avda. Reina Mercedes s/n,
41012 Sevilla, Spain
armario@us.es

[2] School of Mathematics, Statistics and Applied Mathematics, National University of
Ireland Galway, Galway H91TK33, Ireland
dane.flannery@nuigalway.ie

Abstract. We introduce *almost supplementary difference sets* (ASDS). For odd m, certain ASDS in $\mathbb{Z}_m$ that have amicable incidence matrices are equivalent to quaternary sequences of odd length m with optimal autocorrelation. As one consequence, if $2m-1$ is a prime power, or $m \equiv 1 \mod 4$ is prime, then ASDS of this kind exist. We also explore connections to optimal binary sequences and group cohomology.

Mathematics Subject Classification: 05B10 · 05B20 · 94A55

1 Introduction

A sequence $\phi = (\phi(0), \ldots, \phi(n-1))$ with all entries in $\{\pm 1\}$ or $\{\pm 1, \pm \mathrm{i}\}$, where $\mathrm{i} = \sqrt{-1}$, is called *binary* or *quaternary*, respectively. For a non-negative integer w, the *periodic autocorrelation of ϕ at shift w* is

$$R_\phi(w) = \sum_{k=0}^{n-1} \phi(k)\overline{\phi(k+w)}, \tag{1}$$

reading arguments modulo n; the overline denotes complex conjugate as usual. It is easy to see that

$$\max_{0<w<n} |R_\phi(w)| \geq \begin{cases} 0 & n \equiv 0 \mod 4 \\ 1 & n \equiv 1 \mod 2 \\ 2 & n \equiv 2 \mod 4 \end{cases} \tag{2}$$

To appear in *Cryptography and Communications*

when ϕ is binary, and

$$\max_{0<w<n} |R_\phi(w)| \geq \begin{cases} 0 & n \text{ even} \\ 1 & n \text{ odd} \end{cases} \tag{3}$$

when ϕ is quaternary. A complex sequence ϕ such that $R_\phi(w) = 0$ for $0 < w < n$ is said to be *perfect*. Existence of a perfect binary (resp., quaternary) sequence is equivalent to existence of a Menon-Hadamard difference set in a cyclic group [8] (resp., a semi-regular relative difference set in a cyclic group with forbidden subgroup of size 2 [1]). No perfect binary (resp., quaternary) sequences of length $n > 4$ (resp., $n > 16$) are known; see [2, 13]. Furthermore, if p is an odd prime and $s > 2$ then there do not exist perfect sequences of length p^s over pth roots of unity [12].

Setting aside perfect sequences, we enlarge the notion of optimality consistent with (2) and (3); cf. [3, p. 2940] and [11]. A binary sequence ϕ of length n has *optimal autocorrelation* if, for all w, $0 < w < n$:

$R_\phi(w) \in \{0, \pm 4\}$ $(n \equiv 0 \mod 4)$
$R_\phi(w) \in \{1, -3\}$ $(n \equiv 1 \mod 4)$
$R_\phi(w) \in \{2, -2\}$ $(n \equiv 2 \mod 4)$
$R_\phi(w) = -1$ $(n \equiv 3 \mod 4)$.

A quaternary sequence ϕ of length n has optimal autocorrelation—we say that ϕ is an OQS (*optimal quaternary sequence*)—if

$|R_\phi(w)| = 1$ for all w, $0 < w < n$ (n odd)
$\max_{0<w<n} |R_\phi(w)| = 2$ (n even).

Actually, we will see that if n is odd and ϕ is an OQS then $R_\phi(w)$ is real.

Table 1 records some existence data, extracted from Tables II and IV of [11], about odd length sequences with optimal autocorrelation. There are infinite families in all cases bar one, namely binary sequences ϕ of length $n \equiv 1 \mod 4$ with $|R_\phi(w)| = 1$ for $0 < w < n$. Here examples are known only for $n = 5$ and $n = 13$.

Table 1. Optimal sequences of odd length n (p, q, r, $q+4$, $r+2$ are prime)

$n \mod 4$	Binary		Quaternary	
	$\max \lvert R_\phi(w)\rvert$	n	$\max \lvert R_\phi(w)\rvert$	n
1	1 3	5, 13 p, $q(q+4)$	1	$\frac{p^a+1}{2}$, p
3	1	p $2^a - 1$ $r(r+2)$	1	$\frac{p^a+1}{2}$

Binary sequences of length $2m$ with optimal 'odd autocorrelation' find practical applications in communication systems. The paper [14] gives a procedure to construct such a binary sequence from an OQS of odd length m. More is true: we demonstrate that these binary and quaternary sequences are equivalent.

Optimal binary sequences of (even or odd) length n may be characterized in terms of difference sets and almost difference sets in $\mathbb{Z}_n$; see [3]. A similar result for quaternary sequences was lacking until now. We explain how to characterize quaternary sequences of odd length n with optimal autocorrelation as *almost supplementary difference sets* in $\mathbb{Z}_n$.

This paper is a natural successor to [4, 5], which initiated the theory of quasi-orthogonal cocycles and their applications in design theory. We obtain new existence results for such cocycles from a connection to optimal quaternary sequences.

2 Quasi-orthogonal cocycles and optimal sequences

Let G and U be finite groups, with U abelian. A map $\psi : G \times G \to U$ such that

$$\psi(g,h)\psi(gh,k) = \psi(g,hk)\psi(h,k) \qquad \forall g,h,k \in G \tag{4}$$

is a *cocycle* over G. The set of cocycles under pointwise multiplication is an abelian group, denoted $Z^2(G,U)$. Given any map $\phi : G \to U$, 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 $Z^2(G,U)$. All cocycles are assumed to be normalized, i.e., $\psi(1,1) = 1$.

We display $\psi \in Z^2(G,U)$ as a *cocyclic matrix* $M_\psi = [\psi(g,h)]_{g,h\in G}$. If $U = \langle -1 \rangle \cong \mathbb{Z}_2$ and M_ψ is a Hadamard matrix then ψ is *orthogonal*; in that event of course $|G| = 2$ or $|G| \equiv 0 \mod 4$.

Let $\psi \in Z^2(G,\mathbb{Z}_2)$. The *row excess* $RE(M_\psi)$ of M_ψ is the sum of the absolute values of all row sums of M_ψ, apart from the row indexed by 1_G. Using (4), it may be shown that ψ is orthogonal precisely when $RE(M_\psi)$ is least, i.e., $RE(M_\psi) = 0$.

Henceforth we will treat mainly the case $|G| \equiv 2 \mod 4$; say $|G| = 4t + 2 > 2$.

Proposition 1 ([4, Proposition 1]). *If $\psi \in Z^2(G,\mathbb{Z}_2)$ then $RE(M_\psi) \geq 4t$, whereas $RE(M_\psi) \geq 8t + 2$ if $\psi \in B^2(G,\mathbb{Z}_2)$.*

By analogy with orthogonal cocycles, we call ψ *quasi-orthogonal* if the row excess of M_ψ is least possible: either $\psi \notin B^2(G,\mathbb{Z}_2)$ and $RE(M_\psi) = 4t$, or $\psi \in B^2(G,\mathbb{Z}_2)$ and $RE(M_\psi) = 8t+2$. The existence problem for quasi-orthogonal cocycles is open; in contrast to the situation for orthogonal cocycles, we do not know of any group over which they do not exist.

2.1 Generalized optimal binary arrays and optimal quaternary sequences

Let G be the additive abelian group $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$ where $s_i > 1$ for all i, and put $\mathbf{s} = (s_1, \dots, s_r)$. A (binary or quaternary) $\mathbf{s}$-*array* is simply a map $\phi : G \to C$ where $C = \{\pm 1\}$ or $\{\pm 1, \pm \mathrm{i}\}$. So a binary or quaternary sequence is an $\mathbf{s}$-array with $r = 1$.

For a *type vector* $\mathbf{z} = (z_1, \dots, z_r) \in \{0, 1\}^r$, let

$$\begin{aligned} &E = \mathbb{Z}_{(z_1+1)s_1} \times \cdots \times \mathbb{Z}_{(z_r+1)s_r}, \\ &H = \{(h_1, \dots, h_r) \in E \mid h_i = 0 \text{ if } z_i = 0, \text{ and } h_i = 0 \text{ or } s_i \text{ if } z_i = 1\}, \\ &K = \{h \in H \mid h \text{ has even weight}\}. \end{aligned}$$

Then K is a subgroup of the elementary abelian 2-subgroup H of E, and $E/H \cong G$. The *expansion* of a binary $\mathbf{s}$-array ϕ with respect to $\mathbf{z}$ is the map ϕ' on E defined by

$$\phi'(x) = \begin{cases} \phi(\tilde{x}) & x \in \tilde{x} + K \\ -\phi(\tilde{x}) & x \notin \tilde{x} + K \end{cases}$$

where $\tilde{x}$ denotes the projection of x in G (the ith component of $\tilde{x}$ is the ith component of x reduced modulo s_i).

We extend the definition of periodic autocorrelation given in (1) to arbitrary arrays $\varphi : A \to C$, i.e.,

$$R_\varphi(a) := \sum_{b \in A} \varphi(b)\overline{\varphi(a+b)}.$$

A binary $\mathbf{s}$-array ϕ is a *generalized perfect binary array* (GPBA($\mathbf{s}$)) *of type* $\mathbf{z}$ if

$$R_{\phi'}(x) = 0 \quad \forall x \in E \setminus H.$$

When $\mathbf{z} = \mathbf{0}$, this condition becomes $R_\phi(x) = 0$ for all $x \in G \setminus \{0\}$, and if it holds then ϕ is a *perfect binary array.* A GPBA($\mathbf{s}$) is equivalent to a relative difference set in E/K relative to H/K, thus equivalent to a cocyclic Hadamard matrix over G: see [7, Theorem 5.3] and [8, Theorem 3.2]. In particular, a binary array ϕ is perfect if and only if $\partial\phi$ is orthogonal.

Now we assume that $|G| \equiv 2 \mod 4$. In particular, we assume that $s_1/2, s_2, \dots, s_r$ are odd. A *generalized optimal binary array of type* $\mathbf{z}$ is a binary $\mathbf{s}$-array ϕ such that

- $R_{\phi'}(x) \in \{0, \pm 2|H|\}\ \forall x \in E \setminus H$
- $\big|\{x \in E \mid R_{\phi'}(x) = 0\}\big| = |E|/2$ if $z_1 = 1$.

We write GOBA($\mathbf{s}$) for short. A *generalized optimal binary sequence* (GOBS) is a GOBA($\mathbf{s}$) with $r = z_1 = 1$.

Since the abelian group G does not have a canonical form as a direct product of cyclic groups, the same array is a GOBA($\mathbf{s}$) for various $\mathbf{s}$. The following lemma reflects this fact (elements of $\mathbb{Z}_2 \times \mathbb{Z}_m$ and of $\mathbb{Z}_4 \times \mathbb{Z}_m$ are denoted as ordered pairs; context will indicate which direct product is meant).

Lemma 1. *Let φ be a binary sequence of length $2m$, $m > 1$ odd. Define the $(2,m)$-array ϕ 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 $m \equiv 3 \mod 4$:

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

Then φ is a GOBS if and only if ϕ is a GOBA$(2,m)$ of type $(1,0)$.

Proof. The identification is based on the isomorphism $\mathbb{Z}_4 \times \mathbb{Z}_m \to \mathbb{Z}_{4m}$ defined by $(1,1) \mapsto 1$. Signs are allocated so that $|R_{\varphi'}|$ always agrees with $|R_{\phi'}|$. □

Recall that $f : \mathbb{Z}_m \to \{\pm 1, \pm \mathrm{i}\}$ of odd length m is an OQS if $|R_f(w)| = 1$ for all w, $1 \le w \le m-1$. We proceed to establish the link between these quaternary sequences and binary arrays with optimal autocorrelation.

Remark 1. There is a one-to-one correspondence between the set of binary $(2,m)$-arrays ϕ and the set of quaternary sequences f on $\mathbb{Z}_m$, given by

$$f(k) = \frac{1-\mathrm{i}}{2}(\phi(0,k) + \mathrm{i}\phi(1,k)),$$

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

Translating between additive and multiplicative versions of $\mathbb{Z}_2 \times \mathbb{Z}_2$, we also observe that

$$f(k) = \mathrm{i}^{\Phi^{-1}\left(\frac{1-\phi(1,k)}{2}, \frac{1-\phi(0,k)}{2}\right)}$$

where $\Phi^{-1}\colon \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_4$ is the inverse Gray mapping, i.e., $\Phi^{-1}(0,0) = 0$, $\Phi^{-1}(0,1) = 1$, $\Phi^{-1}(1,1) = 2$, and $\Phi^{-1}(1,0) = 3$.

Lemma 2. *For f, ϕ as in Remark 1 and $0 \le w \le m-1$,*

$$R_f(w) = \frac{1}{4}(R_{\phi'}(0,w) - \mathrm{i}R_{\phi'}(1,w))$$

where ϕ' is the expansion of ϕ with respect to $\mathbf{z} = (1,0)$.

Proof. Routine. □

Theorem 1. *A quaternary sequence f of odd length m is an OQS if and only if its corresponding binary array ϕ is a GOBA$(2, m)$ of type $(1, 0)$.*

Proof. We have

$$R_{\phi'}(2, w) = -R_{\phi'}(0, w), \;\; R_{\phi'}(3, w) = -R_{\phi'}(1, w), \;\; \text{and } R_{\phi'}(0, w) + R_{\phi'}(1, w) \equiv 4 \mod 8.$$

Thus, if ϕ is a GOBA$(2, m)$ of type $(1, 0)$ then $R_{\phi'}(0, w)$ and $R_{\phi'}(1, w)$ cannot both be non-zero; so f is an OQS by Lemma 2.

Suppose that f is an OQS. By Lemma 2, again just one of $R_{\phi'}(0, w)$ or $R_{\phi'}(1, w)$ for $1 \leq w \leq m - 1$ is zero, while the other is ± 4. This also implies that the number of $x \in E$ such that $R_{\phi'}(x) = 0$ is $2m$, as required. □

Corollary 1. *A quaternary sequence of odd length m is an OQS if and only if the binary sequence to which it corresponds via Lemma 1 and Remark 1 is a GOBS of length $2m$.*

Previously, GOBS have appeared under other names. They are *binary sequences with optimal odd autocorrelation* in [14] (elsewhere, 'negaperiodic' replaces 'odd'). Corollary 1 furnishes a method to construct GOBS of length $2m$ from OQS of length m that is simpler than the one in [14, Construction A, p. 389].

Example 1. Let $f = (-1, 1, \mathrm{i}, 1, -\mathrm{i}, 1, \mathrm{i}, 1, -1)$. We calculate that

$$R_f = (9, -1, -1, -1, 1, 1, -1, -1, -1),$$

so f is an OQS of length 9. By Theorem 1,

$$\begin{bmatrix} -1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 \end{bmatrix}$$

is a GOBA$(2, 9)$ of type $(1, 0)$. Then by Lemma 1,

$$(-1, 1, 1, -1, 1, 1, 1, -1, -1, -1, -1, -1, 1, -1, -1, -1, 1, -1)$$

is a GOBS of length 18.

The next result was mentioned in the Introduction.

Corollary 2. *If f is an OQS of odd length m then $R_f(w) = \pm 1$ for $1 \leq w \leq m - 1$.*

Proof. We appeal to Lemma 2 once more. The GOBS φ corresponding to f has $R_{\varphi'}(u) = 0$ if $u \in \mathbb{Z}_{4m}$ is odd; i.e., $R_{\phi'}(1, w) = 0$ for all $w \not\equiv 0 \mod m$. □

We need the next result in Section 3, to prove the equivalence between OQS and almost supplementary difference sets. Denote the periodic cross-correlation $\sum_{k=0}^{n-1} a(k)b(k + w)$ of binary sequences a and b of length n by $R_{a,b}(w)$.

Corollary 3. *A quaternary sequence f of odd length m is an OQS if and only if*

$$R_{\phi(1,-)}(w) = R_{\phi(0,-)}(w) = \pm 1 \quad \textit{and} \quad R_{\phi(1,-),\phi(0,-)}(w) = R_{\phi(0,-),\phi(1,-)}(w)$$

for $1 \leq w \leq m-1$, where ϕ is as in Remark 1.

Proof. By [10, (6)], we have

$$R_f(w) = \frac{1}{2}(R_{\phi(1,-)}(w) + R_{\phi(0,-)}(w)) + \frac{\mathrm{i}}{2}(R_{\phi(1,-),\phi(0,-)}(w) - R_{\phi(0,-),\phi(1,-)}(w)).$$

The claim is then obvious from Corollary 2. □

2.2 Quasi-orthogonal cocycles over $\mathbb{Z}_2 \times \mathbb{Z}_m$

We now return the discussion to quasi-orthogonal cocycles, with a focus on indexing group $G = \mathbb{Z}_2 \times \mathbb{Z}_m$, m odd.

Define $\lambda \in Z^2(G, \langle -1 \rangle)$ by

$$\lambda((a,u),(b,w)) = \begin{cases} -1 & a = b = 1 \\ 1 & \text{otherwise.} \end{cases}$$

Order the elements of G as $g_1 = (0,0), g_2 = (0,1), \ldots, g_m = (0, m-1), g_{m+1} = (1,0), \ldots,$ $g_{2m} = (1, m-1)$. For $1 \leq i \leq m$, and with rows and columns indexed by G under this ordering, define the coboundary matrices M_{∂_i} and $M_{\partial_{i+m}}$ to be the respective normalizations of

$$\begin{bmatrix} C_i & J \\ J & C_i \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} J & C_i \\ C_i & J \end{bmatrix}, \tag{5}$$

where C_i is the $m \times m$ back circulant $\{\pm 1\}$-matrix whose first row is 1s except in position i, and J is the $m \times m$ all 1s matrix. Then $\{\lambda, \partial_2, \ldots, \partial_{2m-1}\}$ is a basis of $Z^2(G, \langle -1 \rangle)$.

Proposition 2 ([5, Theorem 2]). *A normalized binary $(2,m)$-array ϕ is a GOBA$(2,m)$ of type $(1,0)$ if and only if $\lambda\partial\phi$ is quasi-orthogonal.*

Remark 2. $\partial\phi = \prod_{i=2}^{2m-1} \partial_i^{e_i} = \partial_{2m} \prod_{i=2}^{m} \partial_i^{e_i} \cdot \prod_{i=m+1}^{2m-1} \partial_i^{1-e_i}$ where $e_i = \delta_{\phi(g_i),-1}$ (Kronecker delta).

Corollary 4. *There exists an OQS of 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.*

Proof. Immediate from Theorem 1 and Proposition 2. □

Remark 3. Corollary 4 and Table 1 provide new infinite families of quasi-orthogonal cocycles.

Example 2. $\phi_1 = \begin{bmatrix} 1 & -1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ is a GOBA$(2,3)$, and $\phi_2 = \begin{bmatrix} 1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 \end{bmatrix}$ is a GOBA$(2,5)$, both of type $(1,0)$. The corresponding OQS are $f_1 = (1, \mathrm{i}, 1)$ and $f_2 = (1, -1, 1, 1, 1)$, with $R_{f_1} = (3,1,1)$ and $R_{f_2} = (5,1,1,1,1)$; their GOBS are $\varphi_1 = (1,1,-1,-1,-1,1)$ and $\varphi_2 = (1,-1,-1,-1,1,1,1,-1,1,1)$. The quasi-orthogonal cocycles $\lambda\partial\phi_i$ have matrices

$$M_\lambda \circ M_{\partial_2} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 \end{bmatrix},$$

$$M_\lambda \circ M_{\partial_2} \circ M_{\partial_7} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 \end{bmatrix}$$

where $\circ$ denotes Hadamard (componentwise) product.

3 Almost supplementary difference sets

Let $B = \{x_1, \dots, x_{k_1}\}$ and $D = \{y_1, \dots, y_{k_2}\}$ be subsets of $\mathbb{Z}_m$. Suppose that the congruences

$$x_i - x_j \equiv a \mod m, \qquad y_{i'} - y_{j'} \equiv a \mod m$$

have exactly μ solutions for t values $a \not\equiv 0 \mod m$, and exactly $\mu + 1$ solutions for the remaining $m - 1 - t$ values $a \not\equiv 0 \mod m$. Then we call B and D *almost supplementary difference sets* (ASDS); in more detail, B and D are 2-$\{m; k_1, k_2; \mu; t\}$ ASDS. Clearly

$$k_1(k_1 - 1) + k_2(k_2 - 1) = t\mu + (m - 1 - t)(\mu + 1), \tag{6}$$

so that $t = (m-1)(\mu+1) - k_1(k_1-1) - k_2(k_2-1)$. We may therefore drop 't' in the specification of the parameters of ASDS.

Example 3. $B = \{1,4,5,6,7\}$ and $D = \{0,2\}$ are 2-$\{9;5,2;2;2\}$ ASDS.

Remark 4. If $t = m - 1$ then B, D are 2-$\{m; k_1, k_2; \mu\}$ *supplementary difference sets* (SDS) [9]. Another extreme is $k_1 \le 1 < k_2$; then D is an *almost difference set* [3].

Sometimes we can obtain ASDS from SDS by enlarging or reducing one of the supplementary sets. This places further constraints on the parameters, according to (6).

Lemma 3. *Suppose that B, D are 2-$\{m; k_1, k_2; \mu\}$ SDS.*

(i) *If $B \setminus \{b\}$ for some $b \in B$ and D are 2-$\{m; k_1 - 1, k_2; \mu - 1; \frac{m-1}{2}\}$ ASDS then $k_1 = (m+3)/4$ and $\mu = (m+3)/16 + (k_2^2 - k_2)/(m-1)$.*

(ii) *If $B \cup \{b\}$ for some $b \in \mathbb{Z}_m \setminus (B \cup D)$ and D are 2-$\{m; k_1 + 1, k_2; \mu; \frac{m-1}{2}\}$ ASDS then $k_1 = (m-1)/4$ and $\mu = (m-5)/16 + (k_2^2 - k_2)/(m-1)$.*

Example 4. (i) $B = \{1, 2, 4, 8, 11, 16\}$, $D = \{0, 5, 9, 10, 13, 15, 17, 18, 19, 20\}$ are 2-$\{21; 6, 10; 6\}$ SDS. Also $B \setminus \{1\}$, D are 2-$\{21; 5, 10; 5; 10\}$ ASDS.

(ii) $\{7, 8\}$, $\{3, 6, 8\}$ are 2-$\{9; 2, 3; 1\}$ SDS, and $\{4, 7, 8\}$, $\{3, 6, 8\}$ are 2-$\{9; 3, 3; 1; 4\}$ ASDS.

Let S be a subset of $\mathbb{Z}_m$, with characteristic function $\chi_S : \mathbb{Z}_m \to \{0, 1\}$. Then S^c will denote the (circulant) matrix indexed by $\mathbb{Z}_m$ whose (i, j)th entry is $1 - 2\chi_S(j - i)$. We now present a formulation of ASDS using incidence matrices of the supplementary sets; this may be compared with the Appendix of [6].

Theorem 2. (i) *Suppose that B and D are 2-$\{m; k, r; \mu\}$ ASDS. Let A be the set of all $a \in \mathbb{Z}_m \setminus \{0\}$ such that there are exactly μ solutions of*

$$b - b' \equiv a \mod m, \qquad d - d' \equiv a \mod m$$

for $b, b' \in B$ and $d, d' \in D$. Then $[B^c(B^c)^\top + D^c(D^c)^\top]_{i,j}$ is equal to

$$[4(k + r - \mu)I_m + 2(m - 2(k + r - \mu))J_m]_{i,j}$$

if $j - i \in A$, and

$$[4(k + r - \mu - 1)I_m + 2(m - 2(k + r - \mu - 1))J_m]_{i,j}$$

otherwise.

(ii) *Let B^c and D^c be $m \times m$ circulant $\{\pm 1\}$-matrices such that $B^c(B^c)^\top + D^c(D^c)^\top$ is as described in* (i). *Then the subsets B, D of $\mathbb{Z}_m$ determined by the first rows of B^c and D^c are 2-$\{m; k, r; \mu\}$ ASDS, where k (resp., r) is the number of -1s in each row of B^c (resp., D^c).*

Proof. (i) Choose any two different rows i and $i + a$ modulo m in the concatenated matrix $[B^c \mid D^c]$. Put $\bar{\mu} = \mu$ if $a \in A$ and $\bar{\mu} = \mu + 1$ if $a \notin A$. From the definition of ASDS, we deduce that in these two rows the column $[-1, -1]^\top$ appears $\bar{\mu}$ times, and $[-1, 1]^\top$, $[1, -1]^\top$ appear $k + r - \bar{\mu}$ times each. Hence the inner product of the rows is $2m - 4(k + r - \bar{\mu})$.

(ii) Since each row of B^c has k -1s and each row of D^c has r -1s, the inner product of rows i and j of $[B^c \mid D^c]$ is $2m - 4(k + r) + 4s$ where s is the number of columns $[-1, -1]^\top$. Thus, with $a \equiv j - i \mod m$, we have $s = \bar{\mu}$ as in part (i). □

We set down a few auxiliary facts to prepare for Theorem 3 below.

Lemma 4 ([8, Lemma 3.1]). *For any array $\varphi : A \to \{\pm 1\}$,*

$$R_{\varphi}(x) = |A| + 4(d_{\varphi}(x) - |N_{\varphi}|)$$

where $N_{\varphi} = \{a \in A \mid \varphi(a) = -1\}$ and $d_{\varphi}(x) = |N_{\varphi} \cap (x + N_{\varphi})|$.

Proposition 3. *Let B, D be 2-$\{m; k, r; \mu\}$ ASDS. Denote the complement of $X \subseteq \mathbb{Z}_m$ by $\overline{X}$. Then* (i) *$\overline{B}$, D,* (ii) *B, $\overline{D}$, and* (iii) *$\overline{B}$, $\overline{D}$ are also ASDS, with parameters $\{m; m-k, r; m-2k+\mu\}$ in case* (i), *$\{m; k, m-r; m-2r+\mu\}$ in case* (ii), *and $\{m; m-k, m-r; 2m-2k-2r+\mu\}$ in case* (iii).

Proof. Write d_X for d_{χ_X}. Subsets B and D of $\mathbb{Z}_m$ are 2-$\{m; |B|, |D|; \mu\}$ ASDS if and only if $d_B(w) + d_D(w) = \mu$ or $\mu + 1$ for all w, $1 \le w \le m-1$. Then the result follows from the identity $d_{\overline{X}}(w) = m - 2|X| + d_X(w)$. □

For the 2-$\{m; k, r; \mu\}$ ASDS of most interest to us, μ is determined by m, k, and r.

Theorem 3. *Let f be a quaternary sequence of odd length m, with corresponding $(2, m)$-array ϕ as in Remark* 1. *Then f is an OQS if and only if*

$$B = \{j \in \mathbb{Z}_m \mid \phi(0, j) = -1\}, \quad D = \{j \in \mathbb{Z}_m \mid \phi(1, j) = -1\}$$

are 2-$\{m; |B|, |D|; |B| + |D| - \frac{m+1}{2}\}$ ASDS such that the multiset $B - D$ of differences $x - y$ modulo m as (x, y) ranges over $B \times D$ is symmetric, i.e., closed under negation.

Proof. First we deal with a technicality. Although possibly $|B| + |D| < \frac{m+1}{2}$, by Proposition 3 we can take complements if necessary to arrange that $|B| + |D| \ge \frac{m+1}{2}$.

By Lemma 4,

$$d_{\phi(0,-)}(w) = \frac{R_{\phi(0,-)}(w) - m}{4} + |B| \quad \text{and} \quad d_{\phi(1,-)}(w) = \frac{R_{\phi(1,-)}(w) - m}{4} + |D|.$$

Put $d(w) = d_{\phi(0,-)}(w) + d_{\phi(1,-)}(w)$. By Corollary 3, f is an OQS if and only if, firstly, for $1 \le w \le m-1$ either

$$d(w) = |B| + |D| - \frac{m+1}{2} \quad \text{or} \quad d(w) = |B| + |D| - \frac{m-1}{2};$$

secondly,

$$R_{\phi(0,-),\phi(1,-)}(w) = R_{\phi(0,-),\phi(1,-)}(m-w), \tag{7}$$

using that $R_{b,a}(w) = R_{a,b}(n-w)$ for binary sequences a, b of length n.

Now define

$$Z_l = \{(j, j+l) \in \mathbb{Z}_m \times \mathbb{Z}_m \mid \phi(0, j) = \phi(1, j+l) = -1\}$$

and, for X, $Y \subseteq \mathbb{Z}_m$,

$$[X \times Y]_w = \{(x, y) \in X \times Y \mid x - y \equiv w \mod m\}.$$

Since $R_{\phi(0,-),\phi(1,-)}(w) = m - 2(|B| + |D| - 2|Z_w|)$, the requirement (7) is equivalent to $|Z_w| = |Z_{m-w}|$. We also verify that $|[B \times D]_w| = |Z_{m-w}|$ and $|[D \times B]_w| = |Z_w|$. Finally, $B - D = D - B$ if and only if $|[B \times D]_w| = |[D \times B]_w|$ for $1 \leq w \leq m - 1$. □

Example 5. The 2-$\{9; 5, 6; 6\}$ ASDS associated to the OQS $(1, -1, -\mathrm{i}, -1, \mathrm{i}, -1, -\mathrm{i}, -1, 1)$ of length 9 are $\{1, 3, 4, 5, 7\}$, $\{1, 2, 3, 5, 6, 7\}$. For both OQS $(1, \mathrm{i}, 1)$ and $(1, -1, 1, 1, 1)$, we must take complements to get the ASDS $\{1\}$, $\{0, 1, 2\} \subseteq \mathbb{Z}_3$ and $\{1\}$, $\{0, 2, 3, 4\} \subseteq \mathbb{Z}_5$.

Remark 5. Table 1 yields 2-$\{m; |B|, |D|; |B| + |D| - \frac{m+1}{2}\}$ ASDS for any prime $m \equiv 1 \mod 4$ or $m = (p^a + 1)/2$, p prime.

Next we state an equivalence between ASDS and quasi-orthogonal cocycles. This result follows from Proposition 2 and Theorems 1 and 3.

Theorem 4. *Let* $\psi = \lambda \prod_{j=2}^{2m-1} \partial_j^{k_j}$ *where* $k_j \in \{0, 1\}$ *and* $\{\lambda, \partial_2, \ldots, \partial_{2m-1}\}$ *is the basis of* $Z^2(G, \langle -1 \rangle)$ *defined in Section* 2.2. *Then* ψ *is quasi-orthogonal if and only if*

$$B = \{j - 1 \mid 2 \leq j \leq m,\ k_j = 1\},\ D = \{j - m - 1 \mid m + 1 \leq j \leq 2m - 1,\ k_j = 1\}$$

are 2-$\{m; |B|, |D|; |B| + |D| - \frac{m+1}{2}\}$ *ASDS such that the multiset* $B - D$ *of differences* $x - y$ *modulo* m *as* (x, y) *ranges over* $B \times D$ *is symmetric.*

Remark 6. Since ψ is normalized, the ASDS in Theorem 4 are 'normalized' too ($0 \notin B$). Also $m - 1 \notin D$ because of the particular basis of $Z^2(G, \langle - \rangle)$ chosen.

Example 6. 1. The ASDS in Example 3 satisfy the stipulations of Theorem 4, so the cocycle $\lambda\partial_2\partial_5\partial_6\partial_7\partial_8\partial_{10}\partial_{12} \in Z^2(\mathbb{Z}_2 \times \mathbb{Z}_9, \langle -1 \rangle)$ is quasi-orthogonal.
2. $B = \{1, 2\}$ and $D = \{0, 2\}$ are 2-$\{7; 2, 2; 0\}$ ASDS, but $B - D \neq D - B$. Hence $\lambda\partial_2\partial_3\partial_8\partial_{10} \in Z^2(\mathbb{Z}_2 \times \mathbb{Z}_7, \langle -1 \rangle)$ is not quasi-orthogonal. Indeed, two rows in the lower half of M_ψ sum to 4.

Remark 7. We define an equivalence relation $\sim$ on the set of GOBA$(2, m)$ by $\phi \sim \phi' \Leftrightarrow$ ϕ and ϕ' have the same first row and their second rows are negations of each other. Equivalence relations such as this carry over to compatible equivalence relations on sets of ASDS and OQS.

We derive bounds on the size of the ASDS in Theorem 4.

Corollary 5. *Suppose that* B *and* D *are* 2-$\{m; k, r; k + r - \frac{m+1}{2}\}$ *ASDS where* m *is odd,* $0 \notin B$, *and* $m - 1 \notin D$. *Then*

$$\frac{(m-1)^2}{2} \leq (k + r)m - (k^2 + r^2) \leq \frac{m^2 - 1}{2}.$$

Proof. There exists $\psi = \prod_{i\in B} \partial_{i+1} \prod_{i\in D} \partial_{i+m+1}$ such that the number of -1s in row j of M_ψ for $2 \le j \le m$ is $m \pm 1$. Alternatively, counting in M_ψ before row normalization reveals that the total number of -1s in these rows is $2k(m-k) + 2r(m-r)$. The inequalities follow by comparing the counts. □

Our ultimate result is an accompaniment to Theorem 2.

Lemma 5. *For any nonempty subsets B, D of $\mathbb{Z}_m$, the multiset $B - D$ is symmetric if and only if B^c and D^c are amicable, i.e., $B^c(D^c)^\top$ is symmetric.*

Proof. Note that $B^c(D^c)^\top$ and $D^c(B^c)^\top$ are circulant. If $u = (u_0, u_1, \ldots, u_{m-1})$ and $v = (v_0, v_1, \ldots, v_{m-1})$ are the first rows of $B^c(D^c)^\top$ and $D^c(B^c)^\top$, then

$$u_0 = v_0,\ u_1 = v_{m-1},\ \ldots,\ u_i = v_{m-i},\ \ldots,\ u_{m-1} = v_1.$$

Consequently $B^c(D^c)^\top = D^c(B^c)^\top$ if and only if

$$u_1 = u_{m-1},\ u_2 = u_{m-2},\ \ldots,\ u_{\frac{m-1}{2}} = u_{\frac{m+1}{2}}.$$

Let $(b_0, b_1, \ldots, b_{m-1})$ and $(d_0, d_1, \ldots, d_{m-1})$ be the respective first rows of B^c and D^c. Then

$$\begin{aligned} u_i &= b_0 d_{[-i]_m} + b_1 d_{[1-i]_m} + \cdots + b_{m-1} d_{[-1-i]_m} \\ u_{m-i} &= d_0 b_{[-i]_m} + d_1 b_{[1-i]_m} + \cdots + d_{m-1} b_{[-1-i]_m}. \end{aligned}$$

We check that $u_i = u_{m-i}$ if and only if the number of summands $b_j d_k$ in u_i with $b_j = d_k = -1$ is equal to the number of summands $b_{j'} d_{k'}$ in u_{m-i} with $b_{j'} = d_{k'} = -1$. Since $j - k \equiv i \equiv k' - j' \mod m$, the proof is complete. □

In conclusion, and with reference to Remark 5 and the existence problem for quasi-orthogonal cocycles, we pose the open problem of constructing new OQS from new ASDS (cf. the construction in [3] of optimal binary sequences from almost difference sets).

Acknowledgments. The first author thanks Kristeen Cheng for reading the manuscript, and Víctor Álvarez for assistance with computations. This research was partially supported by project FQM-016 funded by JJAA (Spain).

References

1. Arasu, K. T. and de Launey, W.: Two-dimensional perfect quaternary arrays. IEEE Trans. Inform. Theory 47 (2001), no. 4, 1482–1493.
2. Arasu, K. T., de Launey, W., and Ma, S. L.: On circulant complex Hadamard matrices, Des. Codes Cryptogr. 25 (2002), no. 2, 123–142.

3. Arasu, K. T., Ding, C., Helleseth, T., Kumar, P. V., and Martinsen, H.: Almost difference sets and their sequences with optimal autocorrelation. IEEE Trans. Inform. Theory 47 (2001), no. 7, 2934–2943.

4. Armario, J. A. and Flannery, D. L.: On quasi-orthogonal cocycles. J. Combin. Des. 26 (2018), no. 8, 401–411.

5. Armario, J. A. and Flannery, D. L.: Generalized binary arrays from quasi-orthogonal cocycles. Des. Codes Cryptogr. 87 (2019), no. 10, 2405–2417.

6. Chadjipantelis, T. and Kounias, S.: Supplementary difference sets and D-optimal designs for $n \equiv 2 \mod 4$. Discrete Math. 57 (1985), no. 3, 211–216.

7. Hughes, G.: Non-splitting abelian $(4t, 2, 4t, 2t)$ relative difference sets and Hadamard cocycles. European J. Combin. 21 (2000), no. 3, 323–331.

8. Jedwab, J.: Generalized perfect arrays and Menon difference sets. Des. Codes Cryptogr. 2 (1992), no. 1, 19–68.

9. Koukouvinos, C., Kounias, S., and Seberry, J.: Supplementary difference sets and optimal designs. Discrete Math. 88 (1991), no. 1, 49–58.

10. Krone, S. M. and Sarwate, D. V.: Quadriphase sequences for spread-spectrum multiple-access communication. IEEE Trans. Inform. Theory, vol. IT-30 (1984), no. 3, 520–529.

11. Lüke, H. D., Schotten, H. D., and Hadinejad-Mahram, H.: Binary and quadriphase sequences with optimal autocorrelation properties: a survey. IEEE Trans. Inform. Theory 49 (2003), no. 12, 3271–3282.

12. Ma, S. L. and Ng, W. S.: On non-existence of perfect and nearly perfect sequences. Int. J. Inf. Coding Theory 1 (2009), no. 1, 15–38.

13. Schmidt, B.: Towards Ryser's conjecture, European Congress of Mathematics, Vol. I (Barcelona, 2000), Progr. Math., 201, 533–541, Birkhäuser, Basel, 2001.

14. Yang, Y. and Tang, X.: Generic construction of binary sequences of period $2N$ with optimal odd correlation magnitude based on quaternary sequences of odd period N. IEEE Trans. Inform. Theory 64 (2018), no. 1, 384–392.