11-2020

Legendre G-array Pairs and the Theoretical Unification of Several G-array Families

K. T. Arasu
Riverside Research

Dursun A. Bulutoglu
Air Force Institute of Technology

J. R. Hollon
Applied Optimization, Inc.

Recommended Citation

Arasu, K. T., Bulutoglu, D. A., & Hollon, J. R. (2020). Legendre G-array pairs and the theoretical unification of several G-array families. Journal of Combinatorial Designs, 28(11), 814–841. https://doi.org/10.1002/jcd.21745

Legendre G-array pairs and the theoretical unification of several G-array families

K. T. Arasu[a], D. A. Bulutoglu[b] and J. R. Hollon[c]
[a]Riverside Research, 2640 Hibiscus Way,
Beavercreek, OH 45431, USA
[b]Air Force Institute of Technology, WPAFB, OH 45433, USA
[c]Applied Optimization Inc., 3040 Presidential Dr. Suite 100
Fairborn, OH 45324, USA

April 14, 2020

Abstract

We investigate how Legendre G-array pairs are related to several different perfect binary G-array families. In particular we study the relations between Legendre G-array pairs, Sidelnikov-Lempel-Cohn-Eastman $\mathbb{Z}_{q-1}$-arrays, Yamada-Pott G-array pairs, Ding-Helleseth-Martinsen $\mathbb{Z}_2 \times \mathbb{Z}_p^m$-arrays, Yamada $\mathbb{Z}_{(q-1)/2}$-arrays, Szekeres $\mathbb{Z}_p^m$-array pairs, Paley $\mathbb{Z}_p^m$-array pairs, and Baumert $\mathbb{Z}_{p_1}^{m_1} \times \mathbb{Z}_{p_2}^{m_2}$-array pairs. Our work also solves one of the two open problems posed in Ding [J. Combin. Des. 16 (2008), 164-171]. Moreover, we provide several computer search based existence and non-existence results regarding Legendre $\mathbb{Z}_n$-array pairs. Finally, by using cyclotomic cosets, we provide a previously unknown Legendre $\mathbb{Z}_{57}$-array pair.

Keywords: Cyclotomy, Group ring, Hadamard matrix, Skew-symmetric, Supplementary difference set

1 Introduction

In this section, we first survey several known infinite binary G-array families and G-array pairs for a finite abelian group G. In Section 2, we show how these G-array families and G-array pairs are related to each other.

1.1 G-arrays and their correlations

Let n be a positive integer and G be an abelian group of order n. Then $\boldsymbol{a} = (a_g)$ with $g \in G$ and $a_g \in \mathbb{C}$ is called a *G-array*. The *cross-correlation function* of the two G-arrays (a_g) and (b_g) is defined by:

$$C_{\boldsymbol{a},\boldsymbol{b}}(t) = \sum_{g \in G} a_{gt} \bar{b}_g,$$

where $t \in G$ and $\bar{b}_g$ is the complex conjugate of b_g. If $\boldsymbol{a} = \boldsymbol{b}$, then $C_{\boldsymbol{a},\boldsymbol{a}}(t) := C_{\boldsymbol{a}}(t)$ is called the *autocorrelation function* of $\boldsymbol{a}$.

We call a G-array $\boldsymbol{a}$ a $\{0,1\}$ ($\{-1,1\}$) G-array if $a_g \in \{0,1\}$ ($\{-1,1\}$) $\forall g \in G$. In this paper, we consider only $\{-1,1\}$ or $\{0,1\}$ G-arrays. The linear transformation $a_g \to 2a_g - 1$ is a bijection that maps a $\{0,1\}$ G-array to a $\{-1,1\}$ G-array. Throughout, we switch repeatedly between a $\{0,1\}$ G-array and its corresponding $\{-1,1\}$ G-array. The choice between $\{0,1\}$ and $\{-1,1\}$ coefficients in any particular context is dictated by applications or ease of computation. If we refer to a $\{0,1\}$ G-array as a $\{-1,1\}$ G-array we mean the $\{-1,1\}$ G-array obtained from the $\{0,1\}$ G-array by applying the bijection $a_g \to 2a_g - 1$.

By the structure theorem, every finite abelian group G is isomorphic to $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$ for some $r \in \mathbb{Z}^{\geq 1}$. Let $H_i = \langle \omega_i \rangle$ and $|H_i| = s_i$ for $s_i \in \mathbb{Z}^{\geq 2}$. Then, the map $\Theta : \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r} \to H_1 \times \cdots \times H_r$ such that $\Theta(\alpha_1, \ldots, \alpha_r) = \omega_1^{\alpha_1} \ldots \omega_r^{\alpha_r}$ is an isomorphism between $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$ and $H_1 \times \cdots \times H_r$ for each set of fixed $\{\omega_i\}_{i=1}^r$. Throughout the paper we fix the notation Θ for this isomorphism.

For a G-array (a_g) and an isomorphism $\Phi : G \to \Phi(G)$, define the $\Phi(G)$-array $\Phi(a_g)$ via

$$\Phi((a_g)) = (a'_{\Phi(g)}), \text{ where } a'_{\Phi(g)} = a_g.$$

Clearly, both the autocorrelation and the cross-correlation functions are preserved under the map $g \to \Phi(g)$ for any isomorphism Φ, i.e. $C_{a,b}(t) = C_{\Phi(a),\Phi(b)}(\Phi(t))$ for any two G-arrays (a_g) and (b_g) where $g, t \in G$. Also, whenever we are using an isomorphic copy of G that has the form $H_1 \times \cdots \times H_r$, we say that G is *written multiplicatively*, and if G has the form $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$ we say that G is *written additively*. Unless otherwise specified, for a multiplicatively (additively) written group we use 1 (0) as the identity element. We also use e as the identity element of a group G.

Let $n = |G|$. Let $\boldsymbol{a} = (a_g)$ be a $\{-1,1\}$ or $\{0,1\}$ G-array. Then the set $D = \{g \mid g \in G \text{ and } a_g = 1\}$ is called the *set of* 1 *indices* of $\boldsymbol{a}$. Let $d_D(t) = |(Dt) \cap D|$, where Dt is the set of elements of D multiplied by t. Then $d_D(t)$ is called the *difference function* of $D \subseteq G$, and for a $\{0,1\}$ G-array $\boldsymbol{a}$ we have

$$C_{\boldsymbol{a}}(t) = d_D(t).$$

Hence, the autocorrelation function measures how much a $\{0,1\}$ G-array differs from its translates. When $\boldsymbol{a} = (a_g)$ is a $\{-1,1\}$ G-array we get

$$C_{\boldsymbol{a}}(t) = n - 4(k - d_D(t)), \tag{1}$$

where $k = |D|$, see [13]. By equation (1) if $\boldsymbol{a} = (a_g)$ is a $\{-1,1\}$ G-array, then

$$C_{\boldsymbol{a}}(t) \equiv n \pmod 4.$$

A $\{-1,1\}$ G-array $\boldsymbol{a}$ is called *perfect* if for $t \neq e$

$$C_{\boldsymbol{a}}(t) = \begin{cases} 0 & \text{if } n \equiv 0 \pmod 4, \\ 1 & \text{if } n \equiv 1 \pmod 4, \\ \pm 2 & \text{if } n \equiv 2 \pmod 4, \\ -1 & \text{otherwise.} \end{cases}$$

A $\{-1,1\}$ G-array $\boldsymbol{a} = (a_g)$ is called *balanced* if

$$\sum_{g \in G} a_g = \begin{cases} 0 & \text{if } n \equiv 0 \pmod 2, \\ \pm 1 & \text{otherwise,} \end{cases}$$

and *almost balanced* if

$$\sum_{g \in G} a_g = \begin{cases} \pm 2 & \text{if } n \equiv 0 \pmod 2, \\ \pm 3 & \text{otherwise.} \end{cases}$$

Then, based on equation (1), a $\{0,1\}$ G-array $\boldsymbol{a}$ with $\sum_{g \in G} a_g = k$ is defined to be *perfect* if for $t \neq e$

$$C_{\boldsymbol{a}}(t) = d_D(t) = \begin{cases} k - \frac{n}{4} & \text{if } n \equiv 0 \pmod 4, \\ k - \frac{n-1}{4} & \text{if } n \equiv 1 \pmod 4, \\ k - \frac{n \pm 2}{4} & \text{if } n \equiv 2 \pmod 4, \\ k - \frac{n+1}{4} & \text{otherwise,} \end{cases} \tag{2}$$

and a $\{0,1\}$ G-array $\boldsymbol{a} = (a_g)$ is defined to be *balanced* if

$$\sum_{g \in G} a_g = \begin{cases} \frac{n}{2} & \text{if } n \equiv 0 \pmod 2, \\ \frac{n \pm 1}{2} & \text{otherwise,} \end{cases} \tag{3}$$

and *almost balanced* if

$$\sum_{g \in G} a_g = \begin{cases} \frac{n \pm 2}{2} & \text{if } n \equiv 0 \pmod 2, \\ \frac{n \pm 3}{2} & \text{otherwise.} \end{cases} \tag{4}$$

A G-array $\boldsymbol{a}$ is said to have *good matched autocorrelation properties* if

$$\max_{t\in G\setminus\{e\}} |C_{\boldsymbol{a}}(t)|,$$

and

$$\sum_{t\in G} |C_{\boldsymbol{a}}(t)|^2$$

are both small, where $\max_{t\in G\setminus\{e\}} |C_{\boldsymbol{a}}(t)|$ is called the *peak correlation* and $\sum_{t\in G} |C_{\boldsymbol{a}}(t)|^2$ is called the *correlation energy*.

Let G be a group of order v and D be a subset of G with k elements. For any $\alpha \neq e$ and $\alpha \in G$ if the equation

$$d(d')^{-1} = \alpha \tag{5}$$

has exactly λ solution pairs (d, d') with both d and d' in D, then the set D is called a *difference set* in G with parameters (v, k, λ) denoted by $\mathrm{DS}(v, k, \lambda)$. If equation (5) has λ solutions for t of the non-identity elements of G and $\lambda+1$ solutions for every other non-identity element, then D is called an *almost difference set* in G with parameters (v, k, λ, t) denoted by $\mathrm{ADS}(v, k, \lambda, t)$. If G is an abelian (cyclic) group and D is a difference set, then D is called an *abelian (cyclic) difference set* in G. If G is an abelian (cyclic) group and D is an almost difference set, then D is called an *abelian (cyclic) almost difference set*.

Clearly, D is a(n) (almost) difference set in G if and only if $\Phi(D)$ is a(n) (almost) difference set in $\Phi(G)$ for any isomorphism $\Phi : G \to \Phi(G)$. For a survey of almost difference sets, see [2].

A $\{-1, 1\}$ $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$-array with k entries equal to 1 and all nontrivial autocorrelation coefficients equal to $\theta = n - 4(k - \lambda)$ is equivalent to an abelian $\mathrm{DS}(n, k, \lambda)$, see Lemma 1.3 in [10].

Supplementary difference sets generalize the concept of difference sets [19].

Definition 1. Let G be a group of order v. A collection $D_1, D_2, \ldots, D_f$ of f subsets of G with $|D_i| = k_i$ is called a *supplementary difference set* in G denoted by f-$\mathrm{SDS}(v; k_1, \ldots, k_f; \lambda)$ if for each $\alpha \in G \setminus \{e\}$, the constraint

$$\alpha = xy^{-1},$$

where $x, y \in D_i$ for some $i \in \{1, 2, \ldots, f\}$, has exactly λ solutions.

Clearly, $D_1, \ldots, D_f$ is a f-$\mathrm{SDS}(v; k_1, \ldots, k_f; \lambda)$ in G if and only if $\Phi(D_1), \ldots, \Phi(D_f)$ is an f-$\mathrm{SDS}(v; k_1, \ldots, k_f; \lambda)$ in $\Phi(G)$ for any isomorphism $\Phi : G \to \Phi(G)$.

1.2 The group ring notation

First, we introduce the group ring notation that will be used in the proofs.

Definition 2. Let G be a multiplicatively written finite abelian group and R be a ring. Then, the *group ring* of G over R is the set denoted by $R[G]$ defined as:

$$R[G] = \left\{ \sum_{g \in G} a_g g \mid a_g \in R \right\}.$$

$R[G]$ is a free R-module of rank $|G|$. Any group isomorphism $\Phi : G \to \Phi(G)$ extends linearly to a module and group ring isomorphism between $R[G]$ and $R[\Phi(G)]$, where

$$\Phi(\sum_{g \in G} a_g g) = \sum_{g \in G} a_g \Phi(g) = \sum_{\Phi(g) \in \Phi(G)} a_{\Phi(g)} \Phi(g).$$

If G is a multiplicatively written group, then multiplication and addition in $R[G]$ are defined in the same way as in the ring of formal Laurent series $R[[x_1, \ldots x_n]]$. If G is additively written, then there exists an isomorphism $\Phi : G \to \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$ for some $s_1, \ldots, s_r$. In this case, addition in $R[G]$ is defined the same way as in the case when G is multiplicatively written. The multiplication of two elements $u, v \in R[G]$ is defined as

$$u * v = (\Theta\Phi)^{-1}(\Theta\Phi(u)\Theta\Phi(v)).$$

For short hand notation, we define the *power* of a group ring element in the following way.

Definition 3. If $W = \sum_{g \in G} a_g g$ is an element of $R[G]$ and t some integer, then

$$W^{(t)} = \sum_{g \in G} a_g g^t, \quad \overline{W} = \sum_{g \in G} \bar{a}_g g, \quad \text{and} \quad |W| = \sum_{g \in G} |a_g|.$$

The following are two remarks concerning Definition 3.

1. For a group ring element A in this paper we always have $\overline{A} = A$.
2. The element $\left(\sum_{g \in G} a_g g\right)^{(t)}$ is not the same as the element $\left(\sum_{g \in G} a_g g\right)^{t}$.

Let $D \subseteq G$ with $|D| = k$ and $A = \sum_{g \in D} g$. Then, D is a DS(v, k, λ) if and only if

$$AA^{(-1)} = (k - \lambda)(1) + \lambda \left(\sum_{g \in G} g \right) \in \mathbb{Z}[G].$$

We can think of a G-array as a matrix. Let $\boldsymbol{M}$ be a matrix whose rows and columns are indexed by the elements in G. Define

$$P = \{g \,|\, m_{1,g} = +1\},$$

and

$$N = \{g \,|\, m_{1,g} = -1\}.$$

Let the G-array $m_{1,g}$ be the first row of $\boldsymbol{M}$. Then, the remaining rows of $\boldsymbol{M}$ can be obtained by setting

$$m_{g,h} = \begin{cases} 1, & \text{if } gh^{-1} \in P, \\ -1, & \text{if } gh^{-1} \in N. \end{cases}$$

A matrix developed this way is called *G-developed* or *G-circulant*.

For a cyclic group G, if the rows and columns of a matrix $\boldsymbol{M}$ are indexed by successive powers of a generator of G, then the G-developed matrix $\boldsymbol{M}$ is called *circulant*. Alternatively, a circulant matrix $\boldsymbol{A} = circ(\boldsymbol{a})$ is determined by its first column, where each column (row) of $\boldsymbol{A}$ is a cyclic down (right) shift of the vector $\boldsymbol{a}$. An $m_1m_2 \times m_1m_2$ matrix $\boldsymbol{C}$ is said to be *block-circulant* if it is of the form

$$\boldsymbol{C} = circ(\boldsymbol{C}_0, \boldsymbol{C}_1, \ldots, \boldsymbol{C}_{m_2-1}) = \begin{bmatrix} \boldsymbol{C}_0 & \boldsymbol{C}_{m_2-1} & \cdots & \boldsymbol{C}_1 \\ \boldsymbol{C}_1 & \boldsymbol{C}_0 & \cdots & \boldsymbol{C}_2 \\ \boldsymbol{C}_2 & \boldsymbol{C}_1 & \cdots & \boldsymbol{C}_3 \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{C}_{m_2-1} & \boldsymbol{C}_{m_2-2} & \cdots & \boldsymbol{C}_0 \end{bmatrix}, \tag{6}$$

where the $\boldsymbol{C}_j$ are $m_1 \times m_1$ matrices. If each $\boldsymbol{C}_i$ in equation (6) is itself also circulant then $\boldsymbol{C}$ is a block-circulant matrix of circulant matrices. More generally, if the group G is abelian but not cyclic then $G \cong \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$ for some $r \geq 2$ and the G-developed matrix is *r-circulant* that is obtained after applying the $circ(.)$ operator r times.

For a permutation Π of indices in $\{1, \ldots, n\}$, let $\boldsymbol{P}_\Pi$ be the corresponding $n \times n$ permutation matrix. Then, the *automorphism group* $\mathrm{Aut}(\boldsymbol{A})$ of an $n \times n$ matrix $\boldsymbol{A}$ is defined to be

$$\mathrm{Aut}(\boldsymbol{A}) = \{\Pi \,|\, \boldsymbol{P}_\Pi \boldsymbol{A} \boldsymbol{P}_\Pi^\top = \boldsymbol{A}\}.$$

For a G-developed matrix $\boldsymbol{A}$, if we permute the indices of $\boldsymbol{A}$ by the action of multiplication by elements of G, then the elements of G can be thought of as a set of permutations matrices that form a subgroup of $\mathrm{Aut}(\boldsymbol{A})$. Hence, $\mathrm{Aut}(\boldsymbol{A}) \geq G$ and it is easy to construct examples where $\mathrm{Aut}(\boldsymbol{A}) > G$. The set of all matrices whose automorphism group contains G and entries are in R is isomorphic to $R[G]$. This follows by taking $X = G$ on page 4 in [9]. In particular, the products and integer linear combinations of circulant (r-circulant) matrices is circulant (r-circulant).

There is an injection Ψ of $\{0,1\}$ or $\{-1,1\}$ G-arrays into $\mathbb{Z}[G]$ given by

$$\Psi(\boldsymbol{a}) = \sum_{g\in G} a_g g.$$

We say that the G-array $\boldsymbol{a}$ *corresponds* to $A \in \mathbb{Z}[G]$ if $A = \sum_{g\in G} a_g g$. For a group ring element $\sum_{g\in G} a_g g$ corresponding to a G-array (a_g) and an isomorphism $\Phi : G \to \Phi(G)$ we define $\Phi(A)$ to be

$$\Phi(A) = \sum_{g\in G} a_g \Phi(g) = \sum_{\Phi(g)\in\Phi(G)} a_g \Phi(g).$$

Throughout the paper, by abuse of notation, if a set $H \subseteq G$ appears in a group ring equation, it is understood that $H = \sum_{h\in H} h$. Moreover, for $A = \sum_{g\in G} a_g g \in \mathbb{Z}[G]$, we define

$$\{A\} := \{g \in G \mid a_g = 1\}.$$

The group ring elements that correspond to G-arrays are used to calculate the autocorrelation and cross-correlation functions of G-arrays, i.e., for a multiplicatively written group G, and G-arrays $\boldsymbol{a}$ and $\boldsymbol{b}$

$$C_{\boldsymbol{a},\boldsymbol{b}}(t) = \text{coefficient of } t \text{ in } A\overline{B}^{(-1)}, \tag{7}$$

where $A = \sum_{g\in G} a_g g$, $B = \sum_{g\in G} b_g g$.

A matrix $\boldsymbol{M}$ with entries in $\mathbb{R}$ is *symmetric (skew-symmetric)* if $\boldsymbol{M} = \boldsymbol{M}^\top$ ($\boldsymbol{M} = -\boldsymbol{M}^\top$). Next, we define symmetric, skew-symmetric G-arrays, and skew-type matrices.

Definition 4. Let G be a finite group with identity e. Let $\boldsymbol{m} = (m_g)$ be a $\{0,1\}$ G-array and $M = \sum_{g\in G} m_g g$. Then, $\boldsymbol{m}$ or M is *symmetric* if $M = M^{(-1)}$ and *skew-symmetric* if $M + M^{(-1)} = G + e$ (implying $e \in \{M\}$) or $M + M^{(-1)} = G - e$ (implying $e \notin \{M\}$).

The following lemma shows that an isomorphism $\Phi : G \to \Phi(G)$ maps a symmetric (skew-symmetric) G-array to a symmetric (skew-symmetric) $\Phi(G)$-array.

Lemma 1. Let (a_g) be a symmetric (skew-symmetric) G-array. Let Φ be an isomorphism $\Phi : G \to \Phi(G)$. Then $\Phi((a_g))$ is a symmetric (skew-symmetric) G-array.

Proof. Let $A = \sum_{g\in G} a_g g \in \mathbb{Z}[G]$ and Φ be extended linearly to an isomorphism of $R[G]$ and $R[\Phi(G)]$. Then, $A = A^{(-1)}$ implies $\Phi(A) = \Phi(A^{(-1)})$ ($M + M^{(-1)} = G + e$ implies $\Phi(M) + \Phi(M^{(-1)}) = \Phi(G) + \Phi(e)$ and $M + M^{(-1)} = G - e$ implies $\Phi(M) + \Phi(M^{(-1)}) = \Phi(G) - \Phi(e)$). □

The following lemma follows immediately from Definition 4.

Lemma 2. Let G be a finite group with identity e and M be the group ring element corresponding to $\boldsymbol{m}$. Then, a $\{0,1\}$ G-array $\boldsymbol{m}$ is symmetric (skew-symmetric) if and only if $\{M\} = \{M^{(-1)}\}$ ($\{M\} \cup \{M^{(-1)}\} = G\backslash e$, $\{M\} \cap \{M^{(-1)}\} = \emptyset$ when $e \notin \{M\}$ and $\{M\} \cup \{M^{(-1)}\} = G$, $\{M\} \cap \{M^{(-1)}\} = e$ when $e \in \{M\}$).

A matrix $\boldsymbol{M}$ is of *skew-type* if $\mathrm{Diag}(\boldsymbol{M}) = \boldsymbol{I}$ and $(\boldsymbol{M} - \mathrm{Diag}(\boldsymbol{M}))$ is skew-symmetric, where $\mathrm{Diag}(\boldsymbol{M})$ is the diagonal matrix obtained from $\boldsymbol{M}$ by replacing each non-diagonal entry of $\boldsymbol{M}$ with 0. Now, it is plain to see the following lemma.

Lemma 3. Let $\boldsymbol{m} = (m_g)$ be a $\{0,1\}$ G-array with $m_e = 1$. Let $\boldsymbol{M}$ be the group developed matrix obtained by using $m_{e,g} = m_g$ as its first row and $\boldsymbol{J}_{|G|\times|G|}$ be the $|G| \times |G|$ matrix of all 1s. Then $2\boldsymbol{M} - \boldsymbol{J}_{|G|\times|G|}$ is symmetric (skew-type) if and only if $M = \sum_{g\in G} m_g g$ is symmetric (skew-symmetric).

1.3 Legendre G-array pairs

First, we define Legendre G-array pairs.

Definition 5. Let G be a multiplicatively written finite abelian group with $|G| = n$. Then, a pair of $\{-1,1\}$ G-arrays $(\boldsymbol{a} = (a_g), \boldsymbol{b} = (b_g))$ form a *Legendre G-array pair* if $\sum_{g\in G} a_g = \sum_{g\in G} b_g$ and

$$AA^{(-1)} + BB^{(-1)} = (|A| + |B|)\,(1) - 2(G-1), \tag{8}$$

where A and B are the group ring elements associated with $\boldsymbol{a}$ and $\boldsymbol{b}$.

By applying the principal character to the group ring equation (8) we get

$$\begin{aligned} \chi_0\left(AA^{(-1)} + BB^{(-1)}\right) &= \chi_0\left((|A| + |B|)(1) - 2(G-1)\right) \\ \chi_0(A)^2 + \chi_0(B)^2 &= 2n - 2(n-1) \\ a^2 + b^2 &= 2. \end{aligned} \tag{9}$$

This equation implies that $a = b \in \{-1, 1\}$, where $a = \sum_{g\in G} a_g = b = \sum_{g\in G} b_g$. Thus $|G| = n$ must be odd for a Legendre G-array pair to exist. Hence, each G-array in a Legendre G-array pair must be balanced.

By equations (1), (8), and (9) we get the following definition of Legendre $\{0,1\}$ G-array pairs.

Definition 6. Let G be a multiplicatively written finite abelian group. A pair of $\{0,1\}$ G-arrays $(\boldsymbol{a} = (a_g), \boldsymbol{b} = (b_g))$ form a *Legendre G-array pair* if $\sum_{g\in G} a_g = \sum_{g\in G} b_g$, and

$$AA^{(-1)} + BB^{(-1)} = \begin{cases} 2\left(\frac{|G|+1}{2}\right)(1) + \frac{|G|+1}{2}(G-1) & \text{if } \sum_{g\in G} a_g = \sum_{g\in G} b_g = \frac{|G|+1}{2}, \\ 2\left(\frac{|G|-1}{2}\right)(1) + \frac{|G|-3}{2}(G-1) & \text{if } \sum_{g\in G} a_g = \sum_{g\in G} b_g = \frac{|G|-1}{2}. \end{cases}$$

The following lemma is plain to prove.

Lemma 4. Let $\Phi : G \to \Phi(G)$ be an isomorphism. Then, $((a_g), (b_g))$ is a Legendre $\{-1, 1\}$ ($\{0, 1\}$) G-array pair if and only if $(\Phi((a_g)), \Phi((b_g)))$ is a Legendre $\{-1, 1\}$ ($\{0, 1\}$) $\Phi(G)$-array pair. Hence, whenever we construct a Legendre $\{-1, 1\}$ ($\{0, 1\}$) G-array pair we have also constructed a Legendre $\{-1, 1\}$ ($\{0, 1\}$) $\Phi(G)$-array pair.

The following well-known theorem connects supplementary difference sets in finite abelian groups and Legendre G-array pairs.

Theorem 1. Let G be an abelian group of order n. Let $(\boldsymbol{a}, \boldsymbol{b})$ be a $\{0, 1\}$ or $\{-1, 1\}$ G-array pair and (M, N) be the subsets of G such that $M = \{g \in G \mid a_g = 1\}$ and $N = \{g \in G \mid b_g = 1\}$. Then, (M, N) is a 2-SDS$(n; (n + 1)/2, (n + 1)/2; (n + 1)/2)$ or a 2-SDS$(n; (n - 1)/2, (n - 1)/2; (n - 3)/2)$ if and only if $(\boldsymbol{a}, \boldsymbol{b})$ is a Legendre G-array pair.

Proof. If G is written multiplicatively, then the result follows by comparing Definition 1 for $f = 2$ to Definition 5 (Definition 6) for $\{-1, 1\}$ ($\{0, 1\}$) G-arrays. □

It is conjectured that a Legendre $\mathbb{Z}_n$-array pair exists for all odd n [8]. A Legendre $\mathbb{Z}_n$-array pair is known to exist when:

- n is a prime, see [8];
- $2n + 1$ is a prime power (Szekeres, [20]);
- $n = 2^m - 1$ for $m \geq 2$, see [15];
- $n = p_1(p_1 + 2)$, with $p_2 = p_1 + 2$, where p_1, p_2 are odd primes [4].

Currently, $n = 77$ is the smallest n for which no Legendre $\mathbb{Z}_n$-array pair is known.

An $N \times N$ *Hadamard matrix*, $\boldsymbol{H}$, is a ± 1 matrix such that $\boldsymbol{H}\boldsymbol{H}^\top = N\boldsymbol{I}_N$ where $\boldsymbol{I}_N$ is the identity matrix of order N. The following theorem showing that the existence of a Legendre G-array pair implies the existence of a $(2|G| + 2) \times (2|G| + 2)$ Hadamard matrix is well-known.

Theorem 2. Let $(\boldsymbol{a}, \boldsymbol{b})$ be a Legendre $\{-1, 1\}$ G-array pair, with $|G| = n$ such that $\sum_{g \in G} a_g = \sum_{g \in G} b_g = 1$. Let $(\boldsymbol{a}, \boldsymbol{b})$ be developed into G indexed $n \times n$ matrices $\boldsymbol{A}$ and

$\boldsymbol{B}$ by taking $\boldsymbol{a}$ and $\boldsymbol{b}$ as the first row of $\boldsymbol{A}$ and $\boldsymbol{B}$ respectively. Let

$$\boldsymbol{H}_{sym} = \begin{bmatrix} - & - & + & \cdots & + & + & \cdots & + \\ - & + & + & \cdots & + & - & \cdots & - \\ + & + & & & & & & \\ \vdots & \vdots & & \boldsymbol{A} & & & \boldsymbol{B} & \\ + & + & & & & & & \\ + & - & & & & & & \\ \vdots & \vdots & & \boldsymbol{B}^\top & & & -\boldsymbol{A}^\top & \\ + & - & & & & & & \end{bmatrix}$$

and

$$\boldsymbol{H}_{skew} = \begin{bmatrix} + & + & + & \cdots & + & + & \cdots & + \\ - & + & + & \cdots & + & - & \cdots & - \\ - & - & & & & & & \\ \vdots & \vdots & & \boldsymbol{A} & & & \boldsymbol{B} & \\ - & - & & & & & & \\ - & + & & & & & & \\ \vdots & \vdots & & -\boldsymbol{B}^\top & & & \boldsymbol{A}^\top & \\ - & + & & & & & & \end{bmatrix}.$$

Then, both $\boldsymbol{H}_{sym}$ and $\boldsymbol{H}_{skew}$ are Hadamard matrices. Moreover, $\boldsymbol{H}_{sym}$ ($\boldsymbol{H}_{skew}$) is symmetric (skew-type) Hadamard matrix if and only if $\boldsymbol{a}$ is symmetric (skew-symmetric).

Proof. Let e be the identity element in G. The matrix $\boldsymbol{H}_{sym}$ ($\boldsymbol{H}_{skew}$) is a Hadamard matrix if and only if $C_{\boldsymbol{a}}(t)+C_{\boldsymbol{b}}(t) = -2$ for all $t \in G\setminus\{e\}$. Then, by using equation (7) for $C_{\boldsymbol{a},\boldsymbol{a}}$ and $C_{\boldsymbol{b},\boldsymbol{b}}$, we get $C_{\boldsymbol{a}}(t)+C_{\boldsymbol{b}}(t) = -2$ for all $t \in G\setminus\{e\}$ if and only if $(\boldsymbol{a},\boldsymbol{b})$ is a Legendre G-array pair. The matrix $\boldsymbol{H}_{sym}$ ($\boldsymbol{H}_{skew}$) is symmetric (skew-type) if and only if $\boldsymbol{A}$ is symmetric (skew-type). The result now follows as $\boldsymbol{A}$ is symmetric (skew-type) if and only if $\boldsymbol{a}$ is symmetric (skew-symmetric). □

Consider the action of the group $(\mathbb{Z}_{s_1}\rtimes\mathbb{Z}^*_{s_1})\times\cdots\times(\mathbb{Z}_{s_r}\rtimes\mathbb{Z}^*_{s_r})$ on the group $\mathbb{Z}_{s_1}\times\cdots\times\mathbb{Z}_{s_r}$ defined by

$$((a_1,b_1),\ldots,(a_r,b_r))(g_1,\ldots,g_r) = (b_1g_1+a_1,\ldots,b_rg_r+a_r)$$

if the group $\mathbb{Z}_{s_1}\times\cdots\times\mathbb{Z}_{s_r}$ is written additively, and

$$((a_1,b_1),\ldots,(a_r,b_r))(g_1,\ldots,g_r) = (g_1^{b_1}a_1,\ldots,g_r^{b_r}a_r)$$

if $\mathbb{Z}_{s_1}\times\cdots\times\mathbb{Z}_{s_r}$ is written multiplicatively, where $\mathbb{Z}^*_{s_i}$ is the multiplicative group of the ring $\mathbb{Z}_{s_i}$ and $\rtimes$ is the *semidirect product* as defined in [14, p. 167]. This group action can be extended linearly to $\mathbb{Z}[G]$. Then, $(\mathbb{Z}_{s_1} \rtimes \mathbb{Z}_{s_1}^*) \times \cdots \times (\mathbb{Z}_{s_r} \rtimes \mathbb{Z}_{s_r}^*)$ acts on a $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$-array, and two $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$-arrays are called *equivalent* if one can be obtained from the other by applying the elements of the group

$$(\mathbb{Z}_{s_1} \rtimes \mathbb{Z}_{s_1}^*) \times \cdots \times (\mathbb{Z}_{s_r} \rtimes \mathbb{Z}_{s_r}^*).$$

It is well-known that if $\boldsymbol{a}$ and $\boldsymbol{a}'$ are equivalent $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$-arrays then $\boldsymbol{a}$ and $\boldsymbol{a}'$ have the same peak correlation and the same correlation energy. We call two Legendre pairs $(\boldsymbol{a}, \boldsymbol{b})$ and $(\boldsymbol{a}', \boldsymbol{b}')$ *equivalent* if $\{\boldsymbol{a}, \boldsymbol{b}\} = \{\tau \boldsymbol{a}', \beta \boldsymbol{b}'\}$, where $\tau = ((\tau_1, \tau_1^*), \ldots, (\tau_r, \tau_r^*))$, $\beta = ((\beta_1, \beta_1^*), \ldots, (\beta_r, \beta_r^*))$ such that $\beta_i, \tau_i \in \mathbb{Z}_{s_i}$, $\beta_i^*, \tau_i^* \in \mathbb{Z}_{s_i}^*$ and $\tau_i^* = \pm \beta_i^*$ for $i = 1, \ldots, r$ [8]. If $(\boldsymbol{a}, \boldsymbol{b})$ is a Legendre $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$-array pair, and $(\boldsymbol{a}', \boldsymbol{b}')$ is equivalent to $(\boldsymbol{a}, \boldsymbol{b})$, then $(\boldsymbol{a}', \boldsymbol{b}')$ is also a Legendre $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$-array pair.

The following lemma determines exactly which subgroup of $(\mathbb{Z}_{s_1} \rtimes \mathbb{Z}_{s_1}^*) \times \cdots \times (\mathbb{Z}_{s_r} \rtimes \mathbb{Z}_{s_r}^*)$ preserves symmetry (skew-symmetry) of a symmetric (skew-symmetric) $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$-array.

Lemma 5. The group $(\{0\} \rtimes \mathbb{Z}_{s_1}^*) \times \cdots \times (\{0\} \rtimes \mathbb{Z}_{s_r}^*)$ preserves the symmetry (skew-symmetry) of a symmetric (skew-symmetric) $\{-1, 1\}$ or $\{0, 1\}$ $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$-array.

Proof. Let $\boldsymbol{a}$ be a symmetric (skew-symmetric) $\{-1, 1\}$ or $\{0, 1\}$ $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$-array, and $A \subset \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$ be the set of 1 indices of $\boldsymbol{a}$. Then, $A = -A$ (($A \cup -A = \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r} \setminus \{0\}$ and $A \cap -A = \emptyset$) or ($A \cup -A = \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r}$ and $A \cap -A = 0$)) implies for any $((0, \beta_1^*), \ldots, (0, \beta_r^*)) \in (\{0\} \rtimes \mathbb{Z}_{s_1}^*) \times \cdots \times (\{0\} \rtimes \mathbb{Z}_{s_r}^*)$

$$((0, \beta_1^*), \ldots, (0, \beta_r^*))A = -((0, \beta_1^*), \ldots, (0, \beta_r^*))A$$

$$\begin{aligned} (((0, \beta_1^*), \ldots, (0, \beta_r^*))A \cap -((0, \beta_1^*), \ldots, (0, \beta_r^*))A &= \emptyset \quad \text{or} \\ ((0, \beta_1^*), \ldots, (0, \beta_r^*))A \cap -((0, \beta_1^*), \ldots, (0, \beta_r^*))A &= 0). \end{aligned}$$

□

In general, Lemma 5 can not be improved as it is easy to construct a symmetric (skew-symmetric) $\mathbb{Z}_s$-array whose symmetry (skew-symmetry) is not preserved by any circulant shifts other than the 0 shift.

We fix some notation that will be used in the rest of the paper. Let $q = p^m$ for some prime p and positive integer m. Let $\mathbb{F}_q$ be the finite field with q elements and $\mathbb{F}_q^* = \langle \alpha \rangle$ be the multiplicative group of $\mathbb{F}_q$, where α is a generator for $\mathbb{F}_q^*$. Let $C_0^{(d,q,\alpha)} = \langle \alpha^d \rangle$ be the multiplicative group generated by α^d in the finite field $\mathbb{F}_q$, where d divides $q-1$. Observe that $C_0^{(d,q,\alpha)}$ does not depend on α. Let $C_i^{(d,q,\alpha)} = \alpha^i C_0^{(d,q,\alpha)}$ for $i = 0, 1, \ldots, d-1$, where $C_i^{(d,q,\alpha)}$ are called *cyclotomic classes of order* d, see [17]. We will denote $C_i^{(d,q,\alpha)}$ with C_i^d when there is no need to specify q and α. The labeling of $C_1^{(d,q,\alpha)}, \ldots, C_{d-1}^{(d,q,\alpha)}$ depends on α, but taking a different choice of primitive root just permutes $C_1^{(d,q,\alpha)}, \ldots, C_{d-1}^{(d,q,\alpha)}$.

1.4 Infinite families of perfect G-arrays

First, we survey several known infinite families of perfect G-arrays.
The Sidelnikov-Lempel-Cohn-Eastman $\mathbb{Z}_{q-1}$-arrays:
Let

$$S = \{\alpha^{2i+1} - 1\}_{i=0}^{\frac{q-1}{2}-1}.$$

Let $\boldsymbol{a}$ be a $\{-1,1\}$ or $\{0,1\}$ $(q-1) \times 1$ vector such that

$$a_i = 1 \quad \text{if } \alpha^i \in S.$$

Then, $\boldsymbol{a}$ is the Sidelnikov-Lempel-Cohn-Eastman $\mathbb{Z}_{q-1}$-array. The Sidelnikov-Lempel-Cohn-Eastman $\mathbb{Z}_{q-1}$-array is always balanced. However, it is perfect if and only if $q = p^m \equiv 3 \pmod 4$, see [12] and [16].
The Ding-Helleseth-Martinsen $\mathbb{Z}_2 \times \mathbb{Z}_p^m$-arrays:
Let $p \equiv 1 \pmod 4$ and $p^m = s^2 + 4t^2$, where $s^2 = 1$ or $t^2 = 1$. Let $q = p^m \equiv 5 \pmod 8$, or equivalently, let $p \equiv 5 \pmod 8$ and m be odd. Let $C_{i,j,\ell} = \left(C_i^4 \cup C_j^4, C_j^4 \cup C_\ell^4\right)$ for $\{i,j,l\} \subset \{0,1,2,3\}$, where i,j,l are distinct integers. Let

$$(A_1,B_1) = (C_0^4 \cup C_1^4, C_1^4 \cup C_3^4), \;\; (A_2,B_2) = (C_0^4 \cup C_2^4, C_2^4 \cup C_3^4) \quad \text{if } t^2 = 1,$$
$$(A_3,B_3) = (C_0^4 \cup C_1^4, C_0^4 \cup C_3^4) \quad \text{if } s^2 = 1.$$

Identify the elements of the finite field $\mathbb{F}_{p^m}$ with its additive group $\mathbb{Z}_p^m$, and let $\langle\omega\rangle = \Theta(\mathbb{Z}_2)$, where Θ be the isomorphism in Section 1.1. We now use the group $\Theta(\mathbb{Z}_2 \times \mathbb{Z}_p^m)$ as an indexing set. For each $i \in \{1,2,3\}$, let the equivalence class i Ding-Helleseth-Martinsen $\{-1,1\}$ or $\{0,1\}$ $\Theta(\mathbb{Z}_2 \times \mathbb{Z}_p^m)$-array be such that $\Theta(A_i) \cup \Theta(B_i)\omega$ is the set of 1 indices of the array. Then, each equivalence class of Ding-Helleseth-Martinsen $\Theta(\mathbb{Z}_2 \times \mathbb{Z}_p^m)$-array is almost balanced, and equivalence class 3 is always perfect, see Theorem 2 in [7]. In Section 2.2 we determine exactly when each of the equivalence class 1 and 2 Ding-Helleseth-Martinsen $\Theta(\mathbb{Z}_2 \times \mathbb{Z}_p^m)$-array is perfect. This solves one of the two open problems posed in [6]. Finally, each equivalence class of $\{-1,1\}$ or $\{0,1\}$ Ding-Helleseth-Martinsen $\Theta(\mathbb{Z}_2 \times \mathbb{Z}_p^m)$-array (a_g) is used to construct the corresponding $\{-1,1\}$ or $\{0,1\}$ Ding-Helleseth-Martinsen $\mathbb{Z}_2 \times \mathbb{Z}_p^m$-array as $\Theta^{-1}((a_g))$.

1.5 Infinite families of Legendre G-array pairs

Now, we survey several known infinite families of Legendre G-array pairs.
The Yamada $\mathbb{Z}_{(q-1)/2}$-array pairs:
Let $q = p^m \equiv 3 \pmod 4$. Let

$$M = \{a : \alpha^{2a} + 1 \in C_0^2\},$$

and

$$N = \{a : \alpha^{2a} - 1 \in C_0^2\}.$$

Then the pair (M, N) is a 2-SDS$((q-1)/2; (q-3)/4, (q-3)/4; (q-7)/4)$ in $\mathbb{Z}_{(q-1)/2}$. Let $\mathbb{Z}_{(q-1)/2}$ index the arrays $\boldsymbol{a}, \boldsymbol{b}$, and (M, N) be the sets of 1 indices of $(\boldsymbol{a}, \boldsymbol{b})$. Then the $\{-1, 1\}$ or $\{0, 1\}$ $\mathbb{Z}_{(q-1)/2}$-array pair $(\boldsymbol{a}, \boldsymbol{b})$ is called a *Yamada* $\mathbb{Z}_{(q-1)/2}$*-array pair*, see [22]. The $\mathbb{Z}_{(q-1)/2}$-array $\boldsymbol{a}$ is symmetric and $\boldsymbol{b}$ is skew-symmetric.

The Szekeres $\mathbb{Z}_p^m$-array pairs:
Let $q = p^m \equiv 5 \pmod 8$, or equivalently, let $p \equiv 5 \pmod 8$ and m be odd. Let

$$A = C_0^4 \cup C_1^4, \ B = C_0^4 \cup C_3^4.$$

Then the pair (A, B) is a 2-SDS$(p^m; (q-1)/2, (q-1)/2; (q-3)/2)$ in $\mathbb{Z}_p^m$. Let $\mathbb{Z}_p^m$ index the arrays $\boldsymbol{a}, \boldsymbol{b}$, and (A, B) be the sets of 1 indices of $(\boldsymbol{a}, \boldsymbol{b})$. Then the $\{-1, 1\}$ or $\{0, 1\}$ $\mathbb{Z}_p^m$-array pair $(\boldsymbol{a}, \boldsymbol{b})$ is called a *Szekeres* $\mathbb{Z}_p^m$*-array pair*, see [18]. Both $\boldsymbol{a}$ and $\boldsymbol{b}$ are skew-symmetric.

The Szekeres-Whiteman $\mathbb{Z}_p^m$-array pairs:
Let $q = p^m$, $p \equiv 5 \pmod 8$ and m be even with $m \geq 2$. Let

$$A = C_0^8 \cup C_1^8 \cup C_2^8 \cup C_3^8, \ B = C_0^8 \cup C_1^8 \cup C_6^8 \cup C_7^8.$$

Then the pair (A, B) is a 2-SDS$(p^m; (q-1)/2, (q-1)/2; (q-3)/2)$ in $\mathbb{Z}_p^m$. Let $\mathbb{Z}_p^m$ index the arrays $\boldsymbol{a}, \boldsymbol{b}$, and (A, B) be the sets of 1 indices of $(\boldsymbol{a}, \boldsymbol{b})$. Then the $\{-1, 1\}$ or $\{0, 1\}$ $\mathbb{Z}_p^m$-array pair $(\boldsymbol{a}, \boldsymbol{b})$ is called a *Szekeres-Whiteman* $\mathbb{Z}_p^m$*-array pair*. Szekeres [18] proved that a Szekeres-Whiteman $\mathbb{Z}_p^m$-array pair is a Legendre $\mathbb{Z}_p^m$-array pair, while Whiteman [21] independently showed this result however only for $m \equiv 2 \pmod 4$. It is easy to see that both $\boldsymbol{a}$ and $\boldsymbol{b}$ are skew-symmetric.

The Paley $\mathbb{Z}_p^m$-array pairs:
Let

$$\begin{aligned} A = C_0^2, \ B = C_0^2 \quad & \text{if } p^m \equiv 3 \pmod 4, \\ A = C_1^2, \ B = C_0^2 \quad & \text{if } p^m \equiv 1 \pmod 4. \end{aligned}$$

Then the pair (A, B) is a 2-SDS$(p^m; (q-1)/2, (q-1)/2; (q-3)/2)$ in $\mathbb{Z}_p^m$, see [8]. Let $\mathbb{Z}_p^m$ index the arrays $\boldsymbol{a}, \boldsymbol{b}$, and (A, B) be the sets of 1 indices of $(\boldsymbol{a}, \boldsymbol{b})$. Then the $\{-1, 1\}$ or $\{0, 1\}$ $\mathbb{Z}_p^m$-array pair $(\boldsymbol{a}, \boldsymbol{b})$ is called a *Paley* $\mathbb{Z}_p^m$*-array pair*. Both $\boldsymbol{a}$ and $\boldsymbol{b}$ are skew-symmetric if $p^m \equiv 3 \pmod 4$ and symmetric otherwise.

The Baumert $\mathbb{Z}_{p_1}^{m_1} \times \mathbb{Z}_{p_2}^{m_2}$-array pairs:
Let $p_1^{m_1} + 2 = p_2^{m_2}$, where p_1, p_2 are odd primes and m_1, m_2 are positive integers. Let $q_1 = p_1^{m_1}$, $q_2 = p_2^{m_2}$, and

$$A = \left(C_0^{(2,q_1)} \times C_0^{(2,q_2)}\right) \bigcup \left(C_1^{(2,q_1)} \times C_1^{(2,q_2)}\right) \bigcup \left(\mathbb{F}_{q_1} \times \{0\}\right), \ \ B = A.$$

Since A is a DS$(q_1(q_1+2),(q_1^2+2q_1-1)/2,(q_1-1)(q_1+3)/4)$ in $\mathbb{Z}_{p_1}^{m_1}\times\mathbb{Z}_{p_2}^{m_2}$ [4], the pair (A,B) is a 2-SDS$(p_1^{m_1}p_2^{m_2};(q_1^2+2q_1-1)/2,(q_1^2+2q_1-1)/2;(q_1-1)(q_1+3)/2)$ in $\mathbb{Z}_{p_1}^{m_1}\times\mathbb{Z}_{p_2}^{m_2}$. Let $\mathbb{Z}_{p_1}^{m_1}\times\mathbb{Z}_{p_2}^{m_2}$ index the arrays $\boldsymbol{a},\boldsymbol{b}$, and (A,B) be the sets of 1 indices of $(\boldsymbol{a},\boldsymbol{b})$. Then the $\{-1,1\}$ or $\{0,1\}$ $\mathbb{Z}_{p_1}^{m_1}\times\mathbb{Z}_{p_2}^{m_2}$- array pair $(\boldsymbol{a},\boldsymbol{b})$ is called a *Baumert* $\mathbb{Z}_{p_1}^{m_1}\times\mathbb{Z}_{p_2}^{m_2}$*-array pair.* Both $\boldsymbol{a}$ and $\boldsymbol{b}$ are neither symmetric nor skew-symmetric.

2 Results

2.1 Yamada-Pott G-array pairs

Yamada-Pott G-array pairs first appeared in [22] and later in [13]. A Yamada-Pott $\{0,1\}$ G-array pair is a Legendre $\{0,1\}$ G-array pair with the added properties that one G-array is symmetric and the other is skew-symmetric. In group ring notation we have the following definition.

Definition 7. Let G be a finite abelian group written multiplicatively. A Legendre $\{0,1\}$ G-array pair $(\boldsymbol{a},\boldsymbol{b})$ with $A=\sum_{g\in G}a_g g$ and $B=\sum_{g\in G}b_g g$ is a *Yamada-Pott* $\{0,1\}$ *G-array pair* if $|A|=|B|$ and:

1. $A=A^{(-1)}$;
2. $B+B^{(-1)}=G+1$ (implying $1\in\{B\}$) or $B+B^{(-1)}=G-1$ (implying $1\notin\{B\}$)

are satisfied.

The following lemma is plain to prove.

Lemma 6. Let $\Phi:G\to\Phi(G)$ be an isomorphism. Then, $((a_g),(b_g))$ is a Yamada-Pott $\{0,1\}$ G-array pair if and only if $(\Phi((a_g)),\Phi((b_g)))$ is a Yamada-Pott $\{0,1\}$ $\Phi(G)$-array pair.

By Lemma 6, whenever we construct a Yamada-Pott $\{0,1\}$ G-array pair, we have also constructed a Yamada-Pott $\{0,1\}$ $\Phi(G)$-array pair. The following theorem implies that the existence of a Yamada-Pott $\{0,1\}$ $\mathbb{Z}_u$-array pair implies the existence of a perfect $\{0,1\}$ $\mathbb{Z}_{2u}$-array.

Theorem 3. Let H be an abelian group with $|H|=u$ written multiplicatively and (A,B) be a Yamada-Pott $\{0,1\}$ H-array pair. Let $S=A+\omega B$ and $G=\langle\omega\rangle H$, where $\omega^2=1,\omega\neq1$, and $\omega h=h\omega$ for all $h\in H$. Then, $1\in\{B\}$ implies $\{S\}$ is an ADS$(2u,u+1,(u+1)/2,(u+3)/2)$, and $1\notin\{B\}$ implies $\{S\}$ is an ADS$(2u,u-1,(u-1)/2,(u-3)/2)$ in G. In either case, $\boldsymbol{s}$ is an almost balanced perfect $\{0,1\}$ G-array with $G\cong\mathbb{Z}_2\times\Theta(H)\cong\mathbb{Z}_2\times H$, where $\boldsymbol{s}$ is the G-array that corresponds to the group ring element S.

Proof. Since $|S| = u \pm 1$ then $\boldsymbol{s}$ is almost balanced, and by the definition of a Yamada-Pott $\{0,1\}$ H-array pair

$$\begin{aligned} AA^{(-1)} + BB^{(-1)} &= (u \pm 1)(1) + \lambda(H-1) \\ A &= A^{(-1)} \\ B + B^{(-1)} &= H \pm 1, \end{aligned}$$

where

$$\lambda = \begin{cases} \frac{u+1}{2} & \text{if } |A| = |B| = \frac{u+1}{2}, \\ \frac{u-3}{2} & \text{if } |A| = |B| = \frac{u-1}{2}. \end{cases}$$

Now,

$$\begin{aligned} \sum_{t \in G} C_{\boldsymbol{s}}(t)t = SS^{(-1)} &= \ (A + \omega B)\,(A + \omega B)^{(-1)} \\ &= \ (A + \omega B)\left(A^{(-1)} + \omega B^{(-1)}\right) \\ &= AA^{(-1)} + BB^{(-1)} + \omega\left(AB^{(-1)} + BA^{(-1)}\right) \\ &= (u \pm 1)(1) + \lambda(H-1) + \omega\left(AB^{(-1)} + BA^{(-1)}\right) \\ &= (u \pm 1)(1) + \lambda(H-1) + \omega\left(AB^{(-1)} + BA\right) \\ &= (u \pm 1)(1) + \lambda(H-1) + \omega A\left(B^{(-1)} + B\right) \\ &= (u \pm 1)(1) + \lambda(H-1) + \omega A\,(H \pm 1) \\ &= (u \pm 1)(1) + \lambda(H-1) + \omega\,(|A|H \pm A) \\ &= (u \pm 1)(1) + \lambda(H-1) + \omega\left(\left(\frac{u \pm 1}{2}\right)H \pm A\right) \\ &= \begin{cases} \frac{u+1}{2}(1) + \lambda G + A\omega & \text{if } |A| = |B| = \frac{u+1}{2}, \\ \frac{u+1}{2}(1) + \lambda G + (H - A)\omega & \text{if } |A| = |B| = \frac{u-1}{2}, \end{cases} \end{aligned}$$

where we used the group ring equation $G = H + H\omega$. This shows that for $t \neq 1$ the autocorrelation function of $\boldsymbol{s}$ has the following form

$$C_{\boldsymbol{s}}(t) = \begin{cases} \frac{u+1}{2} \text{ or } \frac{u+1}{2} + 1 & \text{if } |A| = |B| = \frac{u+1}{2}, \\ \frac{u-3}{2} \text{ or } \frac{u-3}{2} + 1 & \text{if } |A| = |B| = \frac{u-1}{2}. \end{cases} \tag{10}$$

Thus, by equations (2), (4), and (10), $\boldsymbol{s}$ is an almost balanced and perfect $\{0,1\}$ G-array. □

The following are a few remarks concerning Theorem 3.

1. The equation $AB^{(-1)} + BA = A(B^{(-1)} + B)$ in the proof of Theorem 3 is allowed only when G is abelian. All other steps in the proof would hold for arbitrary finite groups.

2. The converse to Theorem 3 is not true. That is, having a balanced and perfect $\{0,1\}$ $G = \mathbb{Z}_2 \times H$-array does not guarantee the existence of a Yamada-Pott $\{0,1\}$ H-array pair via reversing the construction in Theorem 3. For example,

$$\boldsymbol{s} = (1,1,0,0,1,1,1,1,0,0,1,0,1,1,0,0,0,0,0,0,1,0,1,0,1,1,1,0,1,0,0,1,0,1,1,1,0,0)^\top$$

is a balanced and perfect $\{0,1\}$ $\mathbb{Z}_{38}$-array obtained by applying the $a_g \to \frac{a_g+1}{2}$ transformation to the $\{-1,1\}$ $\mathbb{Z}_{38}$-array in [3]. Let $S = \sum_{i \in \mathbb{Z}_{38}} s_i i$. Now, $\mathbb{Z}_{38} \cong \mathbb{Z}_2 \times \mathbb{Z}_{19}$ via the map $\phi(i) = (i \pmod 2), (i \pmod{19}))$. Let $\hat{S} = \sum_{i \in \mathbb{Z}_{38}} s_{\phi(i)} \phi(i) = \sum_{i' \in \mathbb{Z}_2 \times \mathbb{Z}_{19}} s_{i'} i'$ be the group ring element corresponding to $(\Phi(s_g))$ in $\mathbb{Z}[\mathbb{Z}_2 \times \mathbb{Z}_{19}]$. Write $\hat{S} = \hat{A} + \hat{B}$, where $\hat{A} = \sum_{i' \in \{0\} \times \mathbb{Z}_{19}} s_{i'} i'$ and $\hat{B} = \sum_{i' \in \{1\} \times \mathbb{Z}_{19}} s_{i'} i'$. Let $\pi : \mathbb{Z}_2 \times \mathbb{Z}_{19} \to \mathbb{Z}_{19}$ be the projection map $\pi((x,y)) = y$. Let $A = \sum_{i' \in \{0\} \times \mathbb{Z}_{19}} s_{\pi(i')} \pi(i')$ and $B = \sum_{i' \in \{1\} \times \mathbb{Z}_{19}} s_{\pi(i')} \pi(i')$. Let $\boldsymbol{a}, \boldsymbol{b}$ be the $\{0,1\}$ $\mathbb{Z}_{19}$-arrays corresponding to A and B. Then,

$$\boldsymbol{a} = (1,1,0,1,1,1,1,1,0,1,1,0,1,0,0,1,0,0,0)^\top,$$
$$\boldsymbol{b} = (0,1,0,0,0,1,1,1,0,0,0,0,1,1,1,0,1,0,0)^\top,$$

and $(\boldsymbol{a}, \boldsymbol{b})$ fails all of the Yamada-Pott $\{0,1\}$ $\mathbb{Z}_{19}$-array pair conditions, i.e. none of $\boldsymbol{a}$ and $\boldsymbol{b}$ is symmetric or skew-symmetric and $|A| \neq |B|$. Observe that the isomorphism $\Theta : \mathbb{Z}_2 \times \mathbb{Z}_{19} \to \langle \omega \rangle H$ maps $(\Phi(s_g))$ to the $\langle \omega \rangle H$-array in Theorem 3, where H is a cyclic group of order 19. Hence, by Lemma 6, reversing the construction in Theorem 3 in this case does not produce a Yamada-Pott $\{0,1\}$ H-array pair. In fact, by an exhaustive computer search, we showed that no Yamada-Pott $\{0,1\}$ $\mathbb{Z}_{19}$-pair exists. Similarly, an exhaustive computer search proved that no Yamada-Pott $\{0,1\}$ $\mathbb{Z}_{17}$-array pair exists. However, a balanced and perfect $\{0,1\}$ $\mathbb{Z}_{34}$-array exists as the Ding-Helleseth-Martinsen class 3 $\mathbb{Z}_2 \times \mathbb{Z}_{17}$-array.

3. There are families of balanced, $\{0,1\}$ $\mathbb{Z}_{2u}$-arrays with perfect autocorrelations that can be used to construct Yamada-Pott $\{0,1\}$ $\mathbb{Z}_u$-array pairs or Szekeres $\{0,1\}$ $\mathbb{Z}_u$-array pairs, see Theorems 5 and 6.

4. When $|A| = |B| = (u+1)/2$, the smaller (larger) correlation value appears at the elements of $H \cup (H - A)\omega$ $(A\omega)$.

5. When $|A| = |B| = (u-1)/2$, the smaller (larger) correlation value appears at the elements of $H \cup A\omega$ $((H - A)\omega)$.

Theorem 4. Replacing A with $H - A$ or B with $H - B$ in Theorem 3 does not alter the Yamada-Pott $\{0,1\}$ H-array pair properties 1 and 2, and yields a perfect and balanced $\{0,1\}$ $\langle \omega \rangle H$-array.

Proof. Let $G = \langle \omega \rangle H$ and (A, B) be a Yamada-Pott $\{0,1\}$ H-array pair. Let $S' = (H - A + \omega B)$. Let $\boldsymbol{s}'$ be the $\{0,1\}$ G-array that corresponds to S'. First, $\boldsymbol{s}'$ is balanced as

$$|S'| = |H - A| + |B| = u - \left(\frac{u \pm 1}{2}\right) + \frac{u \pm 1}{2} = u.$$

Secondly, $H - A$ is symmetric as

$$(H - A)^{(-1)} = (H - A^{(-1)}) = H - A.$$

Now,

$$\begin{aligned} S'(S')^{(-1)} = & \\ &= (H - A + \omega B)(H - A + \omega B)^{(-1)} \\ &= (H - A)(H - A)^{(-1)} + BB^{(-1)} + \omega\left(B(H - A)^{(-1)} + (H - A)B^{(-1)}\right). \end{aligned}$$

Then,

$$\begin{aligned} (H - A)(H - A^{(-1)}) + BB^{(-1)} &= HH - HA^{(-1)} - AH + AA^{(-1)} + BB^{(-1)} \\ &= |H|H - HA - AH + AA^{(-1)} + BB^{(-1)} \\ &= uH - 2|A|H + AA^{(-1)} + BB^{(-1)} \\ &= (u - (u \pm 1))H + AA^{(-1)} + BB^{(-1)} \\ &= \mp H + AA^{(-1)} + BB^{(-1)} \\ &= \mp H + (u \pm 1)(1) + \lambda(H - 1) \\ &= \begin{cases} (\frac{u+1}{2} - 1)H + (u - \frac{u+1}{2} + 1)(1) & \text{if } |A| = |B| = \frac{u+1}{2}, \\ (\frac{u-3}{2} + 1)H + (u - \frac{u-3}{2} - 1)(1) & \text{if } |A| = |B| = \frac{u-1}{2} \end{cases} \\ &= \frac{u-1}{2}H + \frac{u+1}{2}(1), \end{aligned}$$

and

$$\begin{aligned} \omega\left(B(H - A)^{(-1)} + (H - A)B^{(-1)}\right) &= \omega(B + B^{-1})(H - A) = \omega(H \pm 1)(H - A) \\ &= \omega\left(\left(\frac{u \pm 1}{2}\right)H \mp A\right). \end{aligned}$$

By examining $S'S'^{(-1)} = (H - A + \omega B)(H - A + \omega B)^{(-1)}$ we see that for $t \neq 1$ the autocorrelation function of $\boldsymbol{s}'$ has the following form

$$C_{\boldsymbol{s}'}(t) = \frac{u \pm 1}{2}. \tag{11}$$

Thus, by equations (2), (3), and (11) the G-array $\boldsymbol{s}'$ is perfect. The case for

$$S' = A + (H - B)\omega$$

is proven similarly. In this case, the skew-symmetry of $H - B$ follows from

$$\begin{aligned}(H-B)+(H-B)^{(-1)} &= H-B+H-B^{(-1)}\\ &= 2H-(B+B^{(-1)})\\ &= 2H-(H\pm 1)\\ &= H\mp 1.\end{aligned}$$

□

2.2 The Ding-Helleseth-Martinsen $\{0,1\}$ $\mathbb{Z}_2 \times \mathbb{Z}_p^m$-array based Yamada-Pott $\{0,1\}$ $\mathbb{Z}_p^m$-array pairs

A Yamada-Pott $\{0,1\}$ $\mathbb{Z}_p^m$-array pair can be obtained from the array pair located by Ding-Helleseth-Martinsen $\{0,1\}$ $\mathbb{Z}_2 \times \mathbb{Z}_p^m$-array in [7] for two cases, where $p^m \equiv 5 \pmod 8$, $p^m = s^2 + 4t^2$, $s \equiv 1 \pmod 4$ and p is a prime. The two cases are $s = 1$ and $t^2 = 1$. When $t^2 = 1$ we get a Yamada-Pott $\{0,1\}$ $\mathbb{Z}_p^m$-array pair, while in the $s = 1$ case or for any $p^m \equiv 5 \pmod 8$, we get a Szekeres $\{0,1\}$ $\mathbb{Z}_p^m$-array pair. First, we present the case of the Ding-Helleseth-Martinsen family of $s = 1$ locating a Szekeres $\{0,1\}$ $\mathbb{Z}_p^m$-array pair for all $p^m \equiv 5 \pmod 8$.

Theorem 5. For each prime power $q = p^m \equiv 5 \pmod 8$ such that $q = s^2+4t^2 = 1+4t^2$, the Ding-Helleseth-Martinsen $\{0,1\}$ $\mathbb{Z}_2 \times \mathbb{Z}_p^m$-array locates the Szekeres $\{0,1\}$ $\mathbb{Z}_p^m$-array pair $(\boldsymbol{a}, \boldsymbol{b})$, where the sets of 1 indices of $(\boldsymbol{a}, \boldsymbol{b})$ are

$$(A, B) = (C_0^{(4,q,\alpha)} \cup C_1^{(4,q,\alpha)}, C_0^{(4,q,\alpha)} \cup C_3^{(4,q,\alpha)}).$$

Proof. The fact that the Ding-Helleseth-Martinsen $\{0,1\}$ $\Theta(\mathbb{Z}_2 \times \mathbb{Z}_p^m)$-array locates the Szekeres $\{0,1\}$ $\Theta(\mathbb{Z}_p^m)$-array pair $(\Theta((a_g)), \Theta((b_g)))$, whose sets of 1 indices are

$$(\Theta(C_0^{(4,q,\alpha)} \cup C_1^{(4,q,\alpha)}), \Theta(C_0^{(4,q,\alpha)} \cup C_3^{(4,q,\alpha)})),$$

follows from the definition of the Ding-Helleseth-Martinsen $\{0,1\}$ $\Theta(\mathbb{Z}_2 \times \mathbb{Z}_p^m)$-array for $s = 1$. The result now follows from Lemma 4. □

Next, we show that exactly one of the equivalence classes 1 and 2 Ding-Helleseth-Martinsen family with $t^2 = 1$ locates a $\{0,1\}$ Yamada-Pott $\mathbb{Z}_p^m$-array pair.

Let $q = p^m$ for some prime p and $n, D \in \mathbb{Z}$. Then a representation $nq = x^2 + Dy^2$ for some $x, y \in \mathbb{Z}$ is called a *proper* if $\gcd(q, x) = 1$ [17, p. 35]. When $p \equiv 1 \pmod 4$ there are many representations of q in the form $q = s^2 + 4t^2$ for some $s, t \in \mathbb{Z}$. However there is precisely one proper representation [17, p. 47].

Let $q = p^m = 4\ell + 1$ for some prime p and odd positive integer ℓ, or equivalently, let p be a a prime with $p \equiv 5 \pmod 8$ and $m \in 2\mathbb{Z}_{\geq 0} + 1$. Then the unique proper representation of q has the form $q = s^2 + 4t^2$ with $s \equiv 1 \pmod 4$ and $t \in \mathbb{Z}$, where the sign of t is undetermined [17, p. 51]. Let α be a generator of $\mathbb{F}_q^*$. Then, by Lemma 19 in [17, p. 48]

$$t(\alpha) = \frac{16 \times (0,3)^4_{q,\alpha} - q - 1 - 2s}{8}, \tag{12}$$

where $t^2 = (t(\alpha))^2$.

The integers $(i,j)^d_{q,\alpha} = |(C_i^{(d,q,\alpha)} + 1) \cap C_j^{(d,q,\alpha)}|$ are called the *cyclotomic numbers of order* d with respect to $\mathbb{F}_q$ and α such that $\mathbb{F}_q^* = \langle \alpha \rangle$. The following lemma is needed to establish our results.

Lemma 7. Let p be a prime, $p \equiv 5 \pmod 8$, $q = p^m$, and $m \in 2\mathbb{Z}_{\geq 0} + 1$. Let $q = s^2 + 4t^2$ be the unique proper representation of q. Let

$$\begin{aligned}
(A_1, B_1) &= (C_0^{(4,q,\alpha)} \cup C_1^{(4,q,\alpha)}, C_1^{(4,q,\alpha)} \cup C_3^{(4,q,\alpha)}),\\
(A_2, B_2) &= (C_0^{(4,q,\alpha)} \cup C_2^{(4,q,\alpha)}, C_2^{(4,q,\alpha)} \cup C_3^{(4,q,\alpha)}),
\end{aligned}$$

where $\mathbb{F}_q^* = \langle \alpha \rangle$ and $t(\alpha)$ is as in equation (12). Then

$$|A_1 \cap (A_1 + x)| + |B_1 \cap (B_1 + x)| = \begin{cases} A + 4E + 2B + D = \frac{q - t(\alpha) - 2}{2} & \text{if } x^{-1} \in C_0^{(4,q,\alpha)} \cup C_2^{(4,q,\alpha)}, \\ 4A + 2E + C + D = \frac{q + t(\alpha) - 4}{2} & \text{if } x^{-1} \in C_1^{(4,q,\alpha)} \cup C_3^{(4,q,\alpha)}, \end{cases} \tag{13}$$

and

$$|A_2 \cap (A_2 + x)| + |B_2 \cap (B_2 + x)| = \begin{cases} 4A + 2E + B + C = \frac{q - t(\alpha) - 4}{2} & \text{if } x^{-1} \in C_0^{(4,q,\alpha)} \cup C_2^{(4,q,\alpha)}, \\ 4E + 2D + A + B = \frac{q + t(\alpha) - 2}{2} & \text{if } x^{-1} \in C_1^{(4,q,\alpha)} \cup C_3^{(4,q,\alpha)}, \end{cases} \tag{14}$$

where

$$\begin{aligned}
A &= \frac{q - 7 + 2s}{16},\\
B &= \frac{q + 1 + 2s - 8t(\alpha)}{16},\\
C &= \frac{q + 1 - 6s}{16},\\
D &= \frac{q + 1 + 2s + 8t(\alpha)}{16},\\
E &= \frac{q - 3 - 2s}{16}.
\end{aligned}$$

Proof. This result is proven in the proof of Theorem 3.1 in [6]. (There are two typos in equation (5) in [6]; "$\frac{q-2-t}{2}$" and "$\frac{q-4+t}{2}$" should be "$\frac{q-4-t}{2}$" and "$\frac{q-2+t}{2}$" respectively. Equation (5) in [6] is equation (14) here.) ∎

Theorem 6. For $i = 1, 2$, let $(\boldsymbol{a}_i, \boldsymbol{b}_i)$ be $\{0, 1\}$ $\mathbb{Z}_p^m$-pair whose sets of 1 indices are (A_i, B_i) in Lemma 7. Then $(\boldsymbol{a}_i, \boldsymbol{b}_i)$ is a Yamada-Pott $\{0, 1\}$ $\mathbb{Z}_p^m$-pair if and only if $t(\alpha) = (-1)^{i+1}$, where $t(\alpha)$ is as in equation (12). Hence, exactly one of the $(\boldsymbol{a}_i, \boldsymbol{b}_i)$ is a Yamada-Pott $\mathbb{Z}_p^m$-array pair.

Proof. First, (A_1, B_1) is a 2-SDS$(q; (q-1)/2, (q-1)/2, (q-3)/2)$ if and only if

$$\frac{q - t(\alpha) - 2}{2} = \frac{q + t(\alpha) - 4}{2} = \frac{q-3}{2} \iff t(\alpha) = 1,$$

and (A_2, B_2) is a 2-SDS$(q; (q-1)/2, (q-1)/2, (q-3)/2)$ if and only if

$$\frac{q - t(\alpha) - 4}{2} = \frac{q + t(\alpha) - 2}{2} = \frac{q-3}{2} \iff t(\alpha) = -1.$$

Hence, the choice of field generator α determines which pair is the supplementary difference set as $(0, 3)^4_{q,\alpha}$ is a function of α. To prove the symmetry of B_1 and the skew-symmetry of A_1 first observe that $q = s^2 + 4$, with $s \equiv 1 \pmod 4$ implies $q = 8j + 5$ for some $j \in \mathbb{Z}^{\geq 0}$. Since

$$-1 = \alpha^{\frac{q-1}{2}} = \alpha^{4j+2},$$

we have

$$-C_1^{(4,q,\alpha)} = \alpha^{4j+2}\alpha C_0^{(4,q,\alpha)} = \alpha^3 C_0^{(4,q,\alpha)} = C_3^{(4,q,\alpha)},$$

and

$$-C_0^{(4,q,\alpha)} = \alpha^{4j+2} C_0^{(4,q,\alpha)} = C_2^{(4,q,\alpha)}.$$

Then

$$B_1^{(-1)} = (C_1^{(4,q,\alpha)} + C_3^{(4,q,\alpha)})^{(-1)} = -C_1^{(4,q,\alpha)} - C_3^{(4,q,\alpha)} = C_3^{(4,q,\alpha)} + C_1^{(4,q,\alpha)} = B_1,$$

and B_1 is symmetric. Moreover,

$$A_1^{(-1)} = (C_0^{(4,q,\alpha)} + C_1^{(4,q,\alpha)})^{(-1)} = -C_0^{(4,q,\alpha)} - C_1^{(4,q,\alpha)} = C_2^{(4,q,\alpha)} + C_3^{(4,q,\alpha)}. \qquad (15)$$

Now, equation (15) implies $\{A_1\} \cap \{A_1^{(-1)}\} = \emptyset$, and $A_1 + A_1^{(-1)} = \mathbb{Z}_p^m - 0$. Hence, A_1 is skew-symmetric. The symmetry of A_2 and the skew-symmetry of B_2 are proven similarly. The result now follows from Theorem 1. □

Let $C_{i,j,l}$ in Section 1.4 be the sets of 1 indices of pairs of $\mathbb{Z}_p^m$-arrays. It is easy to check that the equivalence classes of pairs of $\mathbb{Z}_p^m$-arrays whose sets of 1 indices are $C_{0,1,3}$, $C_{0,2,3}$, and $C_{1,0,3}$ constitute all equivalence classes of all possible pairs of $\mathbb{Z}_p^m$-arrays whose sets of 1 indices have the form $C_{i,j,l}$. Hence, Theorems 5 and 6 cover all equivalence classes of all possible such $\mathbb{Z}_p^m$-arrays.

The following corollary provides two equivalent conditions to the equivalence class i Ding-Helleseth-Martinsen family of $\Theta(\mathbb{Z}_2 \times \mathbb{Z}_p^m)$-array $\boldsymbol{s}_i$ being perfect.

Corollary 1. Let $(\boldsymbol{a}_i, \boldsymbol{b}_i)$ and $t(\alpha)$ be as in Theorem 6. Let $\Theta(\mathbb{Z}_2) = \langle\omega\rangle$, and $S_i = \Theta(A_i)+\Theta(B_i)\omega$ be the set of 1 indices of the equivalence class i Ding-Helleseth-Martinsen family of $\{0,1\}$ $\Theta(\mathbb{Z}_2 \times \mathbb{Z}_p^m)$-array $\boldsymbol{s}_i$. Then the following are equivalent:

(i) The $\{0,1\}$ $\Theta(\mathbb{Z}_2 \times \mathbb{Z}_p^m)$-array $\boldsymbol{s}_i$ is perfect.

(ii) $(\boldsymbol{a}_i, \boldsymbol{b}_i)$ is a Yamada-Pott $\{0,1\}$ $\mathbb{Z}_p^m$-array pair.

(iii) $t(\alpha) = (-1)^{i+1}$.

Proof. The equivalence of (ii) and (iii) follows from Theorem 6. $(ii) \implies (i)$ follows from Theorem 3. To prove $(i) \implies (ii)$, we already proved in the proof of Theorem 6 that $\boldsymbol{a}_1$ and $\boldsymbol{b}_2$ are skew-symmetric and $\boldsymbol{b}_1$ and $\boldsymbol{a}_2$ are symmetric. So, it suffices to show that $(\Theta(\boldsymbol{a}_i), \Theta(\boldsymbol{b}_i))$ is a Legendre pair. By the definition in equation (2), $\boldsymbol{s}_i$ is perfect implies

$$C_{\boldsymbol{s}_i}(t) = \frac{q-1}{2} \quad \text{or} \quad \frac{q-3}{2} \quad \text{if} \quad t \neq 1. \tag{16}$$

Now,

$$\begin{aligned}\sum_{t\in\Theta(\mathbb{Z}_2\times\mathbb{Z}_p^m)} C_{\boldsymbol{s}_i}(t)t = S_iS_i^{(-1)} &= (\Theta(A_i)+\omega\Theta(B_i))\,(\Theta(A_i)+\omega\Theta(B_i))^{(-1)} \\ &= (\Theta(A_i)+\omega\Theta(B_i))\left(\Theta(A_i)^{(-1)}+\omega\Theta(B_i)^{(-1)}\right).\end{aligned}$$

Then,

$$S_iS_i^{-1} = \Theta(A_i)\Theta(A_i)^{(-1)} + \Theta(B_i)\Theta(B_i)^{(-1)} + \omega\left(\Theta(A_i)\Theta(B_i)^{(-1)} + \Theta(A_i)^{(-1)}\Theta(B_i)\right). \tag{17}$$

The isomorphism $\Theta : \mathbb{Z}_2 \times \mathbb{Z}_p^m \to \Theta(\mathbb{Z}_2 \times \mathbb{Z}_p^m)$ extends linearly to an isomorphism of $\mathbb{Z}[\mathbb{Z}_2 \times \mathbb{Z}_p^m]$ and $\mathbb{Z}[\Theta(\mathbb{Z}_2 \times \mathbb{Z}_p^m)]$. If $(\boldsymbol{a}_i, \boldsymbol{b}_i)$ is not a Legendre pair then by equations (13) and (14)

$$A_i(A_i)^{(-1)} + B_i(B_i)^{(-1)}$$

has terms whose coefficients are equal to $(q-5)/2$. Then equation (17) implies

$$\Theta(A_i)\Theta(A_i)^{(-1)} + \Theta(B_i)\Theta(B_i)^{(-1)}$$

has terms whose coefficients are $(q-5)/2$, and this contradicts equation (16). ☐

By establishing $(i) \iff (iii)$ in Corollary 1 we also solved the second of the proposed two open problems at the end of Section 3 in [6]. As far as we know this problem has been open until now.

The second part of Theorem 3.1 of [1] states that the $\mathbb{Z}_p^m$-array pair $(\boldsymbol{a}, \boldsymbol{b})$ with sets of 1 indices $(C_0^{(4,q,\alpha)} \cup C_1^{(4,q,\alpha)}, C_0^{(4,q,\alpha)} \cup C_2^{(4,q,\alpha)})$ satisfies the Legendre $\mathbb{Z}_p^m$-array pair condition. This is not always true. On page 130 of [13], Pott incorrectly credits [1] for this theorem (as it works if and only if $t(\alpha) = -1$). Nevertheless, this does not impact the main theme of [1] on dicyclic designs. The following corollary corrects the second part of Theorem 3.1 of [1].

Corollary 2. Let $t(\alpha)$ and $q = p^m = s^2 + 4t(\alpha)^2$ be as in equation (12). Then, the $\mathbb{Z}_p^m$-array pair $(\boldsymbol{a}, \boldsymbol{b})$ with sets of 1 indices $D_1 = C_0^{(4,q,\alpha)} \cup C_1^{(4,q,\alpha)}$, and $D_2 = C_0^{(4,q,\alpha)} \cup C_2^{(4,q,\alpha)}$ satisfies the Legendre $\mathbb{Z}_p^m$-array pair condition if and only if $t(\alpha) = -1$. Moreover, $\boldsymbol{a}$ is skew-symmetric and $\boldsymbol{b}$ is symmetric.

Proof. Let A_2, B_2 and $\boldsymbol{a}_2$, $\boldsymbol{b}_2$ be as in Theorem 6. Then $\boldsymbol{a}_2$ is symmetric and $\boldsymbol{b}_2$ is skew-symmetric. Observe that $(D_1, D_2) = (\alpha^2 B_2, \alpha^2 A_2)$. Hence, $\mathbb{Z}_p^m$-array pair $(\boldsymbol{b}_2, \boldsymbol{a}_2)$ is equivalent to $(\boldsymbol{a}, \boldsymbol{b})$. Thus, $(\boldsymbol{a}, \boldsymbol{b})$ is a Legendre $\mathbb{Z}_p^m$-array pair if and only if $t(\alpha) = -1$. By Lemma 5, $(D_1, D_2) = (\alpha^2 B_2, \alpha^2 A_2)$ implies $\boldsymbol{a}$ is skew-symmetric and $\boldsymbol{b}$ is symmetric. □

2.3 The Sidelnikov-Lempel-Cohn-Eastman $\mathbb{Z}_{q-1}$-array based Yamada-Pott $\{0,1\}$ $\mathbb{Z}_{(q-1)/2}$-array pairs

An interesting fact about the Sidelnikov-Lempel-Cohn-Eastman $\{0,1\}$ $\mathbb{Z}_{q-1}$-array and the Yamada Yamada-Pott $\{0,1\}$ $\mathbb{Z}_{(q-1)/2}$-array pair is that each pair can be obtained from the other.

Theorem 7. For $q \geq 7$ and $q \equiv 3 \pmod 4$ let (A_1, B_1) and $(A_2 \cup B_2)$ be the pair of sets of 1 indices of the Yamada Yamada-Pott $\{0,1\}$ $\mathbb{Z}_{(q-1)/2}$-array pair and the set of 1 indices of the Sidelnikov-Lempel-Cohn-Eastman $\{0,1\}$ $\mathbb{Z}_{q-1}$-array, where

$$\begin{aligned}
A_1 &= \left\{\log_\alpha x \ (\mathrm{mod}\ \tfrac{q-1}{2}) \mid x \in (C_0^2 + 1) \cap C_0^2\right\}, \\
B_1 &= \left\{\log_\alpha x \ (\mathrm{mod}\ \tfrac{q-1}{2}) \mid x \in (C_0^2 - 1) \cap C_0^2\right\}, \\
A_2 &= \left\{\log_\alpha x \ (\mathrm{mod}\ \tfrac{q-1}{2}) \mid x \in (C_1^2 - 1) \cap C_0^2\right\}, \\
B_2 &= \left\{\log_\alpha x \ (\mathrm{mod}\ \tfrac{q-1}{2}) \mid x \in (C_1^2 - 1) \cap C_1^2\right\}.
\end{aligned}$$

Then, $A_1 = B_2$, and $B_1 = \mathbb{Z}_{\frac{q-1}{2}} \setminus A_2$.

Proof. Observe that

$$\alpha^{\frac{q-1}{2}}[(C_0^2 + 1) \cap C_0^2] = (\alpha^{\frac{q-1}{2}} C_0^2 + \alpha^{\frac{q-1}{2}}) \cap \alpha^{\frac{q-1}{2}} C_0^2.$$

Then, $q \equiv 3 \pmod 4$ implies $\alpha^{(q-1)/2} = -1 \notin C_0^2$ giving

$$\alpha^{\frac{q-1}{2}}[(C_0^2 + 1) \cap C_0^2] = (C_1^2 - 1) \cap C_1^2.$$

After taking the discrete logarithm and reducing modulo $(q-1)/2$, we get $A_1 = B_2$. Since $\mathbb{F}_q = \{0\} \cup C_0^2 \cup C_1^2$ is a partitioning of $\mathbb{F}_q$ and $\phi(x) = x - 1$ is a one-to-one function from $\mathbb{F}_q$ to $\mathbb{F}_q$ we get

$$\mathbb{F}_q = \{-1\} \cup (C_0^2 - 1) \cup (C_1^2 - 1) \tag{18}$$

as another partitioning of $\mathbb{F}_q$. Now, by equation (18) and the fact that $-1 \notin C_0^2$, we get

$$C_0^2 = C_0^2 \cap [(C_0^2 - 1) \cup (C_1^2 - 1)] = (C_0^2 \cap (C_0^2 - 1)) \cup (C_0^2 \cap (C_1^2 - 1))$$

as a partitioning of C_0^2. Then, we get the set equations

$$2\mathbb{Z}_{\frac{q-1}{2}} = \log_\alpha(C_0^2) = \log_\alpha[(C_0^2 \cap (C_0^2 - 1)) \cup (C_0^2 \cap (C_1^2 - 1))] =$$
$$\log_\alpha[(C_0^2 \cap (C_0^2 - 1))] \cup \log_\alpha[(C_0^2 \cap (C_1^2 - 1))] = 2[B_1 \cup A_2]$$

as

$$(C_0^2 \cap (C_0^2 - 1)) \cap (C_0^2 \cap (C_1^2 - 1)) = \emptyset.$$

Hence,

$$\mathbb{Z}_{\frac{q-1}{2}} = \frac{1}{2}\log_\alpha(C_0^2) = B_1 \cup A_2.$$

It is also clear that $A_2 \cap B_1 = \emptyset$. Thus,

$$B_1 = \mathbb{Z}_{\frac{q-1}{2}} \setminus A_2 \quad \text{and} \quad A_2 = \mathbb{Z}_{\frac{q-1}{2}} \setminus B_1.$$

□

Next, we locate an almost balanced perfect $\{0,1\}$ $\mathbb{Z}_{q-1}$-array pair based on a family of $\{0,1\}$ $\mathbb{Z}_{(q-1)/2}$-array pairs. In fact, this result is presented partially in [6], as Theorem 4.1. By Lemma 6 it suffices to locate an almost balanced perfect $\{0,1\}$ $\Theta(\mathbb{Z}_{q-1})$-array.

Theorem 8. Let $q \geq 7$ and $q = p^m \equiv 3 \pmod 4$, α be a generator of $\mathbb{F}_q^*$. Let

$$A = \left\{\log_\alpha x \ (\text{mod } \tfrac{q-1}{2}) \mid x \in (C_0^2 - 1) \cap C_0^2\right\},$$
$$B = \left\{\log_\alpha x \ (\text{mod } \tfrac{q-1}{2}) \mid x \in (C_0^2 - 1) \cap C_1^2\right\}$$

be the pair of sets of 1 indices of the $\{0,1\}$ $\mathbb{Z}_{(q-1)/2}$-array $(\boldsymbol{a}, \boldsymbol{b})$ pair. Then $(\boldsymbol{a}, \boldsymbol{b})$ is a Yamada-Pott $\{0,1\}$ $\mathbb{Z}_{(q-1)/2}$-array pair. Let $\langle\omega\rangle = \Theta(\mathbb{Z}_2)$. Then $\Theta(A) + \Theta(B)\omega \in \mathbb{Z}[\Theta(\mathbb{Z}_2 \times \mathbb{Z}_{(q-1)/2})]$ corresponds to an almost balanced perfect $\{0,1\}$ $\Theta(\mathbb{Z}_2 \times \mathbb{Z}_{(q-1)/2})$-array.

Proof. Let $A' = \sum_{g \in A/2} g$ and $B' = \sum_{g \in (B-1)/2} g$, where $A', B' \in \mathbb{Z}[\mathbb{Z}_{(q-1)/2}]$ and $(\boldsymbol{a}', \boldsymbol{b}')$ be the corresponding $\mathbb{Z}_{(q-1)/2}$-array pair. In Theorem 4.1 of [6] it is shown that

$$A'(A')^{(-1)} + B'(B')^{(-1)} = \frac{q-7}{4}(\mathbb{Z}_{\frac{q-1}{2}} - 0) + \frac{q-3}{2}(0).$$

Now, since $(\boldsymbol{a}', \boldsymbol{b}')$ and $(\boldsymbol{a}, \boldsymbol{b})$ are equivalent $\mathbb{Z}_{(q-1)/2}$-array pairs, we get that $(\boldsymbol{a}, \boldsymbol{b})$ is a Legendre $\{0,1\}$ $\mathbb{Z}_{(q-1)/2}$-array pair. Next, we show that $\boldsymbol{a}$ is a symmetric $\mathbb{Z}_{(q-1)/2}$-array. For a set $A \subseteq \mathbb{Z}_{(q-1)/2}$ let $-A = \{x \mid -x \in A\}$. For any $x \in (C_0^2 - 1) \cap C_0^2$ we have

$$x = \alpha^{2i} - 1 = \alpha^{2j}, \tag{19}$$

for some $i, j \in \mathbb{Z}$. Multiplying both sides of equation (19) by $x^{-1} = \alpha^{-2j}$ yields

$$\alpha^{2i-2j} - \alpha^{-2j} = 1$$

or

$$\alpha^{-2j} = \alpha^{2i-2j} - 1.$$

Then, $x^{-1} \in (C_0^2 - 1) \cap C_0^2 = A$ implying $-2j \in A$. Hence, if $2j \in A$ then $2j \in -A$. Since $|(-A)| = |A|$ we get $A = -A$. Finally, we show that $\boldsymbol{b}$, equivalently B is skew-symmetric. By the definition of B, any $x \in (C_0^2 - 1) \cap C_1^2$ satisfies

$$x = \alpha^{2i} - 1 = \alpha^{2j+1}, \tag{20}$$

for some $i, j \in \mathbb{Z}$. By multiplying both sides of equation (20) with $x^{-1} = \alpha^{-(2j+1)}$ we see that

$$\alpha^{2i-2j-1} - \alpha^{-(2j+1)} = 1.$$

By rearranging terms we get

$$\alpha^{-(2j+1)} = \alpha^{2i-2j-1} - 1,$$

and so $x^{-1} \in (C_1^2 - 1) \cap C_1^2$. Hence, $x^{-1} \notin C_0^2 - 1$, and $-2j - 1 \notin B$. Thus, if $b = 2j + 1 \in B$, then $-b \notin B$ giving that $B \cap (-B) = \emptyset$. Now, $q \equiv 3 \pmod 4$ implies $\alpha^{(q-1)/2} = -1 \notin C_0^2$. Then,

$$\alpha^{\frac{q-1}{2}}[(C_0^2 - 1) \cap C_1^2] = (C_1^2 + 1) \cap C_0^2$$

and consequently $|(C_0^2 - 1) \cap C_1^2| = |(C_1^2 + 1) \cap C_0^2|$. Now, by equation (18) and the fact that $-1 \in C_1^2$, we get

$$C_1^2 = C_1^2 \cap [(C_0^2 - 1) \cup (C_1^2 - 1)] = \{-1\} \cup (C_1^2 \cap (C_0^2 - 1)) \cup (C_1^2 \cap (C_1^2 - 1))$$

as a partitioning of C_1^2. Then, the set equations

$$2\mathbb{Z}_{\frac{q-1}{2}} + 1 = \log_\alpha(C_1^2) = \log_\alpha[-1] \cup \log_\alpha[(C_1^2 \cap (C_0^2 - 1)) \cup (C_1^2 \cap (C_1^2 - 1))] =$$
$$\log_\alpha[-1] \cup \log_\alpha[(C_1^2 \cap (C_0^2 - 1))] \cup \log_\alpha[(C_1^2 \cap (C_1^2 - 1))]$$

gives a partitioning of $2\mathbb{Z}_{(q-1)/2} + 1$ as

$$(C_1^2 \cap (C_0^2 - 1)) \cap (C_1^2 \cap (C_1^2 - 1)) = \emptyset,$$

$-1 \notin (C_1^2 \cap (C_0^2 - 1))$ and $-1 \notin (C_1^2 \cap (C_1^2 - 1))$. Since $\gcd((q-1)/2, 2) = 1$, $\phi(x) = 2x+1$ is an automorphism of $\mathbb{Z}_{(q-1)/2}$. Then

$$\left(2\mathbb{Z}_{\frac{q-1}{2}} + 1\right) (\bmod\ \frac{q-1}{2}) = \left(\log_\alpha[-1] \cup \log_\alpha[(C_1^2 \cap (C_0^2 - 1))] \cup \log_\alpha[(C_1^2 \cap (C_1^2 - 1))]\right) (\bmod\ \frac{q-1}{2})$$

is a partitioning of $\mathbb{Z}_{(q-1)/2}$. This implies that $|B| = |(C_0^2 - 1) \cap C_1^2|$. By part b of Lemma 6 in [17, p. 30], $|(C_0^2 - 1) \cap C_1^2| = |(C_1^2 + 1) \cap C_0^2| = (q-3)/4$. Hence, $|B| = (q-3)/4$. We also have $|B| = |(-B)|$ and $B \cap (-B) = \emptyset$, so $B \cup (-B) = \mathbb{Z}_{(q-1)/2} \backslash 0$. Now, the result follows from Lemma 2. □

While it is believed that a Legendre $\{0,1\}$ $\mathbb{Z}_n$-array pair exists for all odd n, the existence of Yamada-Pott $\{0,1\}$ $\mathbb{Z}_n$-array pairs or $\{0,1\}$ $\mathbb{Z}_n$-array pairs $(\boldsymbol{a}, \boldsymbol{b})$ such that both $\boldsymbol{a}$ and $\boldsymbol{b}$ are symmetric or skew-symmetric has not received as much attention. Table 1 shows the existence and non-existence of $\{0,1\}$ Yamada-Pott $\mathbb{Z}_n$-array pairs. The comment column describes either how the pair is generated or how we have shown nonexistence. “Computer search” means the existence or non-existence of a Yamada-Pott $\{0,1\}$ $\mathbb{Z}_n$-array was proven by an exhaustive computer search. Under the “Exist?” column a “Y” or “N” means yes or no. Our computer search was based on going through all possible pairs of $\{0,1\}$ sequences, $\boldsymbol{a}, \boldsymbol{b}$ such that

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i = \frac{n+1}{2}$$

and screening out the pairs that formed a Legendre pair. At the end of the search, for each found $\{0,1\}$ Legendre $\mathbb{Z}_n$-array pair $(\boldsymbol{a}, \boldsymbol{b})$, we checked for the symmetry and skew symmetry of $\boldsymbol{a}$ and $\boldsymbol{b}$ respectively.

Table 2 shows the existence of a Legendre $\{0,1\}$ $\mathbb{Z}_n$-array pair for all possible combinations of $\boldsymbol{a}$ and $\boldsymbol{b}$ being symmetric, skew-symmetric and neither symmetric nor skew-symmetric. The number at the top of each column is n. The first two columns describe the attributes of $\boldsymbol{a}$ and $\boldsymbol{b}$ respectively. In the first two columns “N” means neither symmetric nor skew-symmetric, “Sk” means skew-symmetric and “S” means symmetric. For each cell that is in a column with an integer at the top, “E” and “NE” mean exists and does not exist respectively.

Exhaustive searches proved that no balanced, perfect $\{0,1\}$ $\mathbb{Z}_{54}$-array exists, on two different supercomputers, with different programs [11]. This is consistent with our computer searches as finding a Yamada-Pott $\{0,1\}$ $\mathbb{Z}_{27}$-array pair would imply a perfect balanced $\{0,1\}$ $\mathbb{Z}_{54}$-array by Theorem 3.

We end this section with a couple of comments.

1. In [13], on page 130, it is claimed that a Yamada-Pott $\{0,1\}$ $\mathbb{Z}_{37}$-array pair exists. This is false as it originated from the mistake in part 2 of Theorem 3.1 in [1]. The

Table 1: The existence of Yamada-Pott $\{0,1\}$ $\mathbb{Z}_n$-array pairs

n	Exist?	Comment
3	Y	Theorem 8 with $q = 2(3)+1 = 7$
5	Y	Theorem 8 with $q = 2(5)+1 = 11$
7	N	Computer search
9	Y	Theorem 8 with $q = 2(9)+1 = 19$
11	Y	Theorem 8 with $q = 2(11)+1 = 23$
13	Y	Theorem 8 with $q = 2(13)+1 = 27$
15	Y	Theorem 8 with $q = 2(15)+1 = 31$
17	N	Computer search
19	N	Computer search
21	Y	Theorem 8 with $q = 2(21)+1 = 43$
23	Y	Theorem 8 with $q = 2(23)+1 = 47$
25	N	Computer search
27	N	Computer search
29	Y	Theorem 8 with $q = 2(29)+1 = 59$
31	N	Computer search

case $n = 37$ with $q = 2 * 37 + 1 = 75$ is not a prime power. However, a symmetric Paley $\{0,1\}$ $\mathbb{Z}_{37}$-array pair and a skew-symmetric Szekeres $\{0,1\}$ $\mathbb{Z}_{37}$-array pair exist. The first example of a Yamada-Pott $\{0,1\}$ $\mathbb{Z}_q$-array pair that arises from Theorem 6 is at $q = 15^2 + 4 = 229$, where $n = 2q + 1 = 459 = 27 * 17$ is not a prime power.

2. Exhaustive searches proved that no Legendre $\{0,1\}$ $\mathbb{Z}_7$-array pair $(\boldsymbol{a}, \boldsymbol{b})$, where $\boldsymbol{a}$ is symmetric, and no Legendre $\{0,1\}$ $\mathbb{Z}_{17}$-array pair $(\boldsymbol{a}, \boldsymbol{b})$, where $\boldsymbol{a}$ is skew-symmetric exists. Exhaustive searches found a Legendre $\{0,1\}$ $\mathbb{Z}_n$-array pair $(\boldsymbol{a}, \boldsymbol{b})$, where at least one of $\boldsymbol{a}$ and $\boldsymbol{b}$ is symmetric or skew-symmetric for each $n \leq 21$, see Table 2.

2.4 An inequivalent Legendre $\{-1,1\}$ $\mathbb{Z}_{57}$-array pair

By using a heuristic computer search the only known example of a Legendre $\{-1,1\}$ $\mathbb{Z}_{57}$-array pair was found in [5]. This resulted in the construction of a 116×116 Hadamard matrix via Theorem 2. The Legendre $\{-1,1\}$ $\mathbb{Z}_{57}$-array pair found is given by

$$\boldsymbol{a}_1 = (-++-+-+-++-++----+-+++++-+++--+++-+-----+-+--+-+++--+-+--)^\top,$$

$$\boldsymbol{b}_1 = (--++--++-++++-++-+++++-----+-+++-++--+-+---++----++-----+)^\top,$$

Table 2: The existence of a Legendre $\{0,1\}$ $\mathbb{Z}_n$-array pair for all possible combinations of $\boldsymbol{a}$ and $\boldsymbol{b}$ being symmetric, skew-symmetric and neither symmetric nor skew-symmetric

Type		n								
A	B	5	7	9	11	13	15	17	19	21
N	N	E	E	E	E	E	E	E	E	E
N	S	E	NE	E	E	E	E	E	E	E
N	Sk	E	E	E	E	E	E	NE	E	E
S	S	E	NE	NE	NE	E	NE	E	NE	NE
S	Sk	E	NE	E	E	E	E	NE	NE	E
Sk	Sk	E	E	NE	E	E	NE	NE	E	NE

where $-$, $+$ are used for -1, 1, and commas are deleted to save space.
This pair can be shown to satisfy the condition given by Definition 5. The distributions of the autocorrelations of A and B are

$$(-11)^2(-7)^{12}(-3)^{10}(1)^{20}(5)^{12},$$

and

$$(-7)^{12}(-3)^{20}(1)^{10}(5)^{12}(9)^2.$$

By using cyclotomy we found a Legendre $\{-1,1\}$ $\mathbb{Z}_3\times\mathbb{Z}_{19}$-array pair $(\boldsymbol{x},\boldsymbol{y})$ that can be used to construct a Legendre $\{-1,1\}$ $\mathbb{Z}_{57}$-array pair that is not equivalent to the previously known $\{-1,1\}$ Legendre $\mathbb{Z}_{57}$-array pair. This construction is displayed in the next example.

Example 1. Construct $C_i^{(6,19)}$ for $i=0,1,\ldots,5$ for $\alpha=2$. For this example, we explicitly construct these cosets for $d=6$, $q=19$ and $\alpha=2$. The elements are given by $C_0^{(6,19,2)}=\{1,7,11\}$ with the remaining cosets being generated by multiplying $C_0^{(6,19,2)}$ by $\alpha=2$ and reducing modulo 19. For brevity, we use C_i^6 for $C_i^{(6,19,2)}$. Let

$$X=\left\{\{0\}\times\{0,C_0^6,C_1^6,C_2^6\}\right\}\cup\left\{\{1\}\times\{C_0^6,C_2^6,C_3^6,C_4^6\}\right\}\cup\left\{\{2\}\times\{C_3^6,C_4^6\}\right\},$$

and

$$Y=\left\{\{0\}\times\{0,C_0^6,C_4^6,C_5^6\}\right\}\cup\left\{\{1\}\times\{C_0^6,C_3^6,C_5^6\}\right\}\cup\left\{\{2\}\times\{C_0^6,C_1^6,C_3^6\}\right\}.$$

Then, the Legendre $\{-1,1\}$ $\mathbb{Z}_3\times\mathbb{Z}_{19}$-array pair $(\boldsymbol{x},\boldsymbol{y})$ obtained by letting

$$x_i=\begin{cases}1 & \text{if } i\in X,\\ -1 & \text{otherwise,}\end{cases}$$

and

$$y_i = \begin{cases} 1 & \text{if } i \in Y, \\ -1 & \text{otherwise} \end{cases}$$

satisfies Definition 5. The distribution of autocorrelations for $\boldsymbol{x}$ and $\boldsymbol{y}$ are

$$(-7)^{14}(-3)^{12}(1)^{18}(5)^{12},$$

$$(-7)^{12}(-3)^{18}(1)^{12}(5)^{14}.$$

The correlation energy for the $\{-1,1\}$ $\mathbb{Z}_3 \times \mathbb{Z}_{19}$ array pair $(\boldsymbol{x}, \boldsymbol{y})$ is $1,112$. To construct a Legendre $\{-1,1\}$ $\mathbb{Z}_{57}$ array pair observe that $\mathbb{Z}_{57} \cong \mathbb{Z}_3 \times \mathbb{Z}_{19}$ via the map $\phi(i) = (i \pmod 3), (i \pmod{19}))$. Then, the $\{-1,1\}$ $\mathbb{Z}_{57}$-array pair $(\phi^{-1}((x_g)), \phi^{-1}((y_g)))$ is a Legendre pair that has the same distribution of autocorrelations and the same correlation energy as those of $(\boldsymbol{x}, \boldsymbol{y})$. The map ϕ^{-1} is constructed as follows. Let $\phi(i) = (i \pmod 3), (i \pmod{19})) = (a, b)$. Then there exists $k_1, k_2 \in \mathbb{Z}^{\geq 0}$ such that $a + 3k_1 = b + 19k_2 = i$, $0 \leq k_1 \leq 19$, and $0 \leq k_2 \leq 3$. Then, $3k_1 + (a - b) = 19k_2$ imply $k_2 = (a - b)19^{-1} \pmod 3$ and $k_1 = -(a - b)3^{-1} \pmod{19}$. Now, k_1, k_2 are uniquely determined by the inequalities $0 \leq k_1 \leq 19$, and $0 \leq k_2 \leq 3$. Hence, $\phi^{-1}(a, b) = a + 3k_1 = b + 19k_2 = i$. This gives us

$$\boldsymbol{a}_2 = (++-+++++++------++---+---+--+-++-+-+-+-+--++-++--++----++)^\top,$$

$$\boldsymbol{b}_2 = (+++----++-++-+++----+---+-+---++--+-++-+-+---++-++++--+-+)^\top.$$

The correlation energy for the Legendre $\{-1,1\}$ $\mathbb{Z}_{57}$-array pair in [5] is $1,240$. Thus $(\boldsymbol{a}_2, \boldsymbol{b}_2)$ is not equivalent to $(\boldsymbol{a}_1, \boldsymbol{b}_1)$.

We propose developing theoretical and computational methods for finding Legendre $\{-1,1\}$ $\mathbb{Z}_n$-array pairs by using cyclotomic cosets as in Example 1 as a future research direction.

Acknowledgements

Dr. K. T. Arasu was supported by the U.S. Air Force Research Lab Summer Faculty Fellowship Program sponsored by the Air Force Office of Scientific Research. The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the US Government. The authors thank two referees for improving the clarity of the paper substantially.

References

[1] K. T. Arasu. Falsity of a conjecture on dicyclic designs. *Util. Math.*, 41:253–258, 1992.

[2] K. T. Arasu, C. Ding, T. Helleseth, and H. M. Martinsen. Almost difference sets and their sequences with optimal autocorrelation. *IEEE Trans. Inform. Theory*, 47:2934–2943, 2001.

[3] K. T. Arasu and Z. Little. Balanced perfect sequences of period 38 and 50. *J. Comb. Inf. Syst. Sci.*, 35:91–95, 2010.

[4] P. Ó Catháin and R. M. Stafford. On twin prime power Hadamard matrices. *Cryptogr. Commun.*, 2:261–269, 2010.

[5] M. Chiarandini, I. S. Kotsireas, C. Koukouvinos, and L. Paquete. Heuristic algorithms for Hadamard matrices with two circulant cores. *Theoret. Comput. Sci.*, 407:274–277, 2008.

[6] C. Ding. Two constructions of $(v,(v-1)/2,(v-3)/2)$ difference families. *J. Combin. Des.*, 16:164–171, 2008.

[7] C. Ding, T. Helleseth, and H. Martinsen. New families of binary sequences with optimal three-level autocorrelation. *IEEE Trans. Inform. Theory*, 47:428–433, 2001.

[8] R. J. Fletcher, M. Gysin, and J. Seberry. Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices. *Australas. J. Combin.*, 23:75–86, 2001.

[9] J. W. Iverson, J. Jasper, and D. G. Mixon. Optimal line packings from finite group actions. *Forum of Mathematics, Sigma*, 8:E6, 2020.

[10] D. Jungnickel and A. Pott. Perfect and almost perfect sequences. *Discrete Appl. Math.*, 95:331–359, 1999.

[11] I. Kotsireas. Email correspondence. Dec 2016.

[12] A. Lempel, M. Cohn, and W. L. Eastman. A class of balanced binary sequences with optimal autocorrelation properties. *IEEE Trans. Inform. Theory*, 23:38–42, 1977.

[13] A. Pott. *Finite Geometry and Character Theory*. Springer, 1995.

[14] J. J. Rotman. *An Introduction to the Theory of Groups*. Springer-Verlag, New York, NY, USA, 4th edition, 1994.

[15] W. D. Schroeder. *Number Theory in Science and Communication*. Springer-Verlag, 1984.

[16] V. M. Sidelnikov. Some k-valued pseudo-random sequences and nearly equidistant codes. *Probl. Inform. Trans.*, 5:12–16, 1969.

[17] T. Storer. *Cyclotomy and Difference Sets*. Markham Pub. Co., 1967.

[18] G. Szekeres. Cyclotomy and complementary difference sets. *ACTA Arith.*, XVIII:348–353, 1971.

[19] J. (Seberry) Wallis. On supplementary difference sets. *Aequationes Math.*, 8:242–257, 1972.

[20] W. D. Wallis, A. P. Street, and J. S. Wallis. *Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices*. Springer-Verlag, 1972.

[21] A. L. Whiteman. An infinite family of skew Hadamard matrices. *Pacific J. Math.*, 38(3):817–822, 1971.

[22] M. Yamada. On a relation between a cyclic relative difference set associated with the quadratic extensions of a finite field and the Szekeres difference sets. *Combinatorica*, 8(2):207–216, 1988.