ON THE EXISTENCE OF APERIODIC COMPLEMENTARY HEXAGONAL LATTICE ARRAYS

YIN TAN AND GUANG GONG

Abstract. Binary (periodic) aperiodic complementary sequences have been studied extensively due to their wide range of applications in engineering, for example in optics, radar and communications. They are also linked to topics in coding theory, combinatorics and Boolean functions. Complementary sequences have been generalized either by being defined over larger alphabets or by being defined from one dimension to multi-dimensions. Recently, Ding and Tarokh introduced and constructed the aperiodic complementary two-dimensional arrays over the alphabet $\mathfrak{A}_p^* = \{\zeta_p^i : 0 \leq i \leq p-1, p \text{ is a prime number}\}$, whose support set is a subset of the hexagonal lattice (mostly is a set of ℓ-layer consecutive hexagons). They demonstrated that such complementary hexagonal lattice arrays can be used on coded aperture imagining with ideal efficiency. In this paper, we study the conditions for which such complementary hexagonal lattice arrays exist. We first show that aperiodic complementary hexagonal lattice arrays over the alphabet $\mathfrak{A}_p^*$ leads to aperiodic (hence periodic) complementary sequences over the alphabet $\mathfrak{A}_p = \mathfrak{A}_p^* \cup \{0\}$. Then we make use of group ring equations to characterize periodic complementary sequences over alphabet $\mathfrak{A}_p$. As of independent interest, we show that, if the alphabet of the periodic complementary sequences is $\mathfrak{A}_p^*$, the notion of periodic complementary sequences is equivalent to the notion of certain relative difference family. The conditions for the existence of periodic complementary sequences over alphabet $\mathfrak{A}_p$ are derived from this characterization. As a result, we determine the existence of a pair (triple) aperiodic complementary binary hexagonal lattice arrays whose support set is an ℓ-layer consecutive hexagons. A table listing the existence status for a pair of complementary hexagonal lattice arrays with $1 \leq \ell \leq 20$ as well as some open problems are presented.

1. Introduction

Let $S = (s_0, \ldots, s_{n-1})$ be a binary sequence over alphabet $\{\pm 1\}$. The aperiodic autocorrelation function of S is defined by $A^S(t) = \sum_{i=0}^{n-1-t} s_i s_{i+t}$; and the periodic autocorrelation function of S is defined by $P^S(t) = \sum_{i=0}^{n-1} s_i s_{i+t}$, where the addition of the indices is performed modulo n and $0 \leq t \leq n-1$. It is well known that the aperiodic and periodic autocorrelation functions are related by $P^S(t) = A^S(t) + A^S(n-1-t)$. By convention, we call the values $A^S(t), P^S(t)$ *out-of-phase* if $(t \mod n) \not\equiv 0$, and *in-phase* otherwise. More generally, we call S a *p-phase sequence* if S is over the alphabet $\mathfrak{A}_p = \{0, \zeta_p^i : 0 \leq i \leq p-1\}$ (one may wonder why do we include 0 in the alphabet: this is for the convenience to state the results in Section III), where p is a prime and ζ_p is a primitive p-th root of unity.

For the applications in engineering, the sequences with small out-of-phase (periodic) aperiodic autocorrelation values are highly preferred. From this point of view, the *Barker sequences*, whose all out-of-phase aperiodic autocorrelation values equal either 0 or 1, are the most ideal objects. Unfortunately, there are very few Barker sequences are known so far. The lengths of the known Barker sequences are $2, 3, 4, 5, 7, 11, 13$; and it has been conjectured that no Barker sequences of the other lengths exist. This conjecture has been verified positively by Bernhard in [23] for the sequences of length n with $13 < n < 10^{22}$. Due to the scarcity of Barker sequences, several approaches of generalization have been

Date: February 9, 2015.

Key words and phrases. Aperiodic autocorrelation, periodic autocorrelation, complementary array, hexagonal lattice, relative difference family.

proposed in order to discover richer patterns. In the following we briefly describe the approaches relevant to our work; readers interested in other approaches may refer to, for instance, [7,8,16–18] and the references therein.

In [16], Golay proposed the notion *Golay pair*, which is a pair of binary sequences of the same length such that the sum of the out-of-phase aperiodic autocorrelation values are 0. It has been shown that a Golay pair exists if the length of its sequences is of the form $2^a10^b26^c$, where a, b, c are non-negative integers and $a^2 + b^2 + c^2 \neq 0$. The existence of Golay pairs with other lengths remains open since 1961. Subsequently, in [24], Tseng and Liu further studied a *set of complementary binary sequences* such that the set may contain more than two sequences and the sum of all out-of-phase aperiodic autocorrelation values are 0. Another two widely adopted approaches to generalize complementary sequences are to define the sequences over a larger alphabet, or to consider complementary d-dimensional arrays, see for example [17,18]. In the rest of the paper, we refer complementary to aperiodic complementary unless explicitly stated. Note that *periodic complementary sequences* are sequences with the sum of all out-of-phase periodic autocorrelation values is zero. They have been studied in [1,2,14].

Recently, in [10], Ding and Tarokh studied the complementary two-dimensional arrays over the alphabet $\mathfrak{A}_p^* = \mathfrak{A}_p \setminus \{0\}$, whose support set can be an arbitrary lattice (Defined in Section 3.1). This generalizes the complementary two-dimensional arrays considered in [18] in the sense that the support sets of the arrays in [18] are square lattices. In particular, Ding and Tarokh demonstrated that, if the support set is a particular subset of the hexagonal lattice, the corresponding complementary arrays may be used in coded aperture imaging with ideal performances. For brevity, we call an array whose support set is a subset of the hexagonal lattice a *hexagonal lattice array*. Several constructions of complementary hexagonal lattice arrays were provided in [10]. However, the conditions for the support sets, the number of arrays in the set and the alphabet $\mathfrak{A}_p^*$, for which this complementary set exits are unclear. It is the aim of this paper to develop more conditions for the existence of such a set.

In Section III, we define a set of points of the hexagonal lattice, which is denoted by Ω_ℓ and is called *ℓ-layer consecutive hexagons* (Definition 1). Such sets are the most commonly chosen support sets for hexagonal lattice arrays in the application of coded aperture imaging described in [10]. Through explicitly determining the coordinates of the points in Ω_ℓ, we are able to express a hexagonal lattice array whose support set is Ω_ℓ by a $(2l-1) \times (2\ell-1)$ matrix with entries in $\mathfrak{A}_p$. According to this expression and by making use of the techniques in [18], a set of complementary sequences of length $4\ell^2 - 6\ell + 3$ over alphabet $\mathfrak{A}_p$ exist, if a complementary set of hexagonal lattice arrays over alphabet $\mathfrak{A}_p^*$ and with Ω_ℓ as the support set exits (Proposition 2).

In Section IV, we focus on the existence of the periodic complementary sequences with length n and alphabet $\mathfrak{A}_p$ (here we use the well-known fact that aperiodic complementary sequences must be periodic complementary). To explore the existence conditions, we establish an important connection between the sequences with length n and alphabet $\mathfrak{A}_p$ and the group ring elements of $\mathbb{Z}[\mathbb{Z}_n \times \mathbb{Z}_p]$. We provide a characterization of the periodic complementary sequences by the group ring equation, from which yields several conditions for the existence of periodic complementary sequences (Corollaries 3,4). As of independent interest, we show that, if the alphabet of the sequences is $\mathfrak{A}_p^*$, then a set of periodic complementary sequences is equivalent to a relative difference family in $\mathbb{Z}_p \times \mathbb{Z}_n$ relative to $\mathbb{Z}_p \times \{1\}$ (Theorem 2). This relationship can be regarded as a generalization of the result in [2], which points out that a set of periodic complementary binary sequences is equivalent to a difference family. To the best of our knowledge, this is the first combinatorial characterization of the periodic complementary p-phase sequences for any prime p.

In the light of the results in Sections III and IV, in Section V we focus on determining the existence of complementary binary hexagonal lattice arrays $\mathcal{C}_\ell^t = \{C_\ell^1, \ldots, C_\ell^t\}$ whose

support set is Ω_ℓ for $t = 2$ and 3 (Theorems 3 and 4). We provide necessary conditions on ℓ such that $\mathcal{C}_\ell^2, \mathcal{C}_\ell^3$ exist. We give a table listing the existence of $\mathcal{C}_\ell^2$ for $1 \le \ell \le 20$. Some open problems are proposed as well. We should mention that in [10] the authors provided examples of $\mathcal{C}_\ell^t$ for $t = 4$.

The rest of the paper is organized as follows. In Section II, we present necessary definitions and results used throughout the paper. In Section III, we will introduce the arrays with support set is a hexagonal lattice array; and show the relationship between complementary hexagonal lattice arrays and complementary sequences. We provide the characterization of periodic complementary sequences through group ring equations in Section IV. The connection between periodic complementary sequences over alphabet $\{\zeta_p^i : 0 \le i \le p-1\}$ and certain relative difference family is presented as well. In Section V, we study the existence of complementary binary hexagonal lattice arrays. Some concluding remarks are given in Section VI.

2. Preliminaries

In this section, we present necessary definitions and results that will be used throughout the paper.

2.1. **Group rings and character theory.** Character theory is one of the most important tools for applying group rings to combinatorial objects. In this section we only review the characters of the group ring $\mathbb{C}[G]$, where G ia an Abelian group. For the theory of the representation of a general group ring, please refer to [21].

Let $\mathbb{F}$ be an arbitrary field (usually we take the complex field $\mathbb{C}$), and let G be a multiplicatively written group. The group algebra $\mathbb{F}[G]$ consists of all formal sums

$$\sum_{g\in G} a_g g, \quad a_g \in \mathbb{F}.$$

The addition and multiplication for elements in $\mathbb{F}[G]$ are defined as follows:

$$\begin{aligned}\sum_{g\in G} a_g g + \sum_{g\in G} b_g g &= \sum_{g\in G}(a_g + b_g)g,\\ \sum_{g\in G} a_g g \cdot \sum_{g\in G} b_g g &= \sum_{g\in G}\left(\sum_{h\in G} a_h \cdot b_{gh^{-1}}\right) g.\end{aligned}$$

Moreover, we have a scalar multiplication

$$\lambda \sum_{g\in G} a_g g = \sum_{g\in G}(\lambda a_g)g, \quad \lambda \in \mathbb{F}.$$

It is easy to verify that with these operations, $\mathbb{F}[G]$ is indeed an algebra over $\mathbb{F}$. In the language of group rings, we identify a subset S of G with the group ring element $\sum_{s\in S} s$, which will also be denoted by S. For an element $A = \sum_{g\in G} a_g g \in \mathbb{F}[G]$ and an integer t, we define $A^{(t)} = \sum_{g\in G} a_g g^t$.

A character χ of a finite Abelian group G is a homomorphism from G to $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$. A character χ is called *principal* if $\chi(c) = 1$ for all $c \in G$; otherwise it is called *non-principal*. A principal character is usually denoted by χ_0. All characters form a group denoted by $\widehat{G}$, which is isomorphic to G. The following result states the well-known *orthogonal relations* of characters.

Result 1 (Orthogonal relations of characters)**.** *Let G be an Abelian group. Then the following equations hold:*

$$\sum_{g\in G} \chi(g) = \begin{cases} 0 & \text{if } \chi \ne \chi_0,\\ |G| & \text{if } \chi = \chi_0;\end{cases}$$

and

$$\sum_{\chi\in\widehat{G}}\chi(g)=\begin{cases}0 & \text{if } g\neq 1_G,\\ |G| & \text{if } g=1_G.\end{cases}$$

By linearity, we may extend each character $\chi\in\widehat{G}$ to a ring homomorphism from $\mathbb{C}[G]$ to $\mathbb{C}$, and we denote this homomorphism by χ, again. In particular, if G is the additive group of the finite field $\mathbb{F}_{p^n}$, all characters of G can be represented as follows. Define $\chi_1:\mathbb{F}_{p^n}\to\mathbb{C}$ as $\chi_1(x)=\zeta_p^{\mathrm{Tr(x)}}$ for all $x\in\mathbb{F}_{p^n}$, where ζ_p is a primitive p-th root of unity and Tr(x) is the absolute trace function defined as $\mathrm{Tr(x)}=\sum_{\mathrm{i}=0}^{\mathrm{n}-1}\mathrm{x}^{\mathrm{p^i}}$. Then χ_1 is an additive character of $\mathbb{F}_{p^n}$ (i.e. χ_1 is a character of the additive group of $\mathbb{F}_{p^n}$). Moreover, every additive character χ is of the form χ_b ($b\in\mathbb{F}_{p^n}$), where χ_b is defined by $\chi_b(x)=\chi_1(bx)$ for all $x\in\mathbb{F}_{p^n}$. Furthermore, if $G=\mathbb{F}_{p^n}\times\mathbb{F}_{p^n}$, all characters of G can be represented by $\chi_{u,v}$, where $\chi_{u,v}(a,b)=\zeta_p^{\mathrm{Tr(au+bv)}}$ for any $(a,b)\in G$. The following results are important properties of group rings.

Result 2 (Inversion Formula)**.** *Let $D=\sum_{g\in G}a_g g\in\mathbb{C}[G]$. Then the following hold:*

$$a_g = \frac{1}{|G|}\sum_{\chi\in\widehat{G}}\chi(D)\chi(g^{-1}), \tag{1}$$

$$\sum_{g\in G}|a_g|^2 = \frac{1}{|G|}\sum_{\chi\in\widehat{G}}|\chi(D)|^2. \tag{2}$$

The above Inversion Formula provides a useful method for showing two group ring elements are equal.

Corollary 1. *Let $A=\sum_{g\in G}a_g g$ and $B=\sum_{g\in G}b_g g$ be two group ring elements of $\mathbb{C}[G]$. Then $A=B$ if and only if $\chi(A)=\chi(B)$ for all $\chi\in\widehat{G}$.*

2.2. **Relative difference family.** Let G be an Abelian group of order v and let N be a subgroup of order n. A $(v,n,K,\lambda;u)$ *relative difference family* (RDF for short) in G relative to N is a collection of subsets of G, $\mathcal{D}=\{D_1,D_2,\ldots,D_u\}$, such that the following equation holds for the multiset union

$$\sum_{i=1}^{u}\left\{xy^{-1}:x,y\in D_i,x\neq y\right\}=\lambda(G-N),$$

where K is the set of cardinalities of all the base blocks D_i. In the case of $K=\{k\}$, it is called a $(v,n,k,\lambda;u)$ relative difference family for brevity. If a $(v,n,k,\lambda;u)$ relative difference family exists, we have

$$uk(k-1)=\lambda(v-n). \tag{3}$$

According to the Inversion formula (Corollary 1), the set $\mathcal{D}$ is a $(v,n,K,\lambda;u)$ if and only if the following equation holds:

$$\sum_{i=1}^{u}\chi(D_iD_i^{(-1)})=\begin{cases}\sum_{i=1}^{u}k_i+\lambda(v-n), & \text{if } \chi=\chi_0,\\ \sum_{i=1}^{u}k_i-\lambda n, & \text{if } \chi|_N=\chi_0,\chi\neq\chi_0\\ \sum_{i=1}^{u}k_i, & \text{if } \chi|_N\neq\chi_0.\end{cases}$$

The notion of relative difference family generalizes previously well-studied objects in combinatorics. For example, $\mathcal{D}$ is called a *difference family* if $N=\{1\}$; it is called a *difference set* if $u=1$ and $N=\{1\}$; it is called a relative difference set if $u=1$. Relative difference families and its variants are well studied [3, 4, 6, 9, 11, 12, 15, 20, 25]. Difference families have applications in coding theory and cryptography, see for instance [5, 22].

3. Complementary Hexagonal Lattice Arrays

In this section, we will first briefly review the definitions of the lattices and the (periodic) aperiodic complementary hexagonal lattice arrays. Then we show the relationship between them and (periodic) aperiodic complementary sequences.

3.1. **Hexagonal lattice array.** A *lattice* in $\mathbb{R}^n$ is a subgroup of $\mathbb{R}^n$ which is generated by forming all linear combinations with integer coefficients of the elements in a basis. In other words, a lattice $\mathfrak{L}$ in $\mathbb{R}^n$ has the form

$$\mathfrak{L} = \left\{ \sum_{i=1}^{n} c_i \mathbf{e}_i \mid c_i \in \mathbb{Z} \right\},$$

where $\{\mathbf{e}_i\}_{i=1}^n$ forms a basis of $\mathbb{R}^n$. In the following we only introduce the arrays whose support set is a subset of hexagonal lattices. Interested readers may refer to [10] for the definition of the array whose support set is an arbitrary lattice. When $n = 2$, the lattice $\mathbb{A}_2$ is called *hexagonal* if $\mathbf{e}_1 = (1, 0), \mathbf{e}_2 = (1/2, \sqrt{3}/2)$. Note that some authors choose the basis vectors of $\mathbb{A}_2$ as $\mathbf{e}'_1 = (1, 0), \mathbf{e}'_2 = (-1/2, \sqrt{3}/2)$, but it is not difficult to see that $\{\mathbf{e}_1, \mathbf{e}_2\}$ and $\{\mathbf{e}'_1, \mathbf{e}'_2\}$ generate the same lattice. A *hexagonal lattice array* (HLA for short) over an alphabet $\mathfrak{A}$ and with a support set Ω, denoted by $C^{\Omega,\mathfrak{A}}$, is a mapping $C[\cdot] : \mathbb{A}_2 \to \mathfrak{A}$ such that $C[\mathbf{a}] = 0$ for all $\mathbf{a} \notin \Omega$ and $C[\mathbf{a}] \in \mathfrak{A}$ for all $\mathbf{a} \in \Omega$. For a hexagonal lattice array $C^{\Omega,\mathfrak{A}}$, the aperiodic autocorrelation function $A^C(\cdot)$ is defined by

$$A^C(\mathbf{u}) = \sum_{\mathbf{s}\in\Omega} C[\mathbf{s}]\overline{C[\mathbf{s}+\mathbf{u}]}, \quad \mathbf{u} \in \mathbb{A}_2, \tag{4}$$

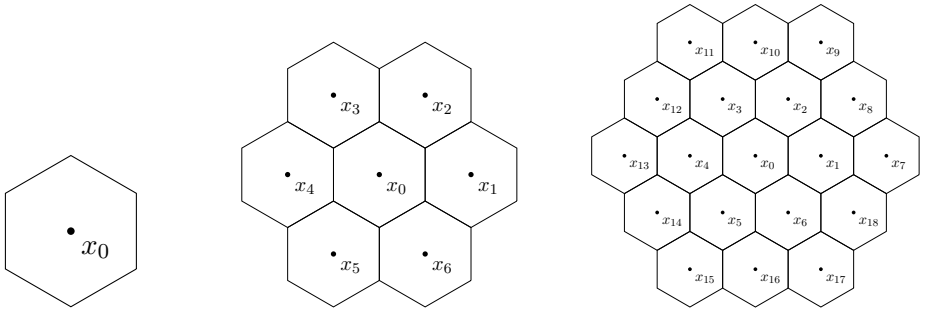
where $\overline{x}$ denotes the complex conjugate of $x \in \mathbb{C}$. A set of hexagonal lattice arrays $\mathcal{C} = \{C_1^{\Omega,\mathfrak{A}}, \ldots, C_t^{\Omega,\mathfrak{A}}\}$ with the same alphabet and support set is called *aperiodic complementary* if

$$A^{C_1}(\mathbf{u}) + \cdots + A^{C_t}(\mathbf{u}) = 0, \quad \forall \mathbf{u} \neq \mathbf{0}.$$

3.2. **ℓ-layer Hexagonal lattice arrays.** In the application of complementary hexagonal lattice arrays to the coded aperture imagining described in [10], the support set of a hexagonal lattice array is often chosen as ℓ consecutive layers of hexagons (defined below). We call such special hexagonal lattice arrays *ℓ-layer hexagonal lattice arrays*; their definition is given below.

Definition 1. *Let Ω be a set of points of the hexagonal lattice $\mathbb{A}_2$. We call Ω a 1-layer consecutive hexagon if Ω consists of only one hexagon. For $\ell > 1$, if Ω is the union of the $(\ell-1)$-layer consecutive hexagons and the hexagons adjacent with the $(\ell-1)$-layer consecutive hexagons, then Ω is called ℓ-layer consecutive hexagons and denoted it by Ω_ℓ. We call a hexagonal lattice array with support set as Ω_ℓ an ℓ-layer hexagonal lattice array (ℓ-HLA for short).*

We give below the 1-, 2- and 3-HLAs to illustrate Definition 1.



(A) 1-HLA (B) 2-HLA (C) 3-HLA

To compute the aperiodic autocorrelation function (defined in (4)) for an ℓ-HLA, in the following result we give the coordinates of the points (using the chosen basis vectors $\mathbf{e}_1 = (1,0), \mathbf{e}_2 = (1/2, \sqrt{3}/2)$ of $\mathbb{A}_2$) in the support set Ω_ℓ (defined in Definition 1). Furthermore, we make use of a $(2\ell-1)\times(2\ell-1)$ matrix to represent an ℓ-HLA. The proof of the following result may be given by induction on ℓ, we omit the details here due to its simplicity.

Proposition 1. *Let Ω_ℓ be the ℓ-layer consecutive hexagons. The set of the coordinates of the points in Ω_ℓ (by abusing our notations, we still use Ω_ℓ to denote the set of coordinates) is*

$$\begin{aligned} \Omega_\ell &= \{(i,j) : 1 \le i \le \ell-1, -(\ell-1) \le j \le \ell-i-1\} \\ &\cup \{(i,j) : -(\ell-1) \le i \le -1, -\ell-i+1 \le j \le \ell-1\} \\ &\cup \{(0,j) : -(\ell-1) \le j \le (\ell-1)\}. \end{aligned} \tag{5}$$

An ℓ-layer hexagonal lattice array can be represented by a $2\ell-1$ by $2\ell-1$ matrix $\mathcal{T}_\ell$ defined as

(6)

$$\begin{array}{c} \\ -(\ell-1) \\ -(\ell-2) \\ \cdots \\ -1 \\ 0 \\ 1 \\ \cdots \\ \ell-1 \end{array} \begin{array}{c} \begin{array}{ccccccccc} -(\ell-1) & -(\ell-2) & \cdots & -1 & 0 & 1 & \cdots & \ell-1 \end{array} \\ \begin{pmatrix} 0 & 0 & \cdots & 0 & a_{-(\ell-1),0} & a_{-(\ell-1),1} & \cdots & a_{-(\ell-1),\ell-1} \\ 0 & 0 & \cdots & a_{-(\ell-2),-1} & a_{-(\ell-2),0} & a_{-(\ell-2),1} & \cdots & a_{-(\ell-2),\ell-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & a_{-1,-(\ell-2)} & \cdots & \cdots & \cdots & a_{-1,1} & \cdots & a_{-1,\ell-1} \\ a_{0,-(\ell-1)} & \cdots & \cdots & \cdots & \cdots & a_{0,1} & \cdots & a_{0,\ell-1} \\ a_{1,-(\ell-1)} & \cdots & \cdots & \cdots & \cdots & a_{1,1} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{\ell-1,-(\ell-1)} & \cdots & \cdots & a_{\ell-1,-1} & a_{\ell-1,0} & 0 & \cdots & 0 \end{pmatrix} \end{array},$$

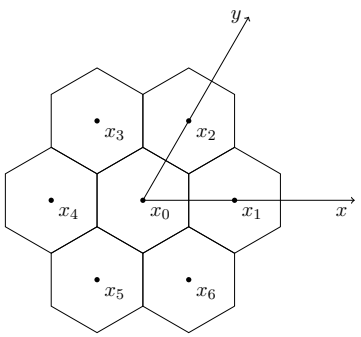
where the rows (resp. columns) are indexed from $-(\ell-1)$ to $\ell-1$ from top to bottom (resp. left to right).

By Proposition 1, the aperiodic autocorrelation for an ℓ-HLA C_ℓ can be computed as

$$A^{C_\ell}(\mathbf{u}) = \sum_{\mathbf{s}\in\Omega_\ell} C[\mathbf{s}]\overline{C[\mathbf{s}+\mathbf{u}]}, \quad \mathbf{u} \in \mathbb{A}_2, \tag{7}$$

where Ω_ℓ is defined in (5). Let us use a 2-HLA to illustrate Proposition 1.

Example 1. *Given a 2-layer hexagonal lattice array below, the set of the coordinates of the points $\{x_0, x_1, x_2, x_3, x_4, x_5, x_6\}$ is $\Omega_2 = \{(0,0),(1,0),(0,1),(-1,1),(-1,0),(0,-1),(1,-1)\}$. Now we define a 3 by 3 matrix $\mathcal{T}_2$ as described in (6). If the point with coordinate (i,j)*



belongs to Ω_2, say x_k, the element $\mathcal{T}_2(i,j)$ is then x_k. Thus, we get

$$\mathcal{T}_2 = \begin{array}{c} \\ -1 \\ 0 \\ 1 \end{array} \begin{array}{c} \begin{array}{ccc} -1 & 0 & 1 \end{array} \\ \begin{pmatrix} 0 & x_4 & x_3 \\ x_5 & x_0 & x_2 \\ x_6 & x_1 & 0 \end{pmatrix} \end{array}.$$

3.3. **Complementary ℓ-HLAs and complementary sequences.** In [17, 18], Jedwab and Parker constructed complementary s-dimensional arrays from complementary $(s+1)$-dimensional arrays. The following result is one of the key steps to apply for their technique.

Proposition 2. *Let $\mathcal{C} = \{C_1^{\Omega_\ell,\mathfrak{A}}, \ldots, C_t^{\Omega_\ell,\mathfrak{A}}\}$ be a set of ℓ-layer hexagonal lattice arrays over the alphabet $\mathfrak{A}$. For each i with $1 \le i \le t$, define a sequence S_i of length $(2\ell-1)^2$ as*

$$S_i(u(2\ell-1)+v) = C_i^{\Omega_\ell,\mathfrak{A}}(u,v), \quad 0 \le u, v \le 2\ell-2. \tag{8}$$

Then, for any integer α, β, we have the following relationship between the aperiodic autocorrelations

$$A^{S_i}(\alpha(2\ell-1)+\beta) = A^{C_i^{\Omega_\ell,\mathfrak{A}}}(\alpha,\beta) + A^{C_i^{\Omega_\ell,\mathfrak{A}}}(\alpha+1, \beta-(2\ell-1)).$$

Therefore, the sequence set $\mathcal{S} = \{S_1, \ldots, S_t\}$ is aperiodic complementary if $\mathcal{C}$ is aperiodic complementary.

Proof. For simplicity, we denote $C_i^{\Omega_\ell,\mathfrak{A}}$ by C_i for $1 \le i \le t$. The aperiodic autocorrelation function of C_i is computed as equation (7). Since shifting the support set of C_i will not change the autocorrelation function values (see [10, Lemma 1]), we may assume the support set of C_i to be $\Omega_\ell + (\ell-1, \ell-1)$, and still denote this set by Ω_ℓ. Note that for $\mathbf{s} = (i,j) \in \Omega_\ell$, we have $0 \le i, j \le 2(\ell-1)$. By Proposition 1, for the points with coordinates (i,j), where $0 \le i, j \le 2(\ell-1)$ but $(i,j) \notin \Omega_\ell$, the corresponding element in the matrix $\mathcal{T}_\ell$ (defined in (6)) is 0, therefore we may compute the autocorrelation function for C_i as

$$A^{C_i}(a,b) = \sum_{0 \le i,j \le 2\ell-2} C(i,j)\overline{C[i+a, j+b]}, \quad \mathbf{u} = (a,b) \in \mathbb{A}_2.$$

Note that any integer t in the range $[0, (2\ell-1)^2-1]$ can be represented uniquely in the form $u(2\ell-1)+v$ for some $0 \le u, v \le 2\ell-2$. Also note that when we compute the aperiodic autocorrelation function for the sequence S_i, we take $S_i(t) = 0$ for $t \notin [0, (2\ell-1)^2-1]$. Now for each $t = \alpha(2\ell-1)+\beta, 0 \le \alpha, \beta \le 2\ell-2$, we have

$$\begin{aligned}
A^{S_i}(\alpha(2\ell-1)+\beta) &= \sum_{j=0}^{(2\ell-1)^2-1} S_i(j)\overline{S_i(j+\alpha(2\ell-1)+\beta)} \\
&= \sum_{u,v=0}^{2\ell-2} S_i(u(2\ell-1)+v)\overline{S_i(u(2\ell-1)+v+\alpha(2\ell-1)+\beta)} \\
&= \sum_{u,v} S_i(u(2\ell-1)+v)\overline{S_i((u+\alpha)(2\ell-1)+v+\beta)} \\
&= \sum_u \left(\sum_{v=0}^{(2\ell-1)-\beta-1} S_i(u(2\ell-1)+v)\overline{S_i((u+\alpha)(2\ell-1)+v+\beta)} \right. \\
&\qquad \left. + \sum_{v=(2\ell-1)-\beta}^{2\ell-2} S_i(u(2\ell-1)+v)\overline{S_i((u+\alpha+1)(2\ell-1)+v+\beta-(2\ell-1))} \right) \\
&= \sum_u \left(\sum_{v=0}^{(2\ell-1)-\beta-1} C_i(u,v)\overline{C_i(u+\alpha, v+\beta)} \right. \\
&\qquad \left. + \sum_{v=(2\ell-1)-\beta}^{2\ell-2} C_i(u,v)\overline{C_i(u+\alpha+1, v+\beta-(2\ell-1)} \right) \\
&= A^{C_i}(\alpha,\beta) + A^{C_i}(\alpha+1, \beta-(2\ell-1)).
\end{aligned}$$

The last statement of the theorem is clear from the above equation. □

Remark 1. *If the alphabet of an ℓ-HLA is $\mathfrak{A}$, then the sequence obtained from an ℓ-HLA described in Proposition 2 has the alphabet $\mathfrak{A} \cup \{0\}$.*

Let us use the 2-HLA stated in Example 1 to illustrate how to obtain a sequence from an HLA as described in Proposition 1.

Example 2. *Let C_2 be a 2-HLA stated in Example 1. The sequence defined in 8 from C_2 is $S = (0, x_4, x_3, x_5, x_0, x_2, x_6, x_1, 0)$.*

One may see from the matrix representation of an ℓ-HLA (6) and the definition of the sequence S from an ℓ-HLA (8) that the first and the last $(\ell - 1)$ elements of the sequence S are 0s. Let us define a *shortened* sequence of length $(2\ell - 1)^2 - 2(\ell - 1) = 4\ell^2 - 6\ell + 3$ by removing the first and last consecutive $(\ell - 1)$ zeros. The following result shows that the set of sequences derived from ℓ-HLAs is aperiodic complementary if and only if the set of the shortened sequences is aperiodic complementary.

Proposition 3. *Let $\mathbf{0}$ be an all-zero sequence of length a and $\boldsymbol{S}$ be a sequence of length b. Let $\boldsymbol{T} = \mathbf{0} \,||\, S \,||\, \mathbf{0}$ be the sequence of length $2a + b$ defined by concatenating the sequences $\mathbf{0}$ and $\boldsymbol{S}$. Then we have $A^{\boldsymbol{T}}(\alpha) = A^{\boldsymbol{S}}(\alpha)$ for $1 \le \alpha \le b - 1$ and $A^{\boldsymbol{T}}(\alpha) = 0$ for $b \le \alpha \le 2a + b - 1$. Furthermore, let $\mathcal{S} = \{\boldsymbol{S}_1, \ldots, \boldsymbol{S}_t\}$ be a set of sequences of length b and $\mathcal{T} = \{\mathbf{0} \,||\, \boldsymbol{S}_1 \,||\, \mathbf{0}, \ldots, \mathbf{0} \,||\, \boldsymbol{S}_t \,||\, \mathbf{0}\}$ be the set of sequences of length $2a + b$. Then $\mathcal{T}$ is aperiodic complementary if and only if $\mathcal{S}$ if aperiodic complementary.*

Proof. Note that for the sequence $\mathbf{T}$ we have

$$\mathbf{T}_i = \begin{cases} 0, & \text{if } 1 \le i \le a, \\ S_i, & \text{if } a + 1 \le i \le a + b, \\ 0, & \text{if } a + b + 1 \le i \le 2a + b. \end{cases}$$

For α with $1 \le \alpha \le b-1$, we have $A^{\mathbf{T}}(\alpha) = \sum_{i=1}^{2a+b-\alpha} T_i\overline{T_{i+\alpha}} = \sum_{i=1}^{a} T_i\overline{T_{i+\alpha}} + \sum_{i=a+1}^{a+b-\alpha} T_i\overline{T_{i+\alpha}} + \sum_{i=a+b-\alpha+1}^{2a+b-\alpha} T_i\overline{T_{i+\alpha}} = \sum_{i=1}^{a} 0 \cdot \overline{T_{i+\alpha}} + \sum_{j=1}^{b-\alpha} T_{a+j}\overline{T_{a+j+\alpha}} + \sum_{j=1}^{a} T_{(a+b-\alpha)+j}\overline{T_{(a+b)+j}} = \sum_{j=1}^{b-\alpha} S_j\overline{S_{j+\alpha}} = A^{\mathbf{S}}(\alpha)$. Similarly, one may show that $A^{\mathbf{T}}(\alpha) = 0$ for $b \le \alpha \le 2a + b - 1$.

Now assume $\mathcal{S}$ is a set of aperiodic complementary sequences, then

$$\sum_{i=1}^{t} A^{\mathbf{T}_i}(\alpha) = \begin{cases} \sum_{i=1}^{t} A^{\mathbf{S}_i}(\alpha) = 0, & \text{if } 1 \le \alpha \le a, \\ 0, & \text{if } a + 1 \le \alpha \le 2a + b - 1, \end{cases}$$

which follows that $\mathcal{T}$ is a set of aperiodic complementary sequences. The converse part is similar and we omit it here. □

Thanks to Proposition 3, we will consider the *shortened* sequence S of length $(2\ell-1)^2 - 2(\ell - 1) = 4\ell^2 - 6\ell + 3$ obtained by removing the first and last consecutive $2(\ell - 1)$ zeros in the rest of the paper. By abusing the notations, we still use S to denote this shortened sequence.

The following result will be used later to show the non-existence of complementary ℓ-HLAs.

Corollary 2. *If there exists a set of t aperiodic complementary ℓ-HLAs over alphabet $\mathfrak{A}$, then a set of aperiodic complementary sequences of length $4\ell^2 - 6\ell + 3$ over alphabet $\mathfrak{A} \cup \{0\}$ also exists. Moreover, there exists a set of t periodic complementary sequences of period $4\ell^2 - 6\ell + 3$ over alphabet $\mathfrak{A} \cup \{0\}$.*

By Corollary 2, one can see clearly that if a set of t periodic complementary sequences of period $4\ell^2 - 6\ell + 3$ over alphabet $\mathfrak{A} \cup \{0\}$ does not exist, then a set of t aperiodic complementary ℓ-HLAs over alphabet $\mathfrak{A}$ does not exist either.

4. Characterization of Periodic Complementary Sequences by Group Rings

First we fix some notation to be used in remaining sections. Let p be a prime and $\mathfrak{A}_p = \{0, \zeta_p^i : 0 \le i \le p-1\}$, where ζ_p is a primitive p-th root of unity. Let $\mathfrak{A}_p^* = \mathfrak{A}_p \backslash \{0\}$. As mentioned in the previous section, the non-existence of periodic complementary sequences with period $4\ell^2 - 6\ell + 3$ and over alphabet $\mathfrak{A}_p$ implies the non-existence of aperiodic complementary ℓ-HLAs over alphabet $\mathfrak{A}_p^*$. In this section, we will make use of group rings to study periodic complementary sequences with period n and alphabet $\mathfrak{A}_p$. In particular, we show that a set of periodic complementary sequences with period n and over alphabet $\mathfrak{A}_p^*$ is equivalent to a relative difference family in the group $\mathbb{Z}_p \times \mathbb{Z}_n$ relative to $\mathbb{Z}_p \times \{1\}$.

4.1. **Periodic complementary sequences.** Let $\mathcal{S} = \{S_1, S_2, \ldots, S_t\}$ be a set of sequences. All sequences S_i have the period n and alphabet $\mathfrak{A}_p$. We may write each sequence S_i in the following form

$$S_i = \left\{ a_{i,0}\zeta_p^{b_{i,0}}, a_{i,1}\zeta_p^{b_{i,1}}, \ldots, a_{i,n-1}\zeta_p^{b_{i,n-1}} \right\},$$

where $a_{i,j} \in \{0,1\}, b_{i,j} \in \{0, \ldots, p-1\}$ for $1 \le i \le t$ and $0 \le j \le n-1$. If $a_{i,j} = 0$, we may choose any $b_{i,j} \in \{0, \ldots, p-1\}$ which gives the same value of $a_{i,j}\zeta_p^{b_{ij}}$. Without loss of generality, we assume $b_{i,j} = 0$ when $a_{i,j} = 0$. For each S_i, we define an associated sequence $T_i = \{a_{i,0}, a_{i,1}, \ldots, a_{i,n-1}\}$ over alphabet $\{0,1\}$. Now, let us define a group $G = \mathbb{Z}_p \times \mathbb{Z}_n$, where $\mathbb{Z}_p = \langle g \rangle$ and $\mathbb{Z}_n = \langle h \rangle$. For each S_i, we introduce a group ring element $D_i \in \mathbb{Z}[G]$ defined by

$$D_i = \sum_{j=0}^{n-1} a_{ij} g^{b_{ij}} h^j. \tag{9}$$

Given a character θ_α of the group $\mathbb{Z}_p$ defined by $\theta_\alpha(g) = \zeta_p^\alpha$ ($\alpha \in \{0, \ldots, p-1\}$), it is easy to see that $\theta_\alpha(D_i) = \sum_{j=0}^{n-1} a_{ij}\zeta_p^{\alpha b_{ij}} h^j$. The above arguments relate a set of sequences $\{S_1, \ldots, S_t\}$ to a set of group ring elements $\{D_1, \ldots, D_t\}$ in $\mathbb{Z}[G]$, which enables us to make use of the group rings to characterize the periodic complementary sequences. To present the main result of this section, we need the following two lemmas.

Lemma 1. *Let $X \in \mathbb{Z}[\mathbb{Z}_p]$, where p is a prime. Then $\chi(X) = 0$ for any non-principal character χ of $\mathbb{Z}_p$ if and only if there exists an integer n such that $X = n\mathbb{Z}_p$.*

Proof. If $X = n\mathbb{Z}_p$, then by Result 1, clearly $\chi(X) = 0$ for all non-principal characters χ. Conversely, assume that $X = \sum_{j=0}^{p-1} a_j g^j \in \mathbb{Z}[\mathbb{Z}_p]$. Let χ_i be a non-principal character defined by $\chi_i(g) = g^i$. Then we have $\chi_i(X) = \sum_{j=0}^{p-1} a_j \zeta_p^{ij} = \sigma_i(\sum_{j=0}^{p-1} a_j \zeta_p^j) = 0$, where $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ defined as $\sigma_i(\zeta_p) = \zeta_p^i$. Since $\{1, \zeta_p, \ldots, \zeta^{p-1}\}$ forms the integral basis of the algebraic integer ring $\mathbb{Z}[\zeta_p]$, we have $a_0 = a_1 = \cdots = a_{p-1}$ and therefore $X = a_0\mathbb{Z}_p$, which completes the proof. □

Lemma 2. *Let $S = (s_0, s_1, \ldots, s_{n-1})$ be a sequence over the alphabet $\{0,1\}$ and with length n. Assume the size of its support set is k. Then we have $\sum_{t=0}^{n-1} P^S(t) = k^2$, where P^S is the periodic autocorrelation function of the sequence S.*

Proof. We have that $\sum_{t=0}^{n-1} P^S(t) = \sum_{t=0}^{n-1}\sum_{j=0}^{n-1} s_j s_{j+t} = (\sum_{j=0}^{n-1} a_j)(\sum_{t=0}^{n-1} s_{j+t}) = k^2$. □

Now we are ready to present the theorem.

Theorem 1. *Using the same notation as above and letting the size of the support set of each sequence S_i be k_i for $1 \le i \le t$, then $\mathcal{S}$ is a set of periodic complementary sequences*

if and only if the set of group ring elements defined in (9) $\mathcal{D} = \{D_1, \ldots, D_t\}$ satisfies the following group ring equation

$$D_1 D_1^{(-1)} + \cdots + D_t D_t^{(-1)} = \sum_{i=1}^{t} k_i + \sum_{u=1}^{n-1} \left(\sum_{i=1}^{t} \frac{P^{T_i}(u)}{p} \mathbb{Z}_p \right) h^u, \tag{10}$$

where $P^{T_i}(u)$ is the periodic autocorrelation function of the sequence T_i.

Proof. For simplicity, we denote $\sum_{i=1}^{t} \frac{P^{T_i}(u)}{p} \mathbb{Z}_p$ by X_u. By Corollary 1, we need to show that for any character χ of G, the character values of both sides of Eq. (10) are equal. First, if χ is principal, for the left hand side of Eq. (10), it follows immediately that $\chi(\text{LHS}) = \sum_{i=1}^{t} k_i^2$. For the right hand side of Eq. (10), by noting that $\chi(X_u) = \sum_{i=1}^{t} P^{T_i}(u)$, we get:

$$\begin{aligned} \chi(\text{RHS}) &= \sum_{i=1}^{t} k_i + \sum_{u=1}^{n-1} \sum_{i=1}^{t} P^{T_i}(u) = \sum_{i=1}^{t} \left(\sum_{u=0}^{n-1} P^{T_i}(u) - P^{T_i}(0) + k_i \right) \\ &= \sum_{i=1}^{t} (k_i^2 - k_i + k_i) = \sum_{i=1}^{t} k_i^2, \end{aligned}$$

where the second last equality uses Lemma 2 and $P^{T_i}(0) = k_i$.

Next, if χ is non-principal but is principal on $\mathbb{Z}_p$, namely $\chi = \theta_0 \eta_\beta$, then

$$\begin{aligned} \chi(D_i D_i^{(-1)}) &= \chi(D_i)\overline{\chi(D_i)} = \sum_{j_1, j_2} a_{i,j_1} a_{i,j_2} \zeta_n^{\beta(j_1 - j_2)} \\ &= \sum_{v} \left(\sum_{j_2} a_{i,j_2+v} a_{i,j_2} \right) \zeta_n^{\beta v} = \sum_{v} P^{T_i}(v) \zeta_n^{\beta t}. \end{aligned}$$

Therefore we have $\chi(\text{LHS}) = \sum_{i=1}^{t} \chi(D_i D_i^{(-1)}) = \sum_{i=1}^{t} \sum_{v} P^{T_i}(v) \zeta_n^{\beta v}$. On the other hand, $\chi(\text{RHS}) = \sum_{i=1}^{t} k_i + \sum_{u=1}^{n-1} \sum_{i=1}^{t} P^{T_i}(u) \zeta_n^{\beta u} = \sum_{i=1}^{t} \left(k_i + \sum_{u=0}^{n-1} P^{T_i}(u) \zeta_n^{\beta u} - P^{T_i}(0) \right) = \sum_{i=1}^{t} \sum_{u=0}^{n-1} P^{T_i}(u) \zeta_n^{\beta u} = \chi(\text{LHS})$.

Finally, if χ is not principal on $\mathbb{Z}_p$, namely $\chi = \theta_\alpha \eta_\beta$ with $\alpha \neq 0$, we have that

$$\begin{aligned}
\chi(\text{LHS}) &= \sum_{i=1}^{t} \theta_\alpha \eta_\beta (D_i D_i^{(-1)}) = \sum_{i=1}^{t} \eta_\beta \left(\theta_\alpha(D_i) \theta_\alpha(D_i^{(-1)}) \right) \\
&= \sum_{i=1}^{t} \eta_\beta \left(\left(\sum_{j_1=0}^{n-1} a_{i,j_1} \zeta_p^{\alpha b_{i,j_1}} h^{j_1} \right) \cdot \left(\sum_{j_2=0}^{n-1} a_{i,j_2} \zeta_p^{-\alpha b_{i,j_2}} h^{-j_2} \right) \right) \\
&= \sum_{i=1}^{t} \eta_\beta \left(\sum_{j_1,j_2=0}^{n-1} a_{i,j_1} a_{i,j_2} \zeta_p^{\alpha(b_{i,j_1} - b_{i,j_2})} h^{j_1 - j_2} \right) \\
&= \sum_{i=1}^{t} \eta_\beta \left(\sum_{u=0}^{n-1} \left(\sum_{j_1} a_{i,j_1} a_{i,j_1+u} \zeta_p^{\alpha(b_{i,j_1} - b_{i,j_1+u})} \right) h^u \right) \\
&= \sum_{i=1}^{t} \eta_\beta \left(\sum_{u} \left(\sum_{j_1} (a_{i,j_1} \zeta_p^{\alpha b_{i,j_1}}) \overline{(a_{i,j_1+u} \zeta_p^{\alpha(b_{i,j_1+u})})} \right) h^u \right) \\
&= \sum_{i=1}^{t} \eta_\beta \left(\sum_{u} P^{S_i}(u)^{\sigma_\alpha} h^u \right) = \sum_{u} \left(\sum_{i=1}^{t} P^{S_i}(u)^{\sigma_\alpha} \right) \zeta_n^{\beta u} \\
&= \sum_{i=1}^{t} k_i,
\end{aligned}$$

where $\sigma_\alpha \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is defined by $\sigma_\alpha(\zeta_p) = \zeta_p^\alpha$ and the last equality uses the property that $\mathcal{S}$ is a complementary set of sequences. On the other hand, it is easy to check that $\chi(\text{RHS}) = \sum_{i=1}^{t} k_i$. This completes the proof. □

Theorem 1 characterizes the periodic complementary sequences by a group ring equation. By exploring this equation using number theory techniques, we obtain the condition for the existence of complementary sequences over the alphabet $\mathfrak{A}_p$. The following results are obtained from Theorem 1. We will make use of them to provide the conditions for the existence of complementary ℓ-HLAs in the next section.

Corollary 3. *Assume $\mathcal{S} = \{S_1, \ldots, S_t\}$ is a set of periodic complementary sequences, where each S_i has period n and alphabet $\mathfrak{A}_p$. Then the following holds:*

(1) *p must be a divisor of $\sum_{i=1}^{t} P^{T_i}(u)$ for each $1 \leq u \leq n-1$.*
(2) *if $p = 2$, the sum of the sizes of the support sets $\sum_{i=1}^{t} k_i$ must be the sum of t squares.*

Proof. The first result follows directly from the Theorem 1 since both sides of Eq. (10) belong to $\mathbb{Z}[G]$ and hence the coefficients are integers. For the second result, when $p = 2$, for any character χ of G, we have $\chi(D_i) \in \mathbb{Z}$ and $\chi(D_i^{-1}) = \chi(D_i)$. In particular, if χ is non-principal on $\mathbb{Z}_p$, we get $\sum_{i=1}^{t} k_i$ on the right hand side of Eq. (10) and the left hand side is the summation of t squares. □

We give several remarks on Theorem 1 and Corollary 3 below.

Remark 2. *In Theorem 1, the condition that p is prime is necessary. For instance, we computed the pair of complementary quaternion sequences listed in [21, page 76] and found that none of them satisfies the group equation (10).*

Let us give an application of Corollary 3 to show that there does not exist a pair of aperiodic complementary 2-HLAs over alphabet $\mathfrak{A}_p^*$ for any prime p. This result was also given in [10] but with a more tricky proof.

Proposition 4. *There does not exist a pair of aperiodic complementary 2-HLAs over alphabet $\mathfrak{A}_p^*$ for any prime p.*

Proof. By Corollary 2, a pair of aperiodic complementary 2-HLAs over $\mathfrak{A}_p^*$ will lead to a pair of periodic complementary sequences of length 7 over $\mathfrak{A}_p^*$ (note that the alphabet is not $\mathfrak{A}_p$ since from the matrix $\mathcal{T}_2$ in Example 1 we may see the shortened sequence from a 2-HLA is $(x_4, x_3, x_5, x_0, x_2, x_6, x_1)$ with alphabet the same as the 2-HLA). By Corollary 3(1) we have $p \mid 2 \cdot 7$ since $P^{T_i}(u) = 7$ for all $1 \le u \le 6$ and $i = 1, 2$. Thus there does not exist a pair of periodic complementary sequences with length 7 unless either $p = 7$ or $p = 2$. By Corollary 3(2), a pair of binary periodic complementary sequences does not exist since $7 + 7 = 14$ is not the sum of two squares. Furthermore, using MAGMA we performed an exhaustive search on a pair of sequences with period 7 and alphabet $\mathfrak{A}_7^*$; and we found that such a pair of periodic complementary sequences does not exist. □

When the alphabet of each sequence S_i is $\mathfrak{A}_p^*$, we have the following result which is of independent interest.

Theorem 2. *Assume $\mathcal{S} = \{S_1, \ldots, S_t\}$ is a set of sequences with length n and alphabet $\mathfrak{A}_p^*$, where p is a prime. Then $\mathcal{S}$ is a set of periodic complementary sequences if and only if $\mathcal{D} = \{D_1, \ldots, D_t\}$ is a $\Big(pn, p, n, \frac{tn}{p}; t\Big)$ relative difference family in $G = \mathbb{Z}_p \times \mathbb{Z}_n$ relative to $\mathbb{Z}_p \times \{1\}$, where D_i is defined as in (9). Equivalently, the following group ring equation holds*

$$D_1 D_1^{(-1)} + \cdots + D_t D_t^{(-1)} = tn + \frac{tn}{p}\Big(G - \mathbb{Z}_p \times \{1\}\Big). \tag{11}$$

Proof. It is easy to see that if the alphabet is $\mathfrak{A}_p^*$, then: (i) $k_i = n$; (ii) $T_i = (1, \ldots, 1)$ and $P^{T_i}(u) = n$ for $1 \le i \le t, 1 \le u \le n-1$. Therefore, by Theorem 1, we have that

$$\begin{aligned} D_1 D_1^{(-1)} + \cdots + D_t D_t^{(-1)} &= tn + \sum_{u=1}^{n-1} \tfrac{tn}{p}\mathbb{Z}_p h^u = tn + \tfrac{tn}{p}\mathbb{Z}_p \sum_{u=0}^{n-1} h^u \\ &= tn + \tfrac{tn}{p}\mathbb{Z}_p(\mathbb{Z}_n - 1) \\ &= tn + \tfrac{tn}{p}\Big(G - \mathbb{Z}_p \times \{1\}\Big). \end{aligned}$$

The proof is completed. □

Remark 3. *When $p = 2$, the characterization of periodic complementary sequences using difference family was given by Bömer and Antweiler in [2]. Therefore we can regard Theorem 2 as a generalization of their result.*

We have the following immediate result.

Corollary 4. *Assume a set of t periodic complementary sequences of length n and alphabet $\mathfrak{A}_p^*$ exits, then $p \mid tn$.*

5. Existence of Aperiodic Complementary Binary Hexagonal Lattice Arrays

In this section we will provide the conditions for the existence of aperiodic complementary binary ℓ-HLAs $\mathcal{C}_\ell^t = \{C_\ell^1, \ldots, C_\ell^t\}$. It is worth to mention that Ding and Tarokh in [10] found an example when $\ell = 2$ and $t = 4$. In this section we provide the conditions for the existence of $\mathcal{C}_\ell^t$ when $t = 2$ and 3.

5.1. **Pair of complementary binary hexagonal lattice arrays.** First we present two useful lemmas. For a prime divisor p of an integer x, we use the notation $o_p(x)$ to denote the highest exponent of p that divides x, i.e. $p^{o_p(x)} \mid x$ but $p^{o_p(x)+1} \nmid x$.

Lemma 3 (Fermat)**.** *An integer x can be represented as the sum of two squares if and only if $o_p(x)$ is even for all prime divisors p of x with $p \equiv 3 \mod 4$.*

Lemma 4. *Let C_ℓ be an ℓ-layer hexagonal lattice array, then there are $3\ell^2-3\ell+1$ elements in C_ℓ.*

Proof. Recall that the coordinates of the points in an ℓ-HLA are determined in (5). Then the number of points in the support set Ω_ℓ is

$$\begin{aligned} 2 \cdot \sum_{i=1}^{\ell-1} (\ell - i - 1 + (\ell-1) + 1) + 2(\ell-1) + 1 &= 2\sum_{i=1}^{\ell-1} (2\ell - i - 1) + 2\ell - 1 \\ &= 3\ell^2 - 3\ell + 1. \end{aligned}$$

This completes the proof. □

Now we can state the following theorem.

Theorem 3. *There does not exist a pair of aperiodic complementary binary ℓ-HLAs when $3\ell(\ell-1)+1$ has a prime divisor p with $p \equiv 3 \mod 4$ and $o_p(3\ell(\ell-1)+1)$ is odd.*

Proof. By Corollary 2 a pair of aperiodic complementary binary ℓ-HLAs will lead to a pair of periodic complementary sequences over the alphabet $\mathfrak{A}_2$. Further by Corollary 3(2) such a pair of periodic complementary sequences exist only if the sum of their support sets, $2(3\ell^2 - 3\ell + 1)$ (Lemma 4) is the sum of two integers. It follows from Lemma 3 that $2(3\ell^2 - 3\ell + 1)$ is the sum of two integers if and only if for all of its prime divisors p with $p \equiv 3 \mod 4$, the order $o_p(2(3\ell^2 - 3\ell + 1))$ is even. Note that $3\ell(\ell-1)+1$ is odd (since $\ell(\ell-1)$ is always even), hence the above statement is equivalent to $3\ell(\ell-1)+1$ cannot have a prime divisor $p \equiv 3 \mod 4$ and $ord_p(3\ell(\ell-1)+1)$ is odd. This completes the proof. □

The following corollary follows immediately.

Corollary 5. *There does not exist a pair of aperiodic complementary binary ℓ-layer hexagonal lattice arrays if $\ell \equiv 2, 3 \mod 4$.*

Proof. By Theorem 3, the existence of a pair of aperiodic complementary binary ℓ-HLAs implies that $3\ell(\ell-1)+1 \equiv 1 \mod 4$ (since for all prime divisors $p \equiv 3 \mod 4$, its order is even). Now assume $3\ell(\ell-1)+1 \equiv 3 \mod 4$ (note that $3\ell(\ell-1)+1$ is odd and then $3\ell(\ell-1)+1 \not\equiv 0, 2 \mod 4$). This can only happen when $3\ell(\ell-1) \equiv 2 \mod 4$, or $\ell(\ell-1) \equiv 2 \mod 4$, which is equivalent to $\ell \equiv 2, 3 \mod 4$. This completes the proof. □

By Theorem 3 and Corollary 5, we use the following table to give the existence status for a pair of aperiodic complementary binary ℓ-HLAs for ℓ up to 20. The question mark "?" denotes the existence status is undetermined. For an ℓ-HLA, we use $|C_\ell|$ to denote the number of non-zero elements in it.

One may see from Table 1 that the smallest undermined case is $\ell = 4$ for a pair of aperiodic complementary ℓ-HLAs. By Proposition 4, there are $3 \cdot 4^2 - 3 \cdot 4 + 1 = 37$ elements in a 4-HLA. Therefore the complexity for an exhaustive search for a pair of aperiodic complementary 4-HLAs is 2^{74}. We leave the following open problem for the future research.

Problem 1. *Determine the existence of a pair of aperiodic complementary binary ℓ-HLAs for the values ℓ which are not excluded in Theorem 3. In particular, determine the existence for the cases where $\ell = 4, 5, 8, 12$ as listed in Table 1.*

TABLE 1. Existence of pair of AC binary ℓ-HLAs for $1 \leq \ell \leq 20$

ℓ	Existence	Reference	ℓ	Existence	Reference
1	No	Trivial	2	No	Corollary 5
3	No	Corollary 5	4	?	
5	?		6	No	Corollary 5
7	No	Corollary 5	8	?	
9	No	Theorem 3 $\lvert C_9\rvert = 7 \cdot 31$	10	No	Corollary 5
11	No	Corollary 5	12	?	
13	No	Theorem 3 $\lvert C_{13}\rvert = 7 \cdot 67$	14	No	Corollary 5
15	No	Corollary 5	16	No	Theorem 3 $\lvert C_{16}\rvert = 7 \cdot 103$
17	No	Theorem 3 $\lvert C_{17}\rvert = 19 \cdot 43$	18	No	Corollary 5
19	No	Corollary 5	20	No	Theorem 3 $\lvert C_{20}\rvert = 7 \cdot 163$

5.2. **Triple of complementary binary hexagonal lattice arrays.** Now we consider the existence of a triple of aperiodic complementary binary ℓ-HLAs.

Lemma 5 (Legendre theorem)**.** *An integer x can be represented as the sum of three squares if and only if x is not of the form $4^a(8b+7)$, where a, b are integers.*

Theorem 4. *There do not exist aperiodic complementary binary ℓ-layer hexagonal lattice arrays $\mathcal{C}_\ell^3 = \{C_\ell^1, C_\ell^2, C_\ell^3\}$ when $\ell \equiv 4, 5 \mod 8$.*

Proof. By Lemma 5, it is clear that $3(3\ell(\ell-1)+1)$ is not the sum of three squares if $3(3\ell(\ell-1)+1)$ is of the form $4^a(8b+7)$. In this case it follows from Corollary 3(2) that there does not exist a set of 3 periodic complementary binary sequences which the sum of the sizes of the support sets equals $3(3\ell(\ell-1)+1)$. This will further show the non-existence of a set of 3 aperiodic complementary binary ℓ-HLAs by Corollary 2. Now assume $3(3\ell(\ell-1)+1) = 4^a(8b+7)$ for some a, b. Since $3(3\ell(\ell-1)+1)$ is odd, the assumption is equivalent to $3(3\ell(\ell-1)+1) = 8b+7$. After simplification we get $9\ell(\ell-1) - 4 = 8b$, hence $\ell(\ell-1) \equiv 4 \mod 8$. The rest of the proof is routine by checking only when $\ell \equiv 4, 5$ one may get $\ell(\ell-1) \equiv 4 \mod 8$. □

We run a computer experiment to search for an aperiodic complementary triple set $\mathcal{C}_\ell^3 = \{C_\ell^1, C_\ell^2, C_\ell^3\}$ for $\ell = 2$ and found no such a triple set exists. The complexity for an exhaustive search for the case $\ell = 3$ is 2^{57} (since by Proposition 4 each 3-HLA has 19 elements). We leave the following open problem.

Problem 2. *Determine the existence of complementary triple set of binary ℓ-HLAs for ℓ with $\ell \not\equiv 4, 5 \mod 8$.*

6. CONCLUSIONS

In this paper we explore the conditions for the existence of aperiodic complementary hexagonal lattice arrays over the alphabet $\mathfrak{A}_p^* = \{\zeta_p^i : 0 \leq i \leq p-1\}$, whose support set is a set of ℓ-layer consecutive hexagons. We call such a hexagonal lattice array an ℓ-HLAs for short. We first show that aperiodic complementary ℓ-HLAs lead to aperiodic complementary (and hence periodic complementary) sequences over the alphabet $\mathfrak{A}_p = \mathfrak{A}_p^* \cup \{0\}$. Through relating the sequences of period n and the alphabet $\mathfrak{A}_p$ to group ring elements in $\mathbb{Z}[\mathbb{Z}_p \times \mathbb{Z}_n]$, we provide a characterization of periodic complementary sequences

by group rings. As of independent interest, we show that set of t periodic complementary sequences with period n and the alphabet $\mathfrak{A}_p^*$ is conceptually equivalent to a $(np, p, n, \frac{tn}{p}; t)$ relative difference family in $\mathbb{Z}_p \times \mathbb{Z}_n$ relative to $\mathbb{Z}_p \times \{1\}$. Let $\mathcal{C}_\ell^t = \{C_\ell^1, \ldots, C_\ell^t\}$ be a set of aperiodic complementary binary ℓ-HLAs. Thanks to the aforementioned characterization of periodic complementary sequences, we are able to give conditions for the existence of $\mathcal{C}_\ell^t$ when $t = 2, 3$. Note that Ding and Tarokh in [10] provided examples of aperiodic complementary binary 2-HLAs when $t = 4$.

There are some cases of ℓ that we cannot determine the existence of a pair or a triple of aperiodic complementary binary ℓ-HLAs. For a pair (resp. a triple) of aperiodic complementary binary ℓ-HLAs, the smallest undermined case of its existence is $\ell = 4$ (resp. $\ell = 3$). It will be interesting to develop more conditions to exclude, or to provide constructions of them for these cases. We leave two open problems (Problems 1 and 2) for the future research.

Acknowledgement

We thank Jie Ding and Vahid Tarokh for sending us their interesting manuscript [10] on hexagonal lattice complementary arrays.

References

[1] K.T. Arasu and Q. Xiang, On the existence of periodic complementary binary sequences, Designs, Codes and Cryptography 2, 257–262, (1992).
[2] L. Bömer and M. Antweiler, Periodic complementary binary sequences, IEEE Transaction on Information Theory 36(6), 1487–1494, (1990).
[3] M. Buratti, Constructions of $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$, Discrete Mathematics 138, 169–175, (1995).
[4] M. Buratti, Recursive constructions for difference matrices and relative difference families, Journal of Combinatorial Designs 6(3), 165–182, (1998).
[5] M. Buratti, Y. Wei, D. Wu, P. Fan, M. Chen, Relative difference families with variable block sizes and their related OOCs, IEEE Transactions on Information Theory 57(11), 7489–7947, (2011).
[6] Y. Chang and C. Ding, Constructions of external difference families and disjoint difference families, Designs, Codes and Cryptography 40(2), 167–185, (2006).
[7] R. Craigen, W. Holzmann and H. Kharaghani, Complex Golay sequences: Structure and applications, Discrete Mathematics 252, 73–89, (2002).
[8] J.A. Davis, J. Jedwab, and K.W. Smith, Proof of the Barker array conjecture, Proceedings of American Mathematical Society 135, 20112018, (2007).
[9] C. Ding, Two constructions of $(v, (v-1)/2, (v-3)/2)$ difference families, Journal of Combinatorial Designs 16(2), 164–171, (2008).
[10] J. Ding and V. Tarokh, Complementary Lattice Arrays for Coded Aperture Imaging, in submission, (2014).
[11] J. H. Dinitz and P. Rbmodney, Disjoint difference families with block size 3, Utilitas Math. 52, 153–160, (1997).
[12] J. H. Dinitz and N. Shalaby, Block disjoint difference families for Steiner triple systems: $v \equiv 1$ (bmod 6), Journal of Statistical and Planning Inference 106, 77–86, (2002).
[13] S. Eliahou, M. Kervaire and B. Saffari, On Golay polynomial pairs, Advances in Applied Mathematics 12, 235–292, (1991).
[14] K. Feng, P. J. Shiue and Q. Xiang, On Aperiodic and Periodic Complementary Binary Sequences, IEEE Transaction on Information Theory 45, 296-303, (1999).
[15] R. Fuji-Hara, Y. Miao and S. Shinohara, Complete sets of of disjoint difference families and their applications, Journal of Statistical and Planning Inference 106, 87–103, (2002).
[16] M.J.E. Golay, Complementary series, IRE Transaction on Information Theory, IT-7:8287, 1961.
[17] J. Jedwab and M.G. Parker, There are no Barker arrays having more than two dimensions, Designs, Codes and Cryptography 43, 79–84, (2007).
[18] J. Jedwab and M.G. Parker, Golay complementary array pairs, Designs, Codes and Cryptography 44, 209216, (2007).
[19] S.L. Ma, Polynomial addition sets, Ph.D. Thesis, University of Hong Kong, (1985).
[20] L. Martinez, D. Z. Dokovic, A. Vera-Lopez, Existence question for difference families and construction of some new families, Journal of Combinatorial Designs 12(4), 256–270, (2004).

[21] C. Milies and S. Sehgal, An Introduction To Group Rings, Algebras and applications, Volume 1. Springer, (2002).
[22] W. Ogata, K. Kurosawa, D. R. Stinson, H. Saido, New combinatorial designs and their applications to authentication codes and secret sharing schemes, Discrete Mathematics 279, 383–405, (2004).
[23] B. Schmidt, Cyclotomic integers and finite geometry, Journal of American Mathematical Society 12(4), 929-952, (1999).
[24] C.C. Tseng and C. Liu, Complementary sets of sequences, IEEE Transaction on Information Theory 18(5), 644-652, (2003).
[25] R. M. Wilson, Cyclotomy and difference families in elementary Abelian groups, Journal of Number Theory 4, 17–42, (1972).

Department of Electrical and Computer Engineering, University of Waterloo, Canada
E-mail address, Yin Tan: yin.tan@uwaterloo.ca

Department of Electrical and Computer Engineering, University of Waterloo, Canada
E-mail address, Guang Gong: ggong@uwaterloo.ca