Two classes of cyclic frames from finite geometries

Su Wang and Jinhua Wang*
School of Sciences, Nantong University
Nantong 226007, P. R. China
jhwang@ntu.edu.cn (J. Wang)

Abstract

Cyclic frames or partially partition-type cyclic relative difference families are combinatorial structures that are used to produce series of optimal families consisting of a single frequency hopping sequence and optimal difference systems of sets for code synchronization. In this paper, two new classes of cyclic frames from finite geometries are obtained.

Keywords : Cyclic frame; Cyclic relative difference family; Partially partition-type

AMS Subject Classifications: 05B05; 05C99; 51E05

1 Introduction

Let k be a positive integer. A *group divisible design* (k,λ)-GDD is a triple $(X,\mathcal{G},\mathcal{B})$ where X is a finite set of points, $\mathcal{G}$ is a set of subsets of X called groups which partition X, $\mathcal{B}$ is a collection of k-subsets of X called blocks such that every pair of points from distinct groups occurs in exactly λ blocks, and no pair of points belonging to a group occurs in any block. We use the usual exponential notation for the type of GDDs. Thus a GDD of type $1^i2^j\ldots$ is one in which there are i groups of size 1, j groups of size 2, and so on. A (k,λ)-GDD of type 1^v is just a *balanced incomplete block design* denoted by (v,k,λ)-BIBD. A (k,λ)-*frame* of type T is a (k,λ)-GDD $(X,\mathcal{G},\mathcal{B})$ of type T in which the collection $\mathcal{B}$ of blocks can be partitioned into holey resolution classes each of which partitions $X\backslash G_i$ for some $G_i\in\mathcal{G}$. Let $(X,\mathcal{G},\mathcal{B})$ be a (k,λ)-GDD of type g^u, and σ be a permutation on X.

* Corresponding author.

For any subset $T = \{x_1, \ldots, x_k\} \subset X$, define $T^\sigma = \{x_1^\sigma, \ldots, x_k^\sigma\}$. If $\mathcal{G}^\sigma = \{G^\sigma : G \in \mathcal{G}\} = \mathcal{G}$ and $\mathcal{B}^\sigma = \{B^\sigma : B \in \mathcal{B}\} = \mathcal{B}$, then σ is an automorphism of the GDD $(X, \mathcal{G}, \mathcal{B})$. Any automorphism σ partitions $\mathcal{B}$ into equivalence classes called the block orbits of $\mathcal{B}$ under σ. An arbitrary set of representatives for these block orbits of $\mathcal{B}$ is the base blocks of the GDD. If there is an automorphism consisting of a single cycle of length $|X| = gu$, then the (k, λ)-GDD is said to be *cyclic* and denoted by (k, λ)-CGDD. For a (k, λ)-CGDD of type g^u, the point set X can be identified with Z_{gu}. In this case, the design has an automorphism $\sigma : i \mapsto i + 1 \pmod{gu}$, and each group must be the subgroup uZ_g of Z_{gu} or its cosets. In the remainder of this paper, when we say a (k, λ)-CGDD, we always mean a (k, λ)-CGDD in which each of its block orbits under the automorphism σ contains exactly gu distinct blocks. In a $(k, k-1)$-frame of type g^u, it is well known (see [6], for example) that there are g holey resolution classes associated with each group, and there are altogether gu holey resolution classes. If the underlying GDD of a $(k, k-1)$-frame of type g^u is cyclic with respect to an automorphism $\sigma : i \mapsto i+1 \pmod{gu}$ of order gu, such that the blocks of the jth holey resolution class $\mathcal{R}_j$ are the jth translates of the blocks of the resolution class $\mathcal{R}_0$, i.e., $\mathcal{R}_j = \mathcal{R}_0^{\sigma^j} = \mathcal{R}_0 + j \pmod{gu}$ for all $j \in Z_{gu}$, then the frame is said to be *cyclic* with respect to σ. The class $\mathcal{R}_0$ is an initial holey resolution class of this cyclic frame. A cyclic $(k, k-1)$-frame of type 1^u is just a *near resolvable cyclic design* .

A *cyclic* (gu, g, k, λ)*-relative difference family* [or (gu, g, k, λ)-CRDF in short] is a collection $\mathcal{B}$ of k-subsets (called base blocks) of Z_{gu} with the property that each element of $Z_{gu} \setminus uZ_g$ occurs exactly λ times in $\Delta\mathcal{B}$, i.e., the multiset of internal differences among the blocks of $\mathcal{B}$. In the case that $g = 1$, we simply call it a (u, k, λ)-CRDF. A (gu, g, k, λ)-CRDF is said to be *partially partition-type* if $\mathcal{B}$ forms a partition of $Z_{gu} \setminus uZ_g$. The number of base blocks in a (gu, g, k, λ)-CRDF and a partially partition-type (gu, g, k, λ)-CRDF are $\lambda(gu - g)/(k(k-1))$ and $(gu - g)/k$, respectively, and hence a necessary condition for the existence of a partially partition type (gu, g, k, λ)-CRDF is that $\lambda \equiv 0 \pmod{k-1}$ and $(gu - g) \equiv 0 \pmod{k}$. It is clear that a partially partition-type $(gu, g, k, k-1)$-CRDF $\mathcal{B}$ forms an initial holey resolution class of a cyclic $(k, k-1)$-frame of type g^u. Converse the initial holey resolution class $\mathcal{R}_0$ of a cyclic $(k, k-1)$-frame of type g^u is just a partially partition-type $(gu, g, k, k-1)$-CRDF. Note that a partially partition-type (gu, g, k, λ)-CRDF are also called a partition-type $((gu - g)/g)$-difference packing $(gu, k, k-1)$ with a u-regular hole uZ_g in [5]. For more details on frames, the reader is referred to [6].

In 1986, Stinson introduced firstly the concept of frame for constructing Kirkman triple systems (see, [13, 14]). So far, the existence and applications of frames have been extensively investigated by many researchers (see,

[6], and references therein). Cyclic frames or partially partition-type cyclic relative difference families are used to produce series of optimal families consisting of a single frequency hopping sequence [8, 9] and optimal difference systems of sets for constructing comma-free codes that allow for synchronization in the presence of errors [4, 11, 12, 15].

In this paper, we describe two geometric constructions for cyclic frames from projective space PG$(2t+1,q)$s and affine geometry AG(n,q)s. Two new classes of cyclic frames are obtained.

For the ease of descriptions, we use some notations. For given subsets A, B and a collection $\mathcal{F}$ of subsets in Z_v, let ΔA and $\Delta\mathcal{F}$ be multisets defined by $\Delta A = \{x-y : x,y \in A, x \neq y$ and $\Delta\mathcal{F} = \bigcup_{A\in\mathcal{F}} \Delta A$, respectively. The notation $\Delta A = \lambda B$, where λ is a positive integer, means that each element of B occurs exactly λ times in ΔA.

2 Cyclic Frames from a Projective Space

In this section, we describe a geometric construction for cyclic frames from some special t-flats in a projective space PG$(2t+1,q)$.

Let q be a prime power and $n \geq 3$ be an integer. An *n-dimensional projective space* PG(n,q) has $v = (q^{n+1}-1)/(q-1)$ points, which can be represented by the elements of Z_v, and $(q^{n+1}-1)(q^n-1)\cdots(q^{n-k+1}-1)/(q^{k+1}-1)(q^k-1)\cdots(q-1)$ k-flats, i.e., k-dimensional subspaces, each having $(q^{k+1}-1)/(q-1)$ points. An $(n-1)$-flat of PG(n,q) is called a hyperplane. Consider t-flats in PG$(2t+1,q)$. In this case, there is a t-flat $H = \{0,u,2u,\ldots,(g-1)u\} = uZ_g$, where $u = q^{t+1}+1$ and $g = (q^{t+1}-1)/(q-1)$. It is clear that there are g $(t+1)$-flats containing H in PG$(2t+1,q)$ (also see, for example, [1, 2, 3]). Let $W = \{F_1, F_2, \ldots, F_g\}$ be the set of all the $(t+1)$-flats. There is an automorphism σ of PG$(2t+1,q)$ such that $\sigma : x \mapsto x+u$, which fixes the t-flat H. This implies that W can be generated from F_1, i.e., $W = \{F_1, \sigma F_1, \ldots, \sigma^{g-1}F_1\}$. Clearly, $\Delta F_i = \Delta F_j$ for any $F_i, F_j \in W$. Let A_i be the affine part of F_i,i.e.,$A_i = F_i \setminus H$ for $i = 1,2,\ldots,g$. The following result comes from [7, 8].

Lemma 2.1 *For any $i = 1,2,\ldots,g$, $\Delta A_i = (q-1)(Z_{gu} \setminus uZ_g)$, where $g = (q^{t+1}-1)/(q-1), u = q^{t+1}+1$.*

Theorem 2.2 *Let $W = \{F_1, F_2, \ldots, F_g\}$ be the set of all the $(t+1)$-flats of PG$(2t+1,q)$ containing t-flat $H = uZ_g$, where $g = (q^{t+1}-1)/(q-1)$, and set $A_i = F_i \setminus H, u = q^{t+1}+1, k = q^{t+1}$. Then $\mathcal{B} = \{A_1, A_2, \ldots, A_g\}$ forms a partially partition-type $(gu, g, k, k-1)$-CRDF. And hence there exists a cyclic $(k, k-1)$-frame of type g^u.*

Proof. Since H is the t-flat fixed by σ, and $F_1, F_2, \ldots, F_g$ are exactly the $(t+1)$-flats containing H, we have that $\{H, A_1, \ldots, A_g\}$ form a partition

of PG(n,q). Meanwhile it follows from Lemma 2.1 that

$$\Delta\mathcal{B} = \bigcup_{i=1}^{g} \Delta A_i = g(q-1)(Z_{gu} \setminus H) = (k-1)(Z_{gu} \setminus uZ_g).$$

The assertion follows then. □

Again carefully observing the affine part A_1 of F_1, we find that A_1 has the following property by Theorem 2.2.

Lemma 2.3 *Let the conditions be as in Theorem 2.2. Let* $e|gcd(q-1,t+1)$, *and* $A^{(e)} = A_1 \pmod{\frac{gu}{e}}$. *Then* $A^{(e)}$ *is a* $(\frac{gu}{e}, \frac{g}{e}, k, e(q-1))$*-CRDF and* $A^{(e)} \pmod{u}$ *forms a partition of* $Z_u \setminus \{0\}$.

Proof. Since $e|gcd(q-1,t+1)$,we have $q \equiv 1 \pmod{e}$ and $t+1 \equiv 0 \pmod{e}$. Thus $g = q^t + q^{t-1} + \cdots + q + 1 = t+1 \equiv 0 \pmod{e}$. By lemma 2.1, we obtain

$$\Delta A^{(e)} = \Delta A_1 \pmod{\frac{gu}{e}} = e(q-1)(Z_{\frac{gu}{e}} \setminus uZ_{\frac{g}{e}}).$$

This establishes the first assertion. Since $A_i = A_1 + (i-1)u$, $1 \le i \le g$, we have $A_i \pmod{u} = A^{(e)} \pmod{u}$. From $\mathcal{B} = \bigcup_{i=1}^{g} A_i = Z_{gu} \setminus uZ_g$ in Theorem 2.2, we obtain $A^{(e)} \pmod{u} = Z_u \setminus \{0\}$. This completes the proof. □

Furthermore, by Lemma 2.3 we have

Theorem 2.4 *Let the conditions be as in Lemma 2.3. Then* $\mathcal{B}^{(e)} = \{A^{(e)} + iu : 0 \le i < \frac{g}{e}\}$ *is a partially partition-type* $(\frac{gu}{e}, \frac{g}{e}, k, k-1)$*-CRDF. And hence there exists a cyclic* $(k, k-1)$*-frame of type* $(\frac{g}{e})^u$.

Proof. By Lemma 2.3, we have

$$\Delta\mathcal{B}^{(e)} = \frac{g}{e}\Delta A^{(e)} = (k-1)(Z_{\frac{gu}{e}} \setminus uZ_{\frac{g}{e}})$$

Again by Lemma 2.3, $A^{(e)} \pmod{u} = Z_u \setminus \{0\}$, so

$$\bigcup_{A \in \mathcal{B}^{(e)}} A = \bigcup_{i=0}^{\frac{g}{e}-1} (A^{(e)} + iu) = Z_{\frac{gu}{e}} \setminus uZ_{\frac{g}{e}}.$$

This completes the proof. □

We illustrate Theorems 2.2 and 2.4 with the following example.

Example 2.5 *Here we give an example in* $PG(3,3)$. *We take a primitive element* x *of* $GF(3^4)$ *with minimal polynomial* $x^4+2x+1=0$, *so that the point set is represented by* Z_{40}, *and* $H=\{0,10,20,30\}$. *The following* A_i*'s are the affine parts of* 4 2*-flats containing* H.

$A_1=\{\ 1,\ 2,\ 9,13,15,16,18,24,37\}$, $A_2=\{\ 7,11,12,19,23,25,26,28,34\}$,

$A_3=\{\ 4,17,21,22,29,33,35,36,38\}$, $A_4=\{\ 3,\ 5,\ 6,\ 8,14,27,31,32,39\}$.

By Theorem 2.2, $\{A_1,\ldots,A_4\}$ *forms a partially partition-type* $(40,4,9,8)$*-CRDF. And hence there exists a cyclic* $(9,8)$*-frame of type* 4^{10}. *Furthermore, applying Lemma 2.3 with* $e=2$, *we get* $A^{(2)}$ *from* A_1 *modulo 20 as follows*

$$A^{(2)}=\{\ 1,\ 2,\ 9,13,15,16,18,\ 4,7\}.$$

Then $\mathcal{B}^{(2)}=\{A^{(2)}+10i : 0\le i<2\}$ *is a partially partition-type* $(20,2,9,8)$*-CRDF. And hence there exists a cyclic* $(9,8)$*-frame of type* 2^{10}.

3 Cyclic Frames from an Affine Geometry

In this section, we describe another geometric construction for cyclic frames from an affine geometry $\mathrm{AG}(n,q)$.

Let q be a prime power, n a positive integer and let $V(n,q)$ denote the n-dimensional vector space over $\mathrm{GF}(q)$. A *d-flat* in $V(n,q)$ is a subspace of $V(n,q)$ having dimension d or an additive coset of such a subspace. 0-Flats, 1-flats and $(n-1)$-flats are called *points, lines* and *hyperplanes*, respectively. A system consisting of all the vectors (points), all the d-flats of $V(n,q)$ and their incidence relation is called an *affine geometry*, denoted by $\mathrm{AG}(n,q)$, and it is well known (see, for example, [1, 2, 3]) that the set $\mathcal{F}_d$ of all d-flats in $\mathrm{AG}(n,q)$ forms the set of blocks of a balance incomplete block design (BIBD). Here we are interested in all lines (1-flats) of $\mathrm{AG}(n,q)$. Let α be a primitive element of $\mathrm{GF}(q^n)$, then the elements of $\mathrm{GF}(q^n)$ can be represented by $\alpha^\infty(=0),\alpha^0(=1),\alpha,\ldots,\alpha^{q^n-2}$. Therefore, there exists a one-to-one correspondence between the point-set of $\mathrm{AG}(n,q)$ and $Z_{q^n-1}\cup\{\infty\}$, and in this case, the mapping $\sigma: i\mapsto i+1 \pmod{q^n-1}$ and $\infty\mapsto\infty$ on $Z_{q^n-1}\cup\{\infty\}$ is an automorphism of $\mathrm{AG}(n,q)$. So, in what follows, we identify the point-set of $\mathrm{AG}(n,q)$ with $Z_{q^n-1}\cup\{\infty\}$. It is clear that $\mathrm{GF}(q)=\{0,1,\alpha^u,\ldots,\alpha^{(q-2)u}\}$, where $u=(q^n-1)/(q-1)$, and $L_{i,0}=\alpha^i\mathrm{GF}(q)=\{0,\alpha^i,\alpha^{u+i},\ldots,\alpha^{(q-2)u+i}\}$, $0\le i\le u-1$ are exactly all 1-dimensional subspace of $V(n,q)$. Let $L_{i,j}, 0\le j\le q^{n-1}-1$ be all cosets of $L_{i,0}$ in $V(n,q)$, then all lines (1-flats) of $\mathrm{AG}(n,q)$ are exactly $L_{i,j}, 0\le i\le u-1, 0\le j\le q^{n-1}-1$. Furthermore, let $\mathcal{L}_i=\{L_{i,j} : 0\le j\le q^{n-1}-1\}$,

then $\mathcal{L}_i, 0 \le i \le u-1$ are exactly u resolution classes of lines in $\mathrm{AG}(n,q)$. These resolution classes have the following property.

Lemma 3.1 *If $L_{i,j} \in \mathcal{L}_i$, then $\alpha^{ku}L_{i,j} = \{\alpha^{ku}\beta : \beta \in L_{i,j}\} \in \mathcal{L}_i$. When $j = 0, \alpha^{ku}L_{i,j} = L_{i,0}$ for $0 \le k \le q-2$; when $j \ne 0$, $\alpha^{k_1 u}L_{i,j} \ne \alpha^{k_2 u}L_{i,j}$ for $0 \le k_1 \ne k_2 \le q-2$.*

Proof. For $j = 0$, it is obvious that $\alpha^{ku}L_{i,j} = L_{i,0}$. Now let $L_{i,j} \in \mathcal{L}_i$, then there is a $\alpha^l \in \mathrm{GF}(q^n)$ such that $L_{i,j} = L_{i,0} + \alpha^l$. Hence $\alpha^{ku}L_{i,j} = \alpha^{ku}L_{i,0} + \alpha^{ku+l} = L_{i,0} + \alpha^{ku+l}$, this shows that $\alpha^{ku}L_{i,j}$ is a coset of $L_{i,0}$, i.e.,$\alpha^{ku}L_{i,j} \in \mathcal{L}_i$. For $j \ne 0$, let $L_{i,j} = \{\alpha^{d_1}, \alpha^{d_2}, \ldots, \alpha^{d_q}\}$, then $d_r \ne d_s \pmod u$ for all $1 \le r \ne s \le q$. If $\alpha^{k_1 u}L_{i,j} = \alpha^{k_2 u}L_{i,j}$, then $\alpha^{k_1 u + d_1} = \alpha^{k_2 u + d_l}$ for some $1 \le l \le q$. This implies that $k_1 u + d_1 \equiv k_2 u + d_l \pmod{q^n - 1}$, hence $d_1 \equiv d_l \pmod u$. This is a contradiction. □

Now we view $L_{i,j}$ as a subset of $Z_{q^n-1} \cup \{\infty\}$. Clearly, $L_{i,0} = \{\infty, i, u+i, \ldots, (q-2)u+i\}$. Define a mapping $\varphi : i \mapsto u + i \pmod{q^n - 1}$ and $\infty \mapsto \infty$ on $Z_{q^n-1} \cup \{\infty\}$, then $\varphi = \sigma^u$. By Lemma 3.1, The automorphism φ partitions $\mathcal{L}_i$ into equivalence classes called the line orbits of $\mathcal{L}_i$ under φ. An arbitrary set of representatives for these line orbits of $\mathcal{L}_i$ is the base lines of the resolution $\mathcal{L}_i$. Without loss of generality, we denote the base lines of the resolution $\mathcal{L}_i$ by $\{L_{i,0}, L_{i,1}, \ldots, L_{i,v}\}$, where $v = \frac{q^{n-1}-1}{q-1}$. Thus we can rewrite $\mathcal{L}_i$ as follows

$$\mathcal{L}_i = \{L_{i,0}, L_{i,1}, \ldots, L_{i,v}, L_{i,v+1}, \ldots, L_{i,(q-1)v}\}$$

where $L_{i,kv+l} = \varphi^k L_{i,l} = ku + L_{i,l}, 0 \le k \le q-2, 1 \le i \le v$.

Lemma 3.2 *Let $\mathcal{B} = \{L_{0,j} : 1 \le j \le q^{n-1} - 1\}$, i.e.,$\mathcal{B} = \mathcal{L}_0 \setminus \{L_{0,0}\}$. Then $\mathcal{B}$ forms a partially partition-type $(q^n - 1, q-1, q, q-1)$-CRDF. And hence there exists a cyclic $(q, q-1)$-frame of type $(q-1)^{\frac{q^n-1}{q-1}}$.*

Proof. Since $\mathcal{L} = \bigcup_{i=0}^{u-1} \mathcal{L}_i$ forms a $(q^n, q, q-1)$-BIBD, and all lines in $\mathrm{AG}(n,q)$ are generated from a set of base lines $\mathcal{L}_0 = \{L_{0,j} : 0 \le j \le q^{n-1} - 1\}$ by the automorphism $\sigma : i \mapsto i + 1 \pmod{q^n - 1}$ and $\infty \mapsto \infty$ on $Z_{q^n-1} \cup \{\infty\}$. So, we have

$$\Delta\mathcal{B} = \Delta\mathcal{L}_0 - \Delta L_{0,0}$$

$$= (q-1)(Z_{q^n-1} \setminus \{0\}) - (q-1)(uZ_{q-1} \setminus \{0\}) = (q-1)(Z_{q^n-1} \setminus uZ_{q-1}).$$

Observe that $\mathcal{L}_0$ forms a partition of $\mathrm{AG}(n,q)$, thus $\mathcal{B}$ forms a partition of $Z_{q^n-1} \setminus uZ_{q-1}$. The assertion follows then. □

Lemma 3.3 *Let* $\mathcal{A} = \{L_{0,j} : 1 \le j \le v\}$. *Then* $\mathcal{A}$ *forms a* $(q^n - 1, q - 1, q, 1)$*-CRDF. Furthermore,* $\mathcal{A}_{\pmod u} = \{L_{0,j} \pmod u : 1 \le j \le v\}$ *forms a partition of* $Z_u \setminus \{0\}$.

Proof. Recall that $\Delta\mathcal{B} = (q-1)(Z_{q^n-1} \setminus uZ_{q-1})$ in Lemma 3.2 and note that $\Delta L_{0,kv+j} = \Delta L_{0,j}$ for $k = 0, 1, \ldots, q-2$, we have $\Delta\mathcal{B} = (q-1)\Delta\mathcal{A}$. So, $\Delta\mathcal{A} = (Z_{q^n-1} \setminus uZ_{q-1})$. This shows that $\mathcal{A}$ forms a $(q^n - 1, q-1, q, 1)$-CRDF. The second assertion follows the fact that $\mathcal{B}$ forms a partition of $Z_{q^n-1} \setminus uZ_{q-1}$ and $\mathcal{B} = \bigcup_{L\in\mathcal{A}} \bigcup_{k=0}^{q-1}(L + ku)$. □

Lemma 3.4 *Let* e *be a positive integer and* $e|(q-1)$, *and let* $D_j^{(e)} = L_{0,j} \pmod{\frac{q-1}{e}u}$, $\mathcal{D}^{(e)} = \{D_j^{(e)} : 1 \le j \le v\}$. *Then* $\mathcal{D}^{(e)}$ *forms a* $(\frac{q^n-1}{e}, \frac{q-1}{e}, q, e)$*-CRDF and* $\mathcal{D}^{(e)}_{\pmod u} = \{D_j^{(e)} \pmod u : 1 \le j \le v\}$ *forms a partition of* $Z_u \setminus \{0\}$.

Proof. Let $\mathcal{A}$ be defined as in Lemma 3.3. First observe that $\mathcal{D}^{(e)} = \mathcal{A}_{\pmod{\frac{q-1}{e}u}}$ and $\Delta\mathcal{A} = Z_{q^n-1} \setminus uZ_{q-1}$ from Lemma 3.3. Thus

$$\Delta\mathcal{D}^{(e)} = \Delta\mathcal{A}_{\pmod{\frac{q-1}{e}u}} = e(Z_{\frac{q^n-1}{e}} \setminus uZ_{\frac{q-1}{e}}).$$

This shows that $\mathcal{D}^{(e)}$ is a $(\frac{q^n-1}{e}, \frac{q-1}{e}, q, e)$-CRDF. Since $\mathcal{D}^{(e)}_{\pmod u} = \mathcal{A}_{\pmod u}$, the second assertion follows from Lemma 3.3. □

The following result is an improvement of the partially partition-type CRDF in Lemma 3.2, meanwhile, it also improves the result of the relative difference set in [10].

Theorem 3.5 *Let* q *be a prime power,* $1 \le e \le q-1$ *and* $e|(q-1)$. *Then there exists a partially partition-type* $(\frac{q^n-1}{e}, \frac{q-1}{e}, q, q-1)$*-CRDF. And hence there exists a cyclic* $(q, q-1)$*-frame of type* $(\frac{q-1}{e})^{\frac{q^n-1}{q-1}}$.

Proof. Let

$$\mathcal{B} = \{D_j^{(e)} + ku : D_j^{(e)} \in \mathcal{D}^{(e)}, 0 \le k \le \frac{q-1}{e} - 1\},$$

where $\mathcal{D}^{(e)}$ defined as in Lemma 3.4. Thus

$$\Delta\mathcal{B} = \bigcup_{D_j^{(e)}\in\mathcal{D}^{(e)}} \bigcup_{k=0}^{\frac{q-1}{e}-1} \Delta(D_j^{(e)} + ku)$$

$$= \frac{q-1}{e}\Delta\mathcal{D}^{(e)} = (q-1)(Z_{\frac{q^n-1}{e}} \setminus uZ_{\frac{q-1}{e}}).$$

The last equality is from Lemma 3.4. Again from Lemma 3.4, $\mathcal{D}^{(e)}_{\pmod u}$ is a partition of $Z_u \setminus \{0\}$, so $\mathcal{B}$ forms a partition of $Z_{\frac{q^n-1}{e}} \setminus uZ_{\frac{q-1}{e}}$. This completes the proof. □

Here giving an example to illustrate our construction.

Example 3.6 *Here we give an example in* $AG(3,5)$. *We take a primitive element* x *of* $GF(5)$ *with minimal polynomial* $x^3+x^2+2=0$, *so that the point set is represented by* $Z_{124}\cup\{\infty\}$, *and* $L_{0,0}=\{\infty,0,31,62,93\}$,$H=\{0,31,62,93\}$. *Take 6 representations from the resolution class* $\mathcal{L}_0$ *as follows*

$$L_{0,1}=\{1,29,80,84,99\}, L_{0,2}=\{2,55,65,101,113\}, L_{0,3}=\{4,42,44,76,81\},$$

$$L_{0,4}=\{5,21,28,48,123\}, L_{0,5}=\{7,15,71,72,89\}, L_{0,6}=\{12,23,26,47,56\}.$$

Set $\mathcal{A}=\{L_{0,j}:1\le j\le 6\}$ *and* $\mathcal{B}=\{L+31k:L\in\mathcal{A},0\le k\le 3\}$. *Then* $\mathcal{B}$ *forms a partially partition-type* $(124,4,5,4)$-*CRDF by Theorem 3.5 with* $e=1$, *and hence there exists a cyclic* $(5,4)$-*frame of type* 4^{31}. *Furthermore, applying Lemma 3.4 with* $e=2$, *we get* $D_j^{(2)}$ *from* $L_{0,j}$ *modulo 62 as follows*

$$D_1^{(2)}=\{1,29,18,22,37\}, D_2^{(2)}=\{2,55,3,39,51\}, D_3^{(2)}=\{4,42,44,14,19\},$$

$$D_4^{(2)}=\{5,21,28,48,61\}, D_5^{(2)}=\{7,15,9,10,27\}, D_6^{(2)}=\{12,23,26,47,56\}.$$

Set $\mathcal{B}^{(2)}=\{D_j^{(2)}+31k:j=1,2,\ldots,6,k=0,1\}$. *Then* $\mathcal{B}^{(2)}$ *forms a partially partition-type* $(62,2,5,4)$-*CRDF by Theorem 3.5 with* $e=2$, *and hence there exists a cyclic* $(5,4)$-*frame of type* 2^{31}.

Acknowledgements
The author would like to thank the referee for his helpful comments and suggestions. This research is supported by the National Natural Science Foundations of China under Grant No. 10971252 and No.61272424.

References

[1] Anderson I.: Combinatorial Designs: Constructions and Methods. Chichester: Ellis Horwood, 1990

[2] Beth T.,Jungnickel D., Lenz H.: Design Theory, 2nd ed., vol. 1 and 2. Cambridge: Cambridge University Press, 1999

[3] Beutelspacher A.: Classical Geometries, in The CRC Handbook of Combinatorial Designs. C. J. Colbourn and J. H. Dinitz, Eds., Boca Raton, FL: CRC Press, pp. 694-708, 1996

[4] Fan C., Lei J., Shan X.: Constructions of optimal difference systems of sets. Science China Math. 54, 173-184 (2011)

[5] Fuji-Hara R., Miao Y., Mishima M.: Optimal frequency hopping sequences: A combinatorial approach. IEEE Trans. Inform. Theory 50, 2408-2420 (2004)

[6] Furino S., Miao Y., Yin J.: Frames and Resolvable Designs: Uses, Constructions, and Existence. CRC Press, Boca Raton, FL, 1996

[7] Fuji-Hara R., Munemasa A., Tonchev V D.: Hyperplane partitions and difference systems of sets. J. Combin. Theory, Ser. A 113, 1689-1698 (2006)

[8] Ge G., Fuji-Hara R., Miao Y.: Further combinatorial constructions for optimal frequency-hopping sequences. J. Combin. Theory, Ser. A 113, 1699-1718 (2006)

[9] Ge G., Miao Y., Yao Z.: Optimal frequency hopping sequences: auto- and cross-correlation properties. IEEE Trans. Inf. Theory 55, 867-879 (2009)

[10] Koukouvinos C., Whiteman A L.: Relative difference sets. J. Combin. Theory, Ser. A 74, 153-157 (1996)

[11] Lei L., Fan C.: Optimal difference systems of sets and partition-type cyclic difference packings. Des. Codes Cryptogr. 58, 135-153 (2010)

[12] Levenshtein V I.: Combinatorial problems motivated by comma-free codes. J. Combin. Des. 12, 184-196 (2004)

[13] Stinson D R.: The equivalence of certain incomplete transversal designs and frames. Ars Combin. 22, 81-87 (1986)

[14] Stinson D R.: Frames for Kirkman triples systems. Discrete Math. 65, 289-300 (1987)

[15] Wang X., Wang J.: Optimal difference systems of sets and difference sets. Aequat. Math. 82, 155-164 (2011)