

External Difference Families

Yanxun Chang

Beijing Jiaotong University

E-mail: yxchang@center.njtu.edu.cn

1. Introduction

Let $(G, +)$ be an Abelian group of order v . A (v, k, λ) difference family over G is a collection of k -subsets of X , $\mathcal{D} = \{D_1, D_2, \dots, D_u\}$, such that the multiset union

$$\bigcup_{i=1}^u \{x - y : x, y \in D_i, x \neq y\} = \lambda(G \setminus \{0\}).$$

Difference families are well studied and have applications in coding theory and cryptography. Recently, Ogata, Kurosawa, Stinson and Saido introduced a new type of combinatorial designs, *external difference families*, which are related to difference families and have applications in authentication codes and secret sharing.

Let $(G, +)$ be an Abelian group of order v . A $(v, k, \lambda; u)$ external difference family $((v, k, \lambda; u)$ -EDF in short) \mathcal{D} over G is a collection of u k -subsets of X , $\mathcal{D} = \{D_1, D_2, \dots, D_u\}$, such that the multiset union

$$\bigcup_{1 \leq i \neq j \leq u} (D_i - D_j) = \lambda(G \setminus \{0\}),$$

where $D_i - D_j$ is the multiset $\{x - y : x \in D_i, y \in D_j\}$.

It is easily seen that if a $(v, k, \lambda; u)$ -EDF over G exists, then

$$\lambda(v - 1) = k^2 u(u - 1). \quad (1)$$

Note that in an external difference family the blocks D_i 's are required to be pairwise disjoint, while this is not the case in difference families. They are different combinatorial designs, but are related.

2. A connection between EDFs and DDFs

Let $Z[G]$ denote the ring of formal polynomials

$$Z[G] = \left\{ \sum_{g \in G} a_g X^g : a_g \in Z \right\},$$

where X is an indeterminate. The ring $Z[G]$ has operations given by

$$\sum_{g \in G} a_g X^g + \sum_{g \in G} b_g X^g = \sum_{g \in G} (a_g + b_g) X^g$$

and

$$\left(\sum_{g \in G} a_g X^g \right) \left(\sum_{g \in G} b_g X^g \right) = \sum_{h \in G} \left(\sum_{g \in G} a_g b_{h-g} \right) X^h.$$

The zero and unit of $Z[G]$ are $\sum_{g \in G} 0X^g := 0$ and $X^0 := 1$, respectively. If S is a subset of G , we will identify S with the group ring element $S(X) = \sum_{g \in S} X^g$.

With the above convention, we can restate the definition of a $(v, k, \lambda; u)$ -EDF $\mathcal{D} = \{D_1, D_2, \dots, D_u\}$ over G as

$$\sum_{1 \leq i \neq j \leq u} D_i(X)D_j(X^{-1}) = -\lambda + \lambda G(X). \quad (2)$$

The following proposition follows directly from (2).

Proposition 0.1 *Let $(G, +)$ be an Abelian group of order v , and let $\mathcal{D} = \{D_1, D_2, \dots, D_u\}$ be a collection of pairwise disjoint k -subsets of G .*

Then \mathcal{D} is a $(v, k, \lambda; u)$ -EDF in G if and only if

$$D(X)D(X^{-1}) - \sum_{i=1}^u D_i(X)D_i(X^{-1}) = -\lambda + \lambda G(X),$$

where $D = \cup_{i=1}^u D_i$.

Let $(G, +)$ be an Abelian group of order v and let H be a subgroup of G with g elements. A (G, H, k, λ) *relative difference family* (or (G, H, k, λ) -DF in short) is a collection $\mathcal{F} = \{B_i : i \in I\}$ of k -subsets (called *base blocks*) of G with the property that its list of differences $\Delta\mathcal{F} = \cup_{i \in I} \Delta B_i$ is λ times $G \setminus H$ where $\Delta B_i = \{a - b : a, b \in B_i, a \neq b\}$.

In the case that $g = 1$, we simply call it a (G, k, λ) -DF (or (v, k, λ) -DF over G).

The number of base blocks in a (G, H, k, λ) -DF is $\lambda(|G| - |H|)/(k(k - 1))$, and hence a necessary condition for the existence of a (G, H, k, λ) -DF is that $\lambda(|G| - |H|) \equiv 0 \pmod{k(k - 1)}$ holds. When G is the cyclic group Z_v and H is a subgroup of order g in Z_v , then $H = (v/g)Z_v = \{0, v/g, 2v/g, \dots, (g - 1)v/g\}$. The $(Z_v, (v/g)Z_v, k, \lambda)$ -DF is called a (v, g, k, λ) cyclic relative difference family, and denoted by (v, g, k, λ) -CDF.

Let G be an Abelian group of order v , and let H be a subgroup of G with g elements. A (G, H, k, λ) -DF $\mathcal{F} = \{B_i : i \in I\}$ is called *disjoint*, denoted by (G, H, k, λ) -DDF, if the base blocks of \mathcal{F} are mutually disjoint and $\cup_{i \in I} B_i \subseteq G \setminus H$. In the case $g = 1$ or $H = \{0\}$, we write a (G, H, k, λ) -DDF briefly as a (G, k, λ) -DDF (or (v, k, λ) -DDF over G).

Let G be an Abelian group of order v , and let $\mathcal{D} = \{D_1, D_2, \dots, D_u\}$ be a $(v, k, \lambda; u)$ -EDF over G . In the case that \mathcal{D} is a partition of $G \setminus \{0\}$, $ku = v - 1$ and by (1) we have $\lambda = k(u - 1) = v - k - 1$. Whence $u = (v - 1)/k$. An equivalence between some DDFs and some EDFs is given in the following proposition.

Proposition 0.2 *Let $(G, +)$ be an Abelian group of order v , and let $\mathcal{D} = \{D_1, D_2, \dots, D_u\}$ be a collection of k -subsets of G . If \mathcal{D} is a partition of $G \setminus \{0\}$, then \mathcal{D} is a $(v, k, v - k - 1; (v - 1)/k)$ -EDF over G if and only if it is a $(v, k, k - 1)$ -DDF over G .*

3. Preliminaries

Let q be a power of an odd prime, and let α be a generator of $\text{GF}(q)^*$. Assume that $q - 1 = el$, where $e > 1$ and $l > 1$ are integers. Define $C_0^{(e)}$ to be the subgroup of $\text{GF}(q)^*$ generated by α^e , and let $C_i^{(e)} := \alpha^i C_0^{(e)}$ for each i with $0 \leq i \leq e - 1$. These $C_i^{(e)}$ are called *cyclotomic classes* of order e with respect to $\text{GF}(q)^*$.

The cyclotomic numbers of order e , denoted $(i, j)_e$, are defined as

$$(i, j)_e = \left| \left(C_i^{(e)} + 1 \right) \cap C_j^{(e)} \right|,$$

where $0 \leq i \leq e - 1$ and $0 \leq j \leq e - 1$, and $|A|$ denotes the number of elements in the set A .

The following lemma lists some formulas about cyclotomic numbers.

Lemma 0.1 *Let symbols and notations be the same as before. Then*

(A) $(i, j)_e = (i', j')_e$ when $i \equiv i' \pmod{e}$ and $j \equiv j' \pmod{e}$;

(B) $(i, j)_e = (e - i, j - i)_e = \begin{cases} (j, i)_e, & l \text{ even,} \\ (j + e/2, i + e/2)_e, & l \text{ odd,} \end{cases}$

(C) $\sum_{j=0}^{e-1} (i, j)_e = l - n_i$, where

$$n_i = \begin{cases} 1, & i \equiv 0 \pmod{e}, \quad l \text{ even,} \\ 1, & i \equiv e/2 \pmod{e}, \quad l \text{ odd,} \\ 0, & \text{otherwise.} \end{cases}$$

(D) $\sum_{i=0}^{e-1} (i, j)_e = l - k_j$, where

$$k_j = \begin{cases} 1, & \text{if } j \equiv 0 \pmod{e}; \\ 0, & \text{otherwise.} \end{cases}$$

Lemma 0.2 *Let notations and symbols be the same as before. Then*

$$\sum_{i=0}^{e-1} (i, i+j)_e = \begin{cases} l-1 & \text{if } j = 0, \\ l & \text{if } j \neq 0. \end{cases}$$

When q is prime, the proof of the following proposition can be regarded as an application of Weil's theorem.

Proposition 0.3 *Let $q \equiv 1 \pmod{n}$ be a prime power with $q - [\sum_{i=0}^{s-2} \binom{s}{i} (s-i-1)(n-1)^{s-i}] \sqrt{q} - sn^{s-1} > 0$. Then, for any given s -tuple $(j_1, j_2, \dots, j_s) \in \{0, 1, \dots, n-1\}^s$ and any given s -tuple (c_1, c_2, \dots, c_s) of pairwise distinct elements of $GF(q)$, there exists an element $x \in GF(q)$ such that $x + c_i \in C_{j_i}^{(n)}$ for each i .*

Corollary 0.3 *Let $q \equiv 1 \pmod{n}$ be a prime power with $q \geq A(n, s)^2$ where $A(n, s) = [B(n, s) + \sqrt{B(n, s)^2 + 4sn^{s-1}}]/2$ and $B(n, s) = \sum_{i=0}^{s-2} \binom{s}{i} (s-i-1)(n-1)^{s-i}$. Then, for any given s -tuple $(j_1, j_2, \dots, j_s) \in \{0, 1, \dots, n-1\}^s$ and any given s -tuple (c_1, c_2, \dots, c_s) of pairwise distinct elements of $GF(q)$, there exists an element $x \in GF(q)$ such that $x + c_i \in C_{j_i}^{(n)}$ for each i .*

Lemma 0.4 *If $q > 25$ is a prime power and $q \equiv 9 \pmod{16}$, then there exists an element $a \in GF(q)$ such that $a \in C_0^{(8)}$ and $a + 1 \in C_1^{(2)}$.*

q	α	a
41	6	18
73	5	4
89	3	2
121	$6 + 3x + x^2$	$2 + 10x$
137	3	88
169	$11 + 6x + x^2$	$6 + 11x$
233	3	2
281	3	236
313	10	9
361	$10 + 13x + x^2$	$3 + 10x$
409	21	184
457	13	361
521	3	405
569	3	302
601	7	151
617	3	398
729	$2 + x + 2x^2 + x^3 + 2x^4 + x^5 + x^6$	$1 + 2x^2 + 2x^4 + x^5$
761	6	498
809	3	411
841	$2 + 18x + x^2$	$25 + 22x$
857	3	404
937	5	833

Table 1: Parameters for $25 < q \leq 937$

Proof: Since 0 and 1 are distinct elements in $GF(q)$, by Corollary 0.3

with $s = 2$ and $n = 8$, there exists an element $a \in C_0^{(8)}$ and $a + 1 \in C_1^{(8)}$ for any prime power $q \equiv 9 \pmod{16}$ and $q \geq 2433$.

For each given prime power $q = p^m$ (p prime) such that $q \equiv 9 \pmod{16}$ and $25 < q < 2433$, with the aid of computer we have found an element $a \in GF(q)$ meeting the requirements of Lemma 0.4. To save space we list in Table 1 for only small prime powers up to 937 the parameters: prime power q , primitive element α when $m = 1$ (or primitive polynomial of degree m over $GF(p)$ when $m \geq 2$), elements a .

Lemma 0.5 *If $q \equiv 1 \pmod{16}$ is a prime power with $q > 17$, then there exists an ordered triple (a, b, c) satisfying*

(1) $\{a, b, c\}$ is a system of representatives for $\{C_2^{(8)}, C_4^{(8)}, C_6^{(8)}\}$; and

(2) $\{a+1, a+b, b+c, c+1\}$ is a system of representatives for $\{C_1^{(8)}, C_3^{(8)}, C_5^{(8)}, C_7^{(8)}\}$.

Lemma 0.6 *If $q \equiv 1 \pmod{8}$ is a prime power and $q \neq 17, 41, 49, 81, 97, 257, 353, 433$, then there exists an element $a \in GF(q)$ such that $a \in C_2^{(4)}$ and $\{a-1, a+1\}$ is a system of representatives of $\{C_1^{(4)}, C_3^{(4)}\}$.*

4. Cyclotomic constructions of $(v, k, k - 1)$ -DDFs

The objective of this section is to describe several classes of EDFs and DDFs using the classical approach of putting a number of cyclotomic classes together to form a base block. This approach was used to construct many combinatorial designs in literature, e.g., the Hall difference sets.

Proposition 0.4 (Wilson) *Let $q - 1 = el$ and let q be a power of an odd prime. Then $\mathcal{D} := \{C_0^{(e)}, \dots, C_{e-1}^{(e)}\}$ is a $(q, (q - 1)/e, (q - 1 - e)/e)$ -DDF over $\text{GF}(q)$.*

The construction of DDFs in Proposition 0.4 leads to a class of EDFs depicted in the following proposition.

Proposition 0.5 *Let $q - 1 = el$ and let q be a power of an odd prime. Then $\mathcal{D} := \{C_0^{(e)}, \dots, C_{e-1}^{(e)}\}$ is a $(q, (q - 1)/e, q - 1 - (q - 1)/e; e)$ -EDF over $\text{GF}(q)$.*

Now we employ cyclotomic classes of order 4 to construct disjoint difference families and external difference families.

Lemma 0.7 *Let $q - 1 = 4l$, where l is even. The cyclotomic numbers of order 4 are determined by Tabel 2 together with the relations*

	0	1	2	3
0	A	B	C	D
1	B	D	E	E
2	C	E	C	E
3	D	E	E	B

Table 2: Relations of cyclotomic numbers of order 4

$$16A = q - 11 - 6s,$$

$$16B = q - 3 + 2s + 8t,$$

$$16C = q - 3 + 2s,$$

$$16D = q - 3 + 2s - 8t,$$

$$16E = q + 1 - 2s,$$

where $q = s^2 + 4t^2$, $s \equiv 1 \pmod{4}$ is the proper representation of $q = p^m$ if $p \equiv 1 \pmod{4}$; the sign of t is ambiguously determined.

Proposition 0.6 *Let $q - 1 = 4l = p^{2m} - 1$, where m is a positive integer and p is an odd prime. Then $\mathcal{D} := \{C_0^{(4)} \cup C_1^{(4)}, C_2^{(4)} \cup C_3^{(4)}\}$ is a $(q, (q - 1)/2, (q - 3)/2)$ -DDF or a $(q, (q - 1)/2, (q - 1)/2; 2)$ -EDF over $\text{GF}(q)$ if and only if*

- m is even, or
- m is odd and $p \equiv 1 \pmod{4}$.

Proof: We first prove the conclusion about the DDF. Define

$$D_0 = C_0^{(4)} \cup C_1^{(4)}, \quad D_1 = C_2^{(4)} \cup C_3^{(4)}.$$

It follows from Lemmas 0.1, 0.2, and 0.7 that

$$\begin{aligned} & \bigcup_{i=0}^1 \{x - y : x, y \in D_i, x \neq y\} \\ &= (A + B + C + D + 2B + 2E) C_0^{(2)} \\ & \quad \cup (A + B + C + D + 2E + 2D) C_1^{(2)} \\ &= \left(\frac{q-5}{4} + 2B + 2E \right) C_0^{(2)} \cup \left(\frac{q-5}{4} + 2E + 2D \right) C_1^{(2)}. \end{aligned}$$

Hence \mathcal{D} is a DDF if and only if $t = 0$.

In our case $q = (p^m)^2$ is the proper representation of q if and only

if m is even or m is odd and $p \equiv 1 \pmod{4}$. In these cases, \mathcal{D} is a $(q, (q-1)/2, (q-3)/2)$ -DDF.

The conclusion about the EDF follows from Proposition 0.2 and that about the DDF just proved above.

Cyclotomic constructions

Let q denote an odd prime power, $GF(q)$ denote the finite field with q elements, and G denote the additive group of $GF(q)$. α is a primitive element of $GF(q)$. Write $C_0^{(2)}$ and $C_1^{(2)}$ briefly as C_0 and C_1 . The objective of this section is to construct $(q, k, \lambda; u)$ -EDFs with $q = 2ku + 1$.

Lemma 0.8 *Let C_0, C_1 be the quadratic cyclotomic classes of order 2 with respect to $GF(q)$. Then*

$$C_0(X)C_0(X^{-1}) = \begin{cases} \frac{q+1}{4} + \frac{q-3}{4}G(X) & \text{if } q \equiv 3 \pmod{4}, \\ \frac{q+3}{4} + \frac{q-5}{4}G(X) + C_1(X) & \text{if } q \equiv 1 \pmod{4}. \end{cases}$$

Lemma 0.9 *Let $q \equiv 1 \pmod{4}$ be a prime power and $q \neq 9$. Then there exists a $(q, 2, (q-5)/4; (q-1)/4)$ -EDF over $GF(q)$; There does not exist a $(9, 2, 1; 2)$ -EDF over $GF(9)$.*

Proof: Firstly, there does not exist a $(9, 2, 1; 2)$ -EDF over $GF(9)$ with a exhausted computer search. By Lemma 0.8, $C_0(X)C_0(X^{-1}) = \frac{q+3}{4} + \frac{q-5}{4}G(X) + C_1(X)$. We divide the problem into three cases.

Case 1. $q \equiv 5 \pmod{8}$: Note that $C_0 = C_0^{(4)} \cup (-C_0^{(4)})$ and $2 \in C_1$. Let $D_i = \{i, -i\}$ for $i \in C_0^{(4)}$. Then $C_0 = \cup_{i \in C_0^{(4)}} D_i$ and $\sum_{i \in C_0^{(4)}} D_i(X)D_i(X^{-1}) = \frac{q-1}{2} + \sum_{i \in C_0^{(4)}} (X^{2i} + X^{-2i}) = \frac{q-1}{2} + C_1(X)$. Hence, $C_0(X)C_0(X^{-1}) - \sum_{i \in C_0^{(4)}} D_i(X)D_i(X^{-1}) = -\frac{q-5}{4} + \frac{q-5}{4}G(X)$. This collection of D_i 's is a $(q, 2, (q-5)/4; (q-1)/4)$ -EDF by Proposition 0.1.

Case 2. $q \equiv 9 \pmod{16}$: For $q = 25$, $GF(q)$ consists of the elements $a + bx$, where $a, b \in Z_5$ and x satisfying $3 + 2x + x^2 = 0$. The collection of 2-subsets of $GF(q)$ $\{\{1+x, x\}, \{4+x, 2+3x\}, \{3x, 4+2x\}, \{1+3x, 1\}, \{2+4x, 1+2x\}, \{2+x, 3+4x\}\}$ forms a $(q, 2, (q-5)/4; (q-1)/4)$ -EDF over $GF(q)$.

For $q > 25$, note that $C_0 = C_0^{(8)} \cup C_2^{(8)} \cup (-C_0^{(8)}) \cup (-C_2^{(8)})$. By

Lemma 0.4 there exists an element $a \in GF(q)$ such that $a \in C_0^{(8)}$ and $a + 1 \in C_1$. Set $D_i = \{i, -ai\}$ for $i \in C_0^{(8)} \cup C_2^{(8)}$. It is easily checked that $C_0 = \cup_{i \in C_0^{(8)} \cup C_2^{(8)}} D_i$ and

$$\sum_{i \in C_0^{(8)} \cup C_2^{(8)}} D_i(X)D_i(X^{-1}) = \frac{q-1}{2} + \sum_{i \in C_0^{(8)} \cup C_2^{(8)}} (X^{(a+1)i} + X^{-(a+1)i}) = \frac{q-1}{2} + C_1(X).$$

Hence, $C_0(X)C_0(X^{-1}) - \sum_{i \in C_0^{(8)} \cup C_2^{(8)}} D_i(X)D_i(X^{-1}) = -\frac{q-5}{4} + \frac{q-5}{4}G(X)$.

This collection of D_i 's forms a $(q, 2, (q-5)/4; (q-1)/4)$ -EDF by Proposition 0.1.

Case 3. $q \equiv 1 \pmod{16}$: For $q = 17$, the collection of 2-subsets of $GF(q) \{\{4, 6\}, \{7, 10\}, \{11, 16\}, \{1, 8\}\}$ forms a $(q, 2, (q-5)/4; (q-1)/4)$ -EDF over $GF(q)$.

For $q > 17$, note that $C_0 = C_0^{(8)} \cup C_2^{(8)} \cup C_4^{(8)} \cup C_6^{(8)}$ and $-1 \in C_0^{(8)}$.

Let $y_1, y_2, \dots, y_{(q-1)/16}$ be all the representatives of the quotient group $C_0^{(8)}/\{1, -1\}$. By Lemma 0.5 there exists an ordered triple (a, b, c) such that $\{a, b, c\}$ is a system of representatives for $\{C_2^{(8)}, C_4^{(8)}, C_6^{(8)}\}$, and $\{a+1, a+b, b+c, c+1\}$ is a system of representatives for $\{C_1^{(8)}, C_3^{(8)}, C_5^{(8)}, C_7^{(8)}\}$.

Set $D_{1i} = \{-y_i, ay_i\}$, $D_{2i} = \{-ay_i, by_i\}$, $D_{3i} = \{-by_i, cy_i\}$ and $D_{4i} = \{-cy_i, y_i\}$ for $i = 1, 2, \dots, (q-1)/16$. It is easily checked that $C_0 =$

$\sum_{t=1}^4 \sum_{i=1}^{(q-1)/16} D_{ti}$ and

$$\begin{aligned}
& \sum_{i=1}^{(q-1)/16} \sum_{t=1}^4 D_{ti}(X) D_{ti}(X^{-1}) \\
&= \frac{q-1}{2} + \sum_{\delta \in \{1, -1\}} \sum_{i=1}^{(q-1)/16} (X^{(a+1)\delta y_i} + X^{(a+b)\delta y_i} + X^{(b+c)\delta y_i} + X^{(c+1)\delta y_i}) \\
&= \frac{q-1}{2} + \sum_{g \in C_0^{(8)}} (X^{(a+1)g} + X^{(a+b)g} + X^{(b+c)g} + X^{(c+1)g}) = \frac{q-1}{2} + C_1(X).
\end{aligned}$$

Hence, $C_0(X)C_0(X^{-1}) - \sum_{i=1}^{(q-1)/16} \sum_{t=1}^4 D_{ti}(X) D_{ti}(X^{-1}) = -\frac{q-5}{4} + \frac{q-5}{4}G(X)$.

This collection of D_{ti} 's is a $(q, 2, (q-5)/4; (q-1)/4)$ -EDF by Proposition 0.1.

Proposition 0.7 *If $q \equiv 1 \pmod{8}$ is a prime power, then there exists a $(q, 4, (q-9)/4; (q-1)/8)$ -EDF over $GF(q)$.*

5. Recursive constructions of $(v, k, k - 1)$ -DDFs

The existence of a $(v, k, v - k - 1; (v - 1)/k)$ -EDF over an Abelian group G of order v is equivalent to that of a $(v, k, k - 1)$ -DDF in G . In this section we will give some recursive constructions for $(v, k, k - 1)$ -DDFs by utilizing incomplete difference matrices in Abelian groups.

Let $(G, +)$ be an Abelian group of order v , and let H be a subgroup of order h in G . A (G, H, k, λ) -incomplete difference matrix (or (G, H, k, λ) -IDM) is a $k \times (v - h)\lambda$ matrix $D = (d_{ij})$, $0 \leq i \leq k - 1$, $1 \leq j \leq \lambda(v - h)$, with entries from G , such that for any $0 \leq i < j \leq k - 1$, the multiset

$$\{d_{il} - d_{jl} : 1 \leq l \leq \lambda(v - h)\}$$

contains every element of $G \setminus H$ exactly λ times. In the case $H = \emptyset$ or $h = 0$, a (G, H, k, λ) -IDM is termed as a (G, k, λ) -DM. When $G = Z_v$, a subgroup H of G with order h can be written as $H = \{iv/h : 0 \leq i \leq h - 1\}$. We usually denote a (Z_v, H, k, λ) -IDM by (v, h, k, λ) -ICDM over Z_v if $|H| = h$. Similarly, a (Z_v, k, λ) -DM is denoted by (v, k, λ) -CDM in Z_v .

Lemma 0.10 [?] *Let v and k be positive integers such that $\gcd(v, (k-1)!) = 1$. Let $d_{ij} \equiv ij \pmod{v}$ for $i = 0, 1, \dots, k-1$ and $j = 0, 1, \dots, v-1$. Then $D = (d_{ij})$ is a $(v, k, 1)$ -CDM in Z_v . In particular, if v is an odd prime number, then there exists a $(v, k, 1)$ -CDM in Z_v for any integer $k \leq v$.*

Let $\{\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_s\}$ be a collection of (G, k, λ) -DDFs. If $\cup_{i=1}^s (\cup_{B \in \mathcal{F}_i} B)$ forms a partition of $G \setminus \{0\}$, then the collection $\{\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_s\}$ is called a *complete set of disjoint difference families* and denoted by (G, k, λ) -CDDF, where each \mathcal{F}_i , $1 \leq i \leq s$, is the *component* of the (G, k, λ) -CDDF. Obviously, $\{B : B \in \cup_{i=1}^s \mathcal{F}_i\}$ forms a $(G, k, s\lambda)$ -DDF, while the number s of components of the (G, k, λ) -CDDF therein is $(k-1)/\lambda$. When $s = 1$ (i.e., $\lambda = k-1$), a (G, k, λ) -CDDF is just a $(G, k, k-1)$ -DDF. Fuji-Hara et al. [?] gave some recursive constructions of (G, k, λ) -CDDF which lead to some recursive constructions of (G, k, λ) -DDFs. We summarize their results in the following proposition.

Lemma 0.11 *Let S be a subgroup of an Abelian group G , and let H be a subgroup of S . If there exist both a $(G, S, k, k - 1)$ -DDF and an $(S, H, k, k - 1)$ -DDF, then so does a $(G, H, k, k - 1)$ -DDF. In particular, if there exist both a $(G, S, k, k - 1)$ -DDF and an $(S, k, k - 1)$ -DDF, so does a $(G, k, k - 1)$ -DDF.*

We give a recursive construction on DDFs by using the concept of incomplete difference matrices.

Proposition 0.8 *Let G_i be an Abelian group and let H_i be a subgroup of G_i , where $i = 1, 2$. Suppose that there exist*

- (1) *a $(G_1, H_1, k, k - 1)$ -DDF,*
- (2) *a $(G_2, H_2, k + 1, 1)$ -IDM, and*
- (3) *a $(G_1 \oplus H_2, H_1 \oplus H_2, k, k - 1)$ -DDF (or an $(H_1 \oplus G_2, H_1 \oplus H_2, k, k - 1)$ -DDF, respectively).*

Then there exists a $(G_1 \oplus G_2, H_1 \oplus G_2, k, k - 1)$ -DDF (or $(G_1 \oplus G_2, G_1 \oplus H_2, k, k - 1)$ -DDF, respectively).

Proposition 0.9 *Let v and m be two positive integers. Suppose that there exist*

- (1) *a $(v, g, k, k - 1)$ -DDF in Z_v , and*
- (2) *an $(m, k + 1, 1)$ -CDM in Z_m .*

Then there exists a $(vm, gm, k, k - 1)$ -DDF in Z_{mv} . Moreover, if there exists a $(gm, k, k - 1)$ -DDF in Z_{gm} , then so does a $(vm, k, k - 1)$ -DDF.

Example 0.12 *Let $v = 8$, $g = 2$, $k = 3$ and $m = 5$. Take a $(8, 2, 3, 2)$ -DDF in Z_8 with base blocks $\mathcal{F} = \{\{1, 6, 7\}, \{2, 3, 5\}\}$. Take a $(5, 4, 1)$ -CDM in Z_5 $D = (d_{ij})$ where $d_{ij} \equiv ij \pmod{5}$ for $0 \leq i \leq 3$ and $1 \leq j \leq 5$. The replacement mentioned in the proof of Proposition 0.9 gives the following 10 base blocks:*

$$\begin{aligned} &\{1, 6, 7\}, \quad \{2, 3, 5\}, \quad \{9, 22, 31\}, \quad \{10, 19, 29\}, \quad \{17, 38, 15\}, \\ &\{18, 35, 13\}, \quad \{25, 14, 39\}, \quad \{26, 11, 37\}, \quad \{33, 30, 23\}, \quad \{34, 27, 21\}. \end{aligned}$$

These base blocks form a $(40, 10, 3, 2)$ -DDF in Z_{40} .

Proposition 0.10 *Let $v = p_1 p_2 \cdots p_r$ where each $p_i \equiv 1 \pmod{6}$ is a prime and greater than 5 for $i = 1, 2, \dots, r$. Then there exist both a $(v, 3, 2)$ -DDF in Z_v and a $(4v, 3, 2)$ -DDF in Z_{4v} , and hence so do both a*

$(v, 3, v - 4; (v - 1)/3)$ -EDF in Z_v and a $(4v, 3, 4(v - 1); 4(v - 1)/3)$ -EDF in Z_{4v} .

Proposition 0.11 *Let $v = p_1 p_2 \cdots p_r$ where each $p_i \equiv 1 \pmod{4}$ is a prime and greater than or equal to 5 for $i = 1, 2, \dots, r$. Then there exists a $(v, 4, 3)$ -DDF in Z_v , and hence so does a $(v, 4, v - 5; (v - 1)/4)$ -EDF in Z_v .*

6. Connections between EDFs and ADSs

Let $(G, +)$ be an Abelian group of order v . Let D be a k -subset of G . The set D is a (v, k, λ) *difference set* (DS) in G if $d_D(w) = \lambda$ for every nonzero element of G , where $d_D(w)$ is the *difference function* defined by

$$d_D(w) = |(D + w) \cap D|, \quad w \in G.$$

A difference set D in G is called *skew* if D , $-D$ and $\{0\}$ form a partition of G . A skew difference set must have parameters $(v, (v-1)/2, (v-3)/4)$ where $v \equiv 3 \pmod{4}$.

Let $(G, +)$ be an Abelian group of order v . A k -subset D of G is a (v, k, λ, t) *almost difference set* (ADS) in G if the difference function $d_D(w)$ takes on λ altogether t times and $\lambda + 1$ altogether $v - 1 - t$ times when w ranges over all the nonzero elements of G .

If a (v, k, λ, t) almost difference set exists, then

$$k(k-1) = t\lambda + (v-1-t)(\lambda+1). \quad (3)$$

The objective of this section is to find connections between EDFs and (almost) difference sets. We now establish the following connection between $(v, (v-1)/2, (v-1)/2; 2)$ -EDFs and a special type of (almost) difference sets.

Proposition 0.12 *Let G be an Abelian group of order v , and let $\{D_1, D_2\}$ be a partition of $G \setminus \{0\}$ with $|D_1| = |D_2| = (v-1)/2$. Then $\{D_1, D_2\}$ is a $(v, (v-1)/2, (v-1)/2; 2)$ -EDF in G if and only if*

1. $v \equiv 3 \pmod{4}$ and D_i is a $(v, (v-1)/2, (v-3)/4)$ skew difference set in G for each i , or
2. $v \equiv 1 \pmod{4}$ and D_i is a $(v, (v-1)/2, (v-5)/4, (v-1)/2)$ almost difference set in G satisfying $D_i = -D_i$ for each i .

Proposition 0.12 establishes a nice connection between $(v, (v-1)/2, (v-1)/2; 2)$ -EDFs and a special type of (almost) difference sets. Any skew difference set D or almost difference set D with $D = -D$ in an Abelian group yields a $(v, (v-1)/2, (v-1)/2; 2)$ -EDF. Unfortunately, skew difference sets seem very rare. The only known inequivalent skew difference sets are the Paley difference sets consisting of all the nonzero quadratic residues in $\text{GF}(q)$, where $q \equiv 3 \pmod{4}$, and the skew difference sets recently discovered by Ding and Yuan.

There are $(v, (v-1)/2, (v-5)/4, (v-1)/2)$ almost difference sets D in Abelian groups G , but some have the property that $D = -D$ while others do not satisfy this condition. The only known inequivalent almost difference sets with these parameters and this property are the Paley partial difference sets formed by all nonzero quadratic residues in $\text{GF}(q)$ with $q \equiv 1 \pmod{4}$. The following are $(v, (v-1)/2, (v-5)/4, (v-1)/2)$ almost difference sets D which do not satisfy $D = -D$:

- $\{1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 13, 16, 17, 20, 24, 25, 30, 31, 33, 36, 38, 40\}$ is a $(45, 22, 10, 22)$ ADS of Z_{45}

- Another example is the following ADS of Z_{33} with parameters $(33, 16, 7, 16)$:

$$\{1, 2, 3, 4, 5, 6, 7, 9, 14, 15, 19, 21, 23, 26, 29, 30\}.$$

It seems that $(v, (v - 1)/2, (v - 5)/4, (v - 1)/2)$ almost difference sets D with $D = -D$ are rare and very hard to construct.

In summary, there are only two classes of $(v, (v - 1)/2, (v - 1)/2; 2)$ -EDFs: one obtained from the quadratic residues and the other is derived from the class of new skew difference sets discovered recently. In view of this, we present the following problem and invite the reader to attack it.

Problem 0.1 *Construct other $(v, (v - 1)/2, (v - 1)/2; 2)$ -EDFs.*

7. Further discussions

External difference families with parameters $(v, k, \lambda; u)$ over an Abelian group G satisfy $\lambda(v-1) = k^2u(u-1)$. It is obvious that $ku \neq v$. In the special case that $v-1 = ku$, the existence of a $(v, k, k-1)$ disjoint difference family in G is equivalent to that of a $(v, k, v-k-1; (v-1)/k)$ external difference family, as described in Proposition 0.5.

By definition a $(v, 2, 1)$ -DDF in an Abelian group G with odd order v is identical to a *starter* in G , a combinatorial structure introduced by Stanton and Mullin for the direct construction of Room squares. When G is isomorphic to Z_v , where v is odd, a $(v, 2, 1)$ -DDF in Z_v is easily constructed by listing its base blocks as follows: $\{i, -i\}$ for $i = 1, 2, \dots, (v-1)/2$. However, for $k \geq 3$ and even if G is a cyclic group, it seems a challenge problem to determine the existence spectrum of $(v, k, k-1)$ -DDFs in G .

Problem 0.2 *Give more constructions of $(v, k, k-1)$ -DDFs in Abelian groups G .*

Problem 0.3 *Complete the existence spectrum of $(v, k, k-1)$ -DDF in*

Z_v for $k = 3, 4$.

Problem 0.4 Find more constructions of $(v, k, \lambda; u)$ -EDFs in Abelian groups G with $ku < v - 1$.