Des Codes Crypt (2006) 40:167–185
DOI 10.1007/s10623-006-0005-7

Constructions of external difference families and disjoint difference families

Yanxun Chang · Cunsheng Ding

Received: 22 February 2005 / Revised: 7 November 2005 /
Accepted: 25 January 2006

Abstract External difference families (EDFs) are a type of new combinatorial designs originated from cryptography. In this paper, some earlier ideas of recursive and cyclotomic constructions of combinatorial designs are extended, and a number of classes of EDFs and disjoint difference families are presented. A link between a subclass of EDFs and a special type of (almost) difference sets is set up.

Keywords Difference sets · Difference systems of sets · Disjoint difference families · External difference families

AMS Classification 05B05 · 94A66

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, $\mathcal{D} = \{D_1, D_2, \ldots, D_u\}$, such that the multiset union

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

Difference families are well studied and have applications in coding theory and cryptography. Recently, Ogata et al. [18] introduced a type of combinatorial designs, *external difference families*, which are related to difference families and have applications in authentication codes and secret sharing.

Communicated by A. Pott.

Y. Chang
Department of Mathematics, Beijing Jiaotong University, Beijing 100044, China
e-mail: yxchang@center.njtu.edu.cn

C. Ding (✉)
Department of Computer Science, The Hong Kong University of Science and Technology,
Clear Water Bay, Kowloon, Hong Kong, China
e-mail: cding@cs.ust.hk

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, $\mathcal{D} = \{D_1, D_2, \ldots, D_u\}$, such that the multiset union

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

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

$$\lambda(v - 1) = k^2 u(u - 1). \tag{1}$$

Note that in an EDF 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.

A *difference system of sets* (DSS) with parameters $(n, \tau_0, \ldots, \tau_{l-1}, \delta)$ is a collection of l disjoint subsets $Q_i \subseteq \{1, 2, \ldots, n\}$, $|Q_i| = \tau_i$, $0 \leq i \leq l - 1$, such that the multiset

$$\{a - b \pmod{n} : a \in Q_i, b \in Q_j, 0 \leq i, j < l, i \neq j\} \tag{2}$$

contains every number i, $1 \leq i \leq n - 1$ at least δ times. A DSS is *perfect* if every number i, $1 \leq i \leq n - 1$, is contained exactly δ times in the multiset (2). A DSS is *regular* if all Q_i are of the same size. Hence, a perfect and regular DSS is an EDF over $\mathbf{Z}_n$. Therefore, EDFs are an extension of perfect and regular DSSs.

Difference systems of sets were introduced by Levenshtein [13], and were used to construct codes that allow for synchronization in the presence of errors [14]. Tonchev [23], Mutoh and Tonchev [17], and Mutoh [16] presented further constructions of DSSs and studied their applications in code synchronization.

Cyclotomy is an important tool for constructing various types of combinatorial designs, including almost difference sets [1], difference sets [21], difference families [2, 5, 24], and DSSs [17]. In this paper, we extend earlier ideas of recursive and cyclotomic constructions of combinatorial designs, present a number of EDFs and disjoint difference families (DDFs), and establish a connection between a subclass of DDFs and a subclass of EDFs. We also set up a link between a special class of EDFs and a special type of (almost) difference sets.

2 Preliminaries

2.1 A connection between external difference families and disjoint difference families

A convenient way to study an external difference family is to use a group ring. Let $(G, +)$ be an additive Abelian group and Z the ring of all integers. 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 $\mathcal{D} = \{D_1, D_2, \ldots, D_u\}$ over G as

$$\sum_{1\le i\ne j\le u} D_i(X)D_j(X^{-1}) = -\lambda + \lambda G(X). \tag{3}$$

The following proposition follows directly from (3).

Proposition 1 *Let $(G, +)$ be an Abelian group of order v, and let $\mathcal{D} = \{D_1, D_2, \ldots, D_u\}$ 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 $D = \bigcup_{i=1}^{u} D_i$.

Before establishing a connection between some DDFs and some EDFs, we need to introduce more notions and notations.

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 $\Delta\mathcal{F} = \bigcup_{i\in I} \Delta B_i$ is λ times $G\setminus H$, where $\Delta B_i = \{a - b : a, b \in B_i, a \ne b\}$. 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 $H = (v/g)Z_v = \{0, v/g, 2v/g, \ldots, (g - 1)v/g\}$. 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 in this paper. A (v, g, k, λ)-CDF is also denoted as a (v, g, k, λ)-DF in [3] and as a *g-regular cyclic packing* $CP(k, 1; v)$ in [25].

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). The (G, k, λ)-DDFs have been investigated intensively (see, e.g., [9–11, 24]).

Let G be an Abelian group of order v, and let $\mathcal{D}=\{D_1, D_2, \ldots, D_u\}$ 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 $u = (v - 1)/k$. A connection between some DDFs and some EDFs is given in the following proposition.

Proposition 2 *Let $(G, +)$ be an Abelian group of order v, and let $\mathcal{D} = \{D_1, D_2, \ldots, D_u\}$ 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.*

Proof The conclusion follows immediately from Proposition 1. □

Let G be an Abelian group of order v. To construct a $(v, k, v-k-1; (v-1)/k)$-EDF over G, by Proposition 2 we need only to construct the corresponding $(G, k, k-1)$-DDF. This idea will be followed in later sections.

2.2 Auxiliary results related to cyclotomy

In this section, we introduce and prove a number of results related to cyclotomy, which will be needed in the sequel.

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

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

The following lemma lists some formulas about cyclotomic numbers [21, p. 25].

Lemma 3 *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*

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

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

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

We need also the following lemma in the sequel.

Lemma 4 [22] *Let notations and symbols be the same as before. Then*

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

It has been shown in [4] that a $(4up, 4u, 5, 1)$-CDF exists if there are certain elements in $GF(q)$ satisfying certain properties. We now establish some results related to the existence of certain elements in $GF(q)$, which are very useful in later sections.

When q is prime, the proof of the following proposition can be found in [4]. The proposition can be regarded as an application of Weil's theorem [15]. For general prime powers q, its proof is the same as that of Theorem 3.2 in [4].

Proposition 5 [4] *Let* $q \equiv 1 \pmod n$ *be a prime power with* $q - \left[\sum_{i=0}^{s-2} \binom{s}{i} (s-i-1) (n-1)^{s-i} \right] \sqrt{q} - sn^{s-1} > 0$. *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 $(c_1, c_2, \ldots, c_s)$ 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.

The following useful result follows from Proposition 5.

Corollary 6 *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 $(j_1, j_2, \ldots, j_s) \in \{0, 1, \ldots, n-1\}^s$ and any given s-tuple $(c_1, c_2, \ldots, c_s)$ 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 7 *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 $a + 1 \in C_1^{(2)}$.*

Proof Since 0 and 1 are distinct elements in $GF(q)$, by Corollary 6 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 7. 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 8 *If $q \equiv 1 \pmod{16}$ is a prime power with $q > 17$, then there exists an ordered triple (a, b, c) satisfying*

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

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

(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* $\{C_1^{(8)}, C_3^{(8)}, C_5^{(8)}, C_7^{(8)}\}$.

Proof We need to find an ordered triple (a, b, c) satisfying

- $a \in C_2^{(8)}$ and $a+1 \in C_1^{(8)}$;
- $b \in C_4^{(8)}$ and $b+a \in C_3^{(8)}$;
- $c \in C_6^{(8)}$, $c+b \in C_5^{(8)}$ and $c+1 \in C_7^{(8)}$.

Applying Corollary 6 with $s = 2$ and $n = 8$, we know that an element $a \in C_2^{(8)}$ with $a+1 \in C_1^{(8)}$ always exists in $GF(q)$ for any prime power $q \equiv 1 \pmod{16}$ and $q \geq 2433$. Clearly, a is not allowed to be equal to 0. Then applying Corollary 6 with $s = 2$ and $n = 8$ once again, we know that, once the element $a \in GF(q)$ has been determined, the required element b also exists in $GF(q)$ for any prime power $q \equiv 1 \pmod{16}$ and $q \geq 2433$. Applying Corollary 6 with $s = 3$ and $n = 8$ the third time, we know that, once the elements $a, b \in GF(q)$ have been determined, the required element c also exists in $GF(q)$ for any prime power $q \equiv 1 \pmod{16}$ and $q \geq 694273$.

For each given prime power $q = p^m$ (p prime) such that $q \equiv 1 \pmod{16}$ and $17 < q < 694273$, with the help of computer we have found an ordered triple (a, b, c) satisfying the requirements of Lemma 8. To save space we list in Table 2 for only small prime powers up to 673 the parameters: prime power q, primitive element α when $m = 1$ (or primitive polynomial of degree m over $GF(p)$ when $m \geq 2$), ordered triples (a, b, c). □

Lemma 9 *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* $\{C_1^{(4)}, C_3^{(4)}\}$.

Table 2 Parameters for $17 < q \leq 673$

q	α	a	b	c
49	$5+3x+x^2$	$5+3x$	$6+x$	$1+3x$
81	$2+x+x^4$	$2x^2$	x^2+2x^3	$1+2x+x^2+2x^3$
97	5	9	95	79
113	3	11	8	95
193	5	18	131	139
241	7	113	237	30
257	3	205	134	118
289	$7+12x+x^2$	$10+5x$	$10+4x$	$14+7x$
337	10	170	255	214
353	3	9	285	172
401	3	47	49	162
433	5	297	324	401
449	3	164	7	289
529	$5+19x+x^2$	$5+4x$	$5+2x$	$19+15x$
577	5	318	288	418
593	3	342	278	101
625	$2+3x+3x^2+2x^3+x^4$	$3x+4x^3$	$3+2x^2+2x^3$	$4x^2+x^3$
641	3	183	118	441
673	5	184	219	257

Table 3 Parameters for $9 \le q \le 457$

q	α	a
9	$2+x+x^2$	$1+2x$
25	$3+2x+x^2$	$3+2x$
73	5	46
89	3	34
113	3	18
121	$6+3x+x^2$	$6+6x$
137	3	107
169	$11+6x+x^2$	$3+5x$
193	5	67
233	2	89
241	7	45
281	3	20
289	$7+12x+x^2$	$1+15x$
313	10	284
337	10	214
361	$10+13x+x^2$	$9+16x$
401	3	162
409	21	209
449	3	280
457	13	359

Proof Since 0, 1, and -1 are distinct elements in $GF(q)$, by Corollary 6 with $s = 3$ and $n = 4$, there exists an element $a \in C_2^{(4)}$ such that $a - 1 \in C_1^{(4)}$ and $a + 1 \in C_3^{(4)}$ for any prime power $q \equiv 1 \pmod 8$ and $q \ge 6657$.

For each given prime power $q = p^m$ (p prime) such that $q \equiv 1 \pmod 8$, $q < 6657$, and $q \ne 17, 41, 49, 81, 97, 257, 353, 433$, with the help of computer we have found an element $a \in GF(q)$ meeting the requirements of Lemma 9. To save space we list in Table 3 for only small prime powers up to 457 the parameters: prime power q, primitive element α when $m = 1$ (or primitive polynomial of degree m over $GF(p)$ when $m \ge 2$), elements a. □

3 Cyclotomic constructions of $(v, k, k-1)$-DDFs and $(v, k, v-k-1; (v-1)/k)$-EDFs

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 [12].

Proposition 10 (Wilson [24]) *Let $q - 1 = el$ and let q be a power of an odd prime. Then $\mathcal{D} := \{C_0^{(e)}, \ldots, C_{e-1}^{(e)}\}$ is a $(q, (q-1)/e, (q-1-e)/e)$-DDF over* GF(q).

The construction of DDFs in Proposition 10 leads to a class of EDFs depicted in the following proposition.

Proposition 11 *Let $q - 1 = el$ and let q be a power of an odd prime. Then $\mathcal{D} := \{C_0^{(e)}, \ldots, C_{e-1}^{(e)}\}$ is a $(q, (q-1)/e, q-1-(q-1)/e; e)$-EDF over* GF$(q)$.

Proof The conclusion follows from Propositions 2 and 10. □

Table 4 Relations of cyclotomic numbers of order 4

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

Now we employ cyclotomic classes of order 4 to construct DDFs and EDFs. To this end, we need cyclotomic numbers of order 4, which are given in the following lemma.

Lemma 12 [21, p. 51] *Let $q-1=4l$, where l is even. The cyclotomic numbers of order* 4 *are determined by Table* 4 *together with the relations*

$$\begin{aligned} 16A &= q-11-6s, \\ 16B &= q-3+2s+8t, \\ 16C &= q-3+2s, \\ 16D &= q-3+2s-8t, \\ 16E &= q+1-2s, \end{aligned}$$

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 13 *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 $\mathrm{GF}(q)$ 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

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

It follows from Lemmas 3, 4, and 12 that

$$\begin{aligned} &\bigcup_{i=0}^{1}\{x-y : x, y \in D_i, x \neq y\} \\ &\quad = ((0,0)_4+(1,1)_4+(2,2)_4+(3,3)_4+2(0,1)_4+2(2,3)_4)\, C_0^{(2)} \\ &\qquad \bigcup ((0,0)_4+(1,1)_4+(2,2)_4+(3,3)_4+2(1,2)_4+2(3,0)_4)\, C_1^{(2)} \\ &\quad = (A+B+C+D+2B+2E)\, C_0^{(2)} \bigcup (A+B+C+D+2E+2D)\, C_1^{(2)} \\ &\quad = \left(\frac{q-5}{4}+2B+2E\right) C_0^{(2)} \bigcup \left(\frac{q-5}{4}+2E+2D\right) C_1^{(2)}. \end{aligned}$$

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 2 and that about the DDF just proved above. □

Table 5 Relations of cyclotomic numbers of order 6

	0	1	2	3	4	5
0	A	B	C	D	E	F
1	G	H	I	E	C	I
2	H	J	G	F	I	B
3	A	G	H	A	G	H
4	G	F	I	B	H	J
5	H	I	E	C	I	G

Proposition 14 *Let $q - 1 = 4l = p^{2m} - 1$, where m is a positive integer and p is an odd prime. Then $\mathcal{D} := \{C_0^{(4)} \cup C_3^{(4)}, C_1^{(4)} \cup C_2^{(4)}\}$ is a $(q, (q-1)/2, (q-3)/2)$-DDF or a $(q, (q-1)/2, (q-1)/2; 2)$-EDF over* GF(q) *if and only if*

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

Proof The proof is similar to that of Proposition 13 and is omitted. □

Cyclotomic classes of order 6 can also be used to construct DDFs and EDFs. For this purpose, again we need information of cyclotomic numbers of order 6.

Lemma 15 [21, p. 29] *Let $q - 1 = 6l$, where $l > 1$ is odd. The cyclotomic numbers of order 6 take on ten possible different values $A, B, C, D, E, F, G, H, I, J$ and are determined by Table 5, together with the relations*

$$\begin{aligned} 2A + 2G + 2H &= l - 1, \\ B + F + G + H + I + J &= l, \\ C + E + G + H + 2I &= l, \\ B + F + G + H + 2I &= l. \end{aligned}$$

Proposition 16 *Let $q - 1 = 6l$, where l is odd. Then*

$$\mathcal{D} := \left\{C_0^{(6)} \cup C_1^{(6)}, C_2^{(6)} \cup C_3^{(6)}, C_4^{(6)} \cup C_5^{(6)}\right\}$$

is a $(q, (q-1)/3, (q-4)/3)$-DDF and a $(q, (q-1)/3, 2(q-1)/3; 3)$-EDF over GF$(q)$.

Proof Define

$$D_0 = C_0^{(6)} \cup C_1^{(6)}, \qquad D_1 = C_2^{(6)} \cup C_3^{(6)}, \qquad D_2 = C_4^{(6)} \cup C_5^{(6)}.$$

It follow from Lemmas 15, 3, and 4 that

$$\begin{aligned} &\bigcup_{i=0}^{2} \{x - y : x, y \in D_i, x \neq y\} \\ &= \left(\sum_{i=0}^{5} (i,i)_6 + (0,1)_6 + (1,0)_6 + (2,3)_6 + (3,2)_6 + (4,5)_6 + (5,4)_6\right) C_0^{(2)} \cup \\ &\quad \left(\sum_{i=0}^{5} (i,i)_6 + (1,2)_6 + (2,1)_6 + (3,4)_6 + (4,3)_6 + (5,0)_6 + (0,5)_6\right) C_1^{(2)} \\ &= \frac{q-4}{3} (\mathrm{GF}(q) \backslash \{0\}). \end{aligned}$$

This proves the the conclusion on the DDF.

The conclusion on the EDF follows from Proposition 2 and that on the DDF just proved above. □

4 Cyclotomic constructions of $(q, k, \lambda; u)$-EDFs with $q = 2ku + 1$

In this section, q will denote an odd prime power, $GF(q)$ will denote the finite field with q elements, and G will denote the additive group of $GF(q)$. For convenience, we select and fix a primitive element α of $GF(q)$. Write $C_0^{(2)}$ and $C_1^{(2)}$ briefly as C_0 and C_1 in this section. The objective of this section is to construct $(q, k, \lambda; u)$-EDFs with $q = 2ku+1$ by extending earlier cyclotomic approaches [12, 24].

Lemma 17 [1] *Let C_0, C_1 be the quadratic cyclotomic classes of order* 2 *with respect to $GF(q)$. Then*

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

The following proposition is proved in Tonchev [23] when q is prime. For prime power q the proposition can be proved in a similar way.

Proposition 18 *Let $q \equiv 3 \pmod 4$ be a prime power and $q - 1 = 2ku$. Then there exists a $(q, k, (q - 2k - 1)/4; u)$-EDF.*

Lemma 19 *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 First, it follows from an exhaustive computer search that there does not exist a $(9, 2, 1; 2)$-EDF over $GF(9)$. By Lemma 17, $C_0(X)C_0(X^{-1}) = \frac{q+3}{4} + \frac{q-5}{4}G(X) + C_1(X)$. We divide the problem into three cases.

Case 1 $q \equiv 5 \pmod 8$: note that $C_0 = C_0^{(4)} \cup \left(-C_0^{(4)}\right)$ and $2 \in C_1$. Let $D_i = \{i, -i\}$ for $i \in C_0^{(4)}$. Then $C_0 = \bigcup_{i \in C_0^{(4)}} D_i$ 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 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 $C_0 = C_0^{(8)} \cup C_2^{(8)} \cup \left(-C_0^{(8)}\right) \cup \left(-C_2^{(8)}\right)$. By Lemma 7, 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 $C_0 = \bigcup_{i\in C_0^{(8)}\cup C_2^{(8)}} D_i$ 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 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 $y_1, y_2, \ldots, y_{(q-1)/16}$ be all the representatives of the quotient group $C_0^{(8)}/\{1, -1\}$. By Lemma 8, 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 $i = 1, 2, \ldots, (q-1)/16$. It is easily checked that $C_0 = \sum_{t=1}^{4} \sum_{i=1}^{(q-1)/16} D_{ti}$ and

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

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 1. □

Lemma 20 *Let* $q \equiv 1 \pmod 8$ *be a prime power and* $q \neq 17, 41, 49, 81, 97, 257, 353, 433$, *then there exists a* $(q, 4, (q-9)/4; (q-1)/8)$*-EDF over* $GF(q)$.

Proof By Lemma 17, $C_0(X)C_0(X^{-1}) = \frac{q+3}{4} + \frac{q-5}{4} G(X) + C_1(X)$. Note that $C_0 = C_0^{(4)} \cup C_2^{(4)}$, $-1 \in C_0^{(4)}$, and $2 \in C_0$. By Lemma 9, 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 $\{C_1^{(4)}, C_3^{(4)}\}$. Let $y_1, y_2, \ldots, y_{(q-1)/8}$ be all the representatives of the quotient group $C_0^{(4)}/\{1, -1\}$.

Set $D_i = \{y_i, -y_i, ay_i, -ay_i\}$ for $i = 1, 2, \ldots, (q-1)/8$. It is easily checked that $C_0 = \cup_{i=1}^{(q-1)/8} D_i$ and

$$\begin{aligned}
&\sum_{i=1}^{(q-1)/8} D_i(X) D_i(X^{-1}) \\
&\quad = \frac{q-1}{2} + \sum_{\delta \in \{1,-1\}} \sum_{i=1}^{(q-1)/8} (X^{2\delta y_i} + X^{2a\delta y_i} + 2X^{(a+1)\delta y_i} + 2X^{(a-1)\delta y_i}) \\
&\quad = \frac{q-1}{2} + \sum_{g \in C_0^{(4)}} (X^{2g} + X^{2ag} + 2X^{(a+1)g} + 2X^{(a-1)g}) \\
&\quad = \frac{q-1}{2} + C_0(X) + 2C_1(X).
\end{aligned}$$

Hence, $C_0(X)C_0(X^{-1}) - \sum_{i=1}^{(q-1)/8} D_i(X) D_i(X^{-1}) = -\frac{q-9}{4} + \frac{q-9}{4} G(X)$. This collection of D_i's forms a $(q, 4, (q-9)/4; (q-1)/8)$-EDF by Proposition 1. □

Proposition 21 *If* $q \equiv 1 \pmod 8$ *is a prime power, then there exists a* $(q, 4, (q-9)/4; (q-1)/8)$*-EDF over* $GF(q)$.

Proof When $q \equiv 1 \pmod 8$ is a prime power and $q \neq 17, 41, 49, 81, 97, 257, 353, 433$, the conclusion follows from Lemma 20.

When $q = 17, 81, 257, 433$, we have $q \equiv 1 \pmod{16}$. In this case $C_0 = C_0^{(8)} \cup C_2^{(8)} \cup C_4^{(8)} \cup C_6^{(8)}$, $2 \in C_0$ and $-1 \in C_0^{(8)}$. Let $y_1, y_2, \ldots, y_{(q-1)/16}$ be all the representatives of the quotient group $C_0^{(8)}/\{1, -1\}$.

For each q, take $(q, \alpha, a, b, c) = (17, 3, 4, 9, 15)$, $(81, 2+x+x^4, 2+\alpha, \alpha^2, 2\alpha^2+\alpha^3)$, $(257, 3, 81, 9, 42)$, $(433, 5, 312, 25, 18)$, where α is a primitive element in $GF(q)$, and α is a root of the primitive polynomial $2 + x + x^4$ over GF(3) when $q = 81$. It is readily checked that in each $GF(q)$, $\{a, b, c\}$ is a system of representatives of $\{C_2^8, C_4^8, C_6^8\}$, and $\{a+1, a-1, b+c, b-c\}$ is a system of representatives of $\{C_1^8, C_3^8, C_5^8, C_7^8\}$. Set $D_{1i} = \{y_i, -y_i, ay_i, -ay_i\}$ and $D_{2i} = \{by_i, -by_i, cy_i, -cy_i\}$ for $i = 1, 2, \ldots, (q-1)/16$. It is easily checked that $C_0 = \sum_{t=1}^{2}\sum_{i=1}^{(q-1)/16} D_{ti}$ and

$$\sum_{t=1}^{2}\sum_{i=1}^{(q-1)/16} D_{ti}(X)D_{ti}(X^{-1}) = \frac{q-1}{2} + C_0(X) + 2C_1(X).$$

Hence, $C_0(X)C_0(X^{-1}) - \sum_{t=1}^{2}\sum_{i=1}^{(q-1)/16} D_{ti}(X)D_{ti}(X^{-1}) = -\frac{q-9}{4} + \frac{q-9}{4}G(X)$. This collection of D_{ti}'s forms a $(q, 4, (q-9)/4; (q-1)/8)$-EDF by Proposition 1.

When $q = 97, 353$, we have $q \equiv 1 \pmod{32}$. In this case $C_0 = \cup_{i=0}^{7} C_{2i}^{(16)}$, and $-1 \in C_0^{(16)}$. Let $y_1, y_2, \ldots, y_{(q-1)/32}$ be all the representatives of the quotient group $C_0^{(16)}/\{1, -1\}$. Take $(q, \alpha, a, b, c, d, e, f, g) = (97, 5, 75, 25, 32, 43, 73, 8, 79)$, $(353, 3, 25, 82, 159, 49, 242, 207, 92)$, where α is a primitive element in $GF(q)$. Set $D_{1i} = \{y_i, -y_i, ay_i, -ay_i\}$, $D_{2i} = \{by_i, -by_i, cy_i, -cy_i\}$, $D_{3i} = \{dy_i, -dy_i, ey_i, -ey_i\}$, and $D_{4i} = \{fy_i, -fy_i, gy_i, -gy_i\}$ for $i = 1, 2, \ldots, (q-1)/32$. It is easily checked that this collection of D_{ti}'s forms a $(q, 4, (q-9)/4; (q-1)/8)$-EDF by Proposition 1.

Finally, we need to deal with the cases of $q = 41, 49$. For $q = 41$, the collection of 4-subsets of $GF(q)$ $\{\{1, 19, 40, 22\}, \{4, 6, 37, 35\}, \{10, 26, 31, 15\}, \{16, 24, 25, 17\}, \{18, 14, 23, 27\}\}$ forms a $(q, 4, (q-9)/4; (q-1)/8)$-EDF by Proposition 1.

For $q = 49$, $GF(q)$ consists of the elements $a + bx$, where $a, b \in Z_7$ and x is the primitive element of $GF(q)$ satisfying $5 + 3x + x^2 = 0$. The collection of 4-subsets of $GF(q)$ $\{\{1, 5x, 6, 2x\}, \{x, 2+2x, 6x, 5+5x\}, \{1+3x, 4, 6+4x, 3\}, \{6+6x, 5, 1+x, 2\}, \{5+x, 3+3x, 2+6x, 4+4x\}, \{4x, 4+5x, 3x, 3+2x\}\}$ forms a $(q, 4, (q-9)/4; (q-1)/8)$-EDF by Proposition 1. □

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

From Proposition 2, we know that 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. We first introduce some terminologies as follows.

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 $D = (d_{ij})$, $0 \le i \le k-1$, $1 \le j \le \lambda(v-h)$, with entries from G, such that for any $0 \le i < j \le k-1$, the multiset

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

contains every element of $G\backslash H$ 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 $H=\{iv/h:\ 0\le i\le h-1\}$. 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.

Difference matrices have been investigated extensively (see, e.g. [7] and the references therein). Here is one example.

Lemma 22 [6] *Let v and k be positive integers such that* $\gcd(v,(k-1)!)=1$. *Let $d_{ij}\equiv ij\ (mod\ v)$ for $i=0,1,\ldots,k-1$ and $j=0,1,\ldots,v-1$. 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 $k\le v$.*

Let $\{\mathcal{F}_1,\mathcal{F}_2,\ldots,\mathcal{F}_s\}$ be a collection of (G,k,λ)-DDFs. If $\cup_{i=1}^{s}(\cup_{B\in\mathcal{F}_i}B)$ forms a partition of $G\backslash\{0\}$, then the collection $\{\mathcal{F}_1,\mathcal{F}_2,\ldots,\mathcal{F}_s\}$ is called a *complete set of disjoint difference families* and denoted by (G,k,λ)-CDDF, where each $\mathcal{F}_i$, $1\le i\le s$, 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. [11] 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.

Proposition 23 [11]

(1) *Let G_1 and G_2 be two Abelian groups. If there exist a $(G_1,k,k-1)$-DDF, a $(G_2,k,k-1)$-DDF, and a $(G_2,k+1,1)$-DM, then there exists a $(G_1\oplus G_2,k,k-1)$-DDF.*
(2) *Let G_2 be a subgroup of an Abelian group G such that the quotient group G/G_2 is isomorphic to an Abelian group G_1 of order not equal to k. If there exist a $(G_1,k,k-1)$-DDF, a $(G_2,k,k-1)$-DDF, and a $(G_2,k+1,1)$-DM, then there exists a $(G,k,k-1)$-DDF.*
(3) *There exists a $(v,3,2)$-DDF in Z_v for $v=25,55$.*

The following lemma is simple but very useful.

Lemma 24 *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.*

Proof Let $\mathcal{F}$ and $\mathcal{E}$ be the collection of base blocks of the given $(G,S,k,k-1)$-DDF and $(S,H,k,k-1)$-DDF, respectively. Then the family $\mathcal{F}\cup\mathcal{E}$ forms the desired $(G,H,k,k-1)$-DDF. □

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

Proposition 25 *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).*

Proof Suppose that $\mathcal{F}$ is the family of base blocks of the given $(G_1, H_1, k, k-1)$-DDF. By definition, we have $\cup_{B\in\mathcal{F}} B = G_1 \backslash H_1$ and $\cup_{B\in\mathcal{F}} \Delta B = (k-1)(G_1 \backslash H_1)$.

Let $D = (d_{ij})$ be a $(G_2, H_2, k+1, 1)$-IDM, where $d_{ij} \in G_2$ for $0 \le i \le k$ and $1 \le j \le |G_2| - |H_2|$. Note that the property of difference matrix is preserved even if adding an element to any columns or any rows. Thus, without loss of generality, we may assume that in D, the elements in the first row are all 0s. Then, for $1 \le i \ne j \le k$, we obtain

$$\{d_{il} - d_{jl} :\ 1 \le l \le |G_2| - |H_2|\} = G_2 \backslash H_2$$

and

$$\{d_{il} :\ 1 \le l \le |G_2| - |H_2|\} = G_2 \backslash H_2.$$

Let $G = G_1 \oplus G_2$ and $U_1 = H_1 \oplus G_2$ (or $U_2 = G_1 \oplus H_2$). By the assumption of (3), let $\mathcal{C}$ be the family of base blocks of an $(U_2, H_1 \oplus H_2, k, k-1)$-DDF (or an $(U_1, H_1 \oplus H_2, k, k-1)$-DDF, respectively). Next, we construct a $(G, U_1, k, k-1)$-DDF (or $(G, U_2, k, k-1)$-DDF, respectively) as follows.

For each base block $B = \{b_1, b_2, \ldots, b_k\} \in \mathcal{F}$, we define $|G_2| - |H_2|$ base blocks

$$B_j = \{(b_i, d_{ij}) :\ 1 \le i \le k\}$$

for $j = 1, \ldots, |G_2| - |H_2|$, where the additive operation is performed in G. Set

$$\mathcal{E} = \{B_j :\ B \in \mathcal{F},\ 1 \le j \le |G_2| - |H_2|\} \cup \mathcal{C}.$$

Clearly, $\mathcal{E}$ partitions $G \backslash U_1$ (or $G \backslash U_2$). It is readily checked that differences arising from the base blocks $\mathcal{E}$ cover each element in $G \backslash U_1$ (or $G \backslash U_2$, respectively) exactly $k-1$ times. □

Now we establish a recursive construction of $(v, k, k-1)$-DDF in Z_v.

Proposition 26 *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.*

Proof Let $\mathcal{F}$ be the family of base blocks of the given $(v, g, k, k-1)$-DDF in Z_v. Hence, we have $\cup_{B\in\mathcal{F}} B = Z_v \backslash (v/g) Z_v$ and $\cup_{B\in\mathcal{F}} \Delta B = (k-1)(Z_v \backslash (v/g) Z_v)$. Let $D = (d_{ij})$ be an $(m, k+1, 1)$-CDM in Z_m where $d_{ij} \in Z_m$ for $0 \le i \le k$ and $1 \le j \le m$. Without loss of generality, we may assume that the elements in the first row of D are all 0's. Then, for $1 \le i \ne j \le k$, we have

$$\{d_{il} - d_{jl} :\ 1 \le l \le m\} = Z_m$$

and

$$\{d_{il} :\ 1 \le l \le m\} = Z_m.$$

Now we construct a $(vm, gm, k, k-1)$-DDF in Z_{vm} as follows: for each base block $B = \{b_1, b_2, \ldots, b_k\} \in \mathcal{F}$, we define m base blocks

$$B_j = \{b_i + vd_{ij} : 1 \le i \le k\}$$

for $j = 1, \ldots, m$, where the additive operation is performed in Z_{vm}. Set

$$\mathcal{E} = \{B_j : B \in \mathcal{F}, 1 \le j \le m\}.$$

Clearly, $\mathcal{E}$ partitions $Z_{vm} \backslash (v/g)Z_{vm}$. It is readily checked that the differences arising from the base blocks $\mathcal{E}$ cover each element in $Z_{vm} \backslash (v/g)Z_{vm}$ exactly $k-1$ times. This proves the first assertion.

The second assertion follows from Lemma 24. □

Example 1 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 $0 \le i \le 3$ and $1 \le j \le 5$. The replacement mentioned in the proof of Proposition 26 gives the following 10 base blocks:

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

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

Proposition 27 *Let $v = p_1 p_2 \ldots p_r$, where each $p_i \equiv 1 \pmod 6$ is a prime and greater than 5 for $i = 1, 2, \ldots, r$. 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}.*

Proof By Proposition 10, there exists a $(p_i, 3, 2)$-DDF for each $i = 1, 2, \ldots, r$. There is a $(p_j, 4, 1)$-CDM in Z_{p_j} by Lemma 22 for each $j = 2, \ldots, r$. Start with a $(p_1, 3, 2)$-DDF and apply Proposition 26 and Lemma 24 recursively to obtain a $(v, 3, 2)$-DDF in Z_v.

A $(4, 3, 2)$-DDF in Z_4 consists of the single base block $\{1, 2, 3\}$. By Lemma 22, there is a $(v, 4, 1)$-CDM in Z_v. Start with a $(4, 3, 2)$-DDF and apply Proposition 26 to obtain a $(4v, v, 3, 2)$-DDF in Z_{4m}. Apply Lemma 24 with a $(v, 3, 2)$-DDF in Z_v as above to get a $(4v, 3, 2)$-DDF in Z_{4v}.

The assertions follows by Proposition 2. □

Proposition 28 *Let $v = p_1 p_2 \ldots p_r$, where each $p_i \equiv 1 \pmod 4$ is a prime and greater than or equal to 5 for $i = 1, 2, \ldots, r$. 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.*

Proof The proof is similar to that of Proposition 27. □

6 Connections between EDFs and (almost) difference sets

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 DS 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) ADS exists, then

$$k(k-1) = t\lambda + (v - 1 - t)(\lambda + 1). \tag{4}$$

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

Proposition 29 *Let G be an Abelian group of order v, and let $\{D_1, D_2\}$ be a partition of $G\backslash\{0\}$ 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 $(v, (v-1)/2, (v-5)/4, (v-1)/2)$ ADS in G satisfying $D_i = -D_i$ for each i.*

Proof Note that $\{D_1, D_2\}$ is a partition of $G\backslash\{0\}$, i.e., $G\backslash\{0\} = D_0 \cup D_1$. We have the following equality of multisets:

$$(D_1 \cup D_2) - (D_1 \cup D_2) = (G\backslash\{0\}) - (G\backslash\{0\}) = (v-1)\{0\} \cup (v-2)(G\backslash\{0\}).$$

On the other hand,

$$(D_1 \cup D_2) - (D_1 \cup D_2) = (D_1 - D_1) \cup (D_2 - D_2) \cup (D_1 - D_2) \cup (D_2 - D_1),$$

where $D_i - D_j := \{x - y : x \in D_i,\ y \in D_j\}$. Hence, $\{D_1, D_2\}$ is a $(v, (v-1)/2, (v-1)/2; 2)$-EDF in G if and only if

$$(D_1 - D_1) \cup (D_2 - D_2) = (v-1)\{0\} \cup \left(\frac{v-3}{2}\right)(G\backslash\{0\}),$$

which is equivalent to

$$|D_1 \cap (D_1 + a)| + |D_2 \cap (D_2 + a)| = \frac{v-3}{2} \tag{5}$$

for all nonzero $a \in G$.

Since $\{D_1, D_2\}$ is a partition of $G\backslash\{0\}$, for any nonzero element $a \in G$ we have

$$|D_2 \cap (D_2 + a)| = \frac{v-1}{2} - |D_1 \cap (D_2 + a)| - |\{-a\} \cap D_2|. \tag{6}$$

Similarly, we obtain

$$|D_1 \cap (D_2 + a)| = \frac{v-1}{2} - |D_1 \cap (D_1 + a)| - |\{a\} \cap D_1|. \tag{7}$$

Combining (6) and (7) yields

$$|D_2 \cap (D_2 + a)| = |D_1 \cap (D_1 + a)| + |\{a\} \cap D_1| - |\{-a\} \cap D_2|. \tag{8}$$

It follows from (8) and (5) that $\{D_1, D_2\}$ is a $(v, (v-1)/2, (v-1)/2; 2)$-EDF over G if and only if for each nonzero $a \in G$

$$\begin{cases} 2\,|D_2 \cap (D_2 + a)| = \frac{v-3}{2} + |\{a\} \cap D_1| - |\{-a\} \cap D_2|\,, \\ 2\,|D_1 \cap (D_1 + a)| = \frac{v-3}{2} - |\{a\} \cap D_1| + |\{-a\} \cap D_2|\,. \end{cases} \tag{9}$$

Assume that (9) holds. If $v \equiv 3 \pmod 4$, then we must have $4|(v-3)$ and $|\{a\} \cap D_1| - |\{-a\} \cap D_2| = 0$ for every nonzero $a \in G$, as $|D_i \cap (D_i + a)|$ is an integer. Hence $\{D_1, D_2\}$ is a $(v, (v-1)/2, (v-1)/2; 2)$-EDF over G if and only if for each nonzero $a \in G$ we have $|D_i \cap (D_i + a)| = \frac{v-3}{4}$ and $|\{a\} \cap D_1| = |\{-a\} \cap D_2|$, i.e., each D_i is a skew DS in G.

If $v \equiv 1 \pmod 4$, since $|D_i \cap (D_i + a)|$ is an integer, $|\{a\} \cap D_1| - |\{-a\} \cap D_2| = \pm 1$ for every nonzero $a \in G$. Hence $\{D_1, D_2\}$ is a $(v, (v-1)/2, (v-1)/2; 2)$-EDF over G if and only if for each nonzero $a \in G$ we have $|D_i \cap (D_i + a)| = \frac{v-5}{4}$ or $\frac{v-1}{4}$ and $|\{a\} \cap D_1| - |\{-a\} \cap D_2| = \pm 1$, i.e., each D_i is a $(v, (v-1)/2, (v-5)/4, (v-1)/2)$ ADS in G satisfying $D_i = -D_i$ for each i by (4). □

Proposition 29 establishes a nice connection between $(v, (v-1)/2, (v-1)/2; 2)$-EDFs and a special type of (almost) DSs. Any skew DS D or ADS D with $D = -D$ in an Abelian group yields a $(v, (v-1)/2, (v-1)/2; 2)$-EDF. Unfortunately, skew DSs seem very rare. The only known inequivalent skew DSs are the Paley DSs [19] consisting of all the nonzero quadratic residues in GF(q), where $q \equiv 3 \pmod 4$, and the skew DSs recently discovered by Ding and Yuan [8].

There are $(v, (v-1)/2, (v-5)/4, (v-1)/2)$ ADSs D in Abelian groups G, but some have the property that $D = -D$ while others do not satisfy this condition. The only known inequivalent ADSs with these parameters and this property are the Paley partial DSs [19] formed by all nonzero quadratic residues in GF(q) with $q \equiv 1 \pmod 4$. The following are $(v, (v-1)/2, (v-5)/4, (v-1)/2)$ ADS 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 $(v, (v-1)/2, (v-5)/4, (v-1)/2)$ ADSs D with $D = -D$ are rare and very hard to construct. We refer to Arasu et al. [1] for information about ADSs.

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 DSs discovered recently [8]. In view of this, we present the following problem and invite the reader to attack it.

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

7 Concluding remarks

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 $(v, k, k-1)$ DDF in G is equivalent to that of a $(v, k, v-k-1; (v-1)/k)$ EDF as described in Proposition 11. Disjoint difference families with parameters $(v, k, k-1)$ are interesting in themselves, as they have other applications [11].

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 [20] 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 $i = 1, 2, \ldots, (v-1)/2$. 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.

In Sections 3 and 4, by extending earlier ideas of cyclotomic constructions of combinatorial designs, we described a number of classes of DDFs and EDFs, which may be used to construct splitting authentication codes and secret sharing schemes with the framework of [18]. We believe that EDFs with certain parameters are very hard to construct, e.g., $(v, (v-1)/2, (v-1)/2; 2)$-EDFs, as justified in Section 6.

Finally we end this paper by presenting the following research problems.

Problem 2 Give more constructions of $(v, k, k-1)$-DDFs in Abelian groups G.

Problem 3 Complete the existence spectrum of $(v, k, k-1)$-DDF in Z_v for $k = 3, 4$.

Problem 4 Find more constructions of $(v, k, \lambda; u)$-EDFs in Abelian groups G with $ku < v - 1$.

We refer the reader to Mutoh and Tonchev [17], and Mutoh [16] for recent results regarding Problem 4.

Acknowledgements The authors thank the referees for their constructive comments and suggestions that much improved the quality of this paper. The authors also thank Tao Feng for his kind help in some computer computation.

The research of the first author is supported by TRAPOYT and NSFC under Grant No. 10371002. The research of the second author is supported by the Research Grants Council of the Hong Kong Special Administrative Region, Proj. No. HKUST6183/04E, China. The research was carried out while the first author was visiting the Hong Kong University of Science and Technology. He wishes to express his gratitude to the Department of Computer Science for their hospitality.

References

1. Arasu KT, Ding C, Helleseth T, Vijay Kumer P, Martinsen H (2001) Almost difference sets and their sequences with optimal autocorrelation. IEEE Trans Inform Theory 47:2834–2843
2. Bose RC (1939) On the construction of balanced incomplete block designs. Ann Eugen 9:353–399
3. Buratti M (1998) Recursive constructions for difference matrices and relative difference families. J Combin Des 6:165–182
4. Chang Y, Ji L (2004) Optimal $(4up, 5, 1)$ optical orthogonal codes. J Combin Des 5:346–361
5. Chen K, Zhu L (1999) Existence of $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$. J Combin Des 7:21–30
6. Colbourn MJ, Colbourn CJ (1984) Recursive constructions for cyclic block designs. J Statist Plann Inference 10:97–103
7. Colbourn CJ, de Launey W (1996) Difference matrices. In: Colbourn CJ, Dinitz JH (eds) The CRC Handbook of Combinatorial Designs. CRC Press, Boca Raton, pp 287–297
8. Ding C, Yuan J (to appear) A family of skew difference sets. J Comb Theory A
9. Dinitz JH, Rodney P (1997) Disjoint difference families with block size 3. Utilitas Math 52:153–160
10. Dinitz JH, Shalaby N (2002) Block disjoint difference families for Steiner triple systems: $v \equiv 1 \pmod 6$. J Statist Plann Inference 106:77–86
11. Fuji-Hara R, Miao Y, Shinohara S (2002) Complete sets of disjoint difference families and their applications. J Statist Plann Inference 106:87–103
12. Hall M Jr (1956) A survey of difference sets. Proc Amer Math Soc 6:975–986
13. Levenshtein VI (1971) One method of constructing quasi codes providing synchronization in the presence of errors. Prob Infor Transm 7(3):215–222

14. Levenshtein VI (2004) Combinatorial problems motivated by comma-free codes. J Combin Des 12: 184–196
15. Lidl R, Niederreiter H (1983) Finite fields. Encyclopedia of mathematics and its applications, vol. 20, Cambridge University Press, Cambridge
16. Mutoh Y *Difference systems of sets and cyclotomoy II*, preprint.
17. Mutoh Y, Tonchev VD (to appear) Difference systems of sets and cyclotomoy. Discrete Math
18. Ogata W, Kurosawa K, Stinson DR, Saido H (2004) New combinatorial designs and their applications to authentication codes and secret sharing schemes. Discrete Math 279:383–405
19. Paley REAC (1933) On orthogonal matrices. J Math Phys MIT 12:311–320
20. Stanton RG, Mullin RC (1968) Construction of room squares. Ann Math Statist 39:1540–1548
21. Storer T (1967) Cyclotomy and difference Sets. Markham, Chicago
22. Sze TW, Chanson S, Ding C, Helleseth T, Parker MG (2003) Logarithm authentication codes. Infor Comput 148(1):93–108
23. Tonchev VD (2003) Difference systems of sets and code synchronization. Rendiconti del Seminario Matematico di Messina Ser II 9:217–226
24. Wilson RM (1972) Cyclotomy and difference families in elementary Abelian groups. J Number Theory 4:17–42
25. Yin J (1998) Some combinatorial constructions for optical orthogonal codes. Discrete Math, 185:201–219