Digraph-defined external difference families and new circular external difference families

Sophie Huczynska[1], Christopher Jefferson[2], and Struan McCartney[3]

[1]*School of Mathematics and Statistics, University of St Andrews, St Andrews, KY16 9SS, Scotland, UK; email: sh70@st-andrews.ac.uk*

[2]*School of Science and Engineering, University of Dundee, Dundee, DD1 4HN, Scotland, UK; email: cjefferson001@dundee.ac.uk*

[3]*School of Mathematics and Statistics, University of St Andrews, St Andrews, KY16 9SS, Scotland, UK; email: sm444@st-andrews.ac.uk*

MSC code: 05B10

Abstract

External difference families (EDFs) are combinatorial objects which were introduced in the early 2000s, motivated by information security applications such as the construction of AMD codes. Various generalizations have since been defined and investigated, in particular strong external difference families (SEDFs) and circular external difference families (CEDFs). In this paper, we present a framework based on graphs and digraphs which offers a new unified way to view these structures, and leads to natural new research questions. We present constructions and structural results about these digraph-defined EDFs, and we obtain new explicit constructions for infinite families of CEDFs, in particular $(ml^2+1, m, l, 1)$-CEDFs. Our techniques include cyclotomy in finite fields and direct constructions in cyclic groups and direct products of cyclic groups. We construct the first infinite family of such CEDFs in non-cyclic abelian groups; these have odd values of m and l. We also present the first CEDF in a non-abelian group.

1 Introduction

External difference families (EDFs) are combinatorial objects which were introduced in the early 2000s, motivated by information security applications [7, 17]. Several variants of these have been introduced subsequently - e.g. strong external difference families (SEDFs) [18], circular external difference families (CEDFs) [21] and others. Such a family consists of a collection $\mathcal{A}$ of disjoint same-size subsets of a group G, with the property that the multiset of pairwise differences between elements of certain distinct sets in $\mathcal{A}$ contains every non-identity element of G the same number of times. This is an external analogue of traditional difference families, which have been studied since the 1930s; for these, the pairwise differences between elements within each set are considered, and their multiset

union is required to contain each non-identity element of G equally often. Relaxations of the conditions (e.g. dropping the requirement of equal set-sizes, leading to generalised EDFs (GEDFs) and generalised SEDFs (GSEDFs)) have also been explored [18].

Connections between graphs and certain internal/external difference families are well known, and have been explored for example in [4] and [14]. In these papers, the vertices of the graph correspond to the elements of the group G and (labelled) edges between them represent the differences. This provides a link to graph decomposition problems. In [3], the concept of strong difference family (SDF) is introduced as a collection of multisets such that the multiset union of their internal differences contains every element of G (including the identity) equally often. In [4], a generalised definition of SDF is introduced, in which the set of internal differences is defined via the edges of a digraph Γ, and the original definition is retrieved upon taking Γ to be complete. In [14], graph decompositions are considered which correspond directly to certain EDFs in $\mathbb{Z}_n$ via the process of development.

In this paper, we present a different connection between graph theory and external difference families and their generalizations, inspired by - but distinct from - these ideas. We observe that the sets of such a family may be associated with the vertices of a digraph, with directed edges between precisely those pairs of vertices for which the external (directed) differences between the corresponding sets contribute to the multiset of external differences. This provides a natural and useful framework in which to view EDFs and their variants, particularly SEDFs and CEDFs.

We note that a somewhat-related idea arises implicitly in [19] when an initial directed cycle is constructed, then a blow-up construction is applied to it to create a CEDF in a cyclic group. However our definition does not require any construction-based relationship between the digraph and the sets involved. The "graceful directed graphs" of [2] give examples of our structures in the specific case when the group is cyclic and every set is a singleton set.

Our work was underpinned by search for examples in GAP [9], using a constraint-satisfaction modelling language [1] and solver [10].

The paper is structured as follows: we first set up the necessary background and new definitions. We present constructions and examples of EDFs defined by complete graphs, cycles and complete bipartite graphs (both oriented and undirected). Those defined by oriented cycles (with the natural orientation) correspond to CEDFs, and we present various new results on CEDFs. In particular, we present a new infinite family of $(ml^2+1, m, l, 1)$-CEDFs in non-cyclic abelian groups; these have both m and l odd. We also give the first example of a CEDF in a non-abelian group. We end by indicating further research questions emerging from this work.

2 Background

Throughout, G will denote a finite group. Unless otherwise stated, we will write G additively. For subsets A, B of G, we define the multiset $\Delta(A,B) = \{a-b : a \in A, b \in B\}$. All unions are multiset unions unless otherwise stated.

We will frequently work in $\mathbb{Z}_n$, the additive group of integers modulo n. We consider its elements as $\{0, 1, \ldots, n-1\}$, with the natural order $0 < 1 < \cdots < n-1$. For $a, b \in \mathbb{Z}_n$,

we refer to the set of consecutive elements $\{a, a+1, \ldots, b\}$ as the *interval* $[a, b]$.

The concept of classical external difference family was first defined in [17], motivated by an application to AMD codes:

Definition 2.1. Let G be a group of order n and let $m > 1$. A family of disjoint l-sets $\{A_1, \ldots, A_m\}$ in G is an (n, m, l, λ)-EDF if the multiset equation $\bigcup_{\{i,j:i\neq j\}} \Delta(A_i, A_j) = \lambda(G \setminus \{0\})$ holds.

The following stronger version of an EDF was first defined in [18], corresponding to a stronger security model. (Note this is distinct from the notion of an SDF mentioned previously.)

Definition 2.2. Let G be a group of order n and let $m > 1$. A family of disjoint l-sets $\{A_1, \ldots, A_m\}$ in G is an (n, m, l, λ)-SEDF if, for each i with $1 \leq i \leq m$, the multiset equation $\bigcup_{\{j:j\neq i\}} \Delta(A_i, A_j) = \lambda(G \setminus \{0\})$ holds.

Note that a strong EDF will always be an EDF, but the converse need not be true.

Recently, Stinson and Veitch introduced new objects called circular external difference families [21].

Definition 2.3. Let G be a group of order n. Suppose $m > 1$ and $1 \leq c \leq m-1$. A family of disjoint l-sets $\{A_1, \ldots, A_m\}$ in G is an (n, m, l, λ)-c-CEDF if the following multiset equation holds: $\bigcup_{i=0}^{m-1} \Delta(A_{i+c \bmod m}, A_i) = \lambda(G \setminus \{0\})$.

If $c = 1$ then the c is sometimes omitted from the notation (as in [19]). We note that when $m > 3$, CEDFs are not special cases of the standard EDFs; a $(n, 3, l, \lambda)$-CEDF is a $(n, 3, l, 2\lambda)$-EDF.

We present the following observation which clarifies the structure of c-CEDFs:

Lemma 2.4. *Let $\mathcal{A} = \{A_1, \ldots, A_m\}$ be a disjoint collection of l-subsets of a group G. Suppose $\mathcal{A}$ is a c-CEDF. Then, if $\gcd(c, m) = d$, the multiset in the definition may be written as a disjoint union of d multiset unions, each involving m/d sets, as follows (where all indices are taken modulo m):*

$$\bigcup_{i=0}^{m-1} \Delta(A_{i+c}, A_i) = \bigcup_{j=0}^{d-1} \left(\bigcup_{i=0}^{(m/d-1)} \Delta(A_{(i+1)c+j}, A_{ic+j}) \right) = \lambda(G \setminus \{0\})$$

Proof. The decomposition of the m sets into d disjoint collections of m/d sets follows from the result on permutations that, if f is a cycle of length m, f^c decomposes as the product of $\gcd(c, m)$ disjoint cycles of length $m/\gcd(c, m)$. The rest of the result follows from the definition. □

The following stronger version of a CEDF has been defined [21].

Definition 2.5. Let G be a group of order n. Suppose $m \geq 2$ and $1 \leq c \leq m-1$. A family of disjoint l-sets $\{A_1, \ldots, A_m\}$ in G is an (n, m, l, λ)-c-SCEDF if, for each $0 \leq i \leq m-1$, the multiset equation $\Delta(A_{i+c}, A_i) = \lambda(G \setminus \{0\})$ holds (indices taken modulo m).

It is observed in [23] that, due to the decomposition structure, any c-SCEDF can be viewed as the disjoint union of 1-SCEDFs; the authors of [23] define a c-SCEDF to be *trivial* if it is the disjoint union of 2-set 1-SCEDFs (ie 2-set SEDFs). Using character theory it is proved that any 1-SCEDF in an abelian group must have $m = 2$ sets, and hence that any SCEDF must be trivial. Note that the use of the word *trivial* in this context does not imply that all subsets have size 1 (in contrast to the trivial difference set which is taken in the literature to be any singleton set). For example, in $\mathbb{Z}_{17}$ a trivial 2-SCEDF is given by sets $A_0 = \{1, 13, 16, 4\}, A_1 = \{3, 5, 14, 12\}, A_2 = \{9, 15, 8, 2\}$ and $A_3 = \{10, 11, 7, 6\}$.

3 A new viewpoint

We now introduce a way of defining external difference families and their generalizations in terms of graphs and digraphs.

Throughout this paper, a graph or digraph G on m vertices will have vertex set $V(G) = \{0, \ldots, m-1\}$. All graphs and digraphs will be finite and simple (no loops or multiple edges), and they will be labelled.

For a digraph G, we denote by $\overrightarrow{E}(G)$ its set of directed edges. A graph is said to be *oriented* if at most one of (i, j) or (j, i) is in the directed edge-set for each pair $i \neq j$.

For an undirected graph G (which will simply be referred to as a graph) we will view it as a digraph, by replacing each undirected edge by a pair of inverse directed edges. We define the following notation. Let the edge-set of G as an undirected graph be $E(G) = \{\{i, j\} : i, j \in V(G)\}$; then we define the *directed edge-set* $\overrightarrow{E}(G)$ of G to be

$$\overrightarrow{E}(G) := \{(i, j) \in V(G) \times V(G) : \{i, j\} \in E(G)\}.$$

Example 3.1. Consider K_3 with $V(K_3) = \{0, 1, 2\}$ and $E(K_3) = \{\{0, 1\}, \{1, 2\}, \{2, 0\}\}$; then $\overrightarrow{E}(K_3) = \{(0, 1), (0, 2), (1, 0), (1, 2), (2, 0), (2, 1)\}$.

All the digraphs which will be considered in this paper will either be oriented digraphs or undirected graphs viewed as digraphs as above.

We are now ready to define our main object of study.

Definition 3.2. Let G be a group of order n, and let $\mathcal{A} = (A_0, \ldots, A_{m-1})$ be an ordered collection of disjoint subsets of G, each of size l. Let H be a labelled digraph on m vertices $\{0, 1, \ldots, m-1\}$ and let $\overrightarrow{E}(H)$ be the set of directed edges of H. Then $\mathcal{A}$ is said to be an $(n, m, l, \lambda; H)$-EDF if the following multiset equation holds:

$$\bigcup_{(i,j) \in \overrightarrow{E}(H)} \Delta(A_j, A_i) = \lambda(G \setminus \{0\}).$$

We will call such a structure a *digraph-defined* EDF. If we wish to emphasise H, we will call it an H-defined EDF.

We introduce the following notation and labelling for commonly-used graphs and digraphs which will appear in this paper. To distinguish between an undirected and oriented version of a given underlying graph, we denote the oriented version by a superscript $*$.

- Complete graph K_m: $V(K_m) = \{0, 1, \ldots, m-1\}$ and $\overrightarrow{E}(K_m) := \{(i,j) : 0 \le i, j \le m-1, i \ne j\}$.
- Oriented complete digraph K_m^* (also known as tournament): $V(K_m^*) = \{0, 1, \ldots, m-1\}$; the standard set of directed edges will be $\overrightarrow{E}(K_m^*) := \{(i,j) : 0 \le i < j \le m-1\}$ (but we will also consider other orientations).
- Cycle graph C_m: $V(C_m) = \{0, 1, \ldots, m-1\}$ and $\overrightarrow{E}(C_m) := \{(i,j) : j \equiv i+1 \mod m \text{ or } i \equiv j+1 \mod m : 0 \le i, j \le m-1\}$.
- Oriented cycle C_m^*: $V(C_m^*) = \{0, 1, \ldots, m-1\}$; the standard set of directed edges will be $\overrightarrow{E}(C_m^*) := \{(i, i+1 \mod m) : 0 \le i \le m-1\}$.
- Complete bipartite graph $K_{a,b}$: bipartition $V(K_{a,b}) = A \cup B$ where $A = \{0, \ldots, a-1\}$ and $B = \{a, \ldots, a+b-1\}$ and $\overrightarrow{E}(K_{a,b}) := \{(i,j) : i \in A, j \in B \text{ or } i \in B, j \in A\}$.
- Oriented complete bipartite digraph $K_{a,b}^*$: bipartition $A \cup B$ where $A = \{0, \ldots, a-1\}$ and $B = \{a, \ldots, a+b-1\}$; the standard set of directed edges will be $\overrightarrow{E}(K_{a,b}^*) := \{(i,j) : i \in A, j \in B\}$.

If H with $V(H) = \{0, \ldots, m-1\}$ is a disjoint union of graphs $H_1 \cup \cdots \cup H_u$, with $|V(H_i)| = h_i$, we will take $V(H) = V(H_1) \cup \cdots \cup V(H_u)$ where $V(H_1) = \{0, \ldots, h_1 - 1\}$, $V(H_2) = \{h_1, \ldots, h_1 + h_2 - 1\}$, $\ldots$, $V(H_u) = \{h_1 + \cdots + h_{m-2}, \ldots, m-1\}$.

For an H-defined digraph when H is (an undirected or oriented) $K_{a,b}$ with bipartition $A \cup B$, we will use a semi-colon to separate the sets corresponding to the vertices of A from those corresponding to the vertices of B. If H is a disjoint union of $H_1 \cup \cdots \cup H_u$, we will similarly use semicolons to separate the sets corresponding to the vertices of distinct H_i.

Example 3.3. In $G = (\mathrm{GF}(13), +)$, let $A_0 = \{1, 5, 8, 12\}, A_1 = \{2, 3, 10, 11\}$ and $A_2 = \{4, 6, 7, 9\}$. Then (A_0, A_1, A_2) is a $(13, 3, 4, 8; C_3)$-EDF, a $(13, 3, 4, 4; C_3^*)$-EDF, a $(13, 3, 4, 8; K_3)$-EDF and a $(13, 3, 4, 4; K_3^*)$-EDF.

Remark 3.4. The structures presented in Section 2 can be put into this new framework as follows. Let $\mathcal{A} = \{A_0, \ldots, A_{m-1}\}$ be a collection of disjoint l-subsets of a group G.

- $\mathcal{A}$ is an (n, m, l, λ)-EDF precisely if $(A_0, \ldots, A_{m-1})$ is an $(n, m, l, \lambda; K_m)$-EDF.
- $\mathcal{A}$ is an (n, m, l, λ)-SEDF precisely if, for each i, $(A_0, A_1, \ldots, A_{i-1}, A_{i+1}, \ldots A_{m-1}; A_i)$ is an $(n, m, l, \lambda; K_{m-1,1}^*)$-EDF.
- $\mathcal{A}$ is an (n, m, l, λ)-1-CEDF precisely if $(A_0, \ldots, A_{m-1})$ is an $(n, m, l, \lambda; C_m^*)$-EDF.
- If $c > 1$ and $\gcd(c, m) = 1$, $\mathcal{A}$ is an (n, m, l, λ)-c-CEDF precisely if $(A_0, A_c, A_{2c}, \ldots, A_{c(m-1)})$ is an $(n, m, l, \lambda; C_m^*)$-EDF (where indices are taken modulo m).
- If $\gcd(c, m) = d > 1$, $\mathcal{A}$ is an (n, m, l, λ)-c-CEDF precisely if

  $$(A_0, A_c, \ldots, A_{(m/d-1)c}; A_1, A_{1+c}, \ldots, A_{1+(m/d-1)c}; \ldots; A_{(d-1)}, \ldots, A_{(d-1)+(m/d-1)c})$$

  is an $(n, m, l, \lambda; H)$-EDF where H is the disjoint union of d oriented cycles $C_{m/d}^*$ if $m/d \ge 3$ and the disjoint union of d undirected paths P_1 if $m/d = 2$.

Example 3.5. The $(17, 4, 4, 4)$-2-CEDF in $\mathbb{Z}_{17}$ given by sets $A_0 = \{1, 13, 16, 4\}, A_1 = \{3, 5, 14, 12\}, A_2 = \{9, 15, 8, 2\}$ and $A_3 = \{10, 11, 7, 6\}$ is a $(17, 4, 4, 4; H)$-EDF, where $V(H) = \{0, 1, 2, 3\}$ and H is the disjoint union $H_1 \cup H_2$ where $\overrightarrow{E}(H_1) = \{(0, 2), (2, 0)\}$ and $\overrightarrow{E}(H_2) = \{(1, 3), (3, 1)\}$.

Finally we present relationships between EDFs defined by directed and undirected versions of the same underlying graph.

Theorem 3.6. *Let G be a group of order n. Let H be a graph on m vertices and let H^* denote any orientation of H. If $\mathcal{A}$ is an $(n, m, l, \lambda; H^*)$-EDF, then $\mathcal{A}$ is an $(n, m, l, 2\lambda; H)$-EDF.*

We also have the following partial converse.

Theorem 3.7. *Let G be a group of order n. Let H be a graph on m vertices and let H^* denote any orientation of H. If $\mathcal{A} = (A_0, \ldots, A_{m-1})$ is an $(n, m, l, \lambda; H)$-EDF and $\Delta(A_i, A_j) = \Delta(A_j, A_i)$ for all edges $\{i, j\}$ of H, then λ is even and $\mathcal{A}$ is an $(n, m, l, \lambda/2; H^*)$-EDF.*

Proof. Denote by $\overline{H^*}$ a copy of H with the reverse orientation to that of H^*. So $(i, j) \in \overrightarrow{E}(\overline{H^*})$ precisely if $(j, i) \in \overrightarrow{E}(H^*)$ and we have $\overrightarrow{E}(H) = \overrightarrow{E}(H^*) \cup \overrightarrow{E}(\overline{H^*})$. Each edge $\{i, j\} \in E(H)$ is the union of $(i, j) \in \overrightarrow{E}(H^*)$ and $(j, i) \in \overrightarrow{E}(\overline{H^*})$. For each $\{i, j\} \in E(H)$, since $\Delta(A_i, A_j) = \Delta(A_j, A_i)$, there is a contribution of $\Delta(A_i, A_j)$ to the difference multisets of the H^*-defined EDF and of the $\overline{H^*}$-defined EDF, corresponding to a contribution of $2\Delta(A_i, A_j)$ to the difference multiset of the EDF, which equals $\lambda(G \setminus \{0\})$. The result follows. □

While these relationships are helpful in understanding the links between directed and undirected versions, they are far from describing the whole picture. There are many examples of both type of EDF which do not result from applying Theorems 3.6 or 3.7 to an EDF of the other type.

4 H-defined EDFs when H is complete

As we have seen, the H-defined EDFs when $H = K_m$ precisely correspond to the standard EDFs. These structures have been much-studied and so we will mention them only briefly here. In contrast, those with $H = K_m^*$ do not - to our knowledge - correspond to previously-investigated types of external difference families.

4.1 External difference families

The standard EDFs have received considerable attention and many results about them are known [14, 18]. However, it is perhaps worth noting that, due to their relative lack of structure compared to other variations of the definition, there are fewer known general constructions for EDFs than there are for EDFs with extra conditions such as SEDFs.

In order to present a useful general construction, we require a few facts about cyclotomy. For more information on cyclotomy, see [20]. Let q be a power of a prime p and let $\mathrm{GF}(q)$ denote the finite field of order q. Let α be a primitive element of $\mathrm{GF}(q)$.

Definition 4.1. Let $q = ef + 1$ where $e, f \in \mathbb{N}$. The cyclotomic classes C_i^e in GF(q) of order e ($0 \leq i \leq e-1$) are defined as:

$$C_i^e = \{\alpha^{es+i} : 0 \leq s \leq f-1\}.$$

Here, C_0^e is the multiplicative subgroup of GF(q) of cardinality f.

We now present the following well-known EDF construction [6, 8]:

Theorem 4.2. *Let $q = ef + 1$ be a prime power. Then the set $\{C_0^e, \ldots, C_{e-1}^e\}$ of all cyclotomic classes of order e in $GF(q)$ forms a $(q, e, f, (e-1)f; K_e)$-EDF.*

Example 4.3. In $GF(13)$, taking $e = 3$ and $\alpha = 2$, we have that (C_0^3, C_1^3, C_2^3) forms a $(13, 3, 4, 8; K_3)$-EDF, where $C_0^3 = \{1, 5, 12, 8\}, C_1^3 = \{2, 10, 11, 3\}$ and $C_2^3 = \{4, 7, 9, 6\}$.

4.2 Tournament-defined EDFs

We establish the following results for EDFs defined by tournaments. By Theorem 3.6, any EDF defined by a tournament yields an EDF in the standard sense, while by Theorem 3.7, a standard EDF which satisfies an extra condition may be used to obtain a tournament-defined EDF.

We present a direct cyclotomic construction for tournament-defined EDFs. We first need a technical lemma (Lemma 3.13 from [11]):

Lemma 4.4. *Let $q = ef + 1$ be a prime power. If either e is odd, or e is even and $q \equiv 1 \mod 2e$, then $-1 \in C_0^e$.*

Theorem 4.5. *Let $q = ef + 1$ be a prime power such that either e is odd, or e is even and $q \equiv 1 \mod 2e$. Let K_e^* be a tournament with an arbitrary orientation. Let $\mathcal{A} = (C_0^e, \ldots, C_{e-1}^e)$. Then $\mathcal{A}$ forms a $(q, e, f, (e-1)f/2; K_e^*)$-EDF in $GF(q)$.*

Proof. By Theorem 4.2, $\mathcal{A}$ is a $(q, e, f, (e-1)f); K_e)$-EDF. In both cases (i) and (ii) of Lemma 4.4, $-1 \in C_0^e$, hence $C_i^e = -C_i^e$ for all $0 \leq i \leq e-1$ and so $\Delta(C_i^e, C_j^e) = \Delta(C_j^e, C_i^e)$ for all $0 \leq i, j \leq m-1$. In both cases, $(e-1)f$ is even and the result follows by Theorem 3.7. □

Example 4.6. In GF(13), consider the cyclotomic classes C_0^3, C_1^3, C_2^3 of order 3. By Theorem 4.5, since $e = 3$ is odd, (C_0^3, C_1^3, C_2^3) form a $(13, 3, 4, 4; K_3^*)$-EDF, where K_3^* is a tournament on 3 vertices with arbitrary orientation. Note that these same sets were discussed in Example 3.3 and Example 4.3.

5 H-defined EDFs when H is a cycle or union of cycles

We have seen that CEDFs correspond to oriented cycles, or disjoint unions of same-size oriented cycles, with the standard orientation (where we include a single undirected edge as a directed cycle of length 2).

5.1 Circular external difference families

CEDFs were introduced in [21] and various results have been established about them. In [21], sufficient conditions for the existence of certain cyclotomic CEDFs in the additive group of a finite field were given in terms of primitive elements of the field. The cyclotomic approach was further extended in [23]; this paper also contains structural characterizations and non-existence results for strong CEDFs. In [19], existence of infinite families of CEDFs with $\lambda = 1$ in cyclic groups was established using graceful labellings of graphs. (We note that the use of graceful labellings in the strong difference family context appeared in [4]). In [5], constructions are given in cyclic groups for CEDFs with $\lambda = 1$, for cases not previously covered. In this section, we present various new results for CEDFs.

In [19], Theorem 1.8 states three main results on $(ml^2+1, m, l, 1)$-1-CEDFs in abelian groups. The second part asserts that if l and m are odd then there is no $(ml^2+1, m, l, 1)$-1-CEDF. It seems that this result holds only in the context of cyclic groups, since we show that an infinite family of 1-CEDFs with such parameters exist in non-cyclic abelian groups.

5.2 CEDFs in abelian non-cyclic groups and non-abelian groups

We present a construction for an infinite family of CEDFs in abelian groups which are not cyclic nor elementary abelian.

Theorem 5.1. *Let $l \equiv 3 \mod 4$ ($l \in \mathbb{N}$). Denote $z = \frac{3}{4}(l-1)^2 \in \mathbb{N}$. Define the following subsets of $\mathbb{Z}_{\frac{3l^2+1}{2}} \times \mathbb{Z}_2$:*

- $A_0 = \bigcup_{i=0}^{l-1}\{(i,0)\}$
- $A_1 = \bigcup_{i=0}^{l-1}\{(z(i-1)-l-i, i+1)\}$
- $A_2 = \bigcup_{i=0}^{l-1}\{(zi-l, i)\}$

where the first component is taken modulo $\frac{3l^2+1}{2}$ and the second component is taken modulo 2.
Then (A_0, A_1, A_2) form a $(3l^2+1, 3, l, 1)$-CEDF in the non-cyclic abelian group $\mathbb{Z}_{\frac{3l^2+1}{2}} \times \mathbb{Z}_2$.

To aid the reader's intuition, we first present some specific examples of Theorem 5.1. While the statement of the construction may look uninuitive, the occurrence of the differences follows a very natural and regular pattern, as can be seen from the associated subtraction tables.

Example 5.2. We consider the following special cases of Theorem 5.1.

(i) Take $l = 3$ in Theorem 5.1. We obtain a $(28, 3, 3, 1)$-CEDF in $\mathbb{Z}_{14} \times \mathbb{Z}_2$ with sets $A_0 = \{(0,0), (1,0), (2,0)\}$, $A_1 = \{(8,1), (10,0), (12,1)\}$ and $A_2 = \{(11,0), (0,1), (3,0)\}$. The subtraction table is shown in Table 1.

(ii) Take $l = 7$ in Theorem 5.1. We obtain a $(148, 3, 7, 1)$-CEDF in $\mathbb{Z}_{74} \times \mathbb{Z}_2$ with sets

- $A_0 = \{(0,0), (1,0), (2,0), (3,0), (4,0), (5,0), (6,0)\}$

– $A_1 = \{(40,1),(66,0),(18,1),(44,0),(70,1),(22,0),(48,1)\}$

– $A_2 = \{(67,0),(20,1),(47,0),(0,1),(27,0),(54,1),(7,0)\}$.

The subtraction tables for $\Delta(A_1, A_0), \Delta(A_2, A_1)$ and $\Delta(A_0, A_2)$ are given in Table 2, Table 3 and Table 4 respectively.

–	$(0,0)$	$(1,0)$	$(2,0)$	$(8,1)$	$(10,0)$	$(12,1)$	$(11,0)$	$(0,1)$	$(3,0)$
$(0,0)$							$(3,0)$	**(0,1)**	$(11,0)$
$(1,0)$							$(4,0)$	**(1,1)**	$(12,0)$
$(2,0)$							$(5,0)$	**(2,1)**	$(13,0)$
$(8,1)$	**(8,1)**	**(7,1)**	**(6,1)**						
$(10,0)$	$(10,0)$	$(9,0)$	$(8,0)$						
$(12,1)$	**(12,1)**	**(11,1)**	**(10,1)**						
$(11,0)$				**(3,1)**	$(1,0)$	**(13,1)**			
$(0,1)$				$(6,0)$	**(4,1)**	$(2,0)$			
$(3,0)$				**(9,1)**	$(7,0)$	**(5,1)**			

Table 1: Subtraction table for the construction in $\mathbb{Z}_{14} \times \mathbb{Z}_2$ from Theorem 5.1

–	$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(4,0)$	$(5,0)$	$(6,0)$
$(40,1)$	**(40,1)**	**(39,1)**	**(38,1)**	**(37,1)**	**(36,1)**	**(35,1)**	**(34,1)**
$(66,0)$	$(66,0)$	$(65,0)$	$(64,0)$	$(63,0)$	$(62,0)$	$(61,0)$	$(60,0)$
$(18,1)$	**(18,1)**	**(17,1)**	**(16,1)**	**(15,1)**	**(14,1)**	**(13,1)**	**(12,1)**
$(44,0)$	$(44,0)$	$(43,0)$	$(42,0)$	$(41,0)$	$(40,0)$	$(39,0)$	$(38,0)$
$(70,1)$	**(70,1)**	**(69,1)**	**(68,1)**	**(67,1)**	**(66,1)**	**(65,1)**	**(64,1)**
$(22,0)$	$(22,0)$	$(21,0)$	$(20,0)$	$(19,0)$	$(18,0)$	$(17,0)$	$(16,0)$
$(48,1)$	**(48,1)**	**(47,1)**	**(46,1)**	**(45,1)**	**(44,1)**	**(43,1)**	**(42,1)**

Table 2: $\Delta(A_1, A_0)$ for the construction in $\mathbb{Z}_{74} \times \mathbb{Z}_2$ from Theorem 5.1

We now provide the proof of Theorem 5.1. The reader may find it helpful to consult the tables for the $l = 3$ and $l = 7$ cases as they navigate the proof.

Proof. Since $l \equiv 3 \mod 4$, $(3l^2+1)/2$ is even and hence $\mathbb{Z}_{\frac{3l^2+1}{2}} \times \mathbb{Z}_2$ is not a cyclic group. We will show that $\Delta(A_1, A_0) \cup \Delta(A_2, A_1) \cup \Delta(A_0, A_2) = G \setminus \{0\}$; note that disjointness of the three sets then follows from the fact that 0 does not occur in the multiset of differences. Since the difference multiset contains $3l^2$ elements by construction, it will suffice to show that each non-identity group element occurs at least once.
For $a, b \in \mathbb{Z}_{\frac{3l^2+1}{2}}$ and $x \in \mathbb{Z}_2$, we will adapt our previous interval notation as follows: we

−	(40, 1)	(66, 0)	(18, 1)	(44, 0)	(70, 1)	(22, 0)	(48, 1)
(67, 0)	**(27,1)**	(1, 0)	**(49,1)**	(23, 0)	**(71,1)**	(45, 0)	**(19,1)**
(20, 1)	(54, 0)	**(28,1)**	(2, 0)	**(50,1)**	(24, 0)	**(72,1)**	(46, 0)
(47, 0)	**(7,1)**	(55, 0)	**(29,1)**	(3, 0)	**(51,1)**	(25, 0)	**(73,1)**
(0, 1)	(34, 0)	**(8,1)**	(56, 0)	**(30,1)**	(4, 0)	**(52,1)**	(26, 0)
(27, 0)	**(61,1)**	(35, 0)	**(9,1)**	(57, 0)	**(31,1)**	(5, 0)	**(53,1)**
(54, 1)	(14, 0)	**(62,1)**	(36, 0)	**(10,1)**	(58, 0)	**(32,1)**	(6, 0)
(7, 0)	**(41,1)**	(15, 0)	**(63,1)**	(37, 0)	**(11,1)**	(59, 0)	**(33,1)**

Table 3: $\Delta(A_2, A_1)$ for the construction in $\mathbb{Z}_{74} \times \mathbb{Z}_2$ from Theorem 5.1

−	(67, 0)	(20, 1)	(47, 0)	(0, 1)	(27, 0)	(54, 1)	(7, 0)
(0, 0)	(7, 0)	**(54,1)**	(27, 0)	**(0,1)**	(47, 0)	**(20,1)**	(67, 0)
(1, 0)	(8, 0)	**(55,1)**	(28, 0)	**(1,1)**	(48, 0)	**(21,1)**	(68, 0)
(2, 0)	(9, 0)	**(56,1)**	(29, 0)	**(2,1)**	(49, 0)	**(22,1)**	(69, 0)
(3, 0)	(10, 0)	**(57,1)**	(30, 0)	**(3,1)**	(50, 0)	**(23,1)**	(70, 0)
(4, 0)	(11, 0)	**(58,1)**	(31, 0)	**(4,1)**	(51, 0)	**(24,1)**	(71, 0)
(5, 0)	(12, 0)	**(59,1)**	(32, 0)	**(5,1)**	(52, 0)	**(25,1)**	(72, 0)
(6, 0)	(13, 0)	**(60,1)**	(33, 0)	**(6,1)**	(53, 0)	**(26,1)**	(73, 0)

Table 4: $\Delta(A_0, A_2)$ for the construction in $\mathbb{Z}_{74} \times \mathbb{Z}_2$ from Theorem 5.1

denote the set $\{(a, x), (a + 1, x), \ldots, (b, x)\}$ by $[a, b] \times \{x\}$.
First, we determine the difference multisets.

$$\begin{aligned}\Delta(A_1, A_0) &= \bigcup_{i=0}^{l-1}\bigcup_{j=0}^{l-1}\{z(i-1) - l - i - j, i + 1)\} \\ &= \bigcup_{i=0}^{l-1}[z(i-1) - 2l + 1 - i, z(i-1) - l - i] \times \{i + 1\}\end{aligned}$$

We may view these differences as consisting of l length-l "runs" of consecutive elements in the first coordinate, which occur horizontally in the difference table, indexed by i. Each run has fixed second coordinate, and the parity of the second coordinate alternates as i takes values from 0 to $l - 1$.

Next we have:

$$\begin{aligned}\Delta(A_2, A_1) &= \bigcup_{i=0}^{l-1}\bigcup_{j=0}^{l-1}\{(zi - l - z(j-1) + l + j, i - j + 1)\} \\ &= \bigcup_{i=0}^{l-1}\bigcup_{j=0}^{l-1}\{(z(i - j + 1) + j, i - j + 1)\}.\end{aligned}$$

We let $k = i - j + 1$: since i and j vary from 0 to $l - 1$, k takes values from $-l + 2$ to l.

We change the indices from i and j to k and j. For $-l+2 \le k \le l$, let

$$J_k = \{j : 0 \le j \le l-1 \text{ and } 0 \le k+j-1 \le l-1\} = [0, l-1] \cap [1-k, l-k]$$

so that

$$\Delta(A_2, A_1) = \bigcup_{k=-l+2}^{l} \bigcup_{j \in J_k} \{(zk+j, k)\}.$$

For $-l+2 \le k \le 0$, we have $J_k = [1-k, l-1]$, while for $1 \le k \le l$ we have $J_k = [0, l-k]$. Thus we have:

$$\Delta(A_2, A_1) = \bigcup_{k=-l+2}^{0} \bigcup_{j=1-k}^{l-1} \{(zk+j, k)\} \cup \bigcup_{k=1}^{l} \bigcup_{j=0}^{l-k} \{(zk+j, k)\}$$

$$= \bigcup_{k=-l+2}^{0} ([zk+1-k, zk+l-1] \times \{k\}) \cup \bigcup_{k=1}^{l} ([zk, zk+l-k] \times \{k\})$$

We may view these differences as "runs" of consecutive elements (in the first coordinate) occurring diagonally in the difference table, indexed by k and "wrapping around" the table to $k-(l-1)$. The set J_k allows for the adjustment of the length of the differences depending on which diagonal we are considering. Again, we have alternation between 0 and 1 in the second coordinate for each run.

Finally:

$$\begin{aligned}\Delta(A_0, A_2) &= \bigcup_{i=0}^{l-1} \bigcup_{j=0}^{l-1} \{(i - zj + l, j)\} \\ &= \bigcup_{j=0}^{l-1} [-zj+l, -zj+2l-1] \times \{j\}\end{aligned}$$

These differences we may view as "runs" of consecutive elements (in the first coordinate) occurring vertically in the difference table, indexed by j, with alternation in the second coordinate.

Having obtained expressions for each part of the difference multiset, we now check that the difference multiset has one occurrence of each non-identity element in $\mathbb{Z}_{\frac{3l^2+1}{2}} \times \{0\}$. We consider the differences corresponding to the following indices, where $0 \le s \le \frac{l-3}{2}$.

- $k = -2s$ in $\Delta(A_2, A_1)$: the difference multiset obtained is

$$\begin{aligned}&[z(-2s)+1+2s, z(-2s)+l-1] \times \{-2s\} \\ &= [(3l-1)s+2s+1, (3l-1)s+l-1] \times \{0\} \\ &= [(3l+1)s+1, (3l-1)s+l-1] \times \{0\}.\end{aligned}$$

  Here we have applied the simplification $2z = \frac{3(l^2-2l+1)}{2} = \frac{3l^2+1}{2} + \frac{2-6l}{2} \equiv 1-3l \mod \frac{3l^2+1}{2}$.

- $j = 2s$ in $\Delta(A_0, A_2)$: the difference multiset obtained is

$$\begin{aligned}&[(-z(2s) + l, -z(2s) + 2l - 1] \times \{2s\}\\ &= [((3l-1)s + l, (3l-1)s + 2l - 1] \times \{0\}.\end{aligned}$$

- $k = l - 1 - 2s$ in $\Delta(A_2, A_1)$: since $2 \le l - 1 - 2s \le l - 1$, the difference multiset obtained is

$$\begin{aligned}&[z(l-1-2s), z(l-1-2s) + l - (l - 2s - 1)] \times \{l - 1 - 2s\}\\ &= [(3l-1)s + z(l-1), (3l-1)s + z(l-1) + 2s + 1] \times \{0\}\\ &= [(3l-1)s + 2l, ((3l-1)s + 2l + 2s + 1] \times \{0\}\\ &= [(3l-1)s + 2l, (3l+1)s + 2l + 1] \times \{0\}.\end{aligned}$$

  Here we have applied the simplification $z(l-1) = \frac{3}{4}(l-1)^3 \equiv (\frac{l-1}{2})(1-3l) = -(\frac{3l^2+1}{2}) + 2l \equiv 2l \mod \frac{3l^2+1}{2}$.

- $i = l - 2 - 2s$ in $\Delta(A_1, A_0)$: the difference multiset obtained is

$$\begin{aligned}&[z(l-3-2s) - 2l + 1 - (l - 2 - 2s),\\ &z(l-3-2s) - l - (l - 2 - 2s)] \times \{l - 1 - 2s\}\\ &= [(3l-1)s + (5l-1) - 3l + 3 + 2s), (3l-1)s + (5l-1) - 2l + 2 + 2s] \times \{0\}\\ &= [(3l+1)s + 2l + 2, (3l+1)s + 3l + 1] \times \{0\}.\end{aligned}$$

The union of these is $[(3l+1)s + 1, (3l+1)(s+1)] \times \{0\}$. As s ranges from 0 to $\frac{l-3}{2}$ we obtain one copy of:

$$[1, \frac{3l^2+1}{2} - l - 1] \times \{0\}$$

Finally, we take $j = l - 1$ in $\Delta(A_0, A_2)$. This contributes the set of differences

$$[\frac{3l^2+1}{2} - l, \frac{3l^2+1}{2} - 1] \times \{0\}.$$

Now we consider the elements of $\mathbb{Z}_{\frac{3l^2+1}{2}} \times \{1\}$. We will use four sets of indices, of which the first and third set apply only to $l \ge 7$. We omit the details of the calculations, since they are very similar to those above.

First, we consider the differences corresponding to the following indices, where $0 \le s \le \frac{l-7}{4}$ (note these terms do not occur when $l = 3$):

- $j = \frac{l-1}{2} + 2s$ in $\Delta(A_0, A_2)$: differences $[(3l-1)s, (3l-1)s + l - 1)] \times \{1\}$;
- $k = \frac{l-1}{2} - 2s$ in $\Delta(A_2, A_1)$: differences $[(3l-1)s + l, (3l+1)s + \frac{3l+1}{2}] \times \{1\}$;
- $i = \frac{l-3}{2} - 2s$ in $\Delta(A_1, A_0)$: differences $[(3l+1)s + \frac{3l+3}{2}, (3l+1)s + \frac{5l+1}{2}] \times \{1\}$;
- $k = \frac{-l-3}{2} - 2s$ in $\Delta(A_2, A_1)$: differences $[(3l+1)s + \frac{5l+3}{2}, (3l-1)s + 3l - 2] \times \{1\}$.

The union of these is $[(3l-1)s, (3l-1)(s+1)-1] \times \{1\}$. As s ranges from 0 to $\frac{l-7}{4}$ we obtain one copy of:

$$[0, \frac{3l^2-10l-1}{4}] \times \{1\}$$

Next we take $j = l-2$ in $\Delta(A_0, A_2)$, $k = 1$ in $\Delta(A_2, A_1)$, and $i = 0$ in $\Delta(A_1, A_0)$; these contribute the differences:

$$[\frac{3l^2-10l+3}{4}, \frac{3l^2-6l-1}{4}] \times \{1\};$$

$$[\frac{3l^2-6l+3}{4}, \frac{3l^2-2l-1}{4}] \times \{1\};$$

$$[\frac{3l^2-2l+3}{4}, \frac{3l^2+2l-1}{4}] \times \{1\};$$

respectively. (Note that, for $l = 3$, this range of differences is $[0, 8] \times \{1\}$.)

We now take the differences corresponding to the following indices, where $0 \leq s \leq \frac{l-7}{4}$ (as in the first case, note these terms do not occur when $l = 3$):

- $k = l - 2s$ in $\Delta(A_2, A_1)$: differences $[(3l-1)s + \frac{3l^2+2l+3}{4}, (3l+1)s + \frac{3l^2+2l+3}{4}] \times \{1\}$;
- $i = l-1-2s$ in $\Delta(A_1, A_0)$: differences $[(3l+1)s + \frac{3l^2+2l+7}{4}, (3l+1)s + \frac{3l^2+6l+3}{4}] \times \{1\}$;
- $k = -1-2s$ in $\Delta(A_2, A_1)$: differences $[(3l+1)s + \frac{3l^2+6l+7}{4}, (3l-1)s + \frac{3l^2+10l-5}{4}] \times \{1\}$;
- $j = 1+2s$ in $\Delta(A_0, A_2)$: differences $[(3l-1)s + \frac{3l^2+10l-1}{4}, (3l-1)s + \frac{3l^2+14l-5}{4}] \times \{1\}$.

The union of these is $[(3l-1)s + \frac{3l^2+2l+3}{4}, (3l-1)(s+1) + \frac{3l^2+2l-1}{4}] \times \{1\}$ As s ranges from 0 to $\frac{l-7}{4}$ this gives one copy of:

$$[\frac{3l^2+2l+3}{4}, \frac{3l^2-4l+1}{2}] \times \{1\}$$

Finally we take $k = \frac{l+3}{2}$ in $\Delta(A_2, A_1)$, $i = \frac{l+1}{2}$ in $\Delta(A_1, A_0)$ and $k = \frac{-l+1}{2}$ in $\Delta(A_2, A_1)$. These contribute the differences:

$$[\frac{3l^2-4l+3}{2}, \frac{3l^2-3l}{2}] \times \{1\};$$

$$[\frac{3l^2-3l+2}{2}, \frac{3l^2-l}{2}] \times \{1\};$$

$$[\frac{3l^2-l+2}{2}, \frac{3l^2+1}{2} - 1] \times \{1\};$$

respectively. (Note that, for $l = 3$, this range of differences is $[9, 13] \times \{1\}$.)

We have shown that $\Delta(A_1, A_0) \cup \Delta(A_2, A_1) \cup \Delta(A_0, A_2)$ comprises one copy of each non-identity element in $\mathbb{Z}_{\frac{3l^2+1}{2}} \times \mathbb{Z}_2$, and so (A_0, A_1, A_2) form a $(3l^2+1, 3, l, 1)$-CEDF in $\mathbb{Z}_{\frac{3l^2+1}{2}} \times \mathbb{Z}_2$. □

We next present the first example of a CEDF in a non-abelian group. This was found by computational search in GAP [9] using a constraint-satisfaction technique.

Example 5.3. Denote by D_{28} the dihedral group with the standard presentation $\langle r, s : \mathrm{ord}(r) = 14, \mathrm{ord}(s) = 2, srs = r^{-1}\rangle$. Consider the following subsets of D_{28}:

- $A_0 = \{id, r^{11}, r^8\}$
- $A_1 = \{r^4, sr^2, sr^6\}$
- $A_2 = \{r^3, r^5, sr^4\}$.

Then (A_0, A_1, A_2) is a $(28, 3, 3, 1)$-CEDF in D_{28}. It can be verified directly that

- $\Delta(A_1, A_0) = \{r^4, r^{10}, r^7, sr^2, sr^8, sr^5, sr^6, sr^{12}, sr^9\}$
- $\Delta(A_2, A_1) = \{r^{13}, sr^{13}, sr^3, r, sr^{11}, sr, s, r^{12}, r^2\}$
- $\Delta(A_0, A_2) = \{r^{11}, r^9, sr^4, r^8, r^6, sr^7, r^5, r^3, sr^{10}\}$.

Observe that this non-abelian CEDF has the same parameters as the abelian CEDF obtained from Theorem 5.1 in $\mathbb{Z}_{14} \times \mathbb{Z}_2$ when $l = 3$.

5.3 Inequivalent CEDFs in cyclic groups

In [19], a construction is given for $(ml^2 + 1, m, l, 1)$-CEDFs in the cyclic group $\mathbb{Z}_{ml^2+1}$ using α-valuations, in the case when m is even. In this section, we define the notion of equivalence for CEDFs and exhibit a CEDF construction in cyclic groups which provides inequivalent CEDFs with the same parameters.

Definition 5.4. Let G be an abelian group. Let $\mathcal{A} = (A_0, \ldots, A_{m-1})$ and $\mathcal{B} = (B_0, \ldots, B_{m-1})$ be two (n, m, l, λ)-c-CEDFs in G. We shall say that $\mathcal{A}$ is equivalent to $\mathcal{B}$ if there exist an automorphism σ of G and an element $\beta \in G$ such that, for all $0 \leq i \leq m-1$, $B_{i+c \mod m} = \sigma(A_i) + \beta$ for some $c \in \{0, \ldots, m-1\}$. If $G = \mathbb{Z}_n$, this simplifies to the following definition: $\mathcal{A}$ is equivalent to $\mathcal{B}$ if there exist $\alpha, \beta \in \mathbb{Z}_n$, where α is a unit of the ring $\mathbb{Z}_n$, such that for all $0 \leq i \leq m-1$, $B_{i+c \mod m} = \alpha A_i + \beta$ for some $c \in \{0, \ldots, m-1\}$.

For a subset D of a group G, we define the multiset of internal differences by $\Delta(D) = \{x - y : x \neq y \in D\}$. Recall that for subsets A, B of G, the multiset $\Delta(A, B)$ is given by $\{x - y : x \in A, y \in B\}$. Note that $\Delta(A, A) = \Delta(A) + |A|\{0\}$.

We will need the following prior result, which we state without proof.

Lemma 5.5. *Let $n \in \mathbb{N}$ and $G = \mathbb{Z}_n$.*

(i) For an interval $I = [0, k]$ in G with $k < n/2$, the maximum multiplicity of an element in $\Delta(I, I)$ is $k + 1$ (attained by element 0).

(ii) For an interval $I = [0, k]$ in G with $k < n/2$, the maximum multiplicity of an element in $\Delta(I)$ is k (attained by elements ± 1).

(iii) For a subset A of G and $\alpha \in G$, the following hold:

1) $\Delta(A) = \Delta(A + \alpha)$ and $\Delta(A, A) = \Delta(A + \alpha, A + \alpha)$

(2) $\Delta(\alpha A) = \alpha(\Delta(A))$ and $\Delta(\alpha A, \alpha A) = \alpha(\Delta(A, A))$

(3) $\Delta(A+\alpha, A) = \Delta(A, A) + \alpha$.

Theorem 5.6. *Let $l \in \mathbb{N}$ and let d be a divisor of l. Define $\mathcal{A} = (A_0, A_1, A_2, A_3)$ to be the following (ordered) collection of sets in $\mathbb{Z}_{4l^2+1}$:*

- $A_0 = \{i : 0 \leq i \leq l-1\}$;
- $A_1 = \bigcup_{k=0}^{d-1} \{\frac{l^2(2k+1)}{d} + (i+1)l : 0 \leq i \leq \frac{l}{d} - 1\}$;
- $A_2 = A_0 + \frac{l^2}{d} = \{\frac{l^2}{d} + i : 0 \leq i \leq l-1\}$;
- $A_3 = A_1 + 2l^2 = \bigcup_{k=0}^{d-1} \{\frac{l^2(2(k+d)+1)}{d} + (i+1)l : 0 \leq i \leq \frac{l}{d} - 1\}$.

Then

(i) $\mathcal{A}$ is a $(4l^2+1, 4, l, 1)$-CEDF in $\mathbb{Z}_{4l^2+1}$.

(ii) For any two distinct proper divisors d_1, d_2 of l such that $l \neq d_1 d_2$, the two $(4l^2+1, 4, l, 1)$-CEDFs obtained in (i) are non-equivalent. In particular, this guarantees at least two non-equivalent $(4l^2+1, 4, l, 1)$-CEDFs for any composite l.

Proof. For (i), we order the elements of $\mathbb{Z}_{4l^2+1}$ in the usual way as $0 < \cdots < 4l^2$. Since $d(l-1) < l^2$ (as $d|l$), we have that all elements of A_0 precede all elements of A_2 (which lie between l^2/d and $l^2/d + l - 1$), which in turn precede all elements of A_1 (which lie between $l^2/d + l$ and $2d(l^2/d) = 2l^2$), which in turn precede all elements of A_3 (which lie between $(2d+1)l^2/d + l$ and $4l^2$). All four sets are pairwise disjoint and have no internal repetition of elements. We now show that the multiset equation $\cup_{i=0}^{3} \Delta(A_{i+1 \mod 4}, A_i) = (\mathbb{Z}_{4l^2+1} \setminus \{0\})$ holds for $\mathcal{A}$. We will show that $\Delta(A_1, A_0) \cup \Delta(A_0, A_3) = [1, 2l^2]$ and $\Delta(A_2, A_1) \cup \Delta(A_3, A_2) = [2l^2+1, 4l^2]$.

$$\begin{aligned}
\Delta(A_1, A_0) &= \bigcup_{k=0}^{d-1} \{\frac{l^2(2k+1)}{d} + (i+1)l - j\} : 0 \leq i \leq \frac{l}{d} - 1, 0 \leq j \leq l-1\} \\
&= \bigcup_{k=0}^{d-1} \bigcup_{i=0}^{\frac{l}{d}-1} \bigcup_{j=0}^{l-1} \{\frac{l^2(2k+1)}{d} + (i+1)l - j\} \\
&= \bigcup_{k=0}^{d-1} \bigcup_{i=0}^{\frac{l}{d}-1} [\frac{l^2(2k+1)}{d} + il + 1, \frac{l^2(2k+1)}{d} + (i+1)l] \\
&= \bigcup_{k=0}^{d-1} [\frac{l^2(2k+1)}{d} + 1, \frac{l^2(2k+2)}{d}]
\end{aligned}$$

Using the fact that $-2l^2 \equiv 2l^2 + 1 \mod 4l^2 + 1$, we have

$$\begin{aligned}
\Delta(A_0, A_3) &= \Delta(A_0, A_1 + 2l^2) \\
&= -\Delta(A_1, A_0) - 2l^2 \\
&= 2l^2 + 1 - \Delta(A_1, A_0) \\
&= 2l^2 + 1 + \bigcup_{k=0}^{d-1} [-\frac{l^2(2k+2)}{d}, -\frac{l^2(2k+1)}{d} - 1] \\
&= \bigcup_{k=0}^{d-1} [\frac{l^2(2d-2k-2)}{d} + 1, \frac{l^2(2d-2k-1)}{d}] \\
&= \bigcup_{k=0}^{d-1} [\frac{l^2(2k)}{d} + 1, \frac{l^2(2k+1)}{d}]
\end{aligned}$$

where in the final step we take $d - 1 - k$ instead of k.

Hence

$$\Delta(A_1, A_0) \cup \Delta(A_0, A_3) = \bigcup_{k=0}^{d-1} [\frac{l^2(2k)}{d} + 1, \frac{l^2(2k+2)}{d}] = [1, 2l^2].$$

Next,

$$\begin{aligned}
\Delta(A_2, A_1) &= \Delta(A_0 + \frac{l^2}{d}, A_1) \\
&= -\Delta(A_1+, A_0) + \frac{l^2}{d} \\
&= -\bigcup_{k=0}^{d-1} [\frac{l^2(2k+1)}{d} + 1, \frac{l^2(2k+2)}{d}] + \frac{l^2}{d} \\
&= \bigcup_{k=0}^{d-1} [\frac{l^2(-2k)}{d} - 1, \frac{l^2(-2k-1)}{d}]
\end{aligned}$$

Now we add $4l^2 + 1$ to make the differences positive; note this reverses the direction of the union.

$$\begin{aligned}
&= \bigcup_{k=0}^{d-1} [\frac{l^2(4d-2k-1)}{d} + 1, \frac{l^2(4d-2k)}{d}] \\
&= \bigcup_{k=0}^{d-1} [\frac{l^2(2(k+d)+1)}{d} + 1, \frac{l^2(2(k+d)+2)}{d}]
\end{aligned}$$

where again in the final step we take $d-1-k$ instead of k.

$$\begin{aligned}\Delta(A_3,A_2) &= \Delta(A_1+2l^2, A_0+\frac{l^2}{d}) \\ &= \Delta(A_1,A_0)+2l^2-\frac{l^2}{d} \\ &= \bigcup_{k=0}^{d-1}[\frac{l^2(2k+1)}{d}+1, \frac{l^2(2k+2)}{d}]+2l^2-\frac{l^2}{d} \\ &= \bigcup_{k=0}^{d-1}[\frac{l^2(2(k+d))}{d}+1, \frac{l^2(2(k+d)+1)}{d}]\end{aligned}$$

Thus

$$\Delta(A_2,A_1)\cup\Delta(A_3,A_2) = \bigcup_{k=0}^{d-1}[\frac{2l^2(k+d)}{d}+1, \frac{2l^2(k+d+1)}{d}] = [2l^2+1, 4l^2]$$

which completes the proof of (i).

For part (ii), let $\mathcal{C}^d = (A_0^d, A_1^d, A_2^d, A_3^d)$ be the CEDF from part (i) corresponding to divisor d of l. Let d_1, d_2 be distinct proper divisors of l. If $\mathcal{C}^{d_1}$ and $\mathcal{C}^{d_2}$ were equivalent, the sets of $\mathcal{C}^{d_1}$ could be mapped onto those of $\mathcal{C}^{d_2}$ via a mapping which would preserve the list of multiplicities of the internal differences of each set. Consider $A_0^d = [0, l-1]$ and $A_2^d = [0, l-1]+\frac{l^2}{d}$ in $\mathbb{Z}_{4l^2+1}$; by Lemma 5.5, the maximum multiplicity of an element in $\Delta(A_0^d)$ or $\Delta(A_2^d)$ is $l-1$. We will show that, for $A_1^d = \cup_{k=0}^{d-1}(\frac{(2k+1)l^2}{d}+l[1,l/d])$ and $A_3^d = 2l^2+A_1^d$, the maximum multiplicity of an element in $\Delta(A_1^d)$ or $\Delta(A_3^d)$ is $\max(l-d, l-\frac{l}{d})$. Note that (since we consider only proper divisors d of l) this is $l-1$ precisely if $d=1$. For distinct proper divisors d_1, d_2 of l such that $l \neq d_1 d_2$, the maximum multiplicity of an element in $\{\Delta(A_1^{d_1}), \Delta(A_3^{d_1})\}$ is different from that of an element in $\{\Delta(A_1^{d_2}), \Delta(A_3^{d_2})\}$. This implies that it is not possible to map $\mathcal{C}^{d_1}$ onto $\mathcal{C}^{d_2}$ as described, and so these CEDFs are not equivalent. For any composite l, we can take $d_1 = 1$ and d_2 any prime divisor of l to obtain two non-equivalent examples.

We now prove the above claim. First consider A_1. Define $J = l([0, \frac{l}{d}-1]+1)$ and $B_k = \{\frac{l^2(2k+1)}{d}+J\}$, so that $A_1 = \cup_{k=0}^{d-1} B_k$ and $\Delta(A_1,A_1) = \cup_{0\le k_1,k_2\le d-1}\Delta(B_{k_2}, B_{k_1})$. Observe that $\Delta(B_{k_2}, B_{k_1}) = \frac{2l^2(k_2-k_1)}{d}+\Delta(J,J)$. By Lemma 5.5, $\Delta(J,J) = l\Delta([0,\frac{l}{d}],[0,\frac{l}{d}])$. So

$$\Delta(A_1,A_1) = \bigcup_{0\le k_1,k_2\le d-1}\{\frac{2l^2(k_2-k_1)}{d}+\Delta(J,J)\}. \tag{1}$$

All elements of $\Delta(J,J)$ lie within $l[-\frac{l}{d}+1, \frac{l}{d}-1]$ and so all elements of $\Delta(B_{k_2}, B_{k_1})$ lie within $[(2(k_2-k_1)-1)\frac{l^2}{d}+l, (2(k_2-k_1)+1)\frac{l^2}{d}-l]$. It is clear that these multisets do not overlap for distinct values of k_2-k_1; moreover since the interval corresponding to $k_2-k_1 = d-1$ is $[(2d-3)\frac{l^2}{d}+l, (2d-1)\frac{l^2}{d}-l]$ while that corresponding to $k_2-k_1 = -(d-1)$ is $[(2d+1)\frac{l^2}{d}+l+1, (2d+3)\frac{l^2}{d}-l+1]$ there is no "wraparound" modulo $4l^2+1$ in the subtraction table for $\Delta(A_1,A_1)$. In $\Delta(B_{k_2}, B_{k_1})$, the maximum multiplicity of a nonzero element is $\frac{l}{d}$ if $k_1 \neq k_2$, and $\frac{l}{d}-1$ if $k_1 = k_2$.

In order to determine the maximum multiplicity of an element in $\Delta(A_1)$, we consider the maximum multiplicity of a nonzero element in $\Delta(A_1, A_1)$. By Equation (1), we must consider the multiset $\{k_2 - k_1 : 0 \leq k_1, k_2 \leq d-1\}$, i.e. $\Delta([0, d-1], [0, d-1])$. Applying Lemma 5.5 to this multiset, element 0 attains maximum multiplicity d while element 1 attains multiplicity $d-1$, the maximum multiplicity in $\Delta([0, d-1])$. From the d multisets $\Delta(B_{k_2,k_1})$ with $k_2 - k_1 = 0$, i.e. $k_1 = k_2$, the maximum possible multiplicity for a nonzero element is $d(\frac{l}{d} - 1) = l - d$. From the $d-1$ multisets $\Delta(B_{k_2,k_1})$ with $k_2 - k_1 = 1$, the maximum possible multiplicity for a nonzero element is $(d-1)\frac{l}{d} = l - \frac{l}{d}$ (and clearly all other multiplicities of nonzero elements arising from the $k_1 \neq k_2$ case do not exceed this). Hence the maximum occurrence of a nonzero element is $\max(l - d, l - \frac{l}{d})$. □

Example 5.7. Let $m = 4$ and $l = 4$; here $G = \mathbb{Z}_{65}$. For $d = 1$, the sets from Theorem 5.6 are $A_0 = \{0, 1, 2, 3\}, A_1 = \{20, 24, 28, 32\}, A_2 = \{16, 17, 18, 19\}$ and $A_3 = \{52, 56, 60, 64\}$. For $d = 2$, the sets are $A_0 = \{0, 1, 2, 3\}, A_1 = \{12, 16, 28, 32\}, A_2 = \{8, 9, 10, 11\}$ and $A_3 = \{44, 48, 60, 64\}$.

5.4 EDFs defined by undirected cycles

In this section, we consider EDFs defined by undirected cycles. By Theorem 3.6, any CEDF yields an EDF defined by an undirected cycle, while by Theorem 3.7, an EDF $(A_1, \ldots, A_m)$ defined by a directed cycle which satisfies the extra condition $\Delta(A_i, A_j) = \Delta(A_j, A_i)$ may be used to obtain a CEDF. However, not all C_m-defined EDFs correspond to CEDFs.

We first note the following, which is straightforward to prove.

Theorem 5.8. *Let $q = ef + 1$ be a prime power. Then the sequence $(C_0^e, C_1^e, \ldots, C_{e-1}^e)$ of all cyclotomic classes of order e in* GF(q) *forms a (q, e, f, f)-CEDF.*

An example of this is given in Example 3.3.

We provide a cyclotomic construction of C_m-defined EDFs which are not CEDFs. Recall that $\{C_0^e, \ldots, C_{e-1}^e\}$ are the cyclotomic classes of order e in GF(q) where $q = ef+1$.

Theorem 5.9. *Let $q = 2ab + 1$, where $a, b > 1$ are both odd.*
Let $\mathcal{A} = (C_0^{2a}, C_2^{2a}, C_4^{2a}, \cdots, C_{2(a-1)}^{2a})$. Then $\mathcal{A}$ is a $(q, a, b, b; C_a)$-EDF which is not a CEDF.

Proof. We note that $q \equiv 3 \mod 4$; it is well-known that in this case -1 is a nonsquare in GF(q). $\mathcal{A}$ consists of the "even" cyclotomic classes of order $2a$ (each of cardinality b), i.e. those multiplicative cosets of C_0^{2a} which partition the squares C_0^2 of GF(q). The "odd" classes $\{C_1^{2a}, C_3^{2a}, \ldots, C_{2a-1}^{2a}\}$ partition the nonsquares C_1^2; since $-1 \in C_1^2$, this is precisely the set $\{-A : A \in \mathcal{A}\}$. Consider the difference multisets: $\Delta(C_2^{2a}, C_0^{2a})$ is the multiset union $\cup_{k=1}^b C_{r_k}^{2a}$ of b (not necessarily distinct) cyclotomic classes $C_{r_1}^{2a}, \ldots, C_{r_b}^{2a}$, and for $1 \leq i \leq a-1$, the multiset $\Delta(C_{2i+2}^{2a}, C_{2i}^{2a}) = \alpha^{2i}\Delta(C_2^{2a}, C_0^{2a})$ comprises the cyclotomic classes $\alpha^{2i}C_{r_1}^{2a}, \ldots, \alpha^{2i}C_{r_b}^{2a}$. By this process, the difference multiset for $\mathcal{A}$ is

$$\cup_{k=1}^b (C_{r_k}^{2a} \cup \alpha^2 C_{r_k}^{2a} \cup \cdots \alpha^{2(a-1)} C_{r_k}^{2a})$$

where $(C_{r_k}^{2a} \cup \alpha^2 C_{r_k}^{2a} \cup \cdots \alpha^{2(a-1)} C_{r_k}^{2a})$ is C_0^2 if r_k is even and C_1^2 if r_k is odd. Hence the difference multiset $\cup_{i=0}^{a-1}\Delta(C_{2i+2}^{2a}, C_{2i}^{2a})$ corresponding to the "clockwise" oriented cycle

is the multiset union of b sets, each from $\{C_0^2, C_1^2\}$. For the opposite orientation, the difference multiset is precisely the negative of this. Since $-C_0^2 = C_1^2$, the multiset union of the differences from both orientations yields b copies of $GF(q)^*$, hence $\mathcal{A}$ is an EDF defined by a cycle of length a, with the given parameters. $\mathcal{A}$ cannot be a CEDF, since the difference multiset for each oriented cycle is the multiset union of an odd number of sets, each from $\{C_0^2, C_1^2\}$, which cannot give an equal number of squares and non-squares. □

Example 5.10. In GF(19), take $a = b = 3$: here 2 is a primitive element and $\mathcal{A} = \{C_0^6, C_2^6, C_4^6\}$ where $C_0^6 = \{1, 7, 11\}$, $C_2^6 = \{4, 9, 6\}$ and $C_4^6 = \{16, 17, 5\}$. Here $\Delta(C_2^6, C_0^6) \cup \Delta(C_4^6, C_2^6) \cup \Delta(C_0^6, C_4^6)$ is a multiset in which the nonzero squares of $\mathbb{Z}_{19}$ appear once and the nonsquares appear 2 times, since $\Delta(C_2^6, C_0^6) = C_1^6 \cup C_3^6 \cup C_4^6$. For $-(\Delta(C_2^6, C_0^6) \cup \Delta(C_4^6, C_2^6) \cup \Delta(C_0^6, C_4^6))$, nonzero squares occur twice and nonsquares occur once. The union of both of these multisets yields 3 copies of each nonzero elements of GF(19), so $\mathcal{A}$ is a $(19, 3, 3, 3; C_3)$-EDF which is not a CEDF.

We also present the following examples (which are not instances of the above construction) found via computational search in GAP [9], using a constraint-satisfaction modelling language [1] and solver [10].

Example 5.11. (i) In $\mathbb{Z}_{13}$, let $A_0 = \{0, 6\}, A_1 = \{1, 2\}, A_2 = \{9, 12\}$. Then (A_0, A_1, A_2) is a $(13, 3, 2, 2, C_3)$-EDF but not a $(13, 3, 2, 1)$-CEDF since $\Delta(A_1, A_0) \cup \Delta(A_2, A_1) \cup \Delta(A_0, A_2)$ is a multiset in which the non-zero elements of $\mathbb{Z}_{13}$ appear $0, 1$ or 2 times. Moreover it can be checked that these sets do not correspond to an $(13, 3, 2, 1; C_3^*)$-EDF for any orientation of C_3.

(ii) In $\mathbb{Z}_{11}$, let $A_0 = \{0, 7\}, A_1 = \{1, 2\}, A_2 = \{4, 9\}, A_3 = \{5, 8\}$ and $A_4 = \{3, 10\}$. Then $(A_0, A_1, A_2, A_3, A_4)$ is an $(11, 5, 2, 4; C_5)$-EDF, but not a $(11, 5, 2, 2)$-CEDF since $\Delta(A_1, A_0) \cup \Delta(A_2, A_1) \cup \Delta(A_3, A_2) \cup \Delta(A_4, A_3) \cup \Delta(A_0, A_4)$ is a multiset in which the nonzero elements of $\mathbb{Z}_{11}$ appear $1, 2$ or 3 times.

6 H-defined EDFs when H is complete bipartite

In this section, we consider EDFs defined by oriented and undirected complete bipartite graphs, and obtain a complete description.

Recall that our notation for a complete bipartite digraph $K_{a,b}$ has bipartition $A \cup B$ (where $|A| = a, |B| = b$), and for the oriented version, the standard set of directed edges is $\overrightarrow{E}(K_{a,b}^*) := \{(i, j) : i \in A, j \in B\}$. We use a semi-colon to separate the sets corresponding to the vertices of A from those corresponding to the vertices of B.

The definition of an m-set SEDF requires that, for each set in turn, the sets form a $K_{m-1,1}^*$-defined EDF (with the standard orientation) having that set at the centre of the star. However, in practice only one SEDF with more than two sets is known [15, 22].

Example 6.1. Let $q = 3^5 = 243$, $e = 11$ and $f = 22$. Let $\mathcal{A} = \{C_i^{11} : 0 \le i \le 10\}$ be the cyclotomic classes of order 11 in $GF(243)$. In [22] it is shown that $\mathcal{A}$ is a $(243, 11, 22, 20)$-SEDF, and hence $(C_0^{11}, \ldots C_{i-1}^{11}, C_{i+1}^{11}, \ldots, C_{10}^{11}; C_i^{11})$ is a $(243, 11, 22, 2; K_{10,1}^*)$-CEDF for each $0 \le i \le 10$.

For what follows, we require the following definitions from [18].

Definition 6.2. Let G be a group of order n and let $m > 1$. A family of disjoint sets $\{A_1, \ldots, A_m\}$ in G, with $|A_i| = k_i$ for $1 \leq k \leq m$, is an $(n, m; k_1, \ldots, k_m; \lambda_1, \ldots, \lambda_m)$-GSEDF (generalised strong external difference family) if, for each i with $1 \leq i \leq m$, the multiset equation $\bigcup_{\{j:j\neq i\}} \Delta(A_i, A_j) = \lambda_i(G \setminus \{0\})$ holds.

Definition 6.3. Let G be a group of order n and let $m > 1$. A family of disjoint sets $\{A_1, \ldots, A_m\}$ in G, with $|A_i| = k_i$ for $1 \leq k \leq m$, is an $(n, m; k_1, \ldots, k_m; \lambda)$-GEDF (generalised external difference family) if the multiset equation $\bigcup_{\{i,j:i\neq j\}} \Delta(A_i, A_j) = \lambda(G \setminus \{0\})$ holds.

Observe that SEDFs are examples of GSEDFs and EDFs are examples of GEDFs, in which all set-sizes are equal.

It turns out that EDFs defined by directed complete bipartite graphs may be completely described in terms of GSEDFs, and that EDFs defined by undirected complete bipartite graphs may be completely described in terms of GEDFs.

Theorem 6.4. *Let $a, b, l \in \mathbb{N}$ and let G be a group of order n. The following statements are equivalent:*

(i) there exists an $(n, a+b, l, \lambda; K^*_{a,b})$-EDF;

(ii) there exists an $(n, la+lb, 1, \lambda; K^*_{la,lb})$-EDF;

(iii) there exists an $(n, 2; la, lb; \lambda, \lambda)$-GSEDF.

Proof. To see that (i) holds if and only if (ii) holds, observe that if

$$(\{v_1\}, \{v_1\}, \ldots, \{v_{la}\}; \{v_{la+1}\}, \ldots, \{v_{la+lb}\})$$

is an $(n, la+lb, 1, \lambda; K^*_{la,lb})$-EDF in G, then partitioning $\{v_1, \ldots, v_{la}\}$ arbitrarily into a size-l sets and partitioning $\{v_{la+1}, \ldots, v_{la+lb}\}$ arbitrarily into b size-l sets yields an $(n, a+b, l, \lambda; K^*_{a,b})$-EDF; the difference multiset in both cases is $\Delta(\{v_{la+1}, \ldots, v_{la+lb}\}, \{v_1, \ldots, v_{la}\})$. Conversely, for an $(n, a+b, l, \lambda; K^*_{a,b})$ comprising the l-sets $(A_1, \ldots, A_a; A_{a+1}, \ldots, A_{a+b})$, we may take the elements of $A_1 \cup \cdots \cup A_a$ as la singleton sets and those of $A_{a+1} \cup \cdots \cup A_{a+b}$ as lb singleton sets to obtain a $(n, la+lb, 1, \lambda; K^*_{la,lb})$-EDF. To see that (ii) holds precisely if (iii) holds, consider the $(n, la+lb, 1, \lambda; K^*_{la,lb})$-EDF above; take the singleton sets on each size of its bipartition to obtain two disjoint sets $X_1 = \{v_1, \ldots, v_{la}\}$ and $X_2 = \{v_{la+1}, \ldots, v_{lb}\}$ of size la and lb respectively. It is clear that $\Delta(X_2, X_1) = \Delta(X_1, X_2) = \lambda(G \setminus \{0\})$. This is precisely the requirement for an $(n, 2; la, lb; \lambda, \lambda)$-GSEDF. The converse easily follows. □

Many constructions for two-set GSEDFs (and in particular, for two-set SEDFs) are known (see for example [13, 15, 22]). Construction 3.10 of [13] demonstrates that the two sets $\{0, 1, \ldots, k_1 - 1\}$ and $\{k_1, 2k_1, \ldots, k_1k_2\}$ form a $(k_1k_2 + 1, 2; k_1, k_2; 1, 1)$-GSEDF in $\mathbb{Z}_{k_1k_2+1}$.

Corollary 6.5. *There exists a $(l^2ab+1, a+b, l, 1; K^*_{a,b})$-EDF in $\mathbb{Z}_{l^2ab+1}$ for any $a, b, l \in \mathbb{N}$.*

Proof. Combining Construction 3.10 of [13] with the process in the proof of Theorem 6.4, take any partition of $\{0, 1, \ldots, la-1\}$ into a size-l sets $(A_1, \ldots, A_a)$ on one side of the bipartition, and any partition of $\{la, 2la, \ldots, (lb)(la)\}$ into b size-l sets $(A_{a+1}, \ldots, A_{a+b})$ on the other. Then $(A_1, \ldots, A_a; A_{a+1}, \ldots, A_{a+b})$ is a $(l^2ab+1, a+b, l, 1; K^*_{a,b})$-defined EDF in $\mathbb{Z}_{l^2ab+1}$. □

Example 6.6. Let $l = 2$ and $a = b = 3$.

(i) In $\mathbb{Z}_{37}$, apply Corollary 6.5 to obtain the $(37, 6, 2, 1; K^*_{3,3})$-EDF given by

$$(\{0, 1\}, \{2, 3\}, \{4, 5\}; \{6, 12\}, \{18, 24\}, \{30, 36\}).$$

(ii) In $\mathbb{Z}_{13}$, apply the well-known construction for a $(q, 2, (q-1)/2, (q-1)/4)$-SEDF in GF(q) ($q \equiv 1 \mod 4$) whose sets are the nonzero squares and the nonsquares of the field ([12]) to obtain the $(13, 2, 6, 3)$-SEDF with sets $\{1, 3, 4, 9, 10, 12\}$ and $\{2, 5, 6, 7, 8, 11\}$ in $\mathbb{Z}_{13}$. Using the relationships of Theorem 6.4 to appropriately partition these sets shows that $(\{1, 3\}, \{4, 9\}, \{10, 12\}; \{2, 5\}, \{6, 7\}, \{8, 11\})$ is a $(13, 6, 2, 3; K^*_{3,3})$-EDF.

We may obtain an analogous result to Theorem 6.4 for the undirected case; we omit the (similar) proof.

Theorem 6.7. *The following statements are equivalent:*

(i) there exists an $(n, a+b, l, \lambda; K_{a,b})$-EDF;

(ii) there exists an $(n, la+lb, 1, \lambda; K_{la,lb})$-EDF;

(iii) there exists an $(n, 2; la, lb; \lambda)$-GEDF.

We can use Corollary 6.5 obtain an undirected construction in a larger cyclic group using the same sets, which is not a $K^*_{a,b}$-defined EDF.

Corollary 6.8. *There exists a $(2l^2ab+1, a+b, l, 1; K_{a,b})$-EDF in $\mathbb{Z}_{l^2ab+1}$ for any $a, b, l \in \mathbb{N}$.*

Proof. Consider the $(l^2ab+1, a+b, l, 1; K^*_{a,b})$-EDF in $\mathbb{Z}_{l^2ab+1}$ from Corollary 6.5, given by $(A_1, \ldots, A_a; A_{a+1}, \ldots, A_{a+b})$. We claim that this also forms the desired construction in $\mathbb{Z}_{2l^2ab+1}$, with $1 < \cdots < l^2ab$ now viewed as elements of $\mathbb{Z}_{2l^2ab+1}$. The difference multiset of the original $(l^2ab+1, a+b, l, 1; K^*_{a,b})$-EDF is $[1, l^2ab]$; since all elements of $A_{a+1}, \ldots, A_{a+b}$ are larger than all elements of $A_1, \ldots, A_a$ (using the natural ordering), the differences were obtained via standard integer subtraction, i.e. without invoking modulo l^2ab. Hence these differences $[1, l^2ab]$ may be considered as elements of $\mathbb{Z}_{2l^2ab+1}$, while in the reverse direction the differences are $-[1, l^2ab] = [l^2ab+1, 2l^2ab]$. □

7 Further work

It is clear that the definition of digraph-defined EDF introduced in this paper naturally leads to a large number of new research questions.

To date, only those digraph-defined EDFs defined in terms of undirected complete graphs (the standard EDFs), undirected complete graphs with oriented stars (SEDFs)

and oriented cycles (CEDFs) have appeared in the literature. It would be of great interest to see constructions and non-existence results for other EDFs defined by natural families of graphs and digraphs.

It is also of interest to understand what role the nature of the group G plays in the possible range of digraph-defined EDFs obtainable in G.

The original EDF definition required all subsets in the family to be pairwise disjoint, partly to ensure unique decoding in the original AMD application [18], and partly because for an EDF defined by a complete graph, overlap would yield the identity as a difference. However, from a purely combinatorial viewpoint, there is no reason to require disjoint sets; indeed, classical difference families do not require this. We propose the following definition:

Definition 7.1. Let G be a group of order n and let $m > 1$. Let H be a labelled digraph on m vertices $\{0, 1, \ldots, m-1\}$. A family of l-sets $\{A_0, \ldots, A_{m-1}\}$ in G is an adjacent-disjoint $(n, m, l, \lambda; H)$-EDF if the multiset equation

$$\bigcup_{(i,j)\in\overrightarrow{E}(H)} \Delta(A_j, A_i) = \lambda(G \setminus \{0\})$$

holds.

It is clear that examples exist with non-disjoint sets; e.g. for even m, any star-defined $(n, m/2+1, l, \lambda; K_{m/2,1})$-EDF $(A_0, \ldots, A_{m/2-1}; A_{m/2})$ is an example of an adjacent-disjoint CEDF, namely the $(n, m, l, \lambda; C_m^*)$-EDF given by $(B_0, \ldots, B_{m-1})$ where $B_i = A_i$ for even i and $B_i = A_{m/2}$ for odd i. We give an example of such an adjacent-disjoint CEDF for which we believe that a standard CEDF with the same parameters does not exist in the same group. In $\mathbb{Z}_{19}$, there is an $(19, 4, 3, 2; C_4^*)$-EDF - which is also a $(19, 3, 3, 2; K_{2,1})$-EDF - with set sequence (A_0, A_1, A_2, A_3) where $A_0 = \{1, 5, 16\}$, $A_1 = A_3 = \{2, 8, 11\}$ and $A_2 = \{4, 10, 17\}$. However, computer search using GAP does not find a standard CEDF in $\mathbb{Z}_{19}$ with the same parameters. We ask whether there are families of adjacent-disjoint EDFs which can be shown to achieve parameters not achievable by EDFs with disjoint sets.

It would also be possible to consider a version of digraph-defined EDFs in which set-sizes are not required to be equal, analogous to the generalisation of EDFs to GEDFs and SEDFs to GSEDFs.

Finally, the concept of equivalence has been considered for EDFs, SEDFs and (in this paper) for CEDFs. We ask whether it is of interest to consider equivalence in the context of more general graph- and digraph-defined EDFs.

Acknowledgements

We thank Maura Paterson for helpful comments. We thank the anonymous referees for their feedback, which greatly improved the exposition of the paper.

References

[1] Ö. Akgün, A. M. Frisch, I. P. Gent, C. Jefferson, I. Miguel and P. Nightingale, Conjure: Automatic Generation of Constraint Models from Problem Specifications, Artificial Intelligence 310 (2022), 103751.

[2] G. S. Bloom and D. F. Hsu, On graceful directed graphs. SIAM J. Algebraic Discrete Methods 6 (1985), 519–536.

[3] M. Buratti, Old and new designs via difference multisets and strong difference families, J Combin Des 7 (1999), 406–425.

[4] M. Buratti and L. Gionfriddo, Strong difference families over arbitrary graphs, Journal of Combinatorial Designs 16 (6), 443-461.

[5] A. Burgess, F. Merola and T. Traetta, On circular external difference families, arXiv:2509.02731.

[6] Y. Chang and C. Ding, Constructions of external difference families and disjoint difference families, Des. Codes and Crypt., 40, 167–185, 2006.

[7] R. Cramer, Y. Dodis, S. Fehr, C. Padro and D. Wichs. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. Lecture Notes in Computer Science 4965 (2008), 471–488 (Advances in Cryp- tology — Eurocrypt 2008)

[8] J.A. Davis, S. Huczynska, and G.L. Mullen, Near-complete external difference families, Designs, Codes and Cryptography. 84, 3, p. 415-424 (2017) 10 p.

[9] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.10.2; 2019. (https://www.gap-system.org)

[10] I. P. Gent, C. Jefferson and I. Miguel, MINION: A Fast, Scalable, Constraint Solver, Proceedings of the 2006 Conference on ECAI 2006, p 98–102, IOS Press, 2006.

[11] S. Huczynska and L. Johnson, Internal and external partial difference families and cyclotomy, Discrete Mathematics 346 (2023), no. 3, Paper No. 113295, 24 pp.

[12] S. Huczynska and M. B. Paterson, Existence and non-existence results for strong external difference families, Discrete Math. 341 (2018) 87–95.

[13] S. Huczynska and M. B. Paterson, Weighted external difference families and R-optimal AMD codes, Discrete Mathematics 342 (2019) 855-867.

[14] S. Huczynska and M. B. Paterson, Decomposing complete graphs into isomorphic complete multipartite graphs, New Advances in Designs, Codes and Cryptography, Fields Institute Communications, ed C.J. Colbourn and J. H. Dinitz, Springer, 2024.

[15] J. Jedwab and S. Li, Construction and nonexistence of strong external difference families. J Algebr Comb 49 (2019) 21–48.

[16] S. Huczynska, C. Jefferson and S. Nepšinská, Strong external difference families in abelian and non-abelian groups,Cryptogr. Commun. 13 (2021), 331–341.

[17] W. Ogata, K. Kurosawa, D.R. Stinson and H. Saido, New combinatorial designs and their application to authentification codes and secret sharing schemes, Discrete Math. 279 (2004), 383-405.

[18] M. B. Paterson and D. R. Stinson, Combinatorial characterizations of algebraic manipulation detection codes involving generalized difference families, Discrete Mathematics 339 (2016) 2891–2906.

[19] M. B. Paterson and D. R. Stinson, Circular external difference families, graceful labellings and cyclotomy, Discrete Mathematics 347 (2024) 114103.

[20] T. Storer, Cyclotomy and difference sets, Lectures in Advanced Mathematics, No. 2 Markham Publishing Co., Chicago, IL, 1967, vii+134 pp.

[21] S. Veitch and D. R Stinson, Unconditionally secure non-malleable secret sharing and circular external difference families. Des. Codes Cryptogr. 92, 941–956 (2024).

[22] J. Wen, M. Yang, F. Fu and K. Feng, Cyclotomic construction of strong external difference families in finite fields. Des. Codes Cryptogr. 86 (2018), 1149–1159.

[23] H. Wu, J. Yang and K. Feng, Circular external difference families: construction and non-existence. Des.Codes. Cryptogr. 212(3–4), 480–488 (2024).