Cryptography and Communications (2021) 13:331–341
https://doi.org/10.1007/s12095-021-00473-3

Strong external difference families in abelian and non-abelian groups

Sophie Huczynska[1] · **Christopher Jefferson**[2] · **Silvia Nepšinská**[2]

Received: 23 June 2020 / Accepted: 19 January 2021 / Published online: 8 February 2021

Abstract
Strong external difference families (SEDFs) have applications to cryptography and are rich combinatorial structures in their own right. We extend the definition of SEDF from abelian groups to all finite groups, and introduce the concept of equivalence. We prove new recursive constructions for SEDFs and generalized SEDFs (GSEDFs) in cyclic groups, and present the first family of non-abelian SEDFs. We prove there exist at least two non-equivalent $(k^2 + 1, 2, k, 1)$-SEDFs for every $k > 2$, and begin the task of enumerating SEDFs, via a computational approach which yields complete results for all groups up to order 24.

Keywords Strong external difference family · R-optimal AMD code

Mathematics Subject Classification (2010) Primary 05B10; Secondary 94A13 · 94A05

1 Introduction

There has been considerable recent interest in strong external difference families (SEDFs), which have applications to cryptography and are rich combinatorial structures in their own right (see [1, 4, 6, 10, 12, 13]). Up till now, all SEDFs have been in abelian groups.

We ask: what is the situation for SEDFs in general finite groups, not simply abelian groups? For given parameters, which groups contain SEDFs with these parameters? How many "different" SEDFs exist with the same parameters?

In this paper, we introduce the notion of equivalence for SEDFs, and characterise admissible parameters. We present a recursive framework for constructing families of SEDFs with $\lambda = 1$ (and related generalized SEDFs) in cyclic groups, which encompasses known results on SEDFs and GSEDFs. We present the first non-abelian SEDFs, a construction for an infinite family using dihedral groups, and establish the existence of at least two non-equivalent

✉ Sophie Huczynska
sh70@st-andrews.ac.uk

Christopher Jefferson
caj21@st-andrews.ac.uk

[1] School of Mathematics and Statistics, University of St Andrews, St Andrews, UK

[2] School of Computer Science, University of St Andrews, St Andrews, UK

$(k^2+1, 2, k, 1)$-SEDFs for every $k > 2$. Finally, we begin the task of enumerating SEDFs, and present complete results for all groups up to order 24, underpinned by a computational approach.

2 Strong external difference families

External difference families (EDFs) were introduced in [11] in relation to AMD codes, while strong EDFs and generalized strong EDFs were introduced in [12]. They were defined in finite abelian groups. We extend these concepts in the natural way to any group of order n: the definitions correspond to the originals, with the removal of the word "abelian". Since the differences are defined in terms of ordered pairs, there is no ambiguity in this definition. For abelian groups, additive notation is generally used; when we focus on the non-abelian and general cases, we will adopt multiplicative notation.

Definition 2.1 Let G be a group of order n.

(i) An (n, m, k, λ)**-external difference family** (or (n, m, k, λ)**-EDF**) is a set of $m \geq 2$ disjoint k-subsets of G, say $A_1, \ldots, A_m$, such that the multiset $M = \{xy^{-1} : x \in A_i, y \in A_j, i \neq j\}$ comprises λ occurrences of each non-identity element of G.

(ii) An (n, m, k, λ)**-strong external difference family** (or (n, m, k, λ)**-SEDF**) is a set of $m \geq 2$ disjoint k-subsets of G, say $A_1, \ldots, A_m$, such that, for every i, $1 \leq i \leq m$, the multiset $M_i = \{xy^{-1} : x \in A_i, y \in \cup_{j \neq i} A_j\}$ comprises λ occurrences of each non-identity element of G.

(iii) An $(n, m; k_1, \ldots, k_m; \lambda_1, \ldots, \lambda_m)$**-generalized strong external difference family** (or $(n, m; k_1, \ldots, k_m; \lambda_1, \ldots, \lambda_m)$**-GSEDF**) is a set of $m \geq 2$ disjoint subsets of G, say $A_1, \ldots, A_m$, such that for every i, $1 \leq i \leq m$, $|A_i| = k_i$ and the multiset $M_i = \{xy^{-1} : x \in A_i, y \in \cup_{j \neq i} A_j\}$ comprises λ_i occurrences of each non-identity element of G.

For every group G, there is at least one SEDF, consisting of the elements of G taken as singleton sets. This has $k = 1$ and is often referred to as the *trivial* SEDF.

The literature contains no examples of non-trivial non-abelian SEDFs. The only explicit construction for non-abelian EDFs is given in [5]; however these are not SEDFs. Recent existence results [2] on disjoint difference families (DDFs) in non-abelian groups should also guarantee non-abelian EDFs, but analysis of parameters shows that these will not be strong.

To enumerate and compare EDFs and SEDFs, we require a notion of equivalence; equivalence of EDFs has not been previously discussed in the literature.

Recall that the holomorph of a group G is the group $Hol(G)$ of all permutations of G of the form $a \to \alpha(a)g$ with $(\alpha, g) \in Aut(G) \times G$. It can be verified that, for an EDF (or SEDF) in a group G, its image under any element of the holomorph of G is still an EDF (or SEDF) with the same parameters.

Definition 2.2 Two external difference families (respectively, strong external difference families) $\mathcal{A} = \{A_1, \ldots, A_m\}$ and $\mathcal{A}' = \{A'_1, \ldots, A'_m\}$ are said to be *equivalent* if, up to isomorphism, they are in the same group G and there exists an element of $Hol(G)$ turning one into the other.

This definition can be naturally extended to GSEDFs (and other EDF-like structures).

Although established in the context of abelian groups [12], the following necessary conditions remain valid in any finite group.

Proposition 2.3 *Necessary conditions for the existence of an (n, m, k, λ)-SEDF in a group G of order n are that $m \geq 2$, $n \geq mk$ and $\lambda(n-1) = k^2(m-1)$. Parameter sets that satisfy these conditions will be called admissible.*

Analysis of these conditions can eliminate parameter sets for SEDFs (see [4, 6]); since the analysis is purely number theoretical on the parameter equation, such results apply equally to abelian and non-abelian groups. We characterise the admissible parameters:

Proposition 2.4 *The set of all admissible parameters (n, m, k, λ) for an SEDF is given by*

$$(n_0 {k_0}^2 k_1 + 1, n_0\lambda_0 + 1, k_0k_1k_2, \lambda_0 k_1 {k_2}^2)$$

where $k_0, k_1, k_2, \lambda_0, n_0 \in \mathbb{N}$ and $n \geq mk$.

Proof Observe that $m - 1 = \frac{\lambda(n-1)}{k^2}$ is an integer. Let A be the multiset of all prime factors of λ, and let B be the multiset of all prime factors of $n-1$. Let C be the multiset of all prime factors of k; then C is contained in multiset $A \cup B$. Let k_0 be the product of all elements of $C \setminus A$; so $k_0 = \frac{k}{\gcd(k,\lambda)}$. These elements are all from B; moreover, $k_0^2 \mid n-1$. Let k_2 be the product of all elements of $C \setminus B$; so $k_2 = \frac{k}{\gcd(k,n-1)}$. These elements are all from A; moreover, $k_2^2 \mid \lambda$. So $k = k_0k_2k_1$, where k_1 is the product of the remaining elements of C. All of these elements occur in both of A and B, so $k_1 \mid \lambda$ and $k_1 \mid n-1$. So $(m-1)k_0^2k_1^2k_2^2 = \lambda(n-1)$; then $\lambda = k_1k_2^2\lambda_0$ for some $\lambda_0 \in \mathbb{N}$, and $n - 1 = k_0^2k_1n_0$ for some $n_0 \in \mathbb{N}$, with $m - 1 = n_0\lambda_0$. □

Table 1 contains all admissible SEDF parameter sets for n up to 24.

An SEDF will not necessarily exist for all admissible parameters. Some parameter sets can be ruled-out in certain classes of group using combinatorial or algebraic arguments. Non-existence results for SEDFs in abelian groups can be found in [1, 4, 8] and [10]. It is possible that SEDFs with some of these forbidden parameters may exist in non-abelian groups.

The following is a summary of constructive existence results known for abelian groups.

Proposition 2.5 *An (n, m, k, λ)-SEDF exists in the group G in the following cases:*

(1) $(n, m, k, \lambda) = (k^2 + 1, 2, k, 1)$ *and* $G = \mathbb{Z}_{k^2+1}$ [12]*; sets given by* $\{0, 1, \ldots, k-1\}, \{k, 2k, \ldots, k^2\}$.

(2) $(n, m, k, \lambda) = (n, 2, \frac{n-1}{2}, \frac{n-1}{4})$, $n \equiv 1 \pmod 4$, *provided there exists an* $(n, \frac{n-1}{2}, \frac{n-5}{4}, \frac{n-1}{4})$ *partial difference set in* G [4]. *When n is a prime power, we may*

Table 1 All admissible SEDF parameters for $n \leq 24$

n	5	9		10		13		17					19					21	
m	2	2	3	2	3	2	4	2	2	3	4	5	2	3	3	5	2	6
k	2	4	2	3	3	6	2	4	8	4	4	2	6	3	6	3	10	2
λ	1	2	1	1	2	3	1	1	4	2	3	1	2	1	4	2	5	1

take the non-zero squares and non-squares in the multiplicative group of the finite field of order n.

(3) $(n, m, k, \lambda) = (q, 2, \frac{q-1}{4}, \frac{q-1}{16})$, *where* $q = 16t^2+1$ *is a prime power and t an integer* [1]*; the sets are cyclotomic classes in the finite field of order q.*

(4) $(n, m, k, \lambda) = (p, 2, \frac{p-1}{6}, \frac{p-1}{36})$, *where* $p = 108t^2 + 1$ *is a prime and t an integer* [1] *the sets are cyclotomic classes in the finite field of order p.*

For $\lambda = 1$, a parameter characterization for the abelian case is given in [12]:

Proposition 2.6 *There exists an abelian* $(n, m, k, 1)$*-SEDF if and only if* $m = 2$ *and* $n = k^2 + 1$ *or* $k = 1$ *and* $m = n$.

3 Abelian SEDFs with $\lambda = 1$: recursive constructions and equivalence

In this section, we consider the situation when $\lambda = 1$. By Proposition 2.6, all non-trivial abelian $(n, m, k, 1)$-SEDFs are $(k^2 + 1, 2, k, 1)$-SEDFs. We show that the construction of Proposition 2.5(1) is one amongst numerous constructions for SEDFs with $\lambda = 1$ in cyclic groups; we provide recursive techniques to obtain these (and related GSEDFs). We show there exist at least two non-equivalent $(k^2+1, 2, k, 1)$-SEDFs for any composite k (later we extend this to any $k > 2$).

We write $\mathbb{Z}_n$ additively; its elements will be $\{0, 1, \ldots, n-1\}$ and we fix the natural ordering $0 < \cdots < n-1$. For $a, b \in \mathbb{Z}_n$ with $a < b$, we will sometimes represent the closed interval $\{x : x \in \mathbb{Z}_n, a \leq x \leq b\}$ by $[a, b]$. For a set A, we denote by ΔA the set of internal differences $\{x - y : x \neq y \in A\}$.

Theorem 3.1 *Let* $G = (\mathbb{Z}_{k^2+1}, +)$*, where* $k = 2a$ *for some positive integer* $a \geq 1$*. Let* $S = (\{0, 1, \ldots, a-1\} \cup \{2a, 2a+1, \ldots 3a-1\}, \bigcup_{i=1}^{a}\{(4i-1)a, 4ia\})$*. Then S is a* $(k^2 + 1, 2, k, 1)$*-SEDF in G and for* $k > 2$*, S is not equivalent to the SEDF in G from Proposition 2.5 (1).*

Proof For $0 \leq h \leq a-1$, let I_h be the closed interval $[ha, (h+1)a - 1]$ and let I_h^+ be $I_h + 1 = [ha + 1, (h+1)a]$. Then $S = \{B_1, B_2\}$, where $B_1 = I_0 \cup I_2$ and $B_2 = \cup_{i=1}^{a} C_i$ with $C_i = \{(4i-1)a, 4ia\}$ for $1 \leq i \leq a$. It suffices to show that $B_2 - B_1$ comprises each non-zero group element precisely once. We have that $C_i - I_0 = I_{4i-2}^+ \cup I_{4i-1}^+$ and $C_i - I_2 = I_{4i-4}^+ \cup I_{4i-3}^+$. Thus $C_i - B_1 = I_{4i-4}^+ \cup I_{4i-3}^+ \cup I_{4i-2}^+ \cup I_{4i-1}^+$ is the closed interval $J_i = [(4i-4)a + 1, 4ia]$. It follows that $B_2 - B_1 = \cup_{i=1}^{a} J_i = \mathbb{Z}_{4a^2+1} \setminus \{0\}$, i.e. $\{B_1, B_2\}$ is a $(4a^2 + 1, 2, 2a, 1)$-SEDF.

Let $A_1 = [0, 2a-1]$ and $A_2 = \{2a, 4a, \ldots, (4a-2)a, 4a^2\}$ be the sets of the SEDF from Proposition 2.5 (1). If $\{A_1, A_2\}$ and $\{B_1, B_2\}$ were equivalent, one of A_1 or A_2 could be mapped onto B_1 via an appropriate mapping which would preserve the lists of multiplicities of the internal differences. It can be verified, using the fact that each of A_1 and A_2 is an arithmetic progression and $|G|$ is odd, that the maximum multiplicity of the elements of G in each of ΔA_1 and ΔA_2 is $2a - 1$. Since $B_1 = I_0 \cup I_2$, ΔB_1 comprises two copies of ΔI_0, one copy of $2a + \Delta I_0$ and one copy of $-2a + \Delta I_0$. It can be verified, since I_0 is an interval and all three of these multisets are mutually disjoint, that the maximum multiplicity in ΔB_1 is $2(a-1)$. Hence the SEDFs are not equivalent. □

The following recursive result for SEDFs with $\lambda = 1$ in cyclic groups encompasses both constructions mentioned in Theorem 3.1 and provides a means of generating new examples.

Theorem 3.2 *Let $S = \{A_1, A_2\}$ be a $(k^2 + 1, 2, k, 1)$-SEDF in $\mathbb{Z}_{k^2+1}$ with $A_1 = \{x_1, \ldots, x_k\}$ and $A_2 = \{y_1, \ldots, y_k\}$, such that $x_i < y_j$ for all $1 \le i, j \le k$. Let $a \in \mathbb{N}$. Then we can obtain from S an $((ak)^2 + 1, 2, ak, 1)$-SEDF $S' = \{B_1, B_2\}$ in $\mathbb{Z}_{(ak)^2+1}$. The blocks are given by*

$$B_1 = \bigcup_{i=1}^{k} \{ax_i + \alpha : 0 \le \alpha \le a - 1\} \text{ and } B_2 = \bigcup_{i=1}^{k} \{a(y_i + k^2\beta) : 0 \le \beta \le a - 1\}.$$

(Here x_i, y_i denote the elements of $\mathbb{Z}_{(ak)^2+1}$ with these labels.)

Proof For any $g \in \mathbb{Z}_{(ak)^2+1}$ with $0 \le g \le ak^2 - 1$, let $I_g = [ag, a(g + 1) - 1]$ and $I_g^+ = I_g + 1 = [ag + 1, a(g + 1)]$; let $R_g = \{a(g + k^2\beta) : 0 \le \beta \le a - 1\}$ and $R_g^+ = R_g + 1$. Then $B_1 = \cup_{i=1}^{k} I_{x_i}$ and $B_2 = \cup_{i=1}^{k} R_{y_i}$. It suffices to show that $B_2 - B_1$ comprises each non-zero group element precisely once. Now, $B_2 - B_1 = \cup_{i=1}^{k} \cup_{j=1}^{k} (R_{y_i} - I_{x_j})$. Observe that $R_{y_i} - I_{x_j} = \cup_{\beta=0}^{a-1} I^+_{y_i - x_j - 1 + \beta k^2}$. Hence $B_2 - B_1 = \cup_{\beta=0}^{a-1} \cup_{i=1}^{k} \cup_{j=1}^{k} I^+_{y_i - x_j - 1 + \beta k^2}$. As (i, j) runs through all possible pairs, $(y_i - x_j)$ takes each value $1, \ldots, k^2$ precisely once, since S is a $(k^2 + 1, 2, k, 1)$-SEDF in $\mathbb{Z}_{k^2+1}$ and all $x_i < y_j$. So $B_2 - B_1 = \cup_{\beta=0}^{a-1} \cup_{z=0}^{k^2-1} I^+_{z+\beta k^2} = \cup_{\beta=0}^{a-1} [a\beta k^2 + 1, a(\beta + 1)k^2] = [1, a^2k^2] = \mathbb{Z}_{(ak)^2+1} \setminus \{0\}$ as required. □

Example 3.3 Using the construction of Theorem 3.2:

- If S is the trivial $(2, 2, 1, 1)$-SEDF $A_1 = \{0\}$, $A_2 = \{1\}$ in $\mathbb{Z}_2$, then S' is the $(a^2 + 1, 2, a, 1)$-SEDF $B_1 = \{0, 1, \ldots, a - 1\}$, $B_2 = \{a, 2a, \ldots, a^2\}$ in $\mathbb{Z}_{a^2+1}$ of Proposition 2.5 (1).
- If S is the $(5, 2, 2, 1)$-SEDF $\{0, 1\}$, $\{2, 4\}$ in $\mathbb{Z}_5$, then S' is the $(4a^2 + 1, 2, 2a, 1)$-SEDF in $\mathbb{Z}_{4a^2+1}$ from Proposition 2.5 (1), whereas if S is $\{0, 2\}$, $\{3, 4\}$ in $\mathbb{Z}_5$ then S' is the $(4a^2 + 1, 2, 2a, 1)$-SEDF in $\mathbb{Z}_{4a^2+1}$ from Theorem 3.1. This shows that, if the recursion is performed using two equivalent SEDFs as S, the resulting S''s need not be equivalent.

Theorem 3.4 *For every $\mathbb{Z}_{k^2+1}$ with k composite, there are at least two non-equivalent $(k^2 + 1, 2, k, 1)$-SEDFs.*

Proof Since k is composite, $k = ar$ for some $a, r \ge 2$. Consider the (equivalent) $(r^2 + 1, 2, r, 1)$-SEDFs in $\mathbb{Z}_{r^2+1}$ given by $S_1 = \{\{0, 1, \ldots, r - 1\}, \{r, 2r, \ldots, r^2\}\}$ and $S_2 = rS_1 = \{\{0, r, \ldots, r^2 - r\}, \{r^2 - r + 1, \ldots, r^2 - 1, r^2\}\}$. Applying Theorem 3.2 to S_1 yields $S_1' = \{A_1, A_2\}$, where $A_1 = \{0, 1, \ldots, ar - 1\}$ and $A_2 = \{ar, 2ar, \ldots, (ar)^2\}$. Applying Theorem 3.2 to S_2 yields $S_2' = \{B_1, B_2\}$, where $B_1 = \cup_{i=1}^{r} I_{x_i}$ with $x_i = (i - 1)r$, and $B_2 = \cup_{i=1}^{r} R_{y_i}$ with $y_i = r^2 - (r - i)$. We claim that the $((ar)^2 + 1, 2, ar, 1)$-SEDFs in $\mathbb{Z}_{k^2+1}$ given by S_1' and S_2' are non-equivalent.

If $\{A_1, A_2\}$ and $\{B_1, B_2\}$ were equivalent, one of A_1 or A_2 could be mapped onto B_1 via an appropriate mapping which would preserve the lists of multiplicities of the internal differences. It can be verified, using the structure of the arithmetic progressions A_1 and

A_2, that the maximum multiplicity in each of ΔA_1 and ΔA_2 is $ar - 1$. However, since $B_1 = \cup_{i=0}^{r-1} iar + I_0$, ΔB_1 comprises r copies of ΔI_0, $r-1$ copies each of $\Delta I_0 + ar$ and $\Delta I_0 - ar$, and in general $r-i$ copies each of $\Delta I_0 + iar$ and $\Delta I_0 - iar$. Using the structure of the interval I_0 and the fact that all of these multisets are disjoint, it can be verified that the maximum multiplicity in ΔB_1 is $(a-1)r = ar - r$ and so the SEDFs are not equivalent. □

In fact, the recursive process of Theorem 3.2 can be performed for GSEDFs with $m = 2$ and $\lambda_1 = \lambda_2 = 1$, and by appropriate choice of parameters we can build new SEDFs using GSEDFs which are not themselves SEDFs. A recursive construction for GSEDFs was given in [9]; our result differs from this in that the value of λ remains unchanged, and the new group is a larger cyclic group rather than a cross-product.

Theorem 3.5 *Let $S = \{A_1, A_2\}$ be a $(st + 1, 2; s, t; 1, 1)$-GSEDF in $\mathbb{Z}_{st+1}$ with $A_1 = \{x_1, \ldots, x_s\}$ and $A_2 = \{y_1, \ldots, y_t\}$, such that $x_i < y_j$ for all $1 \le i \le s$ and $1 \le j \le t$. Let $a, b \in \mathbb{N}$. Then we can obtain from S an $(abst + 1, 2; as, bt; 1, 1)$-GSEDF $S' = \{B_1, B_2\}$ in $\mathbb{Z}_{abst+1}$. The blocks are given by*

$$B_1 = \cup_{i=1}^{s} \{ax_i + \alpha : 0 \le \alpha \le a - 1\} \text{ and } B_2 = \cup_{i=1}^{t} \{a(y_i + \beta st) : 0 \le \beta \le b - 1\}.$$

(Here x_i, y_i denote the elements of $\mathbb{Z}_{abst+1}$ with these labels).

Proof The proof is precisely analogous to that of Theorem 3.2. □

Corollary 3.6 *Let $k = as = bt$ for some $a, b, s, t \in \mathbb{N}$, such that there exists an $(st + 1, 2; s, t; 1, 1)$-GSEDF $\{A_1, A_2\}$ in $\mathbb{Z}_{st+1}$ with $x < y$ for all $x \in A_1$ and $y \in A_2$. Then an $(k^2 + 1, 2; k, 1)$-SEDF can be obtained from S.*

An example of a GSEDF construction which can be used in the recursion is given by $S = (\{0, 1 \ldots, s - 1\}, \{s, 2s, \ldots, ts\})$, of Theorem 4.4 of [9]. The equivalent GSEDF $T = (\{0, t, \ldots (s-1)t\}, \{(s-1)t + 1, (s-1)t + 2, \ldots, st\}$ may also be used.

Example 3.7 Taking $s = 2$ and $t = 3$ with $T = (\{0, 3\}, \{4, 5, 6\})$ in $\mathbb{Z}_7$, Theorem 3.5 may be applied to obtain the following general construction in $\mathbb{Z}_{k^2+1}$ for any k such that $k = 2a = 3b$ for some $a, b \in \mathbb{N}$, i.e. for any k which is a multiple of 6: $S' = (B_1, B_2)$ where

- $B_1 = \{0, 1, \ldots, a - 1\} \cup \{3a, 3a + 1, \ldots, 4a\}$;
- $B_2 = \{4a, 5a, 6a\} \cup \{10a, 11a, 12a\} \cup \cdots \cup \{(6b - 2)a, (6b - 1)a, 6ab\}$.

4 Non-abelian SEDFs with $\lambda = 1$

In the non-abelian setting, it is not known whether every $(n, m, k, 1)$-SEDF must be a $(k^2 + 1, 2, k, 1)$-SEDF. The forward direction of Proposition 2.6 does not apply here, so it is possible that there may exist non-abelian $(k^2(m - 1) + 1, m, k, 1)$-SEDFs with $m > 2$, although no examples are currently known. However, $(k^2 + 1, 2, k, 1)$ is an admissible parameter set. Unlike in the abelian case, there does not exist a non-abelian group of order $k^2 + 1$ for every value of k - for example there exists no non-abelian group of order $k^2 + 1$ for $k \in \{2, 4, 6, 8, 10\}$.

In this section, we exhibit an infinite family of non-abelian $(k^2 + 1, 2, k, 1)$-SEDFs for k odd.

We will consider the dihedral group D_n of order n as being generated by the elements s (reflection) and r (rotation by $\frac{4\pi}{n}$), so that $D_n = \{s^i r^j : 0 \le i \le 1, 0 \le j < \frac{n}{2}\}$ and the generators satisfy $s^2 = 1$, $r^{\frac{n}{2}} = 1$ and $sr = r^{-1}s$.

First, we present two examples, which illustrate the general construction to follow.

Example 4.1 (i) Let $k = 3$ and $G = D_{10}$; take $A_1 = \{e, s, r\}$ and $A_2 = \{sr, r^3, sr^4\}$.
(ii) Let $k = 5$ and $G = D_{26}$; take $A_1 = \{e, s, r, sr, r^2\}$ and $A_2 = \{sr^2, r^5, sr^7, r^{10}, sr^{12}\}$.

Theorem 4.2 *Let $k > 1$ be odd. Let $G = D_{k^2+1}$, the dihedral group of order $n = k^2 + 1$. There exists a $(k^2+1, 2, k, 1)$-SEDF in G. Specifically, $\mathcal{A} = \{A_1, A_2\}$ is a $(k^2+1, 2, k, 1)$-SEDF where*

- $A_1 = \{e, s, r, sr, r^2, sr^2, \ldots, r^{\frac{k-1}{2}}\}$, *i.e.* $\{r^i : 0 \le i \le \frac{k-1}{2}\} \cup \{sr^j : 0 \le j \le \frac{k-3}{2}\}$.
- $A_2 = \{sr^{\frac{k-1}{2}}, r^k, sr^{\frac{k-1}{2}}r^k, r^{2k}, sr^{\frac{k-1}{2}}r^{2k}, \ldots, r^{\frac{k(k-1)}{2}}, sr^{\frac{k-1}{2}}r^{\frac{k(k-1)}{2}}\}$,
  i.e. $\{r^{ik} : 1 \le i \le \frac{k-1}{2}\} \cup \{sr^{jk+\frac{k-1}{2}} : 0 \le j \le \frac{k-1}{2}\}$.

Proof For disjoint subsets X, Y of a group G, let XY^{-1} denote the multiset $\{xy^{-1} : x \in X, y \in Y\}$ (or $X - Y$ its additive equivalent). It suffices to show that $A_1A_2^{-1}$ comprises each non-identity group element precisely once. For $x, y \in G$, xy^{-1} equals r^{i-j} if $x = r^i$ and $y = r^j$; sr^{i-j} if $x = sr^i$ and $y = r^j$; r^{j-i} if $x = sr^i$ and $y = sr^j$; and sr^{j-i} if $x = r^i$ and $y = sr^j$. Note that $r^{(\frac{k^2+1}{2})} = e$. Showing that the elements r^i $(1 \le i \le \frac{k^2-1}{2})$ occur once each is equivalent to verifying that in the additive group $(\mathbb{Z}_{\frac{k^2+1}{2}}, +)$, the multiset $\{0, 1, \ldots, \frac{k-1}{2}\} - \{k, 2k, \ldots, \frac{k(k-1)}{2}\}$ and the multiset $\{\frac{k-1}{2}, \frac{3k-1}{2}, \ldots, \frac{k^2-1}{2}\} - \{0, 1, \ldots, \frac{k-3}{2}\}$ together comprise each non-zero element of $\mathbb{Z}_{\frac{k^2+1}{2}}$ once each:

- $(jk + \frac{k-1}{2}) - \{0, 1, \ldots, \frac{k-3}{2}\} = \{jk + 1, jk + 2, \ldots, jk + \frac{k-1}{2}\}$ where $0 \le j \le \frac{k-1}{2}$;
- $\{0, 1, \ldots, \frac{k-1}{2}\} - k(\frac{k-1}{2} - j) = \{jk + \frac{k+1}{2}, jk + \frac{k+3}{2}, \ldots, jk + k\}$ where $0 \le j \le \frac{k-3}{2}$.

Similarly, showing that the elements sr^i $(0 \le i \le \frac{k^2-1}{2})$ occur once each corresponds to verifying that the multiset $\{0, 1, \ldots, \frac{k-3}{2}\} - \{k, 2k, \ldots, \frac{k(k-1)}{2}\}$ and the multiset$\{\frac{k-1}{2}, \frac{3k-1}{2}, \ldots, \frac{k^2-1}{2}\} - \{0, 1, \ldots, \frac{k-1}{2}\}$ together comprise all the elements of $\mathbb{Z}_{\frac{k^2+1}{2}}$ once each:

- $(jk + \frac{k-1}{2}) - \{0, 1, \ldots, \frac{k-1}{2}\} = \{jk, jk + 1, \ldots, jk + \frac{k-1}{2}\}$ where $0 \le j \le \frac{k-1}{2}$;
- $\{0, 1, \ldots, \frac{k-3}{2}\} - k(\frac{k-1}{2} - j) = \{jk + \frac{k+1}{2}, jk + \frac{k+3}{2}, \ldots, jk + (k-1)\}$ where $0 \le j \le \frac{k-3}{2}$. □

We are now able to prove the following result.

Corollary 4.3 *For every $k > 2$, there exist at least two non-equivalent $(k^2 + 1, 2, k, 1)$-SEDFs.*

Proof For k odd, use Proposition 2.5(1) in $\mathbb{Z}_{k^2+1}$ and Theorem 4.2 in D_{k^2+1}; these SEDFs are non-equivalent as the groups are non-isomorphic. Otherwise, $k = 2a$ for some $a \ge 2$, and so two non-equivalent constructions in $\mathbb{Z}_{k^2+1}$ are guaranteed by Theorem 3.4. □

We end this section with a first step towards addressing the question: are the only non-trivial SEDFs with $\lambda = 1$ those with $m = 2$?

Definition 4.4 Let G be a group of order n.

(i) Let $\mathcal{A}$ be a set of $m \geq 2$ disjoint k-subsets of G, say $A_1, \ldots, A_m$. We say that $\mathcal{A}$ is an (n, m, k, λ)-coEDF if the multiset $N = \{y^{-1}x : x \in A_i, y \in A_j, i \neq j\}$ comprises λ occurrences of each nonzero element of G.

(ii) Let $\mathcal{A}$ be a set of $m \geq 2$ disjoint k-subsets of G, say $A_1, \ldots, A_m$. We say that $\mathcal{A}$ is an (n, m, k, λ)-coSEDF if, for every i, $1 \leq i \leq m$, the multiset $N_i = \{y^{-1}x : x \in A_i, y \in \cup_{j \neq i} A_j\}$ comprises λ occurrences of each nonzero element of G.

Clearly if G is an abelian group, coEDFs and coSEDFs coincide precisely with EDFs and SEDFs. An (n, m, k, λ)-coSEDF must satisfy precisely the same parameter conditions as an (n, m, k, λ)-SEDF.

For a set X in a group G, we denote $X^{-1} = \{x^{-1} : x \in X\}$. For a collection $\mathcal{A}$ of sets $\{A_1, \ldots, A_m\}$ in a group G, we denote $\mathcal{A}^{-1} = \{A_1^{-1}, \ldots, A_m^{-1}\}$.

Lemma 4.5 *$\mathcal{A} = \{A_1, \ldots, A_m\}$ is an (n, m, k, λ)-EDF (respectively, SEDF) if and only if $\mathcal{A}^{-1} = \{A_1^{-1}, \ldots, A_m^{-1}\}$ is an (n, m, k, λ)-coEDF (respectively, coSEDF).*

Proposition 4.6 *Let G be a group of order n. Suppose that $\mathcal{A} = \{A_1, \ldots, A_m\}$ is an $(n, m, k, 1)$-SEDF and an $(n, m, k, 1)$-coSEDF (equivalently, that $\mathcal{A}$ and $\mathcal{A}^{-1}$ are both $(n, m, k, 1)$-SEDFs). Then either $m = 2$ or $k = 1$.*

Proof Suppose that $m > 2$ and $k > 1$. Let $N'_{ij} = \{y^{-1}x : x \in A_i, y \in A_j\}$. The multiset union $\bigcup_{1 \leq i \leq m,\, 1 \leq j \leq n} N'_{ij}$ comprises every non-identity element of G precisely m times. The multiset union $\bigcup_{i \neq 1,\, j \neq 1} N'_{ij}$ comprises $m - 2$ copies of each non-identity element of G, since $\bigcup_{j \neq 1} N'_{1j} (= N_1)$ comprises each non-identity element once, as does $\bigcup_{i \neq 1} N'_{i1}$ (the set of inverses of N_1). Let $x \neq y \in A_1$ (this is possible since $k > 1$). Set $\alpha = y^{-1}x$. Since α is a non-identity element of G and $\mathcal{A}$ is an $(n, m, k, 1)$-coSEDF in G, there exist $u \in A_i$ and $v \in A_j$ for some $i, j \in \{2, \ldots, m\}$ with $i \neq j$ such that $v^{-1}u = \alpha$ (from above, this is possible since $m > 2$). Then $v^{-1}u = \alpha = y^{-1}x$, which rearranges to $v^{-1} = y^{-1}xu^{-1}$, i.e. $yv^{-1} = xu^{-1}$. However, $\mathcal{A}$ is an $(n, m, k, 1)$-SEDF, and this equality corresponds to two equal distinct external differences arising out of A_1 - a contradiction. □

This result generalizes the forward direction of Proposition 2.6. It indicates that, if a non-trivial non-abelian $(n, m, k, 1)$-SEDF exists with $m > 2$, it cannot be a $(n, m, k, 1)$-coSEDF.

5 Computational approach and results

In this section, we describe how we have found and classified all SEDFs in groups up to order 24, using a computational approach. Computational search results were obtained via a constraint-style backtrack search. Preprocessing of the group information was performed using GAP [3], in particular its *SmallGroups* library, while the search for SEDFs was implemented in Java, using a recursive depth-first search algorithm. The algorithm returns all

(n, m, k, λ)-SEDFs in a group G; a final list of non-equivalent SEDFs is then produced using the Images package [7] in GAP.

5.1 Summary of results

Table 1 of Section 2 listed all admissible parameters sets for groups of order at most 24.

For abelian groups, results from the literature rule-out the following parameter sets: $(9, 3, 2, 1)$, $(10, 3, 3, 2)$, $(13, 4, 2, 1)$, $(17, 3, 4, 2)$, $(17, 4, 4, 3)$, $(17, 5, 2, 1)$, $(19, 3, 3, 1)$, $(19, 3, 6, 4)$, $(19, 5, 3, 2)$ [10]; $(21, 6, 2, 1)$ (Proposition 2.6); $(19, 2, 6, 2)$, $(21, 2, 10, 5)$ [6]. This leaves sets: $(5, 2, 2, 1)$, $(9, 2, 4, 2)$, $(10, 2, 3, 1)$, $(13, 2, 6, 3)$, $(17, 2, 4, 1)$, $(17, 2, 8, 4)$.

Table 2 summarizes all non-equivalent abelian SEDFs found by computer search in groups of order up to 24. All found SEDFs can be classified in terms of constructions in the literature: Case (a) corresponds to Proposition 2.5(1), Case (b) corresponds to Proposition 2.5(2), Case (c) corresponds to Proposition 2.5(3) and Case (d) corresponds to Theorem 3.1.

There is no $(9, 2, 4, 2)$-SEDF in the cyclic group of order 9; this is ruled-out by Theorem 4.2 of [6]. The two non-equivalent $(17, 2, 4, 1)$-SEDFs are those guaranteed by Theorem 3.4; here the SEDF from the cyclotomic construction of Proposition 2.5 (3) is equivalent to that from Theorem 3.1.

For non-abelian groups of order $n \leq 24$, we cannot rule-out any of the parameter sets from Table 1 using results from the existing literature. However, there are no non-abelian groups of orders 5, 9, 13, 17, or 19. Therefore non-trivial SEDFs in groups of order up to 24 are possible only for two orders, 10 and 21. In each case there is one non-abelian group: the dihedral group D_{10} of order 10 and the semi-direct product $\mathbb{Z}_7 \rtimes \mathbb{Z}_3$ of order 21. The non-trivial parameter sets for these are $(10, 2, 3, 1)$, $(21, 2, 10, 5)$ and $(21, 6, 2, 1)$. The results are shown in Table 3 - observe that this establishes computationally that there are no SEDFs with parameters $(21, 2, 10, 5)$ and $(21, 6, 2, 1)$.

6 Concluding remarks and open problems

We have introduced the questions: for given parameters, which finite groups contain SEDFs with these parameters? How many non-equivalent SEDFs exist with these parameters? Equivalence raises new questions about known SEDF results - e.g. how many non-equivalent $(243, 11, 22, 20)$-SEDFs exist? Further constructions and theoretical non-existence results for non-abelian SEDFs would be of interest. Does there exist a non-abelian SEDF whose parameters cannot be realised for an abelian SEDF? This is particularly relevant as the range of possible parameters for abelian SEDFs becomes increasingly constrained (in [8] it is conjectured that the known $(243, 11, 22, 20)$-SEDF is the only abelian SEDF with $m > 2$). Do there exist non-abelian SEDFs with $m > 2$?

The case when $\lambda = 1$ possesses a richer structural landscape than previously realised, with new SEDFs found, both abelian and non-abelian. For no other fixed value of λ are explicit families of SEDFs known: can families be found for fixed values of $\lambda > 1$?

Based on the computational results, we may ask: is it the case that for p an odd prime, no SEDF with $m = 2$ can exist in the cyclic group of order p^2? The case when $m > 2$ is resolved in [1]; however we know of no such result for $m = 2$. Does the finite field construction using squares and non-squares yield a unique (up to equivalence) $(p^2, 2, \frac{p-1}{2}, \frac{p-1}{4})$-SEDF?

Table 2 Non-equivalent SEDFs in abelian groups of order up to 24

Parameters	Abelian group	No of non-equiv. SEDFs	Example	Case
(5, 2, 2, 1)	$\mathbb{Z}_5$	1	{0, 1}, {2, 4}	(a), (b), (d)
(9, 2, 4, 2)	$\mathbb{Z}_9$	0	–	–
	$\mathbb{Z}_3 \times \mathbb{Z}_3$	1	{(1, 0), (0, 1,)(2, 0), (0, 2)}, {(1, 1), (1, 2), (2, 1), (2, 2)}	(b)
(10, 2, 3, 1)	$\mathbb{Z}_{10}$	1	{0, 1, 2}, {3, 6, 9}	(a)
(13, 2, 6, 3)	$\mathbb{Z}_{13}$	1	{1, 3, 4, 9, 10, 12}, {2, 5, 6, 7, 8, 11}	(b)
(17, 2, 4, 1)	$\mathbb{Z}_{17}$	2	{0, 1, 2, 3}, {4, 8, 12, 16} {1, 4, 13, 16}, {2, 8, 9, 15}	(a) (c), (d)
(17, 2, 8, 4)	$\mathbb{Z}_{17}$	1	{1, 2, 4, 8, 9, 13, 15, 16}, {3, 5, 6, 7, 10, 11, 12, 14}	(b)

Table 3 Non-equivalent SEDFs in non-abelian groups of order up to 24

Parameters	Non-abelian group	No of non-equiv. SEDFs	Example	Case
$(10, 2, 3, 1)$	D_{10}	1	$\{e, s, r\}, \{sr, r^3, sr^4\}$	Theorem 4.2
$(21, 2, 10, 5)$	$\mathbb{Z}_7 \rtimes \mathbb{Z}_3$	0	–	–
$(21, 6, 2, 1)$	$\mathbb{Z}_7 \rtimes \mathbb{Z}_3$	0	–	–

Acknowledgements Thanks to Maura Paterson for her helpful comments on the paper, and to Gemma Crowe and Ailsa Robertson for related discussions. The second author is supported by a Royal Society University Research Fellowship. We thank the anonymous referees for their comments.

References

1. Bao, J., Ji, L., Wei, R., Zhang, Y.: New existence and nonexistence results for strong external difference families. Discrete Math. **341**(6), 1798–1805 (2018)
2. Buratti, M.: On disjoint $(v, k, k-1)$ difference families. Des. Codes Cryptogr. **87**, 745–755 (2019)
3. The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.10.2; 2019. (https://www.gap-system.org)
4. Huczynska, S., Paterson, M.B.: Existence and non-existence results for strong external difference families. Discrete Math. **341**(1), 87–95 (2018)
5. Huczynska, S., Paterson, M.B.: Weighted external difference families and R-optimal AMD codes. Discrete Math. **342**(3), 855–867 (2019)
6. Jedwab, J., Li, S.: Construction and nonexistence of strong external difference families. J. Algebraic Comb. **49**(1), 21–48 (2019)
7. Jefferson, C., Jonauskyte, E., Pfeiffer, M., Waldecker, R.: Minimal and canonical images. J. Algebra **521**, 481–506 (2019)
8. Leung, K.H., Li, S., Prabowo, T.F.: Nonexistence of strong external difference families in abelian groups of order being product of at most three primes, arXiv preprint
9. Lu, X., Niu, X., Cao, H.: Some results on generalised external difference families. Des. Codes Cryptogr. **86**(12), 2857–2868 (2018)
10. Martin, W.J., Stinson, D.R.: Some nonexistence results for strong external difference families using character theory. Bull. Inst. Combin. Appl. **80**, 79–92 (2017)
11. Ogata, W., Kurosawa, K., Stinson, D.R., Saido, H.: New combinatorial designs and their applications to authentication codes and secret sharing schemes. Discrete Math. **279**(1), 383–405 (2004)
12. Paterson, M.B., Stinson, D.R.: Combinatorial characterizations of algebraic manipulation detection codes involving generalized difference families. Discrete Math. **339**(12), 2891–2906 (2016)
13. Wen, J., Yang, M., Fu, F., Feng, K.: Cyclotomic construction of strong external difference families in finite fields. Des. Codes Cryptogr. **86**(5), 1149–1159 (2018)