Received: 11 May 2023 | Revised: 4 January 2024 | Accepted: 5 January 2024

DOI: 10.1002/jcd.21930

RESEARCH ARTICLE

WILEY

New constructions for disjoint partial difference families and external partial difference families

Sophie Huczynska | **Laura Johnson**

School of Mathematics & Statistics, University of St Andrews, St Andrews, Scotland, UK

Correspondence
Laura Johnson, School of Mathematics & Statistics, University of St Andrews, St Andrews KY16 9SS, Scotland, UK.
Email: lj68@st-andrews.ac.uk

Funding information
Engineering and Physical Sciences Research Council; EPSRC, Grant/Award Number: EP/X021157/1

Abstract

Recently, new combinatorial structures called disjoint partial difference families (DPDFs) and external partial difference families (EPDFs) were introduced, which simultaneously generalize partial difference sets, disjoint difference families and external difference families, and have applications in information security. So far, all known construction methods have used cyclotomy in finite fields. We present the first noncyclotomic infinite families of DPDFs which are also EPDFs, in structures other than finite fields (in particular cyclic groups and nonabelian groups). As well as direct constructions, we present an approach to constructing DPDFs/EPDFs using relative difference sets (RDSs); as part of this, we demonstrate how the well-known RDS result of Bose extends to a very natural construction for DPDFs and EPDFs.

KEYWORDS

disjoint partial difference families, external partial difference families, relative difference families, relative difference sets

1 | INTRODUCTION

Difference sets (DSs) and difference families are well-studied combinatorial objects dating back to the 1930s; difference families are useful for constructing balanced incomplete block designs (BIBDs) [9, 36]. Disjoint difference families (DDFs) have recently received attention [4, 5, 10], with applications to design theory [14] and information security [31]. In the early 2000s, motivated by applications in cryptography, external difference families (EDFs) were introduced [32, 33] and have been much studied (see, e.g., [6, 8, 18, 21]). In a recent paper [20], partial analogues of DDFs and EDFs were introduced; these are called disjoint partial difference families (DPDFs) and external partial difference families (EPDFs). A (v, s, k, λ, μ)-DPDF (respectively, EPDF) is a set S of s disjoint k-subsets of an order-v group, such that the multiset union of internal (respectively, external) differences of the sets in S comprises λ copies of each nonidentity element in S, and μ copies of each nonidentity element not in S. These also generalize the concept of a partial difference set (PDS) (see [28, 29, 35]) and have applications in information security. In [20], construction methods were given for DPDFs and EPDFs in $GF(q)$ (where q is a prime power) using cyclotomic techniques. Cyclotomy has long been used to produce traditional difference families, beginning with the work of [36]. This paper takes the first step in going beyond cyclotomy to present a range of other construction methods in structures other than finite fields.

It is of particular interest to construct families of sets which are simultaneously DPDFs and EPDFs. It is shown in [20] that such families must partition a PDS, which is regular if it is proper. As well as the natural theoretical appeal of such examples, DPDFs which partition a regular PDS correspond to a two-class association scheme which means they can be used to obtain partially balanced incomplete block designs (PBIBDs) (see [24] for details).

In [20], DPDFs/EPDFs are obtained by partitioning cyclotomic PDSs in finite fields; for fields of prime order, these partition the quadratic residues (or nonresidues) modulo p. In this paper, we address the following questions.

- Can DPDF/EPDF constructions be obtained in abelian groups other than $(GF(q), +)$; particularly for cyclic groups $\mathbb{Z}_v$, where v is not prime?
- Can DPDF/EPDF constructions be obtained in nonabelian groups?

We provide explicit constructions answering both of these questions in the affirmative. We observe that the LP-packings introduced in [22] provide other examples of DPDF/EPDFs in a range of finite abelian groups.

It is known [28, 29] that if D is a regular PDS in $\mathbb{Z}_v$, then there are just two possibilities: D or its complement is the set of nonzero squares (equivalently, nonsquares) in $GF(v)$ with $v \equiv 1 \bmod 4$ prime, or else $D \cup \{0\}$ or $G \setminus D$ is a subgroup of G. Constructions of DPDFs and EPDFs partitioning the former type of PDS was addressed in [20]; in this paper we address the latter situation (although not limited to the cyclic group setting). In nonabelian groups, while the definitions of these difference family-type structures remain valid, very little is known. There are just a few nonabelian EDFs in the literature (see, e.g., [19]), and before this paper there were no known constructions for nonabelian DPDFs or EPDFs, so the nonabelian constructions presented here are significant.

We first present explicit constructions in cyclic groups. We next develop constructions in general finite groups based on relative difference sets (RDSs), in which the subgroup not present in the union of the sets of the DPDF/EPDF is precisely the forbidden subgroup for the RDS. In particular, we show how the classic result of Bose [1] which originally constructed RDSs using finite geometry, very naturally extends to a DPDF/EPDF construction in cyclic groups. We obtain a framework for using RDSs for DPDF/EPDF constructions which encompasses this example and generates many others. Finally, we briefly present DPDFs and EPDFs in cyclic groups which demonstrate that not all DPDFs must be EPDFs, and vice versa.

Any $(v, s, k, \lambda, 0)$-DPDF which partitions $G\setminus H$ (for some subgroup H of G) gives an instance of a *relative difference family*. Relative difference families were introduced in [2] and subsequently explored in various further papers (e.g., [3, 30]). These have mostly been studied in abelian groups, and are closely related to the concept of *group divisible designs*. EPDFs also give examples of *bounded external difference families* (see [33]).

2 | BACKGROUND

Throughout what follows, we let G be a group, written additively unless otherwise stated, and let G^* denote $G\setminus\{0\}$.

For a subset D of G, we define the multiset

$$\Delta(D) = \{x - y : x \neq y \in D\}$$

and for sets $D_1, D_2 \subseteq G$, we define the multiset

$$\Delta(D_1, D_2) = \{x - y : x \in D_1, y \in D_2\}.$$

(In multiplicative notation these are $\Delta(D) = \{xy^{-1} : x \neq y \in D\}$ and $\Delta(D_1, D_2) = \{xy^{-1} : x \in D_1, y \in D_2\}$ respectively.)

For a family $A = \{A_1, \ldots, A_s\}$ of disjoint subsets of G, we define

$$\mathrm{Int}(A) = \bigcup_{i=1}^{s} \Delta(A_i)$$

and

$$\mathrm{Ext}(A) = \bigcup_{1\leq i\neq j\leq s} \Delta(A_i, A_j).$$

For $g \in G$ and $S \subseteq G$, we denote the translate $g + S = \{g + s : s \in S\}$ (multiplicatively, $gS = \{gs : s \in S\}$).

We begin with a summary of relevant definitions (see [9, 20]).

Definition 2.1. Let G be a group of order v.

(i) A (v, k, λ, μ)-partial difference set (PDS) is a k-subset D of G with the property that the multiset of differences $\Delta(D)$ comprises each nonidentity element of D precisely λ times, and each nonidentity element of $G\setminus D$ μ times. If $\lambda = \mu$ then D is simply called a (v, k, λ)-difference set (DS); otherwise the PDS is said to be proper. If the PDS D satisfies $0 \notin D$ and $D = -D$ (where $-D = \{-d : d \in D\}$) then it is said to be regular.

(ii) A (v, s, k, λ)-disjoint difference family (DDF) is a collection of disjoint k-subsets $S' = \{A_1, \ldots, A_s\}$ of G^* with the property that $\mathrm{Int}(S')$ comprises each nonidentity element of G precisely λ times. If the disjointness condition is relaxed we obtain a difference family (DF).

(iii) A (v, s, k, λ, μ)-disjoint partial difference family (DPDF) is a collection of disjoint k-subsets $S' = \{A_1, \ldots, A_s\}$ of G^* with the property that $\mathrm{Int}(S')$ comprises each nonidentity element of $S = \cup_{i=1}^{s} A_i$ precisely λ times, and each nonidentity element of $G \setminus S \mu$ times. If $\lambda = \mu$ then S' is a (v, s, k, λ)-disjoint difference family (DDF).

(iv) A (v, s, k, λ)-external difference family (EDF) is a collection of disjoint k-subsets $S' = \{A_1, \ldots, A_s\}$ of G^* with the property that $\mathrm{Ext}(S')$ comprises each nonidentity element of G precisely λ times. An EDF which partitions G^* is called *near-complete*.

(iii) A (v, s, k, λ, μ)-external partial difference family (EPDF) is a collection of disjoint k-subsets $S' = \{A_1, \ldots, A_s\}$ of G^* with the property that $\mathrm{Ext}(S')$ comprises each nonidentity element of $S = \cup_{i=1}^{s} A_i$ precisely λ times, and each nonidentity element of $G \setminus S \mu$ times. If $\lambda = \mu$ then S' is a (v, s, k, λ)-external difference family (EDF).

Lemma 2.2.

(i) *If S' is a $(v, s, k, \lambda_1, \mu_1)$-DPDF then*

$$sk(k-1) = \lambda_1 sk + \mu_1(v - 1 - sk). \tag{1}$$

(ii) *If S' is a $(v, s, k, \lambda_2, \mu_2)$-EPDF then*

$$s(s-1)k^2 = \lambda_2 sk + \mu_2(v - 1 - sk). \tag{2}$$

Proof. This is immediate upon double-counting the elements of $\mathrm{Int}(S')$ and $\mathrm{Ext}(S')$. □

We will also need the definition of an RDS, and its generalization, the divisible difference set. For a comprehensive survey article on these structures, see [34].

Definition 2.3. Let G be a group of order mn and let H be a normal subgroup of G of order n. A k-subset R of G is an (m, n, k, λ)-relative difference set (RDS) in G relative to H if the multiset $\Delta(R)$ comprises each element in $G \setminus H$ exactly λ times, and each nonidentity element in H exactly 0 times. If $n = 1$ then R is a DS.

A counting argument shows that, for an (m, n, k, λ)-RDS, we have the relation $k(k-1) = (mn - n)\lambda$.

Definition 2.4. Let G be a group of order mn and let H be a normal subgroup of G of order n. A k-subset D of G is an (m, n, k, λ, μ)-divisible difference set (DDS) relative to H if the multiset $\Delta(D)$ comprises each nonidentity element of H exactly λ times, and each element of $G \setminus H$ exactly μ times. If $\lambda = 0$ then D is an RDS.

In general, more is known about RDSs than about DDSs.

Remark 2.5. In Definition 2.3, it is possible to relax the condition that H is a normal subgroup. An example of an RDS in A_5 relative to a subgroup H of order 2 is presented in [7], which satisfies all conditions of Definition 2.3, except for the requirement that H is normal (this would be impossible since A_5 is a simple group).

2.1 | DPDFs and EPDFs partitioning PDSs

In this section, we will explore the special properties of DPDFs and EPDFs which partition PDSs.

The following key result was proved in [20]:

Theorem 2.6. *Let G be a group of order v. Let $A = \{A_1, \ldots, A_s\}$ be a family of disjoint subsets of G^*, each of size k. Then any two of the following conditions implies the third:*

(i) *A partitions a (v, k, λ, μ)-PDS in G;*
(ii) *A is a $(v, s, k, \lambda_1, \mu_1)$-DPDF in G;*
(iii) *A is a $(v, s, k, \lambda - \lambda_1, \mu - \mu_1)$-EPDF in G.*

Moreover, if the PDS in Theorem 2.6 is proper, then it is regular.

As mentioned in Section 1, results have been obtained [28, 29] which significantly restrict the possibilities for regular PDSs. For cyclic groups, the following holds:

Theorem 2.7. *Let $\mathbb{Z}_v$ be the cyclic group of order v. Let S' be a $(v, s, k, \lambda_1, \mu_1)$-DPDF and a $(v, s, k, \lambda_2, \mu_2)$-EPDF in $\mathbb{Z}_v$ which partitions a proper PDS. Then*

(i) *if v is a prime and $v \equiv 3 \bmod 4$ then no such S' exists;*
(ii) *if v is a prime and $v \equiv 1 \bmod 4$ then S' partitions the set of nonzero quadratic residues or the nonresidues modulo v;*
(iii) *if v is a composite number then S' partitions a proper nontrivial subgroup H of $\mathbb{Z}_v$ or its complement $\mathbb{Z}_v \backslash H$.*

Proof. It is known [28, 29] that if G is a cyclic group of order v and D is a regular PDS in G then either v is an odd prime such that $v \equiv 1 \bmod 4$ and D is the set of quadratic residues (or nonresidues) modulo v; or $D \cup \{0\}$ or $G \backslash D$ is a subgroup of G. $\square$

Examples of DPDFs and EPDFs partitioning a PDS of each type are given below:

Example 2.8.

(i) Let $G = \mathbb{Z}_{13}$; the sets

$$\{1, 3, 9\}, \{4, 10, 12\}$$

form a $(13, 2, 3, 0, 2)$-DPDF and a $(13, 2, 3, 2, 1)$-EPDF which partition the quadratic residues mod 13 (see [20]).

(ii) Let $G = \mathbb{Z}_{16}$ and $H = \{0, 4, 8, 12\} \leq G$; the sets

$$\{1,9\},\{5,13\},\{2,14\},\{6,10\},\{3,15\},\{7,11\}$$

form a $(16, 6, 2, 0, 4)$-DPDF and $(16, 6, 2, 14, 8)$-EPDF which partition $G\backslash H$ (see Theorem 3.6).

The following basic PDS result is useful (see [29]):

Lemma 2.9. *Let G be a group of order mn with identity 0 and subgroup H of order n.*

(i) *The sets H, $H\backslash\{0\}$, $G\backslash H$ and $(G\backslash H)\cup\{0\}$ are PDSs, with $H\backslash\{0\}$ and $G\backslash H$ being regular.*
(ii) *$H\backslash\{0\}$ is an $(mn, n-1, n-2, 0)$-PDS.*
(iii) *$G\backslash H$ is an $(mn, mn-n, mn-2n, mn-n)$-PDS.*

In the case when a regular PDS D is a subgroup with the identity removed, then we can characterize any DPDF or EPDF which partitions D, as follows.

Theorem 2.10. *Let G be a group of order mn and H be a subgroup of G of order n. Let $D = H\backslash\{0\}$.*

(i) *If S' is an (mn, s, k, λ, μ)-DPDF (respectively, EPDF) partitioning D, then $\mu = 0$ and S' is a near-complete (n, s, k, λ)-DDF (respectively, EDF) in the group H.*
(ii) *Each near-complete (n, s, k, λ)-DDF (respectively, EDF) in the group H corresponds to an $(mn, s, k, \lambda, 0)$-DPDF (respectively, EPDF) in G partitioning D.*

Proof. For (i), we establish the DDF case; the EDF case then follows by Theorem 2.6. Let S' be an (mn, s, k, λ, μ)-DPDF partitioning D. By definition, $\mathrm{Int}(S')$ must comprise every element of D (i.e., every nonidentity element of H) λ times and every nonidentity element of $G\backslash D$ (i.e., $G\backslash H$) μ times. Since $S = D \subseteq H$, all elements of $\mathrm{Int}(S')$ lie in H^*, and so $\mu = 0$. Thus $\mathrm{Int}(S')$ comprises λ copies of the nonidentity elements of H, and S' partitions H^*, so S' is a near-complete DDF in H. Correspondingly S' is also a near-complete EDF in H.

Part (ii) is clear, using the natural embedding of H into G. □

Example 2.11. It can be verified that $\{1,4\},\{2,3\}$ form a $(5, 2, 2, 1)$-DDF and $(5, 2, 2, 2)$-EDF in $\mathbb{Z}_5$.

The group $\mathbb{Z}_{10}$ contains the subgroup $H = \{0, 2, 4, 6, 8\} \cong \mathbb{Z}_5$, via embedding $f: \mathbb{Z}_5 \to \mathbb{Z}_{10}$, $x \mapsto 2x$. Then $\{2,8\},\{4,6\}$ is a $(10, 2, 2, 1, 0)$-DPDF and $(10, 2, 2, 2, 0)$-EPDF in $\mathbb{Z}_{10}$.

Since EDFs have been well-studied elsewhere (see [33] and references therein), we therefore focus on the situation when the PDS D is the complement of a subgroup of G.

The next result guarantees that there exists a DPDF/EPDF of this type, in any group G containing a normal subgroup H.

Theorem 2.12. *Let G be a group of order mn and H a normal subgroup of G of order n. Then the set of cosets of H in G, excepting H itself, forms an $(mn, m-1, n, 0, mn-n)$-DPDF and an $(mn, m-1, n, mn-2n, 0)$-EPDF.*

Proof. By Lemma 2.9, $G\backslash H$ is an $(mn, mn-n, mn-2n, mn-n)$-PDS. The cosets of H in G, other than H itself, partition $G\backslash H$ and for each, its internal difference multiset comprises n copies of H^* and 0 copies of $G\backslash H$. So these cosets from an $(mn, m-1, n, 0, mn-n)$-DPDF and consequently an $(mn, m-1, n, mn-2n, 0)$-EPDF by Theorem 2.6. □

We end this section with a result about the possible parameters for DPDFs/EPDFs which partition the complement of a subgroup. We first need a technical lemma which in fact applies more widely to any DPDF or EPDF; note however it will never apply to any of the DPDFs or EPDFs from [20] which partition a cyclotomic class.

Lemma 2.13. *If* $\gcd(sk, v-1) = 1$ *then*

(i) *For a* $(v, s, k, \lambda_1, \mu_1)$*-DPDF, either* $\mu_1 = 0$ *or* $\mu_1 = sk$.
(ii) *For a* $(v, s, k, \lambda_2, \mu_2)$*-EPDF, either* $\mu_2 = 0$ *or* $\mu_2 = sk$.

Proof. For (i), we use Equation (1); rearranging we see that

$$sk(k-1) = sk(\lambda_1 - \mu_1) + \mu_1(v-1).$$

Hence $sk|\mu_1(v-1)$; since sk and $v-1$ are coprime, $sk|\mu_1$, but note $\mu_1 \le sk$ since there are sk elements in the sets of S'. Hence $\mu_1 = 0$ or $\mu_1 = sk$. Part (ii) follows from a similar rearrangement of Equation (2). □

Theorem 2.14. *Let G be a group of order $v = mn$. Suppose S' is a $(v, s, k, \lambda_1, \mu_1)$-DPDF and a $(v, s, k, \lambda_2, \mu_2)$-EPDF that partitions $G\backslash H$, where $H \le G$ has order n. Then*

(i) $n|\mu_1$ *and* $n|\mu_2$.
(ii) *If* $\gcd(mn-n, mn-1) = 1$ *then S' is one of the following:*
  (a) *an* $(mn, s, k, k-1, 0)$*-DPDF and an* $(mn, s, k, mn-2n-k+1, mn-n)$*-EPDF;*
  (b) *an* $(mn, s, k, k-n, mn-n)$*-DPDF and an* $(mn, s, k, mn-n-k, 0)$*-EPDF.*
(iii) *If $n = 2$ then S' is one of the following:*
  (a) *an* $(2m, s, k, k-1, 0)$*-DPDF and an* $(2m, s, k, 2m-3-k, 2m-2)$*-EPDF;*
  (b) *an* $(2m, s, k, k-2, 2m-2)$*-DPDF and an* $(2m, s, k, 2m-2-k, 0)$*-EPDF.*

Proof. For (i), using the fact that $sk = mn - n$ and $v - 1 = mn - 1$ in Equation (1), we have that

$$n(m-1)(k-1) = \lambda_1 n(m-1) + \mu_1(n-1).$$

So $n|\mu_1(n-1)$, but since $\gcd(n-1, n) = 1$, we must have $n|\mu_1$. We may apply a similar argument using Equation (2) to see $n|\mu_2$. Part (ii) is an application of Lemma 2.13. For part (iii), $\gcd(sk, v-1) = \gcd(mn-n, mn-1)$ and any common divisor of $mn-n$ and $mn-1$ divides $mn-1-(mn-n) = n-1$, i.e., these quantities are coprime when $n = 2$. □

Constructions producing DPDFs/EPDFs of type(a) in Theorem 2.14 (ii)/(iii) are presented in Section 4 using RDSs, while Section 3 includes constructions giving DPDFs/EPDFs of type (b) in cyclic groups.

3 | CYCLIC DPDFs/EPDFs

We present constructions for infinite families of DPDFs/EPDFs such that G is a cyclic group, H is a subgroup of G and the DPDF/EPDF partitions $G\backslash H$.

In this section, we will use the group ring notation whereby λS indicates the multiset comprising λ copies of a set S (so in particular $\lambda\{x\}$ indicates λ copies of the singleton set $\{x\}$). In general we shall avoid this notation in the rest of the paper, to avoid confusion with multiplicative translates of a set.

We first introduce a family of subsets S_i of $\mathbb{Z}_{2m}$ ($m > 3$ odd) which have the useful property that $\Delta(S_i)$ and $\Delta(S_i, S_j)$ consist entirely of unions of S_k's and copies of $H\backslash\{0\}$.

Proposition 3.1. *Let $m > 3$ be an odd integer and let $G = \mathbb{Z}_{2m}$. Let $H = \{0, m\}$ be the order-2 subgroup of G.*

For $1 \leq i \leq 2m - 1$, define

$$S_i = \{i, m - i, m + i, 2m - i\} \subseteq \mathbb{Z}_{2m}.$$

Then

(i) *For $1 \leq i \leq 2m - 1$,*

$$S_i = S_{m-i} = S_{m+i} = S_{2m-i}.$$

In particular $S_1, S_2, ..., S_{\frac{m-1}{2}}$ comprise all the distinct S_j in G ($1 \leq j \leq 2m - 1$).

(ii) *Each $|S_i| = 4$ and $\{S_1, ..., S_{\frac{m-1}{2}}\}$ partition $G\backslash H$.*
(iii) $\Delta(S_i) = 4\{m\} \cup 2S_{2i}$.
(iv) $\Delta(S_i, S_j) = 2S_{i-j} \cup 2S_{i+j}$.

Proof. Part (i) is immediate from the definition of S_i. For part (ii), the fact that m is odd guarantees that all 4 elements are distinct. It is clear that as i runs through $1, ..., \frac{m-1}{2}$, the sets S_i account for all nonidentity elements of G other than m.

For part (iii), write $S_i = A_i \cup B_i$, where $1 \leq i \leq \frac{m-1}{2}$, $A_i = \{i, m + i\}$ and $B_i = \{m - i, 2m - i\}$. Then $\Delta(S_i) = \Delta(A_i) \cup \Delta(A_i, B_i) \cup \Delta(B_i, A_i) \cup \Delta(B_i)$, where $\Delta(A_i) = \Delta(B_i) = \{m, m\}$, $\Delta(A_i, B_i) = \{2i, 2i, m + 2i, m + 2i\} = 2A_{2i}$ and $\Delta(B_i, A_i) = 2B_{2i}$.

For part (iv), $\Delta(S_i, S_j) = \Delta(A_i, A_j) \cup \Delta(A_i, B_j) \cup \Delta(B_i, A_j) \cup \Delta(B_i, B_j)$, where $\Delta(A_i, A_j) = 2A_{i-j}$, $\Delta(A_i, B_j) = 2A_{i+j}$, $\Delta(B_i, A_j) = 2B_{i+j}$ and $\Delta(B_i, B_j) = 2B_{i-j}$. Hence $\Delta(S_i, S_j) = 2S_{i-j} \cup 2S_{i+j}$. □

Theorem 3.2. *Let $m > 3$ be an odd number. Let $G = \mathbb{Z}_{2m}$ and $H = \{0, m\} \leq G$. The family of sets $S' = \{S_i : 1 \leq i \leq \frac{m-1}{2}\}$ in G given by*

$$S_i = \{i, m - i, m + i, 2m - i\}$$

is a $(2m, \frac{m-1}{2}, 4, 2, 2m - 2)$-DPDF and a $(2m, \frac{m-1}{2}, 4, 2m - 6, 0)$-EPDF which partitions $G \backslash H$.

Proof. By Proposition 3.1, the family S' partitions $S = G \backslash H$. We consider $\mathrm{Int}(S') = \cup_{i=1}^{\frac{m-1}{2}} \Delta(S_i)$. Again by Proposition 3.1, the multiset $\Delta(S_i)$ comprises 4 copies of $\{m\}$ and 2 copies of S_{2i}. So

$$\mathrm{Int}(S') = 4\left(\frac{m-1}{2}\right)\{m\} \cup 2(S_2 \cup S_4 \cup \cdots S_{m-3} \cup S_{m-1}).$$

If $m \equiv 1 \bmod 4$,

$$S_2 \cup S_4 \cup \cdots \cup S_{m-1} = S_2 \cup S_4 \cup \cdots S_{\frac{m-1}{2}} \cup S_{m-\frac{m-3}{2}} \cup \cdots \cup S_{m-1}$$

while if $m \equiv 3 \bmod 4$,

$$S_2 \cup S_4 \cup \cdots \cup S_{m-1} = S_2 \cup S_4 \cup \cdots S_{\frac{m-3}{2}} \cup S_{m-\frac{m-1}{2}} \cup \cdots \cup S_{m-1}.$$

In either case this union equals $S_1 \cup S_2 \cup S_3 \cup \cdots S_{\frac{m-1}{2}} = S$. Hence $\mathrm{Int}(S')$ comprises $2m - 2$ copies of $\{m\}$ and 2 copies of $G \backslash H$, so is a $(2m, \frac{m-1}{2}, 4, 2, 2m - 2)$-DPDF. Since $G \backslash H$ is a $(2m, 2m - 2, 2m - 4, 2m - 2)$-PDS, S' is a $(2m, \frac{m-1}{2}, 4, 2m - 6, 0)$-EPDF. $\square$

For $m = 3$, Theorem 3.2 can still be used but, rather than constructing a family of sets, it yields just one set $\{1, 2, 4, 5\}$ which is an RDS.

Example 3.3.

(i) Applying Theorem 3.2 with $m = 5$ demonstrates that

$$\{1, 4, 6, 9\}, \{2, 3, 7, 8\}$$

form a $(10, 2, 4, 2, 8)$-DPDF and $(10, 2, 4, 4, 0)$-EPDF in $\mathbb{Z}_{10}$.

(ii) Applying Theorem 3.2 with $m = 9$ demonstrates that

$$\{1, 8, 10, 17\}, \{2, 7, 11, 16\}, \{3, 6, 12, 15\}, \{4, 5, 13, 14\}$$

form a $(18, 4, 4, 2, 16)$-DPDF and $(18, 4, 4, 12, 0)$-EPDF in $\mathbb{Z}_{18}$.

Next, we present a construction in $\mathbb{Z}_{2p}$, where p is a prime congruent to 1 mod 4. It uses the fact that the nonzero squares in $GF(p)$ form a PDS when $p \equiv 1 \bmod 4$ [29].

Theorem 3.4. *Let p be a prime congruent to* 1 mod 4. *Let G be the additive group $\mathbb{Z}_{2p}$ and let $H = \{0, p\} \leq G$.*

Define subsets A_0, A_1 of $\mathbb{Z}_{2p}$ as follows:

- $A_0 = \{s, s + p \in \mathbb{Z}_{2p} : s$ *is a nonzero quadratic residue modulo* $p\}$
- $A_1 = \{t, t + p \in \mathbb{Z}_{2p} : t$ *is a quadratic nonresidue modulo* $p\}$.

Note $|A_0| = |A_1| = p - 1$ *and* $\mathbb{Z}_{2p} \backslash \{A_0 \cup A_1\} = H$. *Then*

(i) $\Delta(A_0) = \left(\frac{p-5}{2}\right)A_0 \cup \left(\frac{p-1}{2}\right)A_1 \cup (p-1)\{p\}$.

(ii) $\Delta(A_1) = \left(\frac{p-5}{2}\right)A_1 \cup \left(\frac{p-1}{2}\right)A_0 \cup (p-1)\{p\}$.

(iii) $\{A_0, A_1\}$ *forms a* $(2p, 2, p-1, p-3, 2p-2)$*-DPDF and a* $(2p, 2, p-1, p-1, 0)$*-EPDF in* $\mathbb{Z}_{2p}$.

Proof. Let $Q_{2p} = \{a_1, \ldots, a_{\frac{p-1}{2}}\}$ be the quadratic residues modulo p, viewed as elements of $\mathbb{Z}_{2p}$; similarly, let $N_{2p} = \{b_1, \ldots, b_{\frac{p-1}{2}}\}$ be the quadratic nonresidues modulo p, viewed as elements of $\mathbb{Z}_{2p}$. For later convenience, we order the elements of Q_{2p} in increasing order when viewed as integers, i.e., $0 < a_1 < a_2 < \cdots a_{\frac{p-1}{2}} < p$ as integers. Then in $\mathbb{Z}_{2p}$,

$$A_0 = \{a_1, \ldots, a_{\frac{p-1}{2}}\} \cup \{p + a_1, p + a_2, \ldots, p + a_{\frac{p-1}{2}}\} = Q_{2p} \cup (p + Q_{2p}),$$

where $p + Q_{2p} = \{p + x : x \in Q_{2p}\}$.

Consider $\Delta(A_0)$. Clearly

$$\Delta(A_0) = \Delta(Q_{2p}) \cup \Delta(Q_{2p}, p + Q_{2p}) \cup \Delta(p + Q_{2p}, Q_{2p}) \cup \Delta(p + Q_{2p}).$$

The multiset of internal differences of a set is unchanged by the translation of the set, so $\Delta(Q_{2p}) = \Delta(p + Q_{2p})$. Since in $\mathbb{Z}_{2p}$

$$a_i - (p + a_j) = -p + (a_i - a_j) = p + (a_i - a_j) \text{ and } (p + a_i) - a_j = p + (a_i - a_j),$$

we have that $\Delta(Q_{2p}, p + Q_{2p}) = \{a_i - (p + a_j) : a_i, a_j \in Q_{2p}\} = (p + \Delta(Q_{2p}) + (\frac{p-1}{2})\{p\}$ (in this multiset, unlike in $\Delta(Q_{2p})$, we have a contribution from terms with indices $i = j$). A similar argument shows that $\Delta(p + Q_{2p}, Q_{2p}) = (p + \Delta(Q_{2p})) + (\frac{p-1}{2})\{p\}$. Hence, to determine $\Delta(A_0)$, it suffices to determine $\Delta(Q_{2p})$.

Denote by Q_p the nonzero quadratic residues modulo p viewed as elements of $\mathbb{Z}_p$. It is well known (see [29]) that, as a subset of $\mathbb{Z}_p$, Q_p is a $(p, \frac{p-1}{2}, \frac{p-5}{4}, \frac{p-1}{4})$-PDS (where the element $\{0\}$ also occurs as an internal difference with frequency $\frac{p-1}{2}$). Due to the order imposed on the elements of Q_{2p}, it is clear that the elements $D_>^{2p} = \{a_i - a_j : a_i > a_j\}$ of $\Delta(Q_{2p})$ will be precisely the same integers as the corresponding elements $D_>^p = \{a_i - a_j : a_i > a_j\}$ in $\Delta(Q_p)$, while the elements $D_<^{2p} = \{a_i - a_j : a_i < a_j\}$ of $\Delta(Q_{2p})$ will be $p + D_<^p$, where $D_<^p = \{a_i - a_j : a_i < a_j\}$ in $\Delta(Q_p)$. Combining the multisets $\Delta(Q_{2p})$ and $\Delta(Q_{2p}, p + Q_{2p})$ therefore yields $\frac{p-5}{4}$ copies of $Q_p \cup (p + Q_{2p}) = A_0$, $\frac{p-1}{4}$ copies of $N_{2p} \cup (p + N_{2p}) = A_1$, and $\frac{p-1}{2}$ copies of $\{p\}$. Combining all multisets which make up $\Delta(A_0)$ yields the result.

A precisely analogous argument holds for the quadratic nonresidues N_{2p} to yield part (ii) (since N_p, the set of quadratic nonresidues modulo p viewed as elements of $\mathbb{Z}_p$, is also a $(p, \frac{p-1}{2}, \frac{p-5}{4}, \frac{p-1}{4})$-PDS in $\mathbb{Z}_p$). Finally, combining (i) and (ii) shows that the internal differences of $\{A_0, A_1\}$ comprise $\frac{p-5}{2} + \frac{p-1}{2} = p - 3$ copies of each element of $A_0 \cup A_1 = G \backslash H$, and $2(p-1)$ copies of the nonzero elements of H, hence form a DPDF with the stated parameters. Since $G \backslash H$ is a $(2p, 2p-2, 2p-4, 2p-2)$-PDS, the EPDF result follows. □

Example 3.5.

(i) For $p = 5$, $A_0 = \{1, 4, 6, 9\}$ and $A_1 = \{2, 3, 7, 8\}$ in $\mathbb{Z}_{10}$ form a $(10, 2, 4, 2, 8)$-DPDF and a $(10, 2, 4, 4, 0)$-EPDF.

(ii) For $p = 13$,

$$A_0 = \{1, 3, 4, 9, 10, 12, 14, 16, 17, 22, 23, 25\}$$

and

$$A_1 = \{2, 5, 6, 7, 8, 11, 15, 18, 19, 20, 21, 24\}$$

form a $(26, 2, 12, 10, 24)$-DPDF and a $(26, 2, 12, 12, 0)$-EPDF.

Observe that Example 3.5 (i) is the same DPDF/EPDF obtained in Example 3.3. This is because, in $GF(5)$, the set of nonzero squares is $\{1, -1\}$.

In [27], a characterization is given for nontrivial reversible DDSs in cyclic groups (reversible means that $D = D^{-1}$ for the DDS D, where $D^{-1} = \{d^{-1} : d \in D\}$). The result shows that (up to complementation and equivalence) there are only two possibilities for such a DDS D and group G. The first possibility is that $G = \mathbb{Z}_{2p}$, where p is an odd prime with $p \equiv 1 \bmod 4$ and D is precisely $A_0 \cup \{0\}$ from Theorem 3.4; D is a $(p, 2, p, p-1, \frac{p-1}{2})$-DDS in G relative to $H = \{0, p\}$. Our proof of Theorem 3.4 demonstrates directly how the PDS of quadratic residues mod p gives the required properties for this DDS (whereas the proof in [27] follows from a structural characterization using Sylow subgroups, combined with parameter restrictions from [29], so is not constructive).

Finally, we present an infinite family of DPDF/EPDFs constructed via coset partitioning.

Theorem 3.6. *Let $G = \mathbb{Z}_{12d+4}$, where $d \in \mathbb{N}$, and define the subgroups $H = \{0, 3d + 1, 6d + 2, 9d + 3\} \cong \mathbb{Z}_4$ and $K = \{0, 6d + 2\} \cong \mathbb{Z}_2$.*

Let $\{a_1 + H, \ldots, a_{3d} + H\}$ be the cosets of H in G, other than H itself.

Define S' as follows:

- *partition each $a_i + H$ $(1 \le i \le d)$ into two nontrivial cosets of K, namely, $a_i + K$ and $b_i + K$, where $b_i = a_i + (3d + 1)$;*
- *partition each $a_j + H$ $(d + 1 \le j \le 3d)$ into two subsets B_j and C_j, each of the form $\{d_k, d_l\}$, where $d_l - d_k = 3d + 1$ (i.e., $\{a_j, a_j + (3d + 1)\}$ and $\{a_j + (6d + 2), a_j + (9d + 3)\}$ or $\{a_j + (9d + 3), a_j\}$ and $\{a_j + (6d + 2), a_j + (9d + 3)\}$);*
- *take S' to be this collection of $6d$ sets, each of size 2.*

Then S' is a $(12d + 4, 6d, 2, 0, 4d)$-DPDF and a $(12d + 4, 6d, 2, 12d - 4, 8d)$-EPDF.

Proof. It is clear that the sets of S' partition $G \setminus H$. Since $\Delta(K) = 2(K \setminus \{0\})$ and the multiset of internal differences is unchanged by translation, for any $g + K$ $(g \in G)$, the multiset $\Delta(g + K) = 2(K \setminus \{0\})$. So by partitioning each $a_i + H$ $(1 \le i \le d)$ into $a_i + K$ and $b_i + K$, then computing $\Delta(a_i + K)$ and $\Delta(b_i + K)$, we obtain a collection of multisets comprising $4d$ copies of $\{6d + 2\}$ in total. For each set of the form B_j or C_j, we have $\Delta(B_j) = \Delta(C_j) = \{3d + 1, 9d + 3\} = H \setminus K$. By partitioning each $a_j + H$ $(d + 1 \le j \le 3d)$ into B_j and C_j, and for each computing $\Delta(B_j)$ and $\Delta(C_j)$, we obtain $4d$ copies of $H \setminus K$. Hence $\mathrm{Int}(S')$ comprises $4d$ copies of $H \setminus \{0\}$ and zero copies of $G \setminus H$, so S' is a DPDF with the stated parameters. Since G is a $(12d + 4, 12d, 12d - 4, 12d)$-PDS, S' is also an EPDF with the stated parameters. □

For a given d, Theorem 3.6 yields several (equally valid) DPDFs/EPDFs depending on the choices made for the sets.

Example 3.7. Taking $d = 1$ in Theorem 3.6 will produce a $(16, 6, 2, 0, 4)$-DPDF and $(16, 6, 2, 14, 8)$-EPDF which partition $G \setminus H$, where $G = \mathbb{Z}_{16}$ and $H = \{0, 4, 8, 12\}$.

(i) From Example 2.8 (ii), one example is $\{1, 9\}, \{5, 13\}, \{14, 2\}, \{6, 10\}, \{15, 3\}, \{7, 11\}$.
(ii) A different example is $\{3, 11\}, \{7, 15\}, \{13, 1\}, \{5, 9\}, \{2, 6\}, \{10, 14\}$.

4 | RDS-BASED CONSTRUCTIONS FOR DPDFs/EPDFs

In this section, we will show how RDSs can naturally be used to construct DPDFs.

RDSs were first introduced by Bose in [1], though they were not named as such; he presented his result as the "affine analogue" of Singer's Theorem on DSs. The name and concept of RDS were formally introduced by Elliott and Butson in [12]. The original construction of Bose for an RDS has parameters $(q + 1, q - 1, q, 1)$, and is couched in terms of finite geometry; a formulation in terms of finite fields is given in [15]. A more general result with parameters $(\frac{q^r - 1}{q - 1}, q - 1, q^{r-1}, q^{r-2})$ has been proved in various other ways, including via linear recurring sequences [12] and (in a particularly clear exposition) via linear functionals [26].

4.1 | Extending the Bose RDS construction to DPDFs/EPDFs

Our first result demonstrates how Bose's original construction elegantly extends to a construction of a DPDF. Each of the component sets is a Bose RDS. We present it first in finite field terminology then outline the finite geometry viewpoint.

Theorem 4.1. *Let q be a prime power and let α be a primitive element of $GF(q^2)$ with primitive polynomial f over $GF(q)$. For each $\alpha^i \in GF(q^2)$ $(0 \leq i \leq q^2-2)$, there exist $a_i, b_i \in GF(q)$ such that $\alpha^i = a_i + b_i\alpha$.*

(i) *For each $c \in GF(q)^*$, let*

$$S_c := \{\alpha^i \in GF(q^2)^* : \alpha^i = a_i + c\alpha\}.$$

Then the family $\{S_c\}_{c \in GF(q)^*}$ is a multiplicative $(q^2-1, q-1, q, q-1, 0)$-DPDF and a multiplicative $(q^2-1, q-1, q, (q-1)(q-2), q^2-q)$-EPDF in $GF(q^2)^*$.

(ii) *For each $c \in GF(q)^*$, let*

$$S'_c := \{i : \alpha^i \in S_c, 0 \leq i \leq q^2-2\} \subseteq \mathbb{Z}_{q^2-1}.$$

Then the family $\{S'_c\}_{c \in GF(q)^*}$ is an additive $(q^2-1, q-1, q, q-1, 0)$-DPDF and an additive $(q^2-1, q-1, q, (q-1)(q-2), q^2-q)$-EPDF in $\mathbb{Z}_{q^2-1}$.

Proof. Let $c \in GF(q)^*$. To construct the set S_c, we first form the multiplicative cosets of $GF(q)^*$ in $GF(q^2)^*$, and express their elements in the form $a + b\alpha$ $(a, b \in GF(q))$ via the primitive polynomial. There are $\frac{q^2-1}{q-1} = q+1$ cosets, each of the form C_i where $C_0 = \langle \alpha^{q+1} \rangle \cong GF(q)^*$ and $C_i = \alpha^i C_0$ $(0 \leq i \leq q)$ (each of size $q-1$). Each coset has the form

$$C_i = \{t\alpha^i : t \in GF(q)^*\} = \{ta_i + tb_i\alpha : t \in GF(q)^*\}.$$

Observe that, in each C_i other than C_0, there is a unique element whose coefficient of α is c, namely, $cb_i^{-1}(a_i + b_i\alpha)$. Hence for each $c \in GF(q)^*$, we have

$$S_c = \left\{cb_1^{-1}(a_1 + b_1\alpha), cb_2^{-1}(a_2 + b_2\alpha), \ldots, cb_q^{-1}(a_q + b_q\alpha)\right\}.$$

As c runs through $GF(q)^*$, the $q-1$ sets $\{S_c\}$ partition the elements of $GF(q^2)^* \setminus C_0$.

Now, each S_c is a (multiplicative) $(q+1, q-1, q, 1)$-RDS in $GF(q^2)^*$ with respect to the multiplicative subgroup $\langle \alpha^{q+1} \rangle$. In fact, any one of these is a Bose RDS. To see that no element of C_0 arises as a (multiplicative) difference, observe that each element of S_c is in a distinct coset of C_0. It can be shown by direct calculation in the finite field that every element of $GF(q^2) \setminus C_0$ arises precisely once as a difference, by considering the elements of $\Delta(S_c)$ directly (details are left to the reader). Hence the family $\{S_c\}_{c \in GF(q)^*}$ form a (multiplicative) $(q^2-1, q-1, q, q, 0)$-DPDF and $(q^2-1, q-1, q, (q-1)(q-2), q^2-q)$-EPDF.

Finally, take the set of powers of α to convert each S_c to a set $S'_c = \{i : \alpha^i \in S_c, 0 \leq i \leq q^2-2\} \subseteq \mathbb{Z}_{q^2-1}$. It is clear that this yields a collection

$\{S'_c\}_{c \in GF(q)^*}$ of additive $(q+1, q-1, q, 1)$-RDSs which form an additive DPDF and EPDF in $\mathbb{Z}_{q^2-1}$, with the same parameters as in the multiplicative case. □

This has a natural interpretation in finite geometry. Consider $a + b\alpha \in GF(q^2)$ as the point (a, b) in the affine plane $AG(2, q)$. The construction above may be viewed as taking sets which are lines in a given parallel class (in this case, the class with $y = c$). A parallel class has q lines, each with q points, and the lines in the class partition the points of the affine plane.

From Bose's paper [1], each line with $c \neq 0$ in the parallel class gives an RDS with the required parameters, and taking all $q-1$ such lines, we obtain the DPDF described. To see this directly, replace each point in $AG(2, q)$ by the corresponding power of α via the above identification. Since $(0, 0)$ does not correspond to a power of α, the line with $c = 0$ is missing a point: the differences between all remaining points on this line are all multiples of $q+1$. This corresponds to our omitted subgroup. For any other line, the differences will be precisely one occurrence of each of the $q(q-1)$ elements of $\mathbb{Z}_{q^2-1}$ that are not multiples of $q+1$, corresponding to our RDS.

We note that the generalized RDS construction with parameters $(\frac{q^r-1}{q-1}, q-1, q^{r-1}, q^{r-2})$ cannot be used in this way to create a DPDF.

Example 4.2. Consider $GF(25)$ and let α be a primitive element, with primitive polynomial $x^2 + x + 2$ over $GF(5)$. We have

$$\alpha, \quad \alpha^2 = 3 + 4\alpha, \quad \alpha^3 = 2 + 4\alpha, \quad \alpha^4 = 2 + 3\alpha, \quad \alpha^5 = 4 + 4\alpha, \quad \alpha^6 = 2.$$

Here $C_0 = \{1 = \alpha^0, 2 = \alpha^6, 3 = \alpha^{18}, 4 = \alpha^{12}\}$, $C_1 = \{\alpha, 2\alpha, 3\alpha, 4\alpha\}$, $C_2 = \{3 + 4\alpha, 1 + 3\alpha, 4 + 2\alpha, 2 + \alpha\}$, $C_3 = \{2 + 4\alpha, 4 + 3\alpha, 1 + 2\alpha, 3 + \alpha\}$, $C_4 = \{2 + 3\alpha, 4 + \alpha, 1 + 4\alpha, 3 + 2\alpha\}$, $C_5 = \{4 + 4\alpha, 3 + 3\alpha, 2 + 2\alpha, 1 + \alpha\}$.

Hence $S_1 = \{\alpha^1, \alpha^{14}, \alpha^{15}, \alpha^{10}, \alpha^{17}\}$. Taking the powers of α, we obtain $S'_1 = \{1, 14, 15, 10, 17\}$: it can be checked that its internal differences comprise 1 copy each of $\mathbb{Z}_{24} \setminus \{0, 6, 12, 18\}$ and no copies of $\{6, 12, 18\}$.

The other sets are obtained similarly:

- $S_2 = \{\alpha^7, \alpha^{20}, \alpha^{21}, \alpha^{16}, \alpha^{23}\}$ and $S'_2 = \{7, 20, 21, 16, 23\}$.
- $S_3 = \{\alpha^{19}, \alpha^8, \alpha^9, \alpha^4, \alpha^{11}\}$ and $S'_3 = \{19, 8, 9, 4, 11\}$.
- $S_4 = \{\alpha^{13}, \alpha^2, \alpha^3, \alpha^{22}, \alpha^5\}$ and $S'_4 = \{13, 2, 3, 22, 5\}$.

Each S_c *is a* $(6, 4, 5, 1)$*-RDS and* $\{S_1, S_2, S_3, S_4\}$ *is a* $(24, 4, 5, 4, 0)$*-DPDF and a* $(24, 4, 5, 12, 20)$*-EPDF.*

4.2 | A general RDS construction for DPDFs/EPDFs

In this section, we present an important general approach to constructing DPDFs and EPDFs using RDSs. When dealing with groups which are not necessarily abelian, we will use multiplicative notation.

Proposition 4.3. *Let G be a group of order mn and let H be a (not necessarily normal) subgroup of G of order n. If $T = \{D_1, ..., D_s\}$ is a family of disjoint k-subsets of G such that*

(i) *each D_i $(1 \le i \le s)$ is an (m, n, k, λ)-RDS in G relative to H;*
(ii) *T partitions $G \backslash H$;*

then T is an $(mn, s, k, s\lambda, 0)$-DPDF and an $(mn, s, k, mn - 2n - s\lambda, mn - n)$-EPDF.

Proof. The multiset $\mathrm{Int}(T)$ comprises $s\lambda$ copies of each element of $G \backslash H$, and 0 copies of H, and T partitions $G \backslash H$, hence T is an $(mn, s, k, s\lambda, 0)$-DPDF. By Lemma 2.9, $G \backslash H$ is an $(mn, mn - n, mn - 2n, mn - n)$-PDS and so by Theorem 2.6, T is an $(mn, s, k, mn - 2n - s\lambda, mn - n)$-EPDF. □

One natural method of producing a collection of disjoint sets with similar properties is to take an original set and then form a collection of its translates by suitable group elements. The next result, based on a lemma in [15], indicates what "suitable" means in this context.

Lemma 4.4. *Let G be a group, H a (not necessarily normal) subgroup of G and let D be an (m, n, k, λ)-RDS relative to H.*

Let $g_1 \ne g_2 \in G$. The translates g_1D and g_2D of D are disjoint if and only if $g_2^{-1}g_1 \in H$.

Proof. Suppose there is an element in $|g_1D \cap g_2D|$, i.e., $g_1d_1 = g_2d_2$ for some $d_1, d_2 \in D$. Then $g_2^{-1}g_1 = d_2d_1^{-1}$. If $g_2^{-1}g_1 \in H$ then, since there is no nonidentity element of H of the form $d_2d_1^{-1}$, we must have $g_2^{-1}g_1 = 1$, i.e., $g_1 = g_2$, a contradiction. So in this case g_1D and g_2D are disjoint. Otherwise $g_2^{-1}g_1 \in G \backslash H$; this element has $\lambda > 0$ representations in the multiset $\Delta(D)$. So there is at least one pair $(d_1, d_2) \in D \times D$ such that $d_1d_2^{-1} = g_2^{-1}g_1$. Hence $g_2d_1 = g_1d_2$ and so $|g_1D \cap g_2D| > 0$. □

In order for a set of translates of D to partition $G \backslash H$, we require $k | mn - n$. Lemma 4.4 suggests translating by the elements of H; in this case we require $n + kn = mn$, i.e., $k = m - 1$. Combining this with the RDS relation $k(k - 1) = (mn - n)\lambda$ (see comment following Definition 2.3), we have $(m - 1)(m - 2) = (m - 1)n\lambda$, which implies $m = n\lambda + 2$, hence $\lambda = \frac{m-2}{n}$.

We present an explicit example of a DPDF/EPDF satisfying Proposition 4.3, formed from an RDS relative to a subgroup H, translated by the elements of H. It takes as its main ingredient the nonabelian RDS from [7] mentioned in Remark 2.5. This RDS is notable as being the first example of an RDS in a finite simple group with a nontrivial forbidden subgroup. The following DPDF/EPDF construction is noteworthy since it is the first known nonabelian example of a proper DPDF or EPDF. Since the group is nonabelian, the result is written in multiplicative notation.

Proposition 4.5. *Let G be the alternating group A_5 acting on $\{1, 2, 3, 4, 5\}$ and let $\alpha = (25)(34)$.*

Let R be the following set of elements of G:

$$(13542), (154), (14)(23), (13254), (12543), (15324), (245), (132),$$

$$(152), (13)(45), (12435), (235), (15234), (15342), (125), (14)(25),$$

$$(13)(25), (123), (14325), (23)(45), (14235), (253), (254), (13452),$$

$$(12453), (145), (12)(35), (14523), (15)(24).$$

Let $R' = \alpha R$:

$$(13245), (15243), (14253), (13)(24), (124), (15423), (354), (13425),$$

$$(15)(34), (13524), (12)(45), (345), (153), (15)(23), (12)(34), (143),$$

$$(134), (12534), (142), (24)(35), (14532), (234), (243), (135),$$

$$(12354), (14352), (12345), (14)(35), (15432).$$

Then

(i) *R is a $(30, 2, 29, 14)$-RDS in G relative to the subgroup $H = \langle \alpha \rangle \cong \mathbb{Z}_2$.*
(ii) *$A = \{R, R'\}$ is a $(60, 2, 29, 28, 0)$-DPDF and $(60, 2, 29, 28, 58)$-EPDF which partitions $G \backslash H$.*

Proof. For (i), the proof that R is a $(30, 2, 29, 14)$-RDS is the content of the paper [7]. It is obtained using structural properties of Cayley graphs.

For (ii), we show it satisfies Proposition 4.3. Here $m = 30$, $n = 2$, $s = 2$ and $R' = \alpha R$ (the translate of R by α). By inspection, neither element of $H = \{id, \alpha\}$ is contained in R nor R', and these two sets partition $G \backslash H$. By (i), R is a $(30, 2, 29, 14)$-RDS relative to H. To see that the same is true of R', observe that $\Delta(R')$ is the multiset of all elements of the form $(\alpha r_1)(\alpha r_2)^{-1} = \alpha(r_1 r_2^{-1})\alpha$ $(r_1, r_2 \in R)$, i.e., the multiset $\{\alpha x \alpha : x \in \Delta(R)\}$. Now, $\Delta(R)$ comprises 14 copies of $G \backslash H$ and 0 copies of H. We have $\alpha G \alpha = G$ and $\alpha H \alpha = \alpha\{1, \alpha\}\alpha = H$, so $\alpha(G \backslash H)\alpha = G \backslash H$ and hence $\Delta(R') = \Delta(R)$. Hence by Proposition 4.3, A is a $(60, 2, 29, 28, 0)$-DPDF and a $(60, 2, 29, 28, 0)$-DPDF and a $(60, 2, 29, 28, 58)$-EDPF in A_5. □

In general, it is not feasible to perform explicit verification of the properties required for Proposition 4.3: we will therefore establish results which guarantee that large classes of structures satisfy the requirements of Proposition 4.3. Henceforth we will assume that H is a normal subgroup of G.

Lemma 4.6. *Let G be a group, H a normal subgroup of G and let be D an (m, n, k, λ)-RDS relative to H.*

(i) *$\Delta(D) = \Delta(gD)$ for any $g \in G$. In particular, for any $g \in G$, any translate gD is an (m, n, k, λ)-RDS relative to H.*

(ii) *D cannot contain more than one representative from any coset gH $(g \in H)$. In particular, $k \leq m$.*

Proof. For (i), $gd_1(gd_2)^{-1} = g(d_1d_2^{-1})g^{-1}$. By definition, the multiset $\Delta(D)$ comprises λ copies of $G \backslash H$ and 0 copies of H. Since H is a normal subgroup, for any $g \in G$ we have $gHg^{-1} = H$, and since $gGg^{-1} = G$ we also have that $g(G \backslash H)g^{-1} = G \backslash H$. So the multiset $\Delta(gD)$ also has λ copies of $G \backslash H$ and 0 copies of H.

(ii) Suppose D contains elements $d_1 \neq d_2 \in gH$, say $d_1 = gh_1$ and $d_2 = gh_2$. Then $d_1d_2^{-1} = gh_1(gh_2)^{-1} = g(h_1h_2^{-1})g^{-1} \in H$ since H is normal in G. Since D is an RDS relative to H, we must have $d_1d_2^{-1} = e$, i.e., $d_1 = d_2$, a contradiction. □

Theorem 4.7. *Let G be a group of order mn, let H be a normal subgroup of G of order n, and suppose there exists an $(m, n, m-1, \frac{m-2}{n})$-RDS R in G relative to H.*

Then there exists an $(mn, n, m-1, m-2, 0)$-DPDF and an $(mn, n, m-1, (m-2)(n-1), (m-1)n)$-EPDF which partitions $G \backslash H$.

Proof. Suppose we have an $(m, n, m-1, \frac{m-2}{n})$-RDS R. Since $|R| = k = m-1 = [G:H] - 1$, and by Lemma 4.6 R cannot contain a representative of more than one coset of H, there is precisely one coset of H with no representative in R. Without loss of generality, we may replace R by a suitable translate $D := gR$ $(g \in G)$, so that the coset without a representative in D is H itself. (This can be the trivial translation by the identity if $H \cap R = \varnothing$.) By a previous result, any translate of R is also an $(m, n, m-1, \frac{m-2}{n})$-RDS and has its elements in distinct cosets of H. Hence D is an $(m, n, m-1, \frac{m-2}{n})$-RDS comprising a representative of each coset of H except H itself.

Let $\mathcal{D}_{\mathcal{H}} = \{hD : h \in H\}$; we shall show this is the desired DPDF/EPDF. Since D contains no element of H, any translate hD with $h \in H$ must also have empty intersection with H (if $h_1 \in (hD) \cap H$ then $h_1 = hd$ for some $d \in D$, i.e., $d = h^{-1}h_1 \in H$, impossible). By Lemma 4.4, the sets in $\mathcal{D}_{\mathcal{H}}$ are pairwise disjoint, i.e., their union comprises kn distinct elements of G. Hence the sets of $\mathcal{D}_{\mathcal{H}}$ partition the $mn - n = kn$ elements of $G \backslash H$.

By Lemma 4.6, each set in $\mathcal{D}_{\mathcal{H}}$ is an $(m, n, m-1, \frac{m-2}{n})$-RDS relative to H. Finally, by Proposition 4.3 $\mathcal{D}_{\mathcal{H}}$ is an $(mn, n, m-1, m-2, 0)$-DPDF and an $(mn, n, m-1, (m-2)(n-1), (m-1)n)$-EPDF. □

Example 4.8. Let $G = \mathbb{Z}_8$ and consider the $(4, 2, 3, 1)$-RDS $D = \{1, 6, 7\}$ relative to the subgroup $H = \{0, 4\}$. Note that the coset of H not represented in D is H itself. Then $\mathcal{D}_{\mathcal{H}} = \{\{1, 6, 7\}, \{5, 2, 3\}\}$ forms an $(8, 2, 3, 2, 0)$-DPDF and an $(8, 2, 3, 2, 6)$-EPDF.

Remark 4.9. Observe that the construction in Theorem 4.1 extending the Bose approach uses a component RDS with parameters $(q+1, q-1, q, 1)$, which satisfies the requirements of Theorem 4.7. This is not a coincidence; we can view the Bose approach as an instance of Theorem 4.7, in the following way.

In the notation of Theorem 4.1, for each α^i $(1 \leq i \leq q)$, we have $\alpha^i = a_i + b_i\alpha$ $(a_i, b_i \in GF(q))$. The multiplicative coset C_i has the form $C_i = \{ta_i + tb_i\alpha : t \in GF(q)^*\}$, and so for any $c \in GF(q)^*$, the element of C_i which lies in S_c is $cb_i^{-1}\alpha^i$. Hence we can write

$$S_c = \left\{cb_1^{-1}\alpha, cb_2^{-1}\alpha^2, \ldots, cb_q^{-1}\alpha^q\right\}.$$

Taking discrete logs (viewed as elements of $\mathbb{Z}_{q^2-1}$), we have

$$S_c' = \log(S_c) = \log(c) + \left\{\log\left(b_1^{-1}\alpha\right), \log\left(b_2^{-1}\alpha^2\right), \ldots, \log\left(b_q^{-1}\alpha^q\right)\right\} = \log(c) + S_1'.$$

So the $(q^2-1, q-1, q, q-1, 0)$-DPDF and $(q^2-1, q-1, q, (q-1)(q-2), q^2-q)$-EPDF in $\mathbb{Z}_{q^2-1}$ obtained in Theorem 4.1 from the extension of the Bose approach may be viewed as $\mathcal{D}_{\mathcal{H}}$, where $D = S_1'$ and $H = \log(C_0) \cong \mathbb{Z}_{q-1}$, the excluded subgroup.

4.3 | Applications of the general RDS construction

An RDS with parameters $(n+1, n-1, n, 1)$ (and H normal in G) can always be used in the construction of Theorem 4.7. An RDS with these parameters is said to be *affine*; more detail about affine RDSs is given in [15, 34], including nonabelian examples. It is conjectured that in the abelian case, n must be a prime power (see Conjecture 2.4 of [25]).

The following existence result for a nonabelian affine RDS is from [15].

Proposition 4.10. *Let $n = p^r$, where p is prime and $(G, +)$ is the cyclic group of integers modulo $p^{2r} - 1$. We define a new addition on the elements of G. Let $q = p^h$ and suppose $hv = 2r$, where v is an integer all of whose prime factors divide $q - 1$. (If $q \equiv 3 \bmod 4$, we also need $v \not\equiv 0 \bmod 4$). Then, given j, let $r(j)$ denote the unique integer $i \bmod v$ such that*

$$q^i \equiv 1 + j(q-1) \bmod v(q-1).$$

For $i, j \in G$, define the sum $i \oplus j$ as follows:

$$i \oplus j \equiv iq^{r(j)} + j \bmod q^v - 1.$$

Then

(i) *$(G, \oplus)$ is a nonabelian group if $v > 1$.*
(ii) *Let $n = p^r$. If D is an $(n+1, n-1, n, 1)$-RDS in $(G, +)$ relative to $(H, +)$, and the automorphism $x \mapsto px$ fixes D, and $(H, \oplus)$ is a normal subgroup of $(G, \oplus)$, then D is an RDS in $(G, \oplus)$ relative to $(H, \oplus)$.*
(iii) *When $v = 2$ and p is odd, the conditions of (ii) are satisfied and so there exist examples of nonabelian $(n+1, n-1, n, 1)$-RDSs.*

By Theorem 4.7, since $(H, \oplus)$ is required to be a normal subgroup of $(G, \oplus)$ in Proposition 4.10, any RDS from the above construction guarantees the existence of nonabelian $(n^2-1, n-1, n, n-1, 0)$-DPDFs and $(n^2-1, n-1, n, (n-1)(n-2), n(n-1))$-EPDFs.

Next, we seek to identify RDS constructions which satisfy the requirements of Theorem 4.7 but are not of affine type.

We present a general construction for DPDFs and EPDFs using DSs with additional properties. This result extends and generalises ideas from [13, 17], which use such structures in cyclic groups to build optimal frequency-hopping sequences and difference systems of sets.

Theorem 4.11. *Let $n \in \mathbb{N}$ and let $m = (n-1)^2 + 1$.*

Let G be a group of order mn and let H be a normal subgroup of order n.

Suppose D is a $(mn, (n-1)^2 + n, n)$-DS containing H. Let $R = D \backslash H$. Then

(i) *R is an $(m, n, m-1, n-2)$-RDS relative to H;*

(ii) *the sets*

$$\mathcal{R}_{\mathcal{H}} = \{hR : h \in H\}$$

form an $(n[(n-1)^2+1], n, (n-1)^2, n(n-2), 0)$-DPDF and an $(n[(n-1)^2+1], n, (n-1)^2, n(n-1)(n-2), n(n-1)^2)$-EPDF in G.

Proof. We show that R is an RDS with the stated parameters. Part (ii) then follows by observing $\frac{m-2}{n} = \frac{(n-1)^2-1}{n} = n-2$ and applying Theorem 4.7.

We have that

$$\Delta(D) = \Delta(R) \cup \Delta(R, H) \cup \Delta(H, R) \cup \Delta(H);$$

this multiset union comprises n copies of each nonidentity element of G. Since H is a subgroup of order n, the multiset $\Delta(H)$ comprises n copies of each nonidentity element of H and no elements of $G \backslash H$. Thus each of the $n(n-1)^2$ elements of $G \backslash H$ must occur precisely n times across the multiset union $\Delta(R) \cup \Delta(R, H) \cup \Delta(H, R)$, and this accounts for all its $n^2(n-1)^2$ elements.

Nonidentity elements of H are obtained as differences xy^{-1} in $\Delta(G)$ precisely when x and y are distinct and lie in the same coset of H. Since $\Delta(R) \cup \Delta(R, H) \cup \Delta(H, R)$ comprises n copies of $G \backslash H$ and no copies of $H \backslash \{0\}$, it is clear that R consists of at most one representative of each nontrivial coset aH of H (R is disjoint from H by construction). Since there are $(n-1)^2$ such cosets of H and as R has cardinality $(n-1)^2$, R must consist of exactly one representative from each nontrivial coset of H. For any $g \in aH$, where $a \notin H$, the multiset $\Delta(g, H) = aH$. From the structure of R, we see that the multiset $\Delta(R, H) = G \backslash H$. Analogously $\Delta(H, R) = G \backslash H$. Thus, $\Delta(R)$ comprises precisely $n-2$ copies of $G \backslash H$. So R is an $((n-1)^2+1, n, (n-1)^2, n-2)$-RDS relative to subgroup H. Part(ii) now follows by application of Theorem 4.7. □

Example 4.12. We present both a nonabelian and an abelian example of a (40, 13, 4)-DS containing a normal subgroup of order 4 which can be used in Theorem 4.11.

(i) Let G be the semidirect product of C_5 and C_8 acting via $C_8/C_4 = C_2$ [11]. G is a nonabelian group with presentation $\langle a, b : a^5 = b^8 = 1, ba = a^4 b \rangle$. Its centre (a normal subgroup of G by definition) is given by $H = \{1, b^2, b^4, b^6\} \cong C_4$. From [9], a (40, 13, 4)-DS is given by

$$D = \{a^4, 1, a, a^4b, a^2b, b^2, a^2b^2, a^3b^2, b^4, b^5, ab^5, b^6, a^3b^7\}.$$

Here $H \subseteq D$ and

$$R = D \backslash H = \{a, a^4, a^2b, a^4b, a^2b^2, a^3b^2, b^5, ab^5, a^3b^7\}$$

is a $(10, 4, 9, 2)$-RDS relative to H. By Theorem 4.11, it yields a nonabelian $(40, 4, 9, 8, 0)$-DPDF and $(40, 4, 9, 24, 36)$-EPDF.

(ii) Let $G = \mathbb{Z}_{40}$. A $(40, 13, 4)$-DS (from [9], arising from $PG(3, 3)$) is given by

$$D = \{0, 6, 7, 8, 10, 11, 14, 19, 20, 23, 25, 30, 32\}$$

and it contains the subgroup $H = 10\mathbb{Z}_4 = \{0, 10, 20, 30\}$. Here $H \subseteq D$ and

$$R = D \backslash H = \{6, 7, 8, 11, 14, 19, 23, 25, 32\}$$

is a $(10, 4, 9, 2)$-RDS in $\mathbb{Z}_{40}$. By Theorem 4.11, it yields an abelian $(40, 4, 9, 8, 0)$-DPDF and $(40, 4, 9, 24, 36)$-EPDF.

Using a DS result from [17], we can guarantee the existence of an infinite family of DPDFs and EPDFs in cyclic groups via Theorem 4.11. In fact, [17] provides an explicit construction for an appropriate family of cyclic DSs (which possess additional properties not required for our application) using finite geometry; we refer the reader to that paper for more details.

Corollary 4.13. *Let $n = 2^r + 1$, where r is a positive integer and let $m = (n-1)^2 + 1$. There exists an $(mn, n, (n-1)^2, n(n-2), 0)$-DPDF and an $(mn, n, (n-1)^2, n(n-1)(n-2), n(n-1)^2)$-EPDF in $\mathbb{Z}_{mn}$.*

Proof. It is proved in [17] that for $n = 2^r + 1$ there exists an $(n((n-1)^2+1), n+(n-1)^2, n)$-DS D in $\mathbb{Z}_{n((n-1)^2+1)}$ which contains subgroup $H = ((n-1)^2+1)\mathbb{Z}_n$. The result follows by applying Theorem 4.11. □

Example 4.14. Applying Corollary 4.13 using the DS from [17] with $n = 5$ yields a cyclic $(85, 21, 5)$-DS given by

$$D = \{0, 1, 2, 4, 7, 8, 14, 16, 17, 23, 27, 28, 32, 34, 43, 46, 51, 54, 56, 64, 68\}$$

which contains the subgroup $H = 17\mathbb{Z}_5 = \{0, 17, 34, 51, 68\}$. Let $R = D \backslash H = \{1, 2, 4, 7, 8, 14, 16, 23, 27, 28, 32, 43, 46, 54, 56, 64\}$. Then $\mathcal{R}_{\mathcal{H}} = \{R, R+17, R+34, R+51, R+68\}$ is an $(85, 5, 16, 15, 0)$-DPDF and a $(85, 5, 16, 60, 80)$-EPDF in $\mathbb{Z}_{85}$.

We end this section by observing that not all DPDFs/EPDFs with the μ-value of the DPDF equal to zero must have constituent sets which are RDSs; see, for example, the construction below.

Example 4.15. Let $\mathbb{Z}_{3m}$, where $m > 3$ is an odd number, and let $H = \{0, m, 2m\} \cong \mathbb{Z}_3$. Let $S_i = \{i, 3m - i\}$ $(1 \leq i \leq 3m - 1)$. It is straightforward to verify that $\Delta(S_i) = S_{2i}$ and that the family $S' = \{S_i : 1 \le i \le \frac{3m-1}{2}, i \ne m\}$ form a $(3m, \frac{3m-3}{2}, 2, 1, 0)$-DPDF and a $(3m, \frac{3m-3}{2}, 2, 3m-7, 3m-3)$-EPDF.

When $m = 5$, then the sets $\{1, 14\}, \{2, 13\}, \{3, 12\}, \{4, 11\}, \{6, 9\}, \{7, 8\}$ form a $(15, 6, 2, 1, 0)$-DPDF and a $(15, 6, 2, 8, 12)$-EPDF in $\mathbb{Z}_{15}$.

5 | DPDFs WHICH ARE NOT EDPFs AND VICE VERSA

Although the main focus of the paper has been to consider structures which are simultaneously DPDFs and EPDFs, we end with some examples which show there exist DPDFs which are not EPDFs, and EPDFs which are not DPDFs. Our examples occur in cyclic groups.

Proposition 5.1. *Let $n = 2t + 1$ be an odd number, $t > 2$. Then in $\mathbb{Z}_{2t+1}$, the family of sets S'*

$$\{2, 3\}, \{4, 5\}, ..., \{2t-2, 2t-1\}$$

is a $(2t+1, t-1, 2, 0, t-1)$-DPDF which is not an EPDF for $t > 2$.

Proof. It is immediate to check for each set $S_i = \{2i, 2i+1\}$ in S' $(1 \le i \le t-1)$ the multiset $\Delta(S_i) = \{-1, +1\}$ while $S = G^* \backslash \{-1, +1\}$. Hence $\text{Int}(S')$ comprises $t-1$ copies of $\{-1, +1\}$ and 0 copies of $S = G^* \backslash \{-1, +1\}$.

The multiset $\text{Int}(S)$ contains $\{-1, 1\} n - 4$ times, $\{-2, 2\} n - 5$ times and all other elements of $G^* n - 6$ times, hence S is not a PDS and so S is not an EPDF. □

The existence of an infinite family of EPDFs which are not DPDFs is still an open question (see Section 6). The following examples in cyclic groups ([23], obtained via computation in GAP [16]) show that there exist EPDFs which are not DPDFs:

Example 5.2.

(i) $\{1, 8\}, \{3, 6\}$ is a $(9, 2, 2, 0, 2)$-EPDF in $\mathbb{Z}_9$ which is not a DPDF;
(ii) $\{1, 2, 11, 12\}, \{3, 5, 8, 10\}$ is a $(13, 2, 4, 2, 4)$-EPDF in $\mathbb{Z}_{13}$ which is not a DPDF.

6 | CONCLUSIONS AND FURTHER WORK

This paper has demonstrated how the recently introduced combinatorial structures of DPDFs and EPDFs can be constructed in groups other than the additive group of a finite field, using techniques other than the cyclotomic approach introduced in [20]. In particular, it has demonstrated the existence of infinite families and individual examples in noncyclotomic abelian groups and nonabelian groups. In general, our constructions partition the complement of a subgroup.

All constructions in this paper for $(v, s, k, \lambda_1, \mu_1)$-DPDFs which are $(v, s, k, \lambda_2, \mu_2)$-EPDFs have the property that at least one of the frequencies $\{\lambda_1, \lambda_2, \mu_1, \mu_2\}$ takes a zero value (even for constructions not using RDSs). This is in contrast to the cyclotomic constructions of [20], where there were numerous examples with all four frequencies nonzero. This motivates the following:

Open Problem 6.1. Is it possible to obtain families of sets which are both $(v, s, k, \lambda_1, \mu_1)$-DPDFs and $(v, s, k, \lambda_2, \mu_2)$-EPDFs, not corresponding to cyclotomic constructions in the additive group of a finite field, such that $\{\lambda_1, \lambda_2, \mu_1, \mu_2\}$ are all nonzero?

To contextualize this Open Problem, we classify below the types of DPDF/EPDF construction partitioning $G \backslash H$ which we currently know, in terms of the nature of $\{\lambda_1, \lambda_2, \mu_1, \mu_2\}$:

Theorem 6.2. *Let S' be both a $(v, s, k, \lambda_1, \mu_1)$-DPDF and a $(v, s, k, \lambda_2, \mu_2)$-EPDF which partitions $G \backslash H$, H a normal subgroup of G. Then*

(i) *If S' consists of all nontrivial cosets of H then $\lambda_1 = 0$ and $\mu_2 = 0$.*
(ii) *If every set in S' is a union of at least 2 cosets of H, then $\lambda_1 > 0$, $\mu_1 > 0$ and $\mu_2 = 0$.*
(iii) *If the sets of S' are a subdivision of the nontrivial cosets of H (i.e., formed by partitioning the cosets) then $\lambda_1 = 0$, $\mu_1 > 0$ and $\mu_2 > 0$.*
(iv) *If every set in S' has at most one representative from each coset of H, then $\mu_1 = 0$, $\lambda_1 > 0$ and $\mu_2 > 0$.*

Examples of these types are as follows: for (i), see Theorem 2.12; for (ii), see Theorem 3.2, and for (iii) see Theorem 3.6. Illustrations of type (iv) include all RDS-based examples in Section 4.

Hence, any construction satisfying the Open Problem would need to lie outside the list of the categories given in Theorem 6.2 (as well as having $n > 2$ and $gcd(sk, v - 1) > 1$ by Theorem 2.14). We note that these account for all examples of DPDFs/EPDFs partitioning the complement of a subgroup that the authors are currently aware of.

In the final section of this paper, we have provided a brief indication that there exist DPDFs which are not EPDFs, and vice versa. It would be of interest to find more examples of such structures, in a variety of groups. In particular:

Open Problem 6.3. Construct an infinite family of EPDFs which are not DPDFs.

ACKNOWLEDGEMENTS

We thank Maura Paterson for insights into finite geometry, Jim Davis for discussions on relative difference sets, and Chris Jefferson and Matthew McIlree for helpful computation. We thank the anonymous referees for their useful comments. The research of Sophie Huczynska is supported by EPSRC grant EP/X021157/1.

ORCID

Laura Johnson http://orcid.org/0000-0001-8696-4801

REFERENCES

1. R. C. Bose, *An affine analogue of Singer's theorem*, J. Indian Math. Soc. (N.S.). **6** (1942), 1–15.
2. M. Buratti, *Recursive constructions for difference matrices and relative difference families*, J. Combin. Des. **6** (1998), 165–182.
3. M. Buratti, *Old and new designs via difference multisets and strong difference families*, J. Combin. Des. **7** (1999), 406–425.

4. M. Buratti, *On disjoint* $(v, k, k-1)$ *difference families*, Des. Codes Cryptogr. **87** (2019), 745–755.
5. M. Buratti, J. Yan, and C. Wang, *From a 1-rotational RBIBD to a partitioned difference family*, Electron. J. Combin. **17** (2010), no. 1, 23pp. Research Paper 139.
6. Y. Chang and C. Ding, *Constructions of external difference families and disjoint difference families*, Des Codes Crypt. **40** (2006), 167–185.
7. Y. Q. Chen and C. H. Li, *Relative difference sets fixed by inversion and Cayley graphs*, J. Combin. Theory Ser. A. **111** (2005), 165–173.
8. B. Chen, L. Lin, and S. Ling, *External difference families from finite fields*, J. Combin. Des. **25** (2017), 36–48.
9. C. J. Colbourn and J. H. Dinitz, *Handbook of Combinatorial Designs*, 2nd ed., Chapman and Hall/CRC, New York, 2007.
10. C. S. Ding and J. Yin, *Combinatorial constructions of optimal constant-composition codes*, IEEE Trans. Inform. Theory. **51** (2005), no. 10, 3671–3674.
11. T. Dokchitser, *Group names, Personal webpage of Tim Dokchitser (University of Bristol website)*, https://people.maths.bris.ac.uk/~matyd/GroupNames/index.html
12. J. E. H. Elliott and A. T. Butson, *Relative difference sets*, Illinois J. Math. **10** (1966), 517–531.
13. C. Fan, J. Lei, and X. Shan, *Constructions of optimal difference systems of sets*, Sci. China Math. **54** (2011), 173–184.
14. T. Feng, D. Horsley, and X. Wang, *Novak's conjecture on cyclic Steiner triple systems and its generalization*, J. Combin. Theory Ser. A. **184** (2021), 10pp. Paper No. 105515.
15. M. J. Ganley and E. Spence, *Relative difference sets and quasiregular collineation groups*, J. Combin. Theory Ser. A. **19** (1975), 134–153.
16. The GAP Group, *GAP—groups, algorithms, and programming, Version 4.10.2*, https://www.gap-system.org. 2019.
17. G. Ge, R. Fuji-Hara, and Y. Miao, *Further combinatorial constructions for optimal frequency-hopping sequences*, J. Combin. Theory Ser. A. **113** (2006), 1699–1718.
18. B. Huang and D. Wu, *Cyclotomic constructions of external difference families and disjoint difference families*, J. Combin. Des. **17** (2009), no. 4, 333–341.
19. S. Huczynska, C. Jefferson, and S. Nepsinska, *Strong external difference families in abelian and non-abelian groups*, Cryptogr. Commun. **13** (2021), 331–341.
20. S. Huczynska and L. Johnson, *Internal and external partial difference families and cyclotomy*, Discrete Math. **346** (2023), 24pp. Paper No. 113295.
21. J. Jedwab and S. Li, *Construction and nonexistence of strong external difference families*, J. Algebr. Combin. **49** (2019), 21–48.
22. J. Jedwab and S. Li, *Packings of partial difference sets*, Comb. Theory. **1** (2021), 41pp. Paper No. 18.
23. C. Jefferson, Personal communication.
24. L. Johnson and S. Huczynska, *Applications of partial difference families to partial designs*, in preparation.
25. D. Jungnickel, *On affine difference sets*, Sankhyā Ser. A. **54** (1992), 219–240.
26. P. A. Leonard, *Cyclic relative difference sets*, Amer. Math. Monthly. **93** (1986), no. 2, 106–111.
27. K. H. Leung, S. L. Ma, and V. Tan, *Abelian divisible difference sets with multiplier* -1, J. Combin. Theory Ser. A. **59** (1992), 51–72.
28. S. Ma, *Partial difference sets*, Discrete Math. **52** (1984), 75–89.
29. S. Ma, *A survey of partial difference sets*, Des. Codes Cryptogr. **4** (1994), 221–261.
30. K. Momihara, *Strong difference families, difference covers, and their applications for relative difference families*. Des. Codes Cryptogr. **51** (2009), 253–273.
31. S-L Ng and M. B. Paterson, *Disjoint difference families and their applications*. Des. Codes Cryptogr. **78** (2016), 103–127.
32. 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.
33. M. B. Paterson and D. Stinson, *Combinatorial characterizations of algebraic manipulation detection codes involving generalized difference families*. Discrete Math. **339** (2016), 2891–2906.
34. A. Pott, *A survey on relative difference sets*, Groups, Difference Sets, and the Monster (Columbus, OH, 1993), Ohio State Univ. Math. Res. Inst. Publ., vol. **4**, De Gruyter, Berlin, 1996, pp. 195–232.

35. Z. Wan, *New necessary conditions on (negative) Latin square type partial difference sets in abelian groups*, J. Combin. Theory Ser. A. **172** (2020), 105208, 10pp.
36. R. M. Wilson, *Cyclotomy and difference families in elementary abelian groups*, J. Number Theory. **4** (1972), 17–47.

How to cite this article: S. Huczynska and L. Johnson, *New constructions for disjoint partial difference families and external partial difference families*, J. Combin. Des. (2024), 1–24. https://doi.org/10.1002/jcd.21930