BULLETIN of The INSTITUTE of COMBINATORICS and its APPLICATIONS
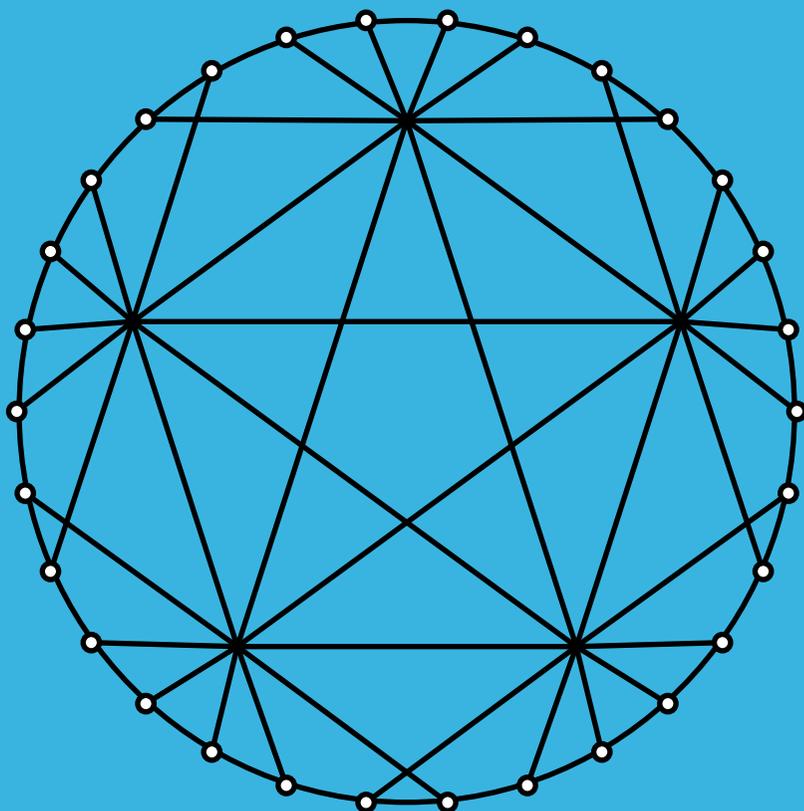
Editors-in-Chief:
    Marco Buratti, Donald Kreher, Ortrud Oellermann, Tran van Trung

A few more Hadamard partitioned difference families

Anamari Nakic

Abstract. A $(G, [k_1, \ldots, k_t], \lambda)$ *partitioned difference family* (PDF) is a partition $\mathcal{B}$ of an additive group G into sets (*blocks*) of sizes k_1, ..., k_t, such that the list of differences of $\mathcal{B}$ covers exactly λ times every non-zero element of G. It is called *Hadamard* (HPDF) if the order of G is 2λ. The study of HPDFs is motivated by the fact that each of them gives rise, recursively, to infinitely many other PDFs. Apart from the *elementary* HPDFs consisting of a Hadamard difference set and its complement, only one HPDF was known. In this article we present three new examples in several groups and we start a general investigation on the possible existence of HPDFs with assigned parameters by means of simple arguments.

1 Introduction

We recall that the list of differences of a subset B of an additive group G, denoted by ΔB, is the multiset of all possible differences between two distinct elements of B:

$$\Delta B := \{x - y : x \neq y, x, y \in B\}.$$

More generally, the list of differences of a collection $\mathcal{F} = \{B_1, \ldots, B_t\}$ of subsets of G is the multiset $\Delta \mathcal{F}$ which is union of the lists of differences of all the B_i's, i.e., $\Delta \mathcal{F} = \bigcup_{i=1}^{t} \Delta B_i$. The collection $\mathcal{F}$ is said to be a *difference family* (DF) if $\Delta \mathcal{F}$ covers every non-zero element of G a constant number λ of times. In this case, if K is the multiset of the sizes of the B_i's, one says that $\mathcal{F}$ is a (G, K, λ)-DF. More specifically, one writes $(G, [k_1, \ldots, k_t], \lambda)$-DF if B_i has size k_i. The B_i's are the *base blocks* of $\mathcal{F}$ and

λ is its *index*. One often speaks of a (v, K, λ)-DF or $(v, [k_1, \ldots, k_t], \lambda)$-DF when the group G (of order v) is understood.

If a DF of index λ has only one block B and its size is k, then one says that B is a (G, k, λ) *difference set* (DS). As before, one generally speaks of a (v, k, λ)-DS if the group G is understood. Among the many classes of difference sets we have, in particular, the so called *Hadamard difference sets* which are those whose parameters are $(4u^2, 2u^2 - u, u^2 - u)$ for some u.

A $(G, [k_1, \ldots, k_t], \lambda)$-DF is *partitioned* (PDF) if its blocks partition G. Here the parameters $v = o(G)$ and λ are completely determined by K. Indeed it is evident that the equalities $k_1 + \cdots + k_t = v$ and $k_1(k_1 - 1) + \ldots + k_t(k_t - 1) = \lambda(v - 1)$ hold. The notion of a PDF was introduced in [12] for the construction of *optimal constant composition codes* [17, 12] which are important in various applications (see, e.g,. [10, 14]) and it is equivalent to that of a *zero difference balanced function* [11] even though, according to [7], it is far preferable to keep the standard notation and terminology.

In a very recent article [8], PDFs have been used to prove the existence of infinitely many *resolvable linear spaces* with a mandatory set of block sizes and an automorphism group acting sharply transitively on the points and transitively on the parallel classes.

If B is (v, k, λ)-DS in G, then $\{B, G \setminus B\}$ is a $(v, [k, v-k], v-2k+2\lambda)$-PDF. So, in particular, a Hadamard $(4u^2, 2u^2 - u, u^2 - u)$-DS gives rise to a $(4u^2, [2u^2 + u, 2u^2 - u], 2u^2)$-PDF. Note that here the order of the group is twice the index. For this reason all PDFs with this property have been called *Hadamard partition difference families* (HPDFs) in the paper were they have been introduced [6]. The motivation of their study is that each HPDF in a group G gives rise to an infinite class of PDFs in suitable supergroups of G.

As pointed out in [7], PDFs with (many) blocks of size 1 are not considered very interesting. However, in the case of HPDFs, the situation is quite different since the PDFs arising from them by using Buratti's construction no longer contain blocks of size 1.

Apart from the HPDFs arising from Hadamard DSs that we call *elementary*, there was only one known example of a HPDF. This makes believe that HPDFs are quite rare. In this paper we determine three new examples in several groups.

Apart from this, the article wants to be the beginning of a general investigation on HPDFs by means of quite simple arguments. It is structured as follows.

In the next section we characterize the PDFs having exactly two blocks. They necessarily consist of a difference set and its complement. In particular, each HPDF with two blocks necessarily consists of a Hadamard difference set and its complement.

In Section 3 we give the trivial necessary conditions for the existence of a HPDF, we list the first admissible parameter sets and then we give some informations on the HPDFs with exactly three blocks.

In Section 4, exploiting *partial difference sets*, we prove that a HPDF with three block sizes one of which is 1 cannot exist.

In Section 5 we give one more necessary condition for the existence of a HPDF in a group having at least one subgroup of index 2.

In Section 6 we present the three new examples mentioned earlier. We have a $(24, [1^3, 2^2, 17], 12)$-HPDF in three pairwise non-isomorphic groups, a $(36, [3, 9, 24], 18)$-HPDF in nine pairwise non-isomorphic groups, and a cyclic $(40, [1, 3, 9, 27], 20)$-HPDF.

In Section 7 we determine the infinite families of *descendants* of our new three examples.

Finally, in Section 8 we pose two open questions. We first ask whether there exists a (v, k, λ)-DS with $v = 2\lambda$ and $k > 4$. The motivation is that such a DS would give a $(v, [1^{v-k}, k], \lambda)$-HPDF. The second question is whether, given positive integers q and n, there exists a PDF whose related K is $[q^0, q^1, q^2, q^3, \ldots, q^{2n-1}]$. The motivation is that such a PDF with $q = 3$ would be Hadamard.

2   PDFs and HPDFs with two blocks

The following fact is extremely well-known (see, e.g., [1]).

Proposition 2.1. *If B is a (v, k, λ)-DS in G, then the complement $\overline{B}$ of B in G is a $(v, v - k, v - 2k + \lambda)$-DS.*

The above explains why, as said in the introduction, a (v, k, λ)-DS and its complement give a $(v, [k, v - k], v - 2k + 2\lambda)$-PDF.

Although the following is a rather straightforward generalization of Proposition 2.1, we are not aware whether it was ever stated explicitly before.

Proposition 2.2. *Let B be a k-subset of an additive group G of order v and let $\overline{B}$ be the complement of B in G. Let g be a non-zero element of G and let $\lambda(g)$ be its multiplicity in ΔB. Then the multiplicity $\overline{\lambda}(g)$ of g in $\Delta \overline{B}$ is $v - 2k + \lambda(g)$.*

Proof. Given subsets X and Y of G, set

$$\Lambda_{X \times Y}(g) = \{(x, y) \in X \times Y \mid x - y = g\}.$$

We have $|\Lambda_{B \times B}(g)| = \lambda$ and $|\Lambda_{\overline{B} \times \overline{B}}(g)| = \overline{\lambda}$ by assumption. Let (x_1, y_1), ..., (x_λ, y_λ) be the λ pairs of $\Lambda_{B \times B}(g)$ and set

$$B' = B \setminus \{x_1, \ldots, x_\lambda\} \quad \text{and} \quad B'' = B \setminus \{y_1, \ldots, y_\lambda\}.$$

It is easy to see that

$$\Lambda_{B \times \overline{B}}(g) = \{(b, -g + b) \mid b \in B'\} \quad \text{and} \quad \Lambda_{\overline{B} \times B}(g) = \{(g + b, b) \mid b \in B''\}$$

so that $|\Lambda_{B \times \overline{B}}(g)| = |B'| = k - \lambda$ and $|\Lambda_{\overline{B} \times B}(g)| = |B''| = k - \lambda$. Finally, it is evident that $\Lambda_{G \times G}(g) = \{(g + y, y) \mid y \in G\}$ so that $|\Lambda_{G \times G}(g)| = |G| = v$. Considering that the four sets $B \times B$, $\overline{B} \times \overline{B}$, $B \times \overline{B}$, and $\overline{B} \times B$ partition $G \times G$, we can write

$$|\Lambda_{B \times B}(g)| + |\Lambda_{\overline{B} \times \overline{B}}(g)| + |\Lambda_{B \times \overline{B}}(g)| + |\Lambda_{\overline{B} \times B}(g)| = |\Lambda_{G \times G}(g)|$$

and hence, from what seen above, $\lambda + \overline{\lambda} + (k - \lambda) + (k - \lambda) = v$ which immediately gives the assertion. $\square$

Proposition 2.3. *A PDF with only two blocks necessarily consists of a difference set and its complement. More specifically, a HPDF with only two blocks necessarily consists of a Hadamard difference set and its complement.*

Proof. If $\mathcal{F}$ is a $(v, [k, v - k], \lambda)$-PDF, then $\mathcal{F} = \{B, \overline{B}\}$ with B a k-subset of an additive group G of order v and $\overline{B} = G \setminus B$. Given any element $g \in G \setminus \{0\}$ denote by $\mu(g)$ and $\overline{\mu}(g)$ the multiplicities of g in ΔB and $\Delta \overline{B}$, respectively. By definition of a PDF we have $\mu(g) + \overline{\mu}(g) = \lambda$ for every $g \in G$. On the other hand we have $\overline{\mu}(g) = v - 2k + \mu(g)$ by Proposition 2.2 and then $v - 2k + 2\mu(g) = \lambda$, i.e., $\mu(g) = \frac{2k - v + \lambda}{2}$ is a constant. This means that B is a difference set and the first assertion follows.

Now assume that $\{B, \overline{B}\}$ is a $(v, [k, v-k], \lambda)$-HPDF so that we have $v = 2\lambda$. Without loss of generality we can assume that $k \leq v - k$, i.e., $k \leq \frac{v}{2}$. Then we deduce that B is a (v, k, μ)-DS with $\mu = \frac{2k-\lambda}{2}$. Considering that v is even, $k - \mu$ must be a square by the Bruck-Ryser-Chowla theorem. It follows that $\frac{\lambda}{2} = u^2$, hence $\mu = k - u^2$ for some integer u. Then, from the trivial identity $\mu(v - 1) = k(k - 1)$, we get $(k - u^2)(4u^2 - 1) = k(k - 1)$. Hence k is a solution of the quadratic equation $x^2 - 4u^2 x + 4u^4 - u^2 = 0$ so that either $k = 2u^2 + u$ or $k = 2u^2 - u$. On the other hand we have assumed $k \leq \frac{v}{2}$, hence $k = 2u^2 - u$ and $\mu = u^2 - u$. We conclude that B is a $(4u^2, 2u^2 - u, u^2 - u)$-DS, i.e., B is a Hadamard difference set. The assertion follows. $\qquad\square$

3   Some necessary conditions

The following proposition is straightforward.

Proposition 3.1. Let $\mathcal{F}$ be a $(G, [k_1, \ldots, k_t], \lambda)$-HPDF. Then

   (i) $k_1 + \cdots + k_t = 2\lambda$;

   (ii) $k_1^2 + \cdots + k_t^2 = \lambda(2\lambda + 1)$;

(iii) λ is even, hence $o(G) \equiv 0 \pmod 4$.

Proof. Let $\mathcal{F}$ be a $(G, [k_1, \ldots, k_t], \lambda)$-HPDF. By definition of a HPDF, we have $k_1 + \cdots + k_t = |G| = 2\lambda$. From $\Delta\mathcal{F} = \lambda(G \setminus \{0\})$ we obtain

$$|\Delta\mathcal{F}| = k_1(k_1 - 1) + \cdots + k_t(k_t - 1) = \lambda(2\lambda - 1)$$

and then

$$k_1^2 + \cdots k_t^2 = \lambda(2\lambda - 1) + k_1 + \cdots + k_t.$$

Then (ii) follows taking into consideration (i).

We obviously have $k_1 + \cdots + k_t \equiv k_1^2 + \cdots + k_t^2 \pmod 2$. Thus, using (i) and (ii), we get $2\lambda \equiv \lambda(2\lambda + 1) \pmod 2$ and (iii) follows. $\qquad\square$

As a consequence of the above proposition, every HPDF in a group G has $o(G)$ necessarily doubly even. However, it is worth to observe that this can be deduced in another way as follows. Assuming that $\mathcal{F}$ is a HPDF in G and $o(G) \equiv 2 \pmod 4$, then $\lambda = \frac{o(G)}{2}$ would be odd and this is absurd since

the multiplicity in $\Delta\mathcal{F}$ of any involution i of G is necessarily even: indeed, if $x - y = i$ is a representation of i as a difference from $\mathcal{F}$, then $y - x = i$ is a representation of i as a difference from $\mathcal{F}$ as well.

In the following table we list the very first parameter sets satisfying the necessary conditions of Proposition 3.1 disregarding those were K has size 2 in view of Proposition 2.3.

v	K	λ
20	$[1, 2, 3, 14]$	10
24	$[1^3, 2^2, 17]$	12
28	$[1, 9, 18]$	14
28	$[3, 6, 19]$	14
32	$[2^2, 6, 22]$	16
36	$[3, 9, 24]$	18
36	$[3, 4^2, 25]$	18
36	$[1^5, 6, 25]$	18
40	$[1, 3, 9, 27]$	20
40	$[3^4, 28]$	20
40	$[1^2, 3^2, 4, 28]$	20
40	$[1^4, 4^2, 28]$	20
40	$[1^3, 2^2, 5, 28]$	20

An HPDF with "blue parameter set" has been found by Buratti [6] and it is the only non-elementary HPDF known at this moment.

In Section 6 we will determine an HPDF with "green parameter set" in several groups.

By exhaustive computer search we have checked that an HPDF with "red parameter set" does not exist.

The existence of an HPDF with "uncolored parameter set" is still in doubt.

The HPDFs with only two blocks have been already characterized in Proposition 2.3. Let us see what we can say about HPDFs with three blocks.

Proposition 3.2. *In a* $(v, [k_1, k_2, k_3], \lambda)$*-HPDF we necessarily have*

$$k_{1,2} = \frac{2\lambda - k_3 \pm \sqrt{2\lambda(2k_3 + 1) - 3k_3^2}}{2}.$$

Proof. By Proposition 3.1 we have

$$k_1 + k_2 + k_3 = 2\lambda$$

and

$$k_1^2 + k_2^2 + k_3^2 = \lambda(2\lambda + 1).$$

The second identity can be rewritten as

$$(k_1 + k_2)^2 - 2k_1k_2 + k_3^2 = 2\lambda^2 + \lambda$$

and then, in view of the first identity, we have

$$(2\lambda - k_3)^2 - 2k_1k_2 + k_3^2 = 2\lambda^2 + \lambda$$

which gives

$$k_1 \cdot k_2 = \frac{2\lambda^2 - (4k_3 + 1)\lambda + 2k_3^2}{2}.$$

Considering that $k_1 + k_2 = 2\lambda - k_3$ and recalling that two numbers having sum s and product p are the solutions of the quadratic equation $x^2 - sx + p = 0$, after trivial computations we get the assertion. $\square$

The possible block-sizes of a $(v, [k_1, k_2, k_3], \lambda)$-HPDF are strongly limited by the above proposition. Indeed we have the following.

Corollary 3.3. *The existence of a $(v, [k_1, k_2, k_3], \lambda)$-HPDF necessarily implies that no prime divisor of $(2k_1 + 1)(2k_2 + 1)(2k_3 + 1)$ is congruent to 5 (mod 6).*

Proof. Assume that a $(v, [k_1, k_2, k_3], \lambda)$-HPDF exists and let p be a prime factor of $(2k_1 + 1)(2k_2 + 1)(2k_3 + 1)$. Up to a reordering of the indices we can assume that p is a divisor of $2k_3 + 1$ and hence p cannot divide k_3. By Proposition 3.2 it is clear that $2\lambda(2k_3 + 1) - 3k_3^2$ must be a perfect square. So, in particular, it must be a square modulo p. Considering that p is a divisor of $2k_3 + 1$ we have that $2k_3 + 1 \equiv 0 \pmod{p}$. Also, k_3^2 is a non-zero square of $\mathbb{Z}_p$ since p does not divide k_3. We conclude that -3 must be a square of $\mathbb{Z}_p$ and then, by the Quadratic Law of Reciprocity, we have either $p = 3$ or $p \equiv 1 \pmod 6$. $\square$

As a consequence of Corollary 3.3, in a $(v, [k_1, k_2, k_3], \lambda)$-HPDF we cannot have, for instance, blocks of size 2, 5, 7, 8, 11, 12, 14, 16, 17, ...

4   Exploiting partial difference sets

Note that Corollary 3.3 does not forbid the existence of a

$$(v, [k_1, k_2, k_3], \lambda)\text{-HPDF}$$

with a block of size 1 and indeed, using Proposition 3.2, we can see, for instance, that for every $n \geq 2$

$$\left(\frac{3^{2n-1} + 1}{2}, \left[\frac{3^{2n-1} + 3^n}{2}, \frac{3^{2n-1} - 3^n}{2}, 1 \right], \frac{3^{2n-1} + 1}{4} \right)$$

is an admissible parameter set for a HPDF. On the other hand we are going to see that a $(v, [k_1, k_2, 1], \lambda)$-HPDF cannot exist. To prove this we have to exploit a result on *partial difference sets*.

A (v, k, α, β) partial difference set (PDS) in a group G is a k-subset B of G such that ΔB covers α times every non-zero element of B and β times every non-zero element of $G \setminus B$.

Among the various necessary conditions for the existence of a non-trivial PDS we will need the following (see Proposition 3(d) in [18]).

Lemma 4.1. *If there exists a (v, k, α, β)-PDS and $\gamma := (\alpha - \beta)^2 + 4(k - \beta)$ is not a square, then we have $(v, k, \alpha, \beta) = (4t + 1, 2t, t - 1, t)$ for a suitable integer t.*

In the next proposition we will see that if a PDF in a group G has exactly three blocks one of which has size 1, then each of the other two blocks is a PDS or a DS in G.

Proposition 4.2. *Let $\mathcal{F} = \{B_1, B_2, \{0\}\}$ be a $(v, [k_1, k_2, 1], \lambda)$-PDF in G. Then, for $i = 1, 2$ we have:*

(i) *B_i is a $(v, \frac{v-1}{2}, \frac{v-3}{4})$-DS if $v - \lambda$ is odd;*

(ii) *B_i is a $(G, k_i, \alpha_i, \alpha_i + 1)$-PDS with $\alpha_i = k_i + \frac{\lambda - v}{2}$ if $v - \lambda$ is even.*

Proof. For $i = 1, 2$ and for $g \in G$, let $\lambda_i(g)$ be the multiplicity of g in ΔB_i. The assumption that $\mathcal{F}$ is a $(v, [k_1, k_2, 1], \lambda)$-PDF means that we have

$$\lambda_1(g) + \lambda_2(g) = \lambda \quad \forall \, g \in G \setminus \{0\}. \tag{1}$$

Let $\overline{B_1}$ be the complement of B_1 in G and let $\overline{\lambda_1}(g)$ be the multiplicity of g in $\Delta \overline{B_1}$. We have $\overline{B_1} = B_2 \cup \{0\}$ so that the possible representations

of $g \in G$ as a difference from $\overline{B_1}$ which are not representations of g as a difference from B_2 are $g = g - 0$ if $g \in B_2$, and $g = 0 - (-g)$ if $-g \in B_2$. Thus we can write:

$$\lambda_2(g) = \begin{cases} \overline{\lambda_1}(g) & \text{if } \{g, -g\} \subset B_1; \\ \overline{\lambda_1}(g) - 2 & \text{if } \{g, -g\} \subset B_2; \\ \overline{\lambda_1}(g) - 1 & \text{if } |\{g, -g\} \cap B_i| = 1 \text{ for } i = 1, 2. \end{cases} \tag{2}$$

In the following, we distinguish two cases according to the parity of $v - \lambda$ and keep in mind that we have

$$\overline{\lambda_1}(g) = v - 2k_1 + \lambda_1(g) \tag{3}$$

in view of Proposition 2.2.

Case 1: $v - \lambda$ is odd.

Observe that for any given $g \in G \setminus \{0\}$ we cannot have $\{g, -g\} \subset B_1$ otherwise (1), (2) and (3) would give $\lambda = v - 2k_1 + 2\lambda_1(g)$ contradicting the assumption that $v - \lambda$ is odd.

Analogously, we cannot have $\{g, -g\} \subset B_2$ otherwise (1), (2) and (3) would give $\lambda = v - 2k_1 + 2\lambda_1(g) - 2$ contradicting again that $v - \lambda$ is odd. We conclude that g and $-g$ lie in different B_i's for every $g \in G \setminus \{0\}$. It follows, in particular, that G is involution-free: if g is an involution, we cannot have $g \in B_1$ and $-g \in B_2$ since g and $-g$ are the same. Thus G has odd order and we have $B_2 = -B_1$ so that $k_1 = k_2 = \frac{v-1}{2}$. Considering that $\mathcal{F}$ is a $(v, [k_1, k_2, 1], \lambda)$-PDF we must have $\lambda(v-1) = k_1(k_1 - 1) + k_2(k_2 - 1)$ and hence $\lambda(v - 1) = 2 \cdot \frac{v-1}{2} \cdot \frac{v-3}{2}$ which gives $\lambda = \frac{v-3}{2}$. Finally, (2) and (3) give $\lambda_2(g) = v - 2 \cdot \frac{v-1}{2} + \lambda_1(g) - 1 = \lambda_1(g)$. It follows, by (1), that $\lambda_1(g) = \lambda_2(g) = \frac{\lambda}{2} = \frac{v-3}{4}$. It is now clear that B_1 and B_2 are $(v, \frac{v-1}{2}, \frac{v-3}{4})$-DSs.

Case 2: $v - \lambda$ is even.

Here, there is no $g \in G$ such that $g \in B_1$ and $-g \in B_2$. Indeed, in the opposite case, (1), (2) and (3) would give $\lambda = v - 2k_1 + 2\lambda_1(g) - 1$ contradicting the assumption that $v - \lambda$ is even. Thus, by (2), we have

$$\lambda_2(g) = \begin{cases} v - 2k_1 + \lambda_1(g) & \text{if } g \in B_1; \\ v - 2k_1 + \lambda_1(g) - 2 & \text{if } g \in B_2. \end{cases}$$

Using again (1) and (3) we get $\lambda = v - 2k_1 + 2\lambda_1(g)$ or $v - 2k_1 + 2\lambda_1(g) - 2$ according to whether $g \in B_1$ or $g \in B_2$, respectively. Solving these identities with respect to $\lambda_1(g)$ we finally get

$$\lambda_1(g) = \begin{cases} \alpha_1 & \text{if } g \in B_1; \\ \alpha_1 + 1 & \text{if } g \in B_2. \end{cases}$$

This precisely means that B_1 is a $(G, k_1, \alpha_1, \alpha_1+1)$-PDS. In the same way, exchanging the roles of B_1 and B_2 one gets that B_2 is a $(G, k_2, \alpha_2, \alpha_2+1)$-PDS. $\qquad\square$

Corollary 4.3. *A $(v, [k_1, k_2, 1], \lambda)$-HPDF cannot exist.*

Proof. Assume that there exists a $(v, [k_1, k_2, 1], \lambda)$-HPDF so that $v - \lambda = \lambda$ is even. Up to a translation we can assume that the block of size 1 is $\{0\}$. Then, by Proposition 4.2, the block of size k_1 is a $(2\lambda, k_1, \alpha, \alpha + 1)$-PDS with $\alpha = k_1 - \frac{\lambda}{2}$. Here the parameter γ mentioned in Lemma 4.1 is $1 + 4(k_1 - k_1 + \frac{\lambda}{2}) = 2\lambda + 1$. Thus, in view of the same lemma, $2\lambda + 1$ is a perfect square, say $2\lambda + 1 = \mu^2$, otherwise we should have $v = 4t + 1$ which is absurd. By Proposition 3.2 it is also necessary that $6\lambda - 3$ is a perfect square. Now note that we have $6\lambda - 3 = 3(2\lambda - 1) = 3(\mu^2 - 2)$ so that 3 should divide $\mu^2 - 2$. This is absurd since 2 is not a square modulo 3. $\quad\square$

5   Exploiting subgroups of index 2

The following proposition exploits the possible existence of a subgroup of index 2.

Proposition 5.1. *Let $\mathcal{F} = \{B_1, \ldots, B_t\}$ be a $(G, [k_1, \ldots, k_t], \lambda)$-HPDF, assume that G has a subgroup H of index 2, and set $|B_i \cap H| = s_i$ for $i = 1, \ldots, t$. Then the following identities hold:*

$$s_1 + \ \ldots \ + s_t = \lambda \qquad \text{and} \qquad 2s_1(k_1 - s_1) + \ \ldots \ + 2s_t(k_t - s_t) = \lambda^2$$

Proof. For $i = 1, \ldots, t$, set $B'_i = B_i \cap H$ and $B''_i = B_i \setminus H$ so that $|B'_i| = s_i$ and $|B''_i| = k_i - s_i$. The first identity follows from the fact that the B_i's partition H which has order λ. Now note that we have

$$\Delta B_i = \Delta B'_i \ \cup \ \Delta B''_i \ \cup \ (B'_i - B''_i) \ \cup \ (B''_i - B_i).$$

Also note that $\Delta B'_i \ \cup \ \Delta B''_i$ is a multisubset of H and that both $B'_i - B''_i$ and $B''_i - B'_i$ are multisubsets of $G \setminus H$ of size $|B'_i| \cdot |B''_i| = s_i(k_i - s_i)$. Thus we can say that ΔB_i has exactly $2s_i(k_i - s_i)$ elements in $G \setminus H$. Then, considering that $\Delta \mathcal{F}$ covers every element of $G \setminus H$ exactly λ times, we conclude that we have $\sum_{i=1}^{t} 2s_i(k_i - s_i) = \lambda \cdot |G \setminus H| = \lambda^2$, i.e., the second identity holds. $\qquad\square$

As a consequence we have the following.

Corollary 5.2. *If there exists a* $(G, [k_1, \ldots, k_t], \lambda)$*-HPDF and* G *has a subgroup of index* 2*, then the diophantine system*

$$
\begin{cases}
x_1 & + \ldots + & x_t & = & \lambda \\
2x_1(k_1 - x_1) & + \ldots + & 2x_t(k_t - x_t) & = & \lambda^2
\end{cases}
$$

has a solution $(s_1, \ldots, s_t)$ *with* $0 \le s_i \le k_i$ *for each* i.

As application of the above corollary one can see that none of these K, though admissible, can be the multiset of block-sizes of a HPDF:

$$[50, 20, 5, 1]; \quad [52, 23, 2, 1, 1, 1]; \quad [73, 38, 3, 2];$$

$$[77, 28, 8, 3]; \quad [79, 31, 7, 3]; \quad [81, 21, 16, 1, 1]; \quad [104, 35, 14, 3].$$

As a matter of fact we have to admit that the admissible K which are ruled out by Corollary 5.2 do not appear so many. On the other hand Proposition 5.1 has been useful to limit our computer search for HPDFs of small orders.

6 New HPDFs

In this section we present HPDFs with the three new parameter sets

$$(24, [1^3, 2^2, 17], 12), \qquad (36, [3, 9, 24], 18) \quad \text{and} \quad (40, [1, 3, 9, 27], 20).$$

We will use, in particular, some dihedral groups and dicyclic groups of small orders. We recall that the dihedral group of order $2n$, denoted D_{2n}, is the group with defining relations

$$\langle x, y \mid x^n = 1; \ y^2 = 1; \ yx^i = x^{-i}y \rangle.$$

We also recall that the dicyclic group of order $4n$, denoted Q_{4n}, is the group with defining relations

$$\langle x, y \mid x^{2n} = 1; \ y^2 = x^n; \ yx^i = x^{-i}y \rangle.$$

6.1 $(24, [1^3, 2^2, 17], 12)$-HPDFs

We found an example of a $(24, [1^3, 2^2, 17], 12)$-HPDF in each of the following groups: $C_3 \rtimes C_8$, $SL(2, 3)$ and $C_3 \times D_8$.

$G = C_3 \rtimes C_8$

This is the semidirect product of C_3 by C_8 with defining relations

$$C_3 \rtimes C_8 = \langle a, b \,|\, a^8 = b^3 = 1, ab^{-1} = ba \rangle.$$

Thus the elements of G are of the form $a^i b^j$ with $0 \le i \le 7$ and $0 \le j \le 2$. The difference (even though we should say "ratio" since we are in multiplicative notation) between two elements $a^{i_1} b^{j_1}$ and $a^{i_2} b^{j_2}$ is given by

$$(a^{i_1} b^{j_1})(a^{i_2} b^{j_2})^{-1} = a^{i_1 - i_2} b^{(-1)^{i_2}(j_1 - j_2)}. \tag{4}$$

Let $\mathcal{F} = \{B_1, B_2, B_3, B_4, B_5, B_6\}$ be the partition of G defined as follows:

$$B_1 = \{1, a, a^2, a^3, a^4, a^6, a^7, b, ab, a^3b, a^4b, a^5b, a^6b, b^2, ab^2, a^2b^2, a^4b^2\};$$

$$B_2 = \{a^3b^2\}; \quad B_3 = \{a^5b^2\}; \quad B_4 = \{a^7b^2\};$$

$$B_5 = \{a^5, a^2b\}; \quad B_6 = \{a^7b, a^6b^2\}.$$

Using (4) it is straightforward to check that $\mathcal{F}$ is a $(G, [1^3, 2^2, 17], 12)$-HPDF.

$G = SL(2, 3)$

This is the 2-dimensional special linear group over $\mathbb{Z}_3$. Its elements are the 2×2 matrices with elements in $\mathbb{Z}_3$ and determinant equal to 1. Let $\mathcal{F} = \{B_1, B_2, B_3, B_4, B_5, B_6\}$ be the partition of G defined as follows:

$$B_1 = \left\{ \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \right\}; \quad B_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right\}; \quad B_3 = \left\{ \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix} \right\};$$

$$B_4 = \left\{ \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \right\}; \quad B_5 = \left\{ \begin{pmatrix} 2 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix} \right\};$$

$$B_6 = G \setminus (B_1 \cup B_2 \cup B_3 \cup B_4 \cup B_5).$$

It is straightforward to check that $\mathcal{F}$ is a $(G, [1^3, 2^2, 17], 12)$-HPDF.

$G = \mathbb{Z}_3 \times D_8$

The reader can easily recognize that the partition of G into the blocks listed below is a $(G, [1^3, 2^2, 17], 12)$-HPDF.

$$B_1 = \{(0, x^2)\}; \quad B_2 = \{(2, xy)\}; \quad B_3 = \{(2, x^3y)\};$$

$$B_4 = \{(1, x^3), (2, x^3)\}; \quad B_5 = \{(1, y), (2, x^2y)\};$$

$$B_6 = G \setminus (B_1 \cup B_2 \cup B_3 \cup B_4 \cup B_5).$$

6.2 $(36, [3, 9, 24], 18)$-HPDFs

We found an example $\mathcal{F} = \{A, B, C\}$ of a $(36, [3, 9, 24], 18)$-HPDF in the groups

$$\mathbb{Z}_6 \times \mathbb{Z}_6, \qquad \mathbb{Z}_3 \times \mathbb{Z}_{12}, \qquad \mathbb{Z}_3 \times Q_{12}, \qquad D_6 \times D_6, \qquad \mathbb{Z}_6 \times D_6,$$

$$\mathbb{Z}_3 \times A_4, \qquad \mathbb{Z}_3 \rtimes Q_{12}, \qquad \mathbb{Z}_3^2 \rtimes \mathbb{Z}_4, \qquad \mathbb{Z}_2 \times \mathbb{Z}_3 \rtimes D_6.$$

We present our example for each of the first five.

$G = \mathbb{Z}_6 \times \mathbb{Z}_6$

$A = \{(1, 1), (1, 3), (1, 5)\};$
$B = \{\{0, 2), (0, 3), (1, 4), (2, 0), (2, 5), (3, 4), (4, 1), (4, 4), (5, 4)\};$
$C = G \setminus (A \cup B).$

$G = \mathbb{Z}_3 \times \mathbb{Z}_{12}$

$A = \{(1, 1), (1, 5), (1, 9)\};$
$B = \{\{0, 2), (0, 3), (0, 4), (1, 2), (1, 8), (1, 11), (2, 0), (2, 2), (2, 7)\};$
$C = G \setminus (A \cup B).$

$G = \mathbb{Z}_3 \times Q_{12}$

$A = \{(0, xy), (1, xy), (2, xy)\};$
$B = \{\{1, 1), (0, x^3), (0, x^2), (2, y), (1, x^5), (2, x^4 y), (2, x^4), (2, x^2 y), (2, x)\};$
$C = G \setminus (A \cup B).$

$G = D_6 \times D_6$

$A = \{(y, xy), (xy, xy), (x^2 y, xy)\};$
$B = \left\{ \begin{matrix} (1, x^2 y), (x, y), (x^2, 1), (x^2, x), (x^2, x^2), \\ (x^2, xy), (y, 1), (xy, x^2), (x^2 y, x) \end{matrix} \right\};$
$C = G \setminus (A \cup B).$

$G = \mathbb{Z}_6 \times D_6$

$A = \{(1, xy), (3, xy), (5, xy)\};$
$B = \{\{0, x), (1, x^2), (2, 1), (3, 1), (4, x^2), (4, y), (4, xy), (4, x^2 y), (5, x)\};$
$C = G \setminus (A \cup B).$

6.3 A cyclic $(40, [1, 3, 9, 27], 20)$-HPDF

This is our unique example of a HPDF in a cyclic group. Also, it has maximum order among the few non-elementary HPDFs that are known at this moment. Thus it is surprising that this is also the unique example that we have been able to get by hand without any use of the computer. The idea was the following. Start from any cyclic $(40, 13, 4)$-DS, that is a *Singer* difference set. Such a difference set is available in the literature. One is, for instance, the following (see [13], page 427):

$$D = \{1, 2, 3, 5, 6, 9, 14, 15, 18, 20, 25, 27, 35\}.$$

By Corollary 2.1, $\overline{D} := \mathbb{Z}_{40} \setminus D$ is a $(40, 27, 18)$-DS. Then, if we are able to partition D into three subsets A, B, C of sizes 1, 3, 9 in such a way that $\Delta A \cup \Delta B \cup \Delta C$ is all $\mathbb{Z}_{40} \setminus \{0\}$ twice, it is obvious that

$$\mathcal{F} = \{A, B, C, \overline{D}\}$$

would be a $(40, [1, 3, 9, 27], 20)$-HPDF. Well, the desired partition of D has A, B, C as follows:

$$A = \{13\}; \quad B = \{5, 15, 25\}; \quad C = \{1, 2, 3, 6, 9, 14, 18, 20, 27\}.$$

This is readily seen from the *difference tables* of B and C below (of course ΔA is empty).

	5	15	25
5	–	30	20
15	10	–	30
25	20	10	–

	1	2	3	6	9	14	18	20	27
1	–	39	38	35	32	27	23	21	14
2	1	–	39	36	33	28	24	22	15
3	2	1	–	37	34	29	25	23	16
6	5	4	3	–	37	32	28	26	19
9	8	7	6	3	–	35	31	29	22
14	13	12	11	8	5	–	36	34	27
18	17	16	15	12	9	4	–	38	31
20	19	18	17	14	11	6	2	–	33
27	26	25	24	21	18	13	9	7	–

It is worth observing that C is a $(10, 4, 9, 2)$ *relative difference set*. It means that ΔC is precisely twice $\mathbb{Z}_{10\cdot4} \setminus N$ where N is the subgroup of $\mathbb{Z}_{10\cdot4}$ of order 4 (see [13]).

7   New infinite families of PDFs

Most composition constructions for PDFs make use of *difference matrices* and lead to PDFs whose block sizes belong, almost all, to the set of block sizes of the component PDFs (see [9, 15]). Buratti [6] motivated the introduction of HPDFs showing that any single (v, K, λ)-HPDF is the *ancestor* of an infinite series of PDFs where, apart from one special block of size 2λ, the size of every other block is the double of some $k \in K$. We are going to recall the main application of his construction and then we determine the *descendants* of our new examples.

Following [4], the maximal prime power factors of a given integer v will be called *components* of v, and $\mathbb{F}_v$ will denote the ring which is the direct product of the fields whose orders are the components of v. Thus, for instance, $\mathbb{F}_{63} = \mathbb{F}_9 \times \mathbb{F}_7$.

Theorem 7.1. *[6] If there exists a $(G, [k_1, \ldots, k_t], \lambda)$-HPDF and all the components of $2n+1$ are greater than $2 \cdot \max\{k_1, \ldots, k_t\}$, then there exists a $(2\lambda(2n + 1), [(2k_1)^n, \ldots, (2k_t)^n, 2\lambda], 2\lambda)$-PDF in $G \times \mathbb{F}_{2n+1}$.*

Applying the above theorem using the new examples of HPDFs obtained in Section 6 we obtain the following results.

Corollary 7.2. *If all the components of $2n+1$ are greater than 34, then there exists a $(48n + 24, [34^n, 4^{2n}, 2^{3n}, 24], 24)$-PDF in $G \times \mathbb{F}_{2n+1}$ for each of the three groups G considered in 6.1.*

The first n for which the above corollary can be applied is 18. In this way one gets a $(984, [34^{18}, 4^{36}, 2^{54}, 24], 24)$-PDF in $G \times \mathbb{F}_{37}$.

Corollary 7.3. *If all the components of $2n+1$ are greater than 48, then there exists a $(72n + 36, [6^n, 18^n, 48^n, 36], 36)$-PDF in $G \times \mathbb{F}_{2n+1}$ for each of the nine groups G considered in 6.2.*

The first n for which the above corollary can be applied is 24. In this way one gets a $(1764, [6^{24}, 18^{24}, 48^{24}, 36], 36)$-PDF.

Corollary 7.4. *If all the components of $2n + 1$ are greater than 54, then there exists a $(80n + 40, [2^n, 6^n, 18^n, 54^n, 40], 40)$-PDF in $\mathbb{Z}_{40} \times \mathbb{F}_{2n+1}$.*

The first n for which the above corollary can be applied is 29. In this way one gets a $(2360, [2^{29}, 6^{29}, 18^{29}, 54^{29}, 40], 40)$-PDF.

8 A pair of open questions

It is obvious that any (v, k, λ) difference set B with $v = 2\lambda$ gives rise to a $(v, [1^{v-k}, k], \lambda)$-HPDF consisting of B and all possible singletons $\{g\}$ with $g \in G \setminus B$. Thus, for our purposes, it is worth to look for difference sets with this property. Let us call them *Pell difference sets*. The existence of a Pell (v, k, λ)-DS obviously requires that $k(k - 1) = \lambda(2\lambda - 1)$ and, by the Bruck-Ryser-Chowla theorem, that $k - \lambda$ is a square. On the other hand the latter condition is redundant. Indeed, as shown in the following, the first condition implies the second.

Proposition 8.1. *If k and λ are integers such that $k(k - 1) = \lambda(2\lambda - 1)$, then $k - \lambda$ is a square.*

Proof. Set $d = \gcd(k, \lambda)$. Thus we have $k = de$ and $\lambda = df$ with e and f coprime integers. From the given equality we get $e(de - 1) = f(2df - 1)$ and then, considering that $\gcd(e, f) = 1$, we necessarily have $de - 1 = fg$ and $2df - 1 = eg$ for some integer g. Subtracting the second equality from the first one we get $d(e - 2f) = g(f - e)$. We clearly have $\gcd(d, g) = 1$ and hence $d = f - e$ and $g = e - 2f$. We conclude that $k - \lambda = d(e - f) = d^2$. □

Apart from the trivial $(4, 3, 2)$-DS, no other Pell difference set is known.

Question 8.2. *Does there exist a Pell difference set of order $v > 4$?*

Here are the first possible triples (v, k, λ) for which a non-trivial Pell (v, k, λ) difference set may exist:

(120, 85, 60)

(4060, 2871, 2030)

(137904, 97513, 68952)

(4684660, 3312555, 2342330)

(159140520, 112529341, 79570260)

Let us consider the first one. A putative $(120, 85, 60)$ is the complement of a $(120, 35, 10)$-DS. Even though several authors investigated the possible

existence of a DS with these parameters, they have been only able to rule out some groups (see [2]).

In view of these consideration and the fact that the admissible values of v grow up very rapidly, we are afraid that Question 8.2 is really hard.

We come now to another question which is probably easier.

The parameter set of the last HPDF constructed in Section 6 can be written as

$$\left(\frac{3^4 - 1}{2}, [3^0, 3^1, 3^2, 3^3], \frac{3^4 - 1}{4}\right).$$

Inspired by this, we have noticed that

$$\left(\frac{q^{2n} - 1}{q - 1}, [q^0, q^1, q^2, q^3, \dots, q^{2n-1}], \frac{q^{2n} - 1}{q + 1}\right)$$

is an admissible parameter set of a PDF for every positive integer q (not necessarily a prime power!). Indeed, if we set $v = \frac{q^{2n}-1}{q-1}$, $k_{i+1} = q^i$ for $0 \leq i \leq 2n - 1$, and $\lambda = \frac{q^{2n}-1}{q+1}$, we see that we have:

1) $k_1 + k_2 + \cdots + k_{2n} = \displaystyle\sum_{i=0}^{2n-1} q^i = \frac{q^{2n} - 1}{q - 1} = v;$

2) $k_1(k_1 - 1) + k_2(k_2 - 1) + \cdots + k_{2n}(k_{2n} - 1)$

$$= (k_1^2 + k_2^2 + \cdots + k_{2n}^2) - (k_1 + k_2 + \cdots + k_{2n})$$

$$= \sum_{i=0}^{2n-1} q^{2i} - \frac{q^{2n} - 1}{q - 1} = \frac{q^{4n} - 1}{q^2 - 1} - \frac{q^{2n} - 1}{q - 1}$$

$$= \frac{(q^{2n} - 1)(q^{2n-1} - q)}{q^2 - 1} = \lambda(v - 1).$$

Thus the following question naturally arises.

Question 8.3. *Given positive integers q and n, does there exist a PDF whose K is $[q^0, q^1, q^2, q^3, \dots, q^{2n-1}]$?*

For now, we know that the answer is positive for $q = 3$ and $n = 1, 2$. A positive answer for $q = 3$ and any n would give the first infinite family of HPDFs.

Acknowledgements

References

[1] I. Anderson, *Combinatorial Designs: Construction Methods*, Ellis Horwood, England, 1990.

[2] P.E. Becker, Investigation of solvable $(120, 35, 10)$ difference sets, *J. Combin. Des.*, **13** (2005), 79–107.

[3] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, 1999.

[4] S. Bonvicini, M. Buratti, M. Garonzi, G. Rinaldi, T. Traetta, The first families of highly symmetric Kirkman triple systems whose orders fill a congruence class, *Des. Codes Crypt.*, **89** (2021), 2725–2757.

[5] M. Buratti, On disjoint $(v, k, k-1)$ difference families, *Des. Codes Cryptogr.*, **87** (2019), 745–755.

[6] M. Buratti, Hadamard partitioned difference families and their descendants, *Cryptogr. Commun.*, **11** (2019), 557–562.

[7] M. Buratti, D. Jungnickel, Partitioned difference families versus Zero difference balanced functions, *Des. Codes Cryptogr.*, **87** (2019), 2461–2467.

[8] M. Buratti, D. Jungnickel, Partitioned difference families and harmonious linear spaces, https://arxiv.org/abs/2303.11416

[9] M. Buratti, J. Yan, C. Wang, From a 1-rotational RBIBD to a partitioned difference family, *Electronic J. Combin.*, **17** (2010), #R139.

[10] W. Chu, C. Colbourn, P. Dukes. Constructions for permutation codes in powerline communications, *Des. Codes Cryptogr.*, **32** (2004), 51–64.

[11] C. Ding, Optimal constant composition codes from zero-difference balanced functions, *IEEE Trans. Inf. Theory*, **54** (2008), 5766–5770.

[12] C. Ding, J. Yin, Combinatorial constructions of optimal constant-composition codes, *IEEE Trans. Inform. Theory*, **51** (2005), 3671–3674.

[13] D. Jungnickel, A. Pott, K.W. Smith, *Difference sets*, chapter VI.18 in "Handbook of Combinatorial Designs", Second Edition, C.J. Colbourn and J.H. Dinitz, ed., Chapman & Hall/CRC, Boca Raton, FL, 419–435, 2006.

[14] G. Ge, R. Fuji-Hara, Y. Miao. Further combinatorial constructions for optimal frequency-hopping sequences, *J. Combin. Theory Ser. A* **113**, 8 (2006), 1699–1718.

[15] S. Li, H. Wei, G. Ge, Generic constructions for partitioned difference families with applications: a unified combinatorial approach, *Des. Codes Cryptogr.* **82** (2017), 583–599.

[16] E. Lander. *Symmetric designs: An Algebraic Approach.* Cambridge University Press, 1983.

[17] Y. Luo, F.-W. Fu, A. J. Han Vinck, and W. Chen, On constant composition codes over $\mathbf{Z}_q$, *IEEE Trans. Inf. Theory* **49** (2003), 3010–3016.

[18] S.L. Ma, A survey of partial difference sets, *Des. Codes Cryptogr.* **4** (1994), 221–261.

Anamari Nakić
Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia
anamari.nakic@fer.hr