Hadamard partitioned difference families and their descendants

Marco Buratti[1]

Abstract If D is a $(4u^2, 2u^2 - u, u^2 - u)$ Hadamard difference set (HDS) in G, then $\{G, G \setminus D\}$ is clearly a $(4u^2, [2u^2 - u, 2u^2 + u], 2u^2)$ partitioned difference family (PDF). Any (v, K, λ)-PDF will be said a Hadamard PDF if $v = 2\lambda$ as the one above. We present a doubling construction which, starting from any Hadamard PDF, leads to an infinite class of PDFs. As a special consequence, we get a PDF in a group of order $4u^2(2n + 1)$ and three block-sizes $4u^2 - 2u$, $4u^2$ and $4u^2 + 2u$, whenever we have a $(4u^2, 2u^2 - u, u^2 - u)$-HDS and the maximal prime power divisors of $2n + 1$ are all greater than $4u^2 + 2u$.

Keywords Partitioned difference family · Hadamard difference set · Strong difference family

Mathematics Subject Classification (2010) 05B10 · 94B25

1 Introduction

Throughout this note the *multiset sum* of two multisets X and Y on a set S is the multiset $X \uplus Y$ where the multiplicity of every element of S is the sum of its multiplicities in X and Y. The multiset sum of μ copies of a multiset X will be denoted by $^{\mu}X$. The multiset $^{\mu_1}\{x_1\} \uplus \ldots \uplus {}^{\mu_t}\{x_t\}$ will be denoted by $[^{\mu_1}x_1, \ldots, {}^{\mu_t}x_t]$.

Given an additive group G and a multiset $X = \{x_1, \ldots, x_k\}$ on G, the *list of differences of X* is the multiset ΔX of all possible differences $x_i - x_j$ with (i, j) an ordered pair of distinct elements in $\{1, \ldots, k\}$. More generally, the list of differences of a collection $\mathcal{X}$ of

✉ Marco Buratti
  buratti@dmi.unipg.it

[1] Dipartimento di Matematica e Informatica, Università di Perugia,
  via Vanvitelli 1, Perugia, 06123, Italy

multisubsets of G is the multiset sum $\Delta \mathcal{X} := \biguplus_{X \in \mathcal{X}} \Delta X$. Assume that K is the multiset of sizes of the members of $\mathcal{X}$. The following cases are important:

- $\Delta \mathcal{X} = {}^{\lambda}(G \setminus H)$ for a suitable λ and a suitable subgroup H of G. Here one says that $\mathcal{X}$ is a (G, H, K, λ) *difference family* (DF).

- $\Delta \mathcal{X} = {}^{\mu}G$ for a suitable μ. Here one says that $\mathcal{X}$ is a (G, K, μ) *strong difference family* (SDF).

Very often one refers to a (G, H, K, λ)-DF as a (v, h, K, λ) difference family in G *relative to H* where v and h denote the orders of G and H, respectively. One speaks of an *ordinary* difference family when $H = \{0\}$. In this case one simply writes (G, K, λ)-DF or (v, K, λ)-DF in G.

The members of a DF or SDF are called *blocks*. It is clear that every block of a DF is a set while a SDF must have at least one block with repeated elements. A DF or SDF with only one block is said to be a *difference set* (DS) or a *difference multiset* (also called a *difference cover* in [1, 14]), respectively. If one writes k instead of K, it means that all blocks have size k.

Partitioned difference families (PDFs), also known as *zero difference balanced functions* (see, e.g., [17, 19]), are (G, K, λ)-DFs whose blocks partition G. They have been introduced by Ding and Yin [10] for the construction of *optimal constant composition codes*. They are also important from the design theory perspective; for instance, it is shown in [6] that a PDF with $K = [{}^{1}(k - 1), {}^{r}k]$ gives rise to a *resolvable 2-design* with block size k.

In the class of PDFs we have, in particular, the $(G, [{}^{1}1, {}^{n}k], k - 1)$-PDFs giving rise to sharply point transitive *near resolvable* $2\text{-}(kn + 1, k, k - 1)$ designs. There are many constructions of PDFs of this kind in the literature. Anyway, as shown in [7], most of them are encompassed in a unique simple algebraic construction.

In this paper we are interested in (v, K, λ)-PDFs having $v = 2\lambda$. The motivation will be given by our main result: each PDF with this property leads to an infinite class of PDFs obtainable by means of a new doubling construction. We point out that, so far, the composition constructions for PDFs essentially made use of difference matrices [6, 13].

Definition 1 A Hadamard PDF is a (G, K, λ)-PDF with $|G| = 2\lambda$.

We choose the name "Hadamard" since every *Hadamard difference set* (HDS) immediately gives a PDF with the required property. For convenience of the reader we recall that a HDS is a difference set of parameters $(4u^2, 2u^2 - u, u^2 - u)$ for some u (see, e.g., [12]).

Proposition 1 *If D is a HDS in G, then $\{D, G \setminus D\}$ is a Hadamard PDF.*

Proof It is known and trivial that if D is a (v, k, λ)-DS in G, then $\{D, G \setminus D\}$ is a $(v, [k, v - k], v - 2k + 2\lambda)$-PDF in G. So, in particular, if D is a $(4u^2, 2u^2 - u, u^2 - u)$-HDS, then $\{D, G \setminus D\}$ is a $(4u^2, [2u^2 - u, 2u^2 + u], 2u^2)$-PDF in G. The assertion follows. $\square$

At the moment to find another class of Hadamard PDFs seems to be quite hard to this author. Anyway the set of Hadamard PDFs not coming from the above proposition is not empty. Indeed we have found a $(32, [{}^{2}2, 6, 22], 16)$-PDF in the non-abelian group G whose elements are all pairs of the Cartesian product $\mathbb{Z}_4 \times \mathbb{Z}_8$ and whose operation law is

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, 5^{x_2} y_1 + y_2).$$

One can check that the four blocks of the mentioned PDF are the following:

$$X_1 = \{(0,0),(2,0)\}; \quad X_2 = \{(1,0),(3,4)\}$$

$$X_3 = \{(0,1),(0,3),(1,2),(1,5),(1,6),(3,3)\}; \quad X_4 = G \setminus (X_1 \cup X_2 \cup X_3).$$

2 Hadamard strong difference families

Strong difference families have been formally introduced in [3] but they have been implicitly used in many earlier papers. Note that they have no known relation to the "strong external difference families" very recently introduced in [15], in spite of the misfortune of inadvertently similar terminology.

Strong difference families might be very useful to construct relative difference families [4, 5, 8, 9, 14]; in a certain sense they are the "skeleton" of the resulting difference family as shown in the following construction which is a little bit more general than the "fundamental construction" in [3].

Theorem 1 *Let $\mathcal{X} = \{X_1, \ldots, X_t\}$ be a (G, K, μ)-SDF. Take a group H and a pair of positive integers (n, λ) with $\mu n = \lambda(|H| - 1)$. Then take a collection $\mathcal{B} = \{B_1, \ldots, B_t\}$ of subsets of $G \times H$ such that the projection of B_i on G coincides with X_i for $i = 1, \ldots, t$. We have*

$$\Delta\mathcal{B} = \biguplus_{g \in G} \{g\} \times L_g$$

for suitable lists L_g of elements of H. Here, by definition of a SDF, every L_g has constant size μ. This is important because it allows for the possible existence of an n-set E of endomorphisms of H for which we have

$$\biguplus_{\varepsilon \in E} \varepsilon(L_g) = {}^\lambda(H \setminus \{0\}) \quad \forall g \in G.$$

If such a set E exists, extend each $\varepsilon \in E$ to the endomorphism $\widehat{\varepsilon}$ of $G \times H$ defined by $\widehat{\varepsilon}(g, h) = (g, \varepsilon(h))$ for each $(g, h) \in G \times H$. Then $\{\widehat{\varepsilon}(B_i) \mid 1 \le i \le t; \varepsilon \in E\}$ is a $(G \times H, G \times \{0\}, {}^n K, \lambda)$-DF.

The "fundamental construction" in [3] corresponds to the case that H is the additive group of a finite field $\mathbb{F}_q$ and each $\varepsilon \in E$ is the multiplication by a suitable non-zero element of the field. Thus, it is in some way related with the "factorization of a group" [16] and, more generally, with the "multifold factorization of a group" [2, 18]. Indeed the construction succeeds if there exists $E \subset \mathbb{F}_q^*$ such that $E \cdot L_g = {}^\lambda \mathbb{F}_q^*$ for every $g \in G$. In most known applications E is a subgroup of $\mathbb{F}_q^*$ and each L_g is the multiset sum of λ complete systems of representatives for the cosets of E in $\mathbb{F}_q^*$.

In [3] it was shown how "playing" with some classic difference sets it is possible to obtain elementary but very useful strong difference families. For instance, it was shown that if D is a *Paley-type* difference set in a group G of order $4n - 1$ - hence of parameters $(4n - 1, 2n - 1, n - 1)$ - then ${}^2(G \setminus D)$ is a $(4n - 1, 4n, 4n)$ difference multiset. Here we will do something similar using Hadamard PDFs.

Proposition 2 *If $\mathcal{X}$ is a Hadamard (G, K, λ)-PDF, then $\{{}^2 X \mid X \in \mathcal{X}\}$ is a $(G, 2K, 4\lambda)$-SDF.*

Proof Let $m(g)$ be the multiplicity of g in $\biguplus_{X \in \mathcal{X}} \Delta(^2 X)$. We have to prove that $m(g) = 4\lambda$ for all $g \in G$. It is quite evident that if X is a subset of G, then $\Delta(^r X)$ contains zero exactly $r(r-1)|X|$ times and it contains a non-zero element g of G exactly $r^2 \lambda_X(g)$ times where $\lambda_X(g)$ is the multiplicity of g in ΔX. Applying this to our case we get

$$m(0) = 2 \sum_{X \in \mathcal{X}} |X| \qquad \text{and} \qquad m(g) = 4 \sum_{X \in \mathcal{X}} \lambda_X(g) \quad \forall g \in G \setminus \{0\}.$$

Considering that $\mathcal{X}$ is a (G, K, λ)-PDF, we have $\sum_{X \in \mathcal{X}} |X| = |G|$ and $\sum_{X \in \mathcal{X}} \lambda_X(g) = \lambda$. Also, considering that $\mathcal{X}$ is a Hadamard PDF, we have $|G| = 2\lambda$. Hence we can write:

$$m(0) = 2|G| = 4\lambda \qquad \text{and} \qquad m(g) = 4\lambda \quad \forall g \in G \setminus \{0\}.$$

The assertion follows.   □

We will refer to the strong difference family constructed in the above proposition as the Hadamard SDF associated with $\mathcal{X}$.

3 The main construction

We are now ready to state and prove our main result.

Theorem 2 *Let $\mathcal{D}$ be a Hadamard (G, K, λ)-PDF and let $R = (H, +, \cdot)$ be a ring with identity of order $2n + 1$ admitting a set Y of units such that:*

Y has size equal to the maximum size K_{max} of the blocks of $\mathcal{D}$;
every element of $\Delta(Y \cup -Y)$ is a unit of R.

Then there exists a $(2\lambda(2n + 1),\ ^n(2K) \uplus \{2\lambda\},\ 2\lambda)$-PDF in $G \times H$.

Proof We get the result by applying Theorem 1 with $\mathcal{X}$ the Hadamard $(G, 2K, 4\lambda)$-SDF associated with $\mathcal{D}$. So, if $\mathcal{D} = \{D_1, \ldots, D_t\}$, we have $\mathcal{X} = \{X_1, \ldots, X_t\}$ with $X_i = {}^2 D_i$ for $i = 1, \ldots, t$.

Take any map $f : G \longrightarrow Y$ which is injective on each block $D_i \in \mathcal{D}$. This is possible since the blocks of $\mathcal{D}$ are disjoint by definition and we have $|Y| = K_{max} \geq |D_i|$ for every i. Now, for $i = 1, \ldots, t$, consider the subset B_i of $G \times H$ defined by

$$B_i = \bigcup_{d \in D_i} \{d\} \times \{f(d), -f(d)\}.$$

As prescribed by Theorem 1 the projection of B_i on G coincides with X_i for $i = 1, \ldots, t$. So we have $\Delta\{B_1, \ldots, B_t\} = \biguplus_{g \in G} \{g\} \times L_g$ where each L_g is a list of 4λ elements of H. Explicitly, these lists are as follows:

$$L_0 = \{\pm 2 f(d) \mid d \in G\};$$

$$L_g = \{\pm f(d) \pm f(d') \mid (d, d') \in \bigcup_{i=1}^{t} D_i \times D_i;\ d - d' = g\} \quad \text{for } g \neq 0$$

with all possible choices of the signs. We notice two things: all elements of these lists are units in view of the properties of Y; each L_g is closed under taking opposites (h and $-h$ have the same multiplicity in L_g for every pair $(g, h) \in G \times H$). Thus we can write $L_g = \{1, -1\} \cdot L'_g$ where each L'_g is a list of 2λ units of R.

For every $h \in H$, let us denote by ε_h the endomorphism of $(H, +)$ which is the multiplication by h in the ring R. Take a complete set S of representatives for the pairs of the patterned starter[1] of $(H, +)$ and consider the set $E = \{\varepsilon_s \mid s \in S\}$. We have:

$$\biguplus_{\varepsilon \in E} \varepsilon(L_g) = \biguplus_{s \in S} \{s, -s\} \cdot L'_g = (H \setminus \{0\}) \cdot L'_g = {}^{2\lambda}(H \setminus \{0\})$$

the last equality being true since every element of L'_g is a unit and $|L'_g| = 2\lambda$. Keeping the same notation used in Theorem 1 we conclude that

$$\mathcal{F} := \{\widehat{\varepsilon}_s(B_i) \mid 1 \le i \le t; s \in S\}$$

is a $(G \times H, G \times \{0\}, {}^n(2K), 2\lambda)$-DF. Now note that we have:

$$\biguplus_{s \in S} \widehat{\varepsilon}_s(B_i) = \biguplus_{s \in S} \biguplus_{d \in D_i} \{d\} \times \{sf(d), -sf(d)\}$$

$$= \biguplus_{d \in D_i} \{d\} \times \biguplus_{s \in S} \{s, -s\} \cdot f(d) = \biguplus_{d \in D_i} \{d\} \times (H \setminus \{0\}) = D_i \times (H \setminus \{0\}).$$

Recalling that the D_i's partition G since $\mathcal{D}$ is partitioned, we conclude that the blocks of $\mathcal{F}$ partition $G \times (H \setminus \{0\}) = (G \times H) \setminus (G \times \{0\})$.

In order to "complete" $\mathcal{F}$ to an ordinary PDF in $G \times H$ we need a set of blocks partitioning $G \times \{0\}$ whose list of differences gives 2λ times $(G \setminus \{0\}) \times \{0\}$. Such a set is trivially given by the singleton $\{G \times \{0\}\}$. We conclude that

$$\{\widehat{\varepsilon}_s(B_i) \mid 1 \le i \le t; s \in S\} \cup \{G \times \{0\}\}$$

is a $(2\lambda(2n + 1), {}^n(2K) \uplus \{2\lambda\}, 2\lambda)$-PDF in $G \times H$.   □

As a corollary we get an infinite class of PDFs applying the above theorem with the use of the Hadamard PDFs of Proposition 1.

Corollary 1 *If D is $(4u^2, 2u^2 - u, u^2 - u)$-HDS in G and the maximal prime power divisors of $2n + 1$ are all greater than $4u^2 + 2u$, then there exists a*

$$(4u^2(2n + 1), [{}^n(4u^2 - 2u), {}^1(4u^2), {}^n(4u^2 + 2u)], 4u^2]\text{-PDF}.$$

Proof Let $q_1, \ldots, q_t$ be the maximal prime power divisors of $2n + 1$, assume that each q_i is greater than $4u^2 + 2u$, and let ρ_i be a primitive root of $\mathbb{F}_{q_i}$. Then the assertion will follow by applying Theorem 2 with $\mathcal{D}$ the Hadamard PDF of Proposition 1, with R the ring $\mathbb{F}_{q_1} \times \cdots \times \mathbb{F}_{q_t}$, and with $Y = \{(\rho_1^j, \ldots, \rho_t^j) \mid 1 \le j \le 2u^2 + u\}$.   □

Applying the above corollary with $u = 1$, namely using the trivial $(4, 1, 0)$-HDS, one obtains a cyclic $(8n + 4, [{}^n 2, {}^1 4, {}^n 6], 4)$-PDF whenever $2n + 1$ is coprime with 15.

It is known that there exists a $(16, 6, 2)$-HDS in every abelian group G of order 16 except $G = \mathbb{Z}_{16}$. Then Corollary 1 gives a $(400, [{}^{12}12, {}^116, {}^{12}20], 16)$-PDF in $G \times \mathbb{Z}_5 \times \mathbb{Z}_5$ for any G as above. Note, however, that Theorem 2 cannot produce a PDF with the same parameters in $G \times \mathbb{Z}_{25}$ since a set Y of units of $\mathbb{Z}_{25}$ such that $\Delta(Y \cup -Y) \subset U(\mathbb{Z}_{25})$ has size at most 3.

---

[1]The *patterned starter* of an additive group H of odd order is the set of all possible pairs $\{h, -h\}$ of opposite elements of $H \setminus \{0\}$ (see, e.g., [11]).

We get another *sporadic* class of PDFs applying our main theorem with the use of the $(32, [^2 2, 6, 22], 16)$-PDF given at the end of the introduction.

Corollary 2 *If the maximal prime power divisors of $2n + 1$ are all greater than 44, then there exists a*

$$(64n + 32, \ [\,^{2n}4, \ ^n 12, \ ^1 32, \ ^n 44], \ 32)\text{-}PDF.$$

The first value of n for which the above corollary can be applied is 23. In this way one gets a $(1504, [^{46}4, \ ^{23}12, \ ^1 32, \ ^{23}44], 32)$-PDF.

References

1. Arasu, K.T., Sehgal, S.: Cyclic difference covers. Aust. J. Commun. **32**, 213–223 (2005)
2. Buratti, M.: Pairwise balanced designs from finite fields. Discret. Math. **208/209**, 103–117 (1999)
3. Buratti, M.: Old and new designs via strong difference families. J. Combin. Des. **7**, 406–425 (1999)
4. Buratti, M., Gionfriddo, L.: Strong difference families over arbitrary graphs. J. Combin. Des. **16**, 443–461 (2008)
5. Buratti, M., Pasotti, A.: Combinatorial designs and the theorem of Weil on multiplicative character sums. Finite Fields Appl. **15**, 332–344 (2009)
6. Buratti, M., Yan, J., Wang, C.: From a 1-rotational RBIBD to a partitioned difference family. Electron. J. Comb. **17**, ♯R139 (2010)
7. Buratti, M.: On disjoint $(v, k, k - 1)$ difference families. arXiv:1705.04844
8. Costa, S., Feng, T., Wang, X.: New 2-designs from strong difference families. Finite Fields Appl. **50**, 391–405 (2018)
9. Costa, S., Feng, T., Wang, X.: Frame difference families and resolvable balanced incomplete block designs. To appear in Des. Codes Crypt.
10. Ding, C., Yin, J.: Combinatorial constructions of optimal constant composition codes. IEEE Trans. Inf. Theory **51**, 3671–3674 (2005)
11. Dinitz, J.H.: Starters. In: Colbourn, C.J., Dinitz, J.H. (eds.) Handbook of Combinatorial Designs. 2nd edn., pp. 622–628. Chapman & Hall/CRC, Boca Raton (2006)
12. Jungnickel, D., Pott, A., Smith, K.W.: Difference sets. In: Colbourn, C.J., Dinitz, J.H. (eds.) Handbook of Combinatorial Designs. 2nd edn., pp. 419–435. Chapman & Hall/CRC, Boca Raton (2006)
13. Li, S., Wei, H., Ge, G.: Generic constructions for partitioned difference families with applications: a unified combinatorial approach. Des. Codes Crypt. **82**, 583–599 (2017)
14. Momihara, K.: Strong difference families, difference covers, and their applications for relative difference families. Des. Codes Crypt. **51**, 253–273 (2009)
15. Paterson, M.B., Stinson, D.R.: Combinatorial characterizations of algebraic manipulation detection codes involving generalized difference families. Discret. Math. **339**, 2891–2906 (2016)
16. Szabo, S., Sands, A.: Factoring Groups into Subsets. Chapman and Hall/CRC, Boca Raton (2009)
17. Wang, Q., Zhou, Y.: Sets of zero-difference balanced functions and their applications. Adv. Math. Commun. **8**, 83–101 (2014)
18. Yamada, K., Mishima, M., Satoh, J., Jimbo, M.: Multifold factorization of cyclic groups into subsets. submitted
19. Zhou, Z., Tang, X., Wu, D., Yang, Y.: Some new classes of zero difference balanced functions. IEEE Trans. Inf. Theory **58**, 139–145 (2012)