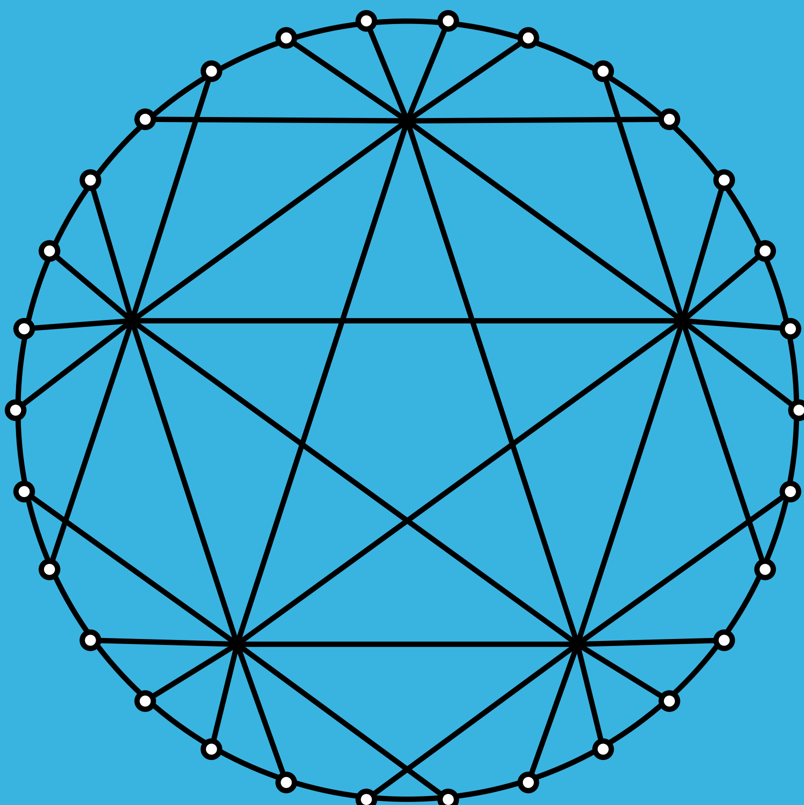
BULLETIN of The INSTITUTE of COMBINATORICS and its APPLICATIONS

Volume 93
October 2021



Boca Raton, FL, U.S.A.

ISSN: 2689-0674 (Online)
ISSN: 1183-1278 (Print)

BULLETIN OF THE ICA
Volume **93** (2021), 45–51

A note on almost partitioned difference families

JINGJUN BAO[1], MARCO BURATTI*[2] AND LIJUN JI[3]

[1]NINGBO UNIVERSITY, ZHEJIANG, CHINA
baojingjun@hotmail.com
[2]UNIVERSITÀ DI PERUGIA, ITALY
buratti@dmi.unipg.it
[3]SOOCHOW UNIVERSITY, SUZHOU, JIANGSU, CHINA
jilijun@suda.edu.cn

Abstract

By *almost partitioned difference family* (APDF) we mean a difference family in an additive group G whose blocks partition $G \setminus \{0\}$. It was shown by the second author that every Frobenius group with abelian kernel G of odd order v and complement A of odd order k gives rise to a disjoint $(v, k, \frac{k-1}{2})$ difference family in G. In this note we observe that it also leads to a (v, K, λ)-APDF in G with $K = [s^{(v-1)/(2s)},\ t^{(v-1)/(2t)}]$ and $\lambda = (s+t-2)/2$ for every pair (s, t) of distinct orders of a non-trivial subgroup of A. As an application, we show that there are infinitely many values of v for which there exists an APDF of order v whose block-sizes are the elements of any prescribed set S of consecutive odd integers.

*Corresponding author.
Key words and phrases: Disjoint difference family; Frobenius group; Ferrero pair.
AMS (MOS) Subject Classifications: 05B10

Received: 1 June 2021
Accepted: 27 July 2021

1 Preliminaries

We recall that a difference family in an additive group G is a collection $\mathcal{F}$ of subsets (*blocks*) of G whose list of differences $\Delta\mathcal{F}$ (the multiset of all differences $x-y$ with (x,y) and ordered pair of distinct elements lying in the same block) covers every non-zero element of G a constant number λ of times. If K is the multiset of the block-sizes and G has order v, one usually speaks of a (v,K,λ)-DF in G. A difference family is said to be *disjoint* (DDF) if its blocks are mutually disjoint and, in particular, it is *partitioned* (PDF) if its blocks partition G. For the multiset K we will use exponential notation. By writing (v,k,λ)-DF it is understood that all elements of K are equal to k, i.e., $K=[k^n]$ with n necessarily equal to $\frac{\lambda(v-1)}{k(k-1)}$.

It is evident that every disjoint difference family can be extended to a partitioned difference family by adding, if necessary, blocks of size 1. As an example, it is easy checkable that $\{\{0,1,3,5\},\{2,8,9\}\}$ is a $(10,[3,4],2)$-DDF in $\mathbb{Z}_{10}$. This DDF can be obviously extended to a $(10,[1^3,3,4],2)$-PDF by adding the blocks of size one $\{4\}$, $\{6\}$ and $\{7\}$.

The literature on difference families is huge (see, e.g., [1] or [7]). The partitioned ones have been introduced in [8] and subsequently they have been defined in a different but equivalent way under the name of *zero difference balanced functions*. Unfortunately, as pointed out in [4, 5], this led to some confusion to the point that several authors, using the new terminology, reproduced in a quite convoluted way results on difference families which were already known for a long time. Some relevant constructions for PDFs can be found in [3, 6, 10].

It is convenient to give the following new definition.

Definition 1.1. An *almost partitioned difference family* (APDF) is a difference family in an additive group G whose blocks partition $G\setminus\{0\}$.

It is obvious that an APDF is completely equivalent to a PDF having one block equal to the singleton $\{0\}$. Indeed we are adopting the above artificial definition just in order to simplify several statements concerning PDFs with this property.

Let G and A be the kernel and the complement of a *Frobenius group*. This means that A is a group of automorphisms of the group G acting semiregularly on the non-identity elements of G: for $\alpha\in A$ and $g\in G\setminus\{0\}$ we have $\alpha(g)=g$ if and only if $\alpha=id_G$. Using the terminology of some nearring theorists we say that (G,A) is a *Ferrero pair* [9]. Of course we could also call it a *Frobenius pair*.

Speaking of a (v,k)-FP we will mean a Ferrero pair (G,A) with G and A of orders v and k, respectively. Luckily, the acronym FP could stand both for Ferrero pair and Frobenius pair.

The following results have been proved in [2].

Theorem 1.2. *Assume that (G,A) is a (v,k)-FP. Then we have:*
(i) the set $\mathcal{F}$ of all A-orbits on $G\setminus\{0\}$ is a $(v,k,k-1)$-DDF;
(ii) if vk is odd and G is abelian, then $\mathcal{F}$ is splittable into two $(v,k,\frac{k-1}{2})$-DDFs.

If $v\equiv 1 \pmod k$ is a prime power, then a (v,k)-FP is given by the pair (G,A) where G is the additive group of $\mathbb{F}_v$ (the finite field of order v), and where A is generated by the map $\alpha: x\in\mathbb{F}_v \longrightarrow rx\in\mathbb{F}_v$ with r a fixed primitive k-th root of unity in $\mathbb{F}_v$. In this special case the result given by Theorem 1.2 can be already found in [11].

In terms of APDFs Theorem 1.2(i) gives a $(v,[k^n],k-1)$-APDF whenever we have a $(kn+1,k)$-FP, and Theorem 1.2(ii) gives a $(v,[1^{kn},k^n],\frac{k-1}{2})$-APDF whenever we have an abelian $(2kn+1,k)$-FP with k odd.

2 A new series of APDFs

Now we show that in the same hypotheses of Theorem 1.2(ii) we can obtain APDFs whose multiset of all the block-sizes is of the form

$$[s^{(v-1)/(2s)},\ t^{(v-1)/(2t)}]$$

for suitable divisors s and t of k.

Theorem 2.1. *Let (G,A) be a (v,k)-FP with G abelian and vk odd, and let s, t be the orders of two subgroups of A. Then there exists a*

$$(v,\ [s^{(v-1)/(2s)},\ t^{(v-1)/(2t)}],\ \tfrac{s+t-2}{2})\text{-APDF}$$

in G which is splittable into a $(v,s,\frac{s-1}{2})$-DDF and a $(v,t,\frac{t-1}{2})$-DDF.

Proof. First recall that the proof of Theorem 1.2(ii) relies on the fact that G abelian and vk odd imply that if $\mathcal{O}$ is an A-orbit on $G\setminus\{0\}$, then $-\mathcal{O}$ is an

A-orbit (distinct from $\mathcal{O}$) as well. This implies that the set $\mathcal{F}$ of all the A-orbits on $G \setminus \{0\}$ can be partitioned into opposite sets $\mathcal{F}^+$ and $\mathcal{F}^- = -\mathcal{F}^+$. Let G^+ and G^- be the set of all elements of G covered by the A-orbits belonging to $\mathcal{F}^+$ and $\mathcal{F}^-$, respectively.

Let S be a subgroup of A and let s be its order. It is obvious that (G, S) is a (v, s)-FP, hence the set $\mathcal{F}(S)$ of all the S-orbits on $G \setminus \{0\}$ is a $(v, s, s-1)$-DDF by Theorem 1.2(i). Every S-orbit is clearly contained in an A-orbit, hence it is contained in G^+ or G^-. Denote by $\mathcal{F}(S)^+$ and $\mathcal{F}(S)^-$ the set of all S-orbits contained in G^+ and G^-, respectively. Note, in particular, that $\mathcal{F}(A)^+ = \mathcal{F}^+$ and $\mathcal{F}(A)^- = \mathcal{F}^-$.

For what said above on the A-orbits, if $\mathcal{O} \in \mathcal{F}(S)^+$, then $-\mathcal{O} \in \mathcal{F}(S)^-$. Thus, considering that two opposite sets clearly have the same lists of differences, we deduce that the lists of differences of $\mathcal{F}(S)^+$ and $\mathcal{F}(S)^-$ coincide. This implies that $\Delta\mathcal{F}(S)$ is two times $\Delta\mathcal{F}(S)^+$ because $\mathcal{F}(S)$ is disjoint union of $\mathcal{F}(S)^+$ and $\mathcal{F}(S)^-$. On the other hand $\Delta\mathcal{F}(S)$ is $s-1$ times $G \setminus \{0\}$ because $\mathcal{F}(S)$ is a $(v, s, s-1)$-DF in G. It necessarily follows that $\Delta\mathcal{F}(S)^+$ is $\frac{s-1}{2}$ times $G \setminus \{0\}$, i.e., both $\mathcal{F}(S)^+$ and $\mathcal{F}(S)^-$ are $(v, s, \frac{s-1}{2})$-DDFs in G. We conclude that for every subgroup S of A there exists a $(v, s, \frac{s-1}{2})$-DDF, that is $\mathcal{F}(S)^+$, whose blocks partition G^+, and a $(v, s, \frac{s-1}{2})$-DDF, that is $\mathcal{F}(S)^-$, whose blocks partition G^-.

Now assume that s and t are orders of non-trivial subgroups of A, say S and T, respectively. In view of what we established in the above paragraph,

$$\mathcal{F}(S)^+ \text{ is a } (v, s, \frac{s-1}{2})\text{-DDF whose blocks partition } G^+$$

and

$$\mathcal{F}(T)^- \text{ is a } (v, t, \frac{t-1}{2})\text{-DDF whose blocks partition } G^-.$$

Then it is obvious that

$$\mathcal{F}(S)^+ \cup \mathcal{F}(T)^- \text{ is a } (v, K, \lambda)\text{-APDF in } G$$

with $K = [s^{(v-1)/(2s)},\ t^{(v-1)/(2t)}]$ and $\lambda = \frac{s+t-2}{2}$. □

Of course the above theorem is interesting only in the case that s and t are distinct. Indeed for $s = t$ we fall back to Theorem 1.2(ii).

Corollary 2.2. *If s and t are divisors of an odd integer k, then there exists a*

$$(v,\ [s^{(v-1)/(2s)},\ t^{(v-1)/(2t)}],\ \tfrac{s+t-2}{2})\text{-APDF}$$

in a group G of order v in each of the following cases:

(1) G is abelian and all the prime factors of $|G|$ are congruent to 1 (mod $2k$);

(2) G is the additive group of $\mathbb{F}_{q_1} \times \cdots \times \mathbb{F}_{q_n}$ and $q_i \equiv 1$ (mod $2k$) for $1 \leq i \leq n$.

Proof. In both cases (1) and (2) there exists a (v, k)-FP (G, A) with A abelian (see Corollary 3.3 and Corollary 3.5 in [2]). Then the assertion immediately follows from Theorem 2.1 and the fact that in an abelian group the inverse of Lagrange's theorem holds. $\square$

By way of illustration, in the next example we determine the APDFs in $\mathbb{Z}_{61}$ obtainable via Theorem 2.1 and not covered by Theorem 1.2, that are a $(61,\ [3^{10}, 5^6],\ 3)$-APDF, a $(61,\ [3^{10}, 15^2],\ 8)$-APDF, and a $(61,\ [5^6, 15^2],\ 9)$-APDF.

Example 2.3. *By abuse of notation, let us identify the automorphism group of* $\mathbb{Z}_{61}$ *with its multiplicative group* $\mathbb{Z}_{61}^*$. *Let* A *be the subgroup of* $\mathbb{Z}_{61}^*$ *of order 15 that is*

$$A = \{1, 12, 22, 20, 57, 13, 34, 42, 16, 9, 47, 15, 58, 25, 56\}.$$

Of course (G, A) *is a* $(61, 15)$*-FP. The set of* A*-orbits on* $\mathbb{Z}_{61} \setminus \{0\}$ *is* $\mathcal{F} = \{A, -A, 2A, -2A\}$. *Thus, keeping the same notation as in the proof of Theorem 2.1, we can take*

$$\mathcal{F}^+ = \mathcal{F}(A)^+ = \{A, 2A\}, \qquad \mathcal{F}^- = \mathcal{F}(A)^- = \{59A, 60A\}.$$

Let S *be the subgroup of* A *of order* 3 *that is* $S = \{1, 13, 47\}$ *and let* T *be the subgroup of* A *order 5, that is* $T = \{1, 9, 20, 58, 34\}$. *The set of all the* S*-orbits contained in* $\mathbb{Z}_{61}^+ = A \cup 2A$ *is*

$$\mathcal{F}(S)^+ = \{S, 2S, 9S, 12S, 16S, 18S, 22S, 24S, 32S, 44S\}$$

and hence

$$\mathcal{F}(S)^- = \{17S, 29S, 37S, 39S, 43S, 45S, 49S, 52S, 59S, 60S\}.$$

The set of all the T*-orbits contained in* $\mathbb{Z}_{61}^+$ *is*

$$\mathcal{F}(T)^+ = \{T, 2T, 12T, 13T, 24T, 26T\}$$

and hence

$$\mathcal{F}(T)^- = \{35T, 37T, 48T, 49T, 59T, 60T\}.$$

The APDFs obtainable by Theorem 2.1 are the following:

$\mathcal{F}(S)^+ \cup \mathcal{F}(T)^-$ *is a* $(61,\ [3^{10}, 5^6],\ 3)$-APDF*;*

$\mathcal{F}(S)^+ \cup \mathcal{F}(A)^-$ *is a* $(61,\ [3^{10}, 15^2],\ 8)$-APDF*;*

$\mathcal{F}(T)^+ \cup \mathcal{F}(A)^-$ *is a* $(61,\ [5^6, 15^2],\ 9)$-APDF.

3 A composition construction

As application of the result seen in the previous section, we give a constructive proof of the existence of an APDF whose block-sizes are precisely the elements of any prescribed set of consecutive integers.

Theorem 3.1. *For any set S of consecutive odd integers, there are infinitely many values of v for which there exists a (v, K, λ)-APDF where the underlying set of K is S and $\lambda = \frac{\min S + \max S - 2}{2}$.*

Proof. Let k be the least common multiple of all integers in S and let p be one of the infinitely many primes congruent to 1 (mod $2k$). Set $\delta = \lceil \frac{|S|}{2} \rceil$ and consider the covering of S consisting of the δ pairs $(s_0, t_0), \ldots, (s_{\delta-1}, t_{\delta-1})$ defined by

$$s_i = \min S + 2i \quad \text{and} \quad t_i = \max S - 2i \quad \text{for } 0 \leq i \leq \delta - 1.$$

By definition of k, each s_i and each t_i is a divisor of k. Also note that we have $\frac{s_i + t_i - 2}{2} = \lambda$ for each i. Thus, by Corollary 2.2, for $0 \leq i \leq \delta - 1$ there exists a (p, K_i, λ)-APDF with $K_i = [s_i^{(p-1)/(2s_i)},\ t_i^{(p-1)/(2t_i)}]$.

Now let $n \geq 2$, set $[n]_p := \frac{p^n - 1}{p-1}$, and consider the set $\{V_1, ..., V_{[n]_p}\}$ of all 1-dimensional subspaces of the vector space $V := \mathbb{Z}_p^n$. Of course $(V_i, +)$ is a group isomorphic to $\mathbb{Z}_p$ for each i. Thus, for what we said above, there exists a (p, K_j, λ)-APDF in V_i for every possible pair (i, j) with $i \in I := \{1, \ldots, [n]_p\}$ and $j \in J := \{0, 1, \ldots, \delta - 1\}$. Take a surjective map $f : I \longrightarrow J$ (which exists because $[n]_p$ is obviously greater than δ) and, for every $i \in I$, let $\mathcal{F}_i$ be a $(p, K_{f(i)}, \lambda)$-APDF in V_i. This means that $\Delta\mathcal{F}_i$ is λ times $V_i \setminus \{0\}$. It is then evident that $\mathcal{F} := \bigcup_{i \in I} \mathcal{F}_i$ is a $(\mathbb{Z}_p^n, K, \lambda)$-APDF with $K = \bigcup_{i \in I} K_{f(i)}$. Considering that f is surjective and that the pairs (s_i, t_i) cover S, it is also clear that the underlying set of K is S. □

Even though constructive, the above proof is not very practical. Indeed, as shown in the following examples, it leads to values of v which are generally huge.

Example 3.2. *Let $S = \{3, 5, 7\}$. Keeping the notation used in Theorem 3.1, we have $k = 105$ and the first prime congruent to 1 mod $2k$ is $p = 211$. Thus the first value of v for which our composition construction works with this set S is $211^2 = 44521$. To be precise, the construction gives a*

$$(211^2, [3^{35a}, 5^{42(212-a)}, 7^{15a}], 4)\text{-APDF}$$

in $\mathbb{Z}_{211}^2$ for every possible a in the range $[1, 211]$.

Example 3.3. *Let* $S = \{3, 5, 7, 9, 11, 13, 15\}$. *Here, we have* $k = 45045$ *and the first prime congruent to* 1 *mod* $2k$ *is* $p = 180181$. *So, the first value of* v *for which our construction works with this* S *is* $p^2 = 32, 465, 192, 761$. *The construction gives a*

$$(180181^2, [3^{30030a}, 5^{18018b}, 7^{12870c}, 9^{20020d}, 11^{8190c}, 13^{6930b}, 15^{6006a}], 8)\text{-APDF}$$

in $\mathbb{Z}_{180181}^2$ *for every possible ordered partition* $[a, b, c, d]$ *of* $p + 1$.

References

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

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

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

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

[5] M. Buratti and D. Jungnickel, Partitioned difference families: the storm has not yet passed, to appear in *Adv. in Math. Commun.*, https://arxiv.org/abs/2103.00646

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

[7] C.J. Colbourn, J.H. Dinitz, *Handbook of Combinatorial Designs, Second Edition*, Chapman & Hall/CRC, Boca Raton, FL, 2006.

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

[9] J.R. Clay, *Nearrings: Geneses and Applications*, Oxford University Press, Oxford, UK, 1992.

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

[11] R.M. Wilson, Cyclotomic and difference families in elementary abelian groups, *J. Number Theory*, **4** (1972), 17–47.