RAD HAZU. MATEMATIČKE ZNANOSTI
Vol. 23 = 538 (2019): 13-29
DOI: https://doi.org/10.21857/ypn4oc88w9

HADAMARD DIFFERENCE SETS AND RELATED COMBINATORIAL OBJECTS IN GROUPS OF ORDER 144

Tanja Vučičić

Abstract. In this paper we address an appealing and so far not completed combinatorial problem of difference set (DS) existence in groups of order 144. We apply our recently established method for DS construction which proves to be very efficient. The result is more than 5000 inequivalent $(144, 66, 30)$ DSes obtained in 131 groups of order 144. The number of non-isomorphic symmetric designs rising from them is 1364.

Using the obtained DSes as a source, new regular $(144, 66, 30, 30)$ and $(144, 65, 28, 30)$ partial difference sets are constructed, together with the corresponding strongly regular graphs. 43 non-isomorphic graphs of valency 66 are obtained and 78 of valency 65. The full automorphism groups of these graphs, as well as those of symmetric designs, are explored using the software package Magma.

1. Introduction

In this paper we consider different types of combinatorial objects related to groups of order 144. There are 197 such groups and 10 of them are abelian. To denote them we take on the notation introduced in the “SmallGroups” library of the software package Magma [3] which we use for computation.

First we focus on $(144, 66, 30)$ difference sets (DSes). Investigating the DS existence has been a major combinatorial task. As combinatorial objects, DSes are interesting in the first place for their connection with coding theory and for having many applications (e.g. in digital communications), primarily in the widely studied abelian case. Our parameters belong to the important and intriguing Hadamard family [5, 7, 9], being among the smallest with the existence problem not completely decided as yet. However, they are large enough so that the underlying DSes are not attainable by exhaustive computer searches within different approaches. In this paper we present an application of our recently established method [15], a sort of prolific DS generating algorithm (Section 3), on solving this existence problem. The current status of

2000 *Mathematics Subject Classification.* 05B05, 05B10.

Key words and phrases. Transitive incidence structure, (partial) difference set, strongly regular graph.

research on the subject exists only in preprint form [12], which appears as a reference in [2]. The two independent dealings with this research problem, although run by applying totally different methods, on the existence side give equal lists containing 131 positively decided groups. Such an outcome leaves a strong hunch that, apart from the detected groups (Section 4, [12]), the remaining groups of order 144 do not support Hadamard difference sets.

The existence of $(144, 66, 30)$ abelian difference sets is completely decided. By direct construction we show that four abelian groups support DSes and in Section 5 we give a very simple proof that the remaining six abelian groups do not allow DSes. Otherwise in the paper we do not bring results on the nonexistence side; in the nonabelian case we rather put an emphasis on successful constructions.

The next combinatorial objects in our focus are partial difference sets (PDSes). Within their construction the existence of reversible $(144, 66, 30)$ DSes is confirmed in 53 groups. Regular PDSes lead to the corresponding graphs. We perform the construction of 43 non-isomorphic strongly regular Cayley graphs with parameters $(144, 66, 30, 30)$ and 78 with parameters $(144, 65, 28, 30)$. The Magma files "SRG144" and "DS144" containing records of the constructed graphs and symmetric designs are available at the site [17], together with the "Info file_144" on how to handle them.

2. Preliminaries to DS construction

An *incidence structure* is a triple $\Gamma = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, where $\mathcal{P}$ and $\mathcal{B}$ are sets of "points" and "blocks", respectively, and $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$ is a binary relation between them. In this research the point set $\mathcal{P}$ is finite and nonempty, while $\mathcal{B} \subseteq 2^{\mathcal{P}}$ is a set of nonempty subsets of $\mathcal{P}$. The incidence relation is membership, so we use a short notation $\Gamma = (\mathcal{P}, \mathcal{B})$. Repeated blocks are not considered, thus our incidence structures are *simple.* They are denoted in accordance with [1], where the interested reader can find more general information and details about incidence structures and other combinatorial objects we consider.

Incidence structures $\Gamma_i = (\mathcal{P}_i, \mathcal{B}_i), i = 1, 2$ are *isomorphic* if there exists a bijection $\varphi : \mathcal{P}_1 \to \mathcal{P}_2$ with $(\mathcal{B}_1)^{\varphi} = \mathcal{B}_2$. In that case φ is called an *isomorphism* from Γ_1 to Γ_2. Every simple incidence structure is isomorphic to an incidence structure of the described type $(\mathcal{P}, \mathcal{B})$.

The set of all isomorphisms of an incidence structure Γ into itself forms its full automorphism group $Aut(\Gamma)$. Each subgroup of $Aut(\Gamma)$ is an *automorphism group* of Γ. An automorphism group of a simple incidence structure $(\mathcal{P}, \mathcal{B})$ is a subgroup of $Sym(\mathcal{P})$. We say that group G *acts* on an incidence structure $\Gamma = (\mathcal{P}, \mathcal{B})$ if it acts on sets $\mathcal{P}$ and $\mathcal{B}$ and preserves incidences.

If there exists an automorphism group acting transitively (regularly) on the set of points and blocks, then we speak of a *transitive (regular) incidence structure.* An incidence structure $(\mathcal{P}, \mathcal{B})$ having automorphism group

$G \leq Sym\,(\mathcal{P})$ which acts transitively on points and blocks we here denote by $I(\mathcal{P}, G, B)$, where $B \subseteq \mathcal{P}$ and $\mathcal{B} = \{B^g \mid g \in G\}$. Using this notation, a well-known assertion that holds for transitive incidence structures may be stated as follows.

Lemma 2.1. *Incidence structures $I(\mathcal{P}, G, B^{\pi})$ and $I(\mathcal{P}, G^{\pi^{-1}}, B)$ are isomorphic for every $\pi \in Sym\,(\mathcal{P})$.*

Connected to our difference set construction method, now we point to the procedure of obtaining transitive substructures of a given transitive incidence structure $\Gamma = I(\mathcal{P}, G, B)$ related to some subgroup of G. Let a subgroup $H \leq G$ act transitively on $\mathcal{P}$, and in l orbits on $\mathcal{B}$, $l \in \mathbb{N}$. If we denote by $B_1, \ldots, B_l$ the representatives of H-orbits on $\mathcal{B}$, then

$$\{I\left(\mathcal{P}, H, B_i\right), i = 1, \ldots, l\} \tag{2.1}$$

is the set of all transitive substructures of Γ having the automorphism group H. Obviously, there exist $g_i \in G, i = 1, \ldots, l$ with the property $B_i = B^{g_i}$, so the set (2.1) can be rewritten as $\{I\left(\mathcal{P}, H, B^{g_i}\right), i = 1, \ldots, l\}$. Lemma 2.1 implies that $I\left(\mathcal{P}, H, B^{g_i}\right)$ is isomorphic to $I\left(\mathcal{P}, H^{g_i^{-1}}, B\right)$. Thus, proceeding in a technically convenient manner and exploring incidence structures $I\left(\mathcal{P}, H^g, B\right)$, with g from the (right) transversal of H in G, will suffice to obtain all transitive substructures of Γ related to the subgroup $H \leq G$.

Incidence structures of our particular interest are block designs.

Definition 2.2. *Incidence structure $D = (\mathcal{P}, \mathcal{B})$ with $|\mathcal{P}| = v$ and $|\mathcal{B}| = b$ we call $t-(v, k, \lambda)$* design *if each block consists of exactly k points and any t different points are contained in exactly λ blocks, $t \leq k$ and $\lambda > 0$. $2-(v, k, \lambda)$ design is called (v, k, λ)* block design *and it is symmetric if $b = v$.*

A difference set is a subset of a group with nice combinatorial property.

Definition 2.3. *A (v, k, λ)* difference set *is a subset $\Delta \subseteq G$ of size k in a group G of order v with the property that the multiset $\left\{xy^{-1} \mid x, y \in \Delta, x \neq y\right\}$ contains each nonidentity element of G exactly λ times.*

Difference set $\Delta \subseteq G$ is often thought of as an element $\Delta = \sum\limits_{d \in \Delta} d$ of the integral group ring $\mathbb{Z}G$. Putting in the same sense (and slight abuse of notation) $G = \sum\limits_{g \in G} g$, the statement that Δ is a difference set is equivalent to the equation

$$\Delta\Delta^{(-1)} = (k - \lambda)1_G + \lambda G,$$

where $\Delta^{(-1)} = \sum\limits_{d \in \Delta} d^{-1}$.

The *development* of a difference set $\Delta \subseteq G$ is the incidence structure $dev\Delta = (G, \{\Delta g \mid g \in G\})$, whose blocks, the so-called Δ-shifts, are difference sets as well. This structure relates difference sets to symmetric designs (SDs) in the following way.

Theorem 2.4. *Let $\Delta \subseteq G$ be a (v, k, λ) difference set. Then $dev\Delta$ is a regular symmetric (v, k, λ) design with respect to $G \leq Aut\, dev\Delta$.*
Vice versa, let $D = (\mathcal{P}, \mathcal{B})$ be a symmetric (v, k, λ) design with automorphism group G acting regularly on $\mathcal{P}$. Then, for any point $p \in \mathcal{P}$ and any block $B \in \mathcal{B}$, the set $\Delta = \{ g \in G \mid p^g \in B\}$ is a (v, k, λ) difference set in G.

If the automorphism group of a symmetric design acts regularly on points, then it acts regularly also on blocks.

Two difference sets Δ_1 (in G_1) and Δ_2 (in G_2) are *isomorphic* if the designs $dev\Delta_1$ and $dev\Delta_2$ are isomorphic; Δ_1 and Δ_2 are *equivalent* if there exists a group isomorphism $\varphi : G_1 \to G_2$ such that $(\Delta_1)^\varphi = \Delta_2 g$ for a suitable $g \in G_2$. It is clear that equivalent difference sets Δ_1 and Δ_2 give rise to isomorphic symmetric designs $dev\Delta_1$ and $dev\Delta_2$.

If a difference set $\Delta \subseteq G$ in group G is known, the latter part of Theorem 2.4 provides also a straightforward procedure for obtaining difference sets in regular subgroups of $Aut\, dev\Delta$ distinct from G, if any. This "reading off" difference sets in regular subgroups of $Aut(dev\Delta)$, having the same parameters as Δ, we will call *Procedure* DS^0. Difference sets obtained in this way are obviously isomorphic and inequivalent to Δ.

Parameter triples of the form

$$(4u^2, 2u^2 - u, u^2 - u),\ u \in \mathbb{N}, \tag{2.2}$$

determine the Hadamard family of DSes and/or the Menon family of SDs.

In 1962 Kesava Menon proved that the set of groups containing a Hadamard difference set (HDS) is closed under direct product [16]. Later improvements and generalizations of this result led to the well-known fact that two HDSes yield a new HDS by the 'product method' which is conveniently illustrated, for instance, by Theorem 2.5 (below), [8, p. 13]. A more general approach to building HDSes from smaller ones found in subgroups of the considered group, under certain conditions, is given in [9, Theorem 5.1] and called *generalized products*.

Theorem 2.5 (Product method). *Let G be the group and G_1, G_2 its subgroups with the property $G = G_1G_2$ and $G_1 \cap G_2 = \{1_G\}$. If difference sets with parameters of type (2.2) exist in G_1 and G_2 for $u = u_1$ and $u = u_2$ respectively, then G contains a difference set with parameters (2.2) for $u = 2u_1u_2$.*

Denoting by $\Delta_1 \subseteq G_1$ and $\Delta_2 \subseteq G_2$ initial difference sets, the product difference set in group G is described by the formula

$$\Delta := (\Delta_1\overline{\Delta_2}) \cup (\overline{\Delta_1}\Delta_2), \tag{2.3}$$

where $\overline{\Delta}_i = G_i \setminus \Delta_i, i = 1, 2$. Formula (2.3) generalizes the one given in [1, p. 368] for direct product $G = G_1 \times G_2$.

Alternatively: from Menon designs $D_i = (\mathcal{P}_i, \mathcal{B}_i)$, $i = 1, 2$ with $u = u_i$ one can obtain their "product", a new Menon design denoted by $D_1 \otimes D_2 = (\mathcal{P}, \mathcal{B})$ with $u = 2u_1u_2$ by taking point set $\mathcal{P} = \mathcal{P}_1 \times \mathcal{P}_2$ and block set $\mathcal{B} = \{\, (B_1 \times B_2^c) \cup (B_1^c \times B_2) |\, B_1 \in \mathcal{B}_1, B_2 \in \mathcal{B}_2\}$. If $G_1 \leq AutD_1$ and $G_2 \leq AutD_2$ then $G_1 \times G_2 \leq Aut(D_1 \otimes D_2)$, [11, p. 129].

In this paper we consider $(144, 66, 30)$ HDSes with $u = 6$ which can obviously be obtained by the product method from $(36, 15, 6)$ HDSes and a trivial HDS in group of order 4. All difference sets in groups of order 36 are known [5, p. 432 (Kibler)]; there exist exactly 9 non-isomorphic (35 inequivalent) $(36, 15, 6)$ HDSes. On the other side, one has two trivial $(4, 1, 0)$ HDSes (two groups of order 4). HDSes with parameters $(144, 66, 30)$ obtained from them by the product method serve as an *initial set* of difference sets needed to launch our construction method. Namely, to start the underlying algorithm at least one known difference set with given parameters is needed. In the next section we describe how the method works, i.e. how we obtain new DSes with the same parameters if we start from a single known DS. Moreover, the bigger initial set of already known difference sets, the more efficient our method becomes. In that sense, upon obtaining 9 non-isomorphic initial $(144, 66, 30)$ HDSes by the product method, we subjected them to the *Procedure* DS^0. This yielded $(144, 66, 30)$ HDSes in new groups so that altogether 61 host groups were detected at the end of the procedure. Finally, in the launching set we included $(144, 66, 30)$ DS in group $[144, 182]$ given in [4]. Thus, before employing our construction method, the launching set enabled us to confirm the HDS existence in 62 groups of order 144.

3. Our DS construction method

As we have seen in Theorem 2.4, (v, k, λ) DSes are equivalent to (v, k, λ) symmetric designs with a regular automorphism group. Our DS construction method [15] uses this equivalence. It is applicable only to transitive incidence structures, being based on the following well-known result of Cameron and Praeger.

Theorem 3.1 ([6, Proposition 1.1]). *If $I(\mathcal{P}, H, B)$ is a $t-(v, k, \lambda)$ design and $H \leq G \leq Sym\,(\mathcal{P})$ holds, then $I(\mathcal{P}, G, B)$ is a $t-(v, k, \lambda^*)$ design with $\lambda^* \geq \lambda$.*

The theorem ensures that a block design can appear as a transitive substructure only within an overstructure which is a block design itself. Further, it justifies that, in general, a task of obtaining all transitive subdesigns of an initial block design $D = I(\mathcal{P}, G, B)$ with transitive group G can be accomplished by a computer search as follows. First one finds, up to conjugation, all maximal subgroups $M \leq G$ that are transitive on $\mathcal{P}$. The next step is checking whether $I\,(\mathcal{P}, M^g, B)$ is a block design, for each M found in the first step and all elements g from the (right) transversal of M in G. All groups

M^g for which the answer is positive have to be further analyzed, so they are stored at this level and the procedure continues by exploring their maximal subgroups. That is repeating of the first step on the lower level which can be continued as long as one obtains transitive block designs in the succeeding check. The procedure is obviously finite; its feasibility and computer time consumption depend on the structure of the lattice of subgroups of G.

In our method we modify the direction of the described procedure and confine it to the regular case. In that sense, starting from a known difference set, say Δ, we accomplish the construction of new difference sets with the same parameters proceeding in the following two steps.

1^0) *Developing a transitive overstructure of the regular symmetric design corresponding to* Δ.
Let $\Delta \subseteq H$ be a given difference set and let G be an overgroup of H, $H \leq G \leq Sym\,(\mathcal{P})$. For any point $p \in \mathcal{P}$ let $B = \{p^g |\, g \in \Delta\}$. Then $I(\mathcal{P}, H, B)$ is the symmetric design corresponding to the starting difference set Δ. Theorem 3.1 implies that the overstructure $D = I(\mathcal{P}, G, B)$ of $I(\mathcal{P}, H, B)$ is also a block design.

2^0) *Exploring the developed block design D for sought-after regular subdesigns.*
Given that the outcome of step 2^0) is a set of regular symmetric designs, it can again be subjected to step 1^0), i.e. the obtained designs can be developed into overstructures and then explored for regular subdesigns. Our construction course runs so that steps 1^0) and 2^0) are consecutively repeated; the repetition makes sense as long as we get new combinatorial possibilities as an input to step 1^0). The method in fact presents a (v, k, λ) *difference set generating algorithm* launched by the initial set Ω of (v, k, λ) difference sets, $|\Omega| \geq 1$.

The most delicate moment in application of our method is the choice of the overgroup by which we develop an overstructure in step 1^0). A desirable overgroup G should contain a considerable number of regular subgroups. On the other hand, this choice affects the feasibility of the task of obtaining regular subgroups of G or, if possible, of $AutD$ in step 2^0). Fact is: if the input group size is convenient, one simple command in the software Magma [3] returns, up to conjugation, all its regular subgroups.

Taking into account also our preliminary experience [15], we decided that the holomorph of H, denoted by $Hol(H)$, is an appropriate choice for G in this research. Although the construction algorithm in that case depends on the automorphism group $Aut(H)$, the choice $G = Hol\,(H)$ ensures that at least regular subgroups of G, together with their transversals in G, stay within the reach of Magma.

Group $Hol\,(H) = Aut(H) \ltimes H$ is a semidirect product with the multiplication formula $(\alpha, x)\,(\beta, y) = \big(\alpha\beta, x^{\beta}y\big)$ for all $x, y \in H$ and $\alpha, \beta \in AutH$. The equation $x^{(\alpha,y)} = x^{\alpha}y$ defines an action of group $Hol\,(H)$ on set H. In this action $H \trianglelefteq Hol\,(H)$ acts regularly. If the action of H on $\mathcal{P}$ is regular, then $Hol\,(H)$ can be observed as embedded in $Sym\,(\mathcal{P})$. This justifies the notation that we use in the next passage to describe how step 2^0) is performed in case $G = Hol\,(H)$.

Upon developing the design $D = I(\mathcal{P}, Hol\,(H)\,, B)$, for each regular subgroup $R \leq Hol\,(H)$ and for every $\widetilde{R}$ from the conjugacy class of R in $Hol\,(H)$, it is necessary to check whether the structure $I(\mathcal{P}, \widetilde{R}, B)$ is a block design. Technically, groups $\widetilde{R}$ are handled in the convenient form R^g, with g taken from the (right) transversal of R in $Hol\,(H)$. The designs detected in this search are necessarily symmetric and in the corresponding regular groups $\widetilde{R}$ difference sets are easily read off.

4. $(144, 66, 30)$ DIFFERENCE SET EXISTENCE RESULTS

We launched our construction method, described in the previous section, by submitting to step 1^0) the initial set of $(144, 66, 30)$ difference sets. The details on how we obtained the initial set are given in the conclusion of Section 2. With multiple repeating steps 1^0) and 2^0) the combinatorial task increased in scope and many non-isomorphic regular symmetric designs emerged. While monitoring the course of our algorithm we focused on different regular groups $[144, cn]$ that occurred, cn being the catalogue number in the “SmallGroups” library of [3]. It was before having exhausted all possibilities of consecutive developing overstructures and checking them upon the existence of regular subdesigns that the number of constructed inequivalent $(144, 66, 30)$ difference sets had risen over 5000 while, at the same time, the absence of new groups appearing in the process was noticed. This was indicative for the question of deciding groups $[144, cn]$ regarding DS existence, so we stopped the algorithm. The outcome of our construction procedure at that stage was proving the existence of HDSes in 69 groups of order 144 which we did not have initially. Thereby the problem of existence is solved for the total of 131 groups $[144, cn]$, ’cn’ belonging to the list

$$\begin{aligned}
&[52, 53, \mathbf{54}, \mathbf{55}, \mathbf{58}, \mathbf{59}, \mathbf{60}, \mathbf{61}, \mathbf{62}, 63, 64, 65, 66, 67, 69, \mathbf{70}, \mathbf{71}, \mathbf{73},\\
&74, \mathbf{75}, 76, 77, 78, 79, \mathbf{81}, \mathbf{82}, \mathbf{83}, 84, 85, \mathbf{86}, \mathbf{87}, \mathbf{89}, 90, \mathbf{91}, 92, 93, 94,\\
&95, \mathbf{97}, \mathbf{98}, \mathbf{99}, 100, \underline{101}, 102, 103, \underline{104}, \mathbf{105}, \mathbf{107}, \mathbf{108}, 115, 116, \mathbf{118},\\
&\mathbf{119}, 120, \mathbf{121}, \mathbf{122}, 123, \mathbf{124}, \mathbf{125}, 126, \mathbf{127}, \mathbf{128}, 129, 130, \mathbf{131}, 132,\\
&133, 134, \mathbf{135}, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146,\\
&147, 148, 149, 150, 151, 152, 153, 154, 155, \mathbf{156}, \mathbf{157}, 158, 159, 160,\\
&161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174,\\
&175, 176, 177, \underline{178}, 179, 180, 181, \mathbf{182}, 183, 184, 185, 186, 187, 188,\\
&189, 190, 191, 192, 193, 194, 195, 196, \underline{197}].
\end{aligned} \tag{4.1}$$

The list reveals that using our algorithm we managed to construct DSes in 37 groups for which product constructions do not work [12]; their catalogue numbers are written in bold type. The research described in [12] was supervised by K.W. Smith and, besides some common construction methods, it involved application of the "spread construction", as it was called at the time, later published in [2]. This resulted in the construction of DSes in the mentioned 37 groups. Interestingly enough, the set of groups for which HDS existence is ultimately confirmed in [12] is the same as the one given with list (4.1). Underlined in (4.1) are abelian groups.

Constructed difference sets (precisely 5765 inequivalent ones) are distributed among 131 groups as the exponents of the group catalogue numbers show in the following list:

$[52^{15}, 53^{5}, 54^{2}, 55^{5}, 58^{7}, 59^{9}, 60^{7}, 61^{7}, 62^{13}, 63^{86}, \mathbf{64}^{195}, 65^{101}, 66^{163}, 67^{99},$
$69^{15}, 70, 71^{8}, 73^{8}, 74^{5}, 75^{4}, 76^{82}, 77^{148}, 78^{91}, \mathbf{79}^{198}, 81^{8}, 82^{10}, 83^{14}, 84^{112},$
$85^{5}, 86^{4}, 87^{4}, 89^{4}, 90^{4}, 91, 92^{36}, 93^{63}, 94^{39}, 95^{65}, 97^{4}, 98^{2}, 99^{6}, 100^{41}, 101^{11},$
$102^{29}, 103^{25}, 104^{5}, 105, 107^{4}, 108^{4}, \mathbf{115}^{209}, 116^{98}, 118^{6}, 119^{2}, 120^{23}, 121^{3},$
$122^{6}, 123^{13}, 124^{3}, 125^{3}, 126^{3}, 127^{9}, 128^{9}, 129^{6}, 130^{7}, 131, 132^{65}, 133^{61},$
$134^{5}, 135, 136^{61}, 137^{67}, 138^{52}, 139^{49}, 140^{64}, 141^{50}, 142^{58}, 143^{145}, 144^{81},$
$145^{89}, 146^{116}, 147^{119}, 148^{55}, 149^{111}, 150^{74}, 151^{142}, 152^{52}, 153^{174}, 154^{173},$
$155^{16}, 156^{19}, 157^{19}, 158^{46}, 159^{108}, 160^{75}, 161^{50}, 162^{80}, 163^{60}, 164^{27}, 165^{20},$
$166^{57}, 167^{152}, 168^{42}, 169^{75}, 170^{28}, 171^{51}, 172^{49}, 173^{50}, 174^{44}, 175^{22}, 176^{29},$
$177^{57}, 178^{27}, 179^{32}, 180^{20}, 181^{27}, 182, 183^{8}, 184^{4}, 185^{5}, 186^{154}, 187^{12},$
$188^{13}, 189^{3}, 190^{6}, 191^{68}, 192^{108}, 193^{10}, 194^{3}, 195^{27}, 196^{16}, 197^{5}].$

Groups $[144, 64]$, $[144, 79]$, and $[144, 115]$ are highlighted in bold for hosting a large number of inequivalent DSes. The developments of the constructed difference sets split into **1364** isomorphism classes of symmetric designs. These designs are given in the Magma file "DS144", [17]. The next table contains the orders of the full automorphism groups and the number of non-isomorphic designs having the full automorphism group of the given order.

$\|AutD\|$	No. of nonisom. designs	$\|AutD\|$	No. of nonisom. designs
144	397	2592	8
288	382	3456	1
432	5	5184	8
576	383	7776	2
864	19	10368	4
1152	118	15552	2
1296	15	46656	1
1440	1	93312	1
1728	16	190080	1

As expected, designs with small automorphism groups are numerous, while few of them have large automorphism groups. In case $|AutD| = 190080$, design D cannot be obtained by the product method. It is primitive and $AutD$ is almost simple group containing M_{12}. The only regular subgroup of $AutD$ is $[144, 182]$ [4]. That group is also the only regular subgroup for the design D with $|AutD| = 1440$. In cases $|AutD| = 46656$ and $|AutD| = 93312$ the designs are obtainable by the product method. Both designs have, besides several others, abelian groups $[144, 101]$ and $[144, 178]$ as regular subgroups of the full automorphism group.

5. Nonexistence in abelian case

As one can see from the list (4.1), $(144, 66, 30)$ difference sets exist in four abelian groups: $[144, 101] \cong C_3^2 \times C_4^2$, $[144, 104] \cong C_3^2 \times C_2 \times C_8$, $[144, 178] \cong C_3^2 \times C_2^2 \times C_4$, and $[144, 197] \cong C_3^2 \times C_2^4$. The remaining six abelian groups: $[144, 2]$, $[144, 20]$, $[144, 23]$, $[144, 30]$, $[144, 47]$, and $[144, 113]$ do not support HDS existence. This is easily proved applying the necessary criteria for DS existence given in Theorem 5.1 and Theorem 5.2 (below). Let us recall that a prime p is called *self-conjugate modulo an integer* w if there exists a non-negative integer j with $p^j \equiv -1 (\bmod\, w')$, where w' denotes the p-free part of w. In case of group $[144, 23]$ we have to employ a more general concept of self-conjugacy. Given positive integers m and w, m is said to be *self-conjugate modulo* w if for each prime divisor p of m there exists an integer j_p such that $p^{j_p} \equiv -1 (\mathrm{mod} w_p)$, where w_p is the largest divisor of w coprime to p.

Theorem 5.1 ([1, p. 424]). *Let D be a (v, k, λ) difference set in an abelian group G, and let p be a prime which is self-conjugate modulo* $\exp G$ *and divides both v and $n = k - \lambda$. Then the Sylow p-subgroup of G is not cyclic.*

In our research $|G| = v = 144$, $n = 36$ and $\exp G$ equals $2^\alpha \cdot 3$ or $2^\alpha \cdot 9, \alpha \leq 4$. Because 2 is self-conjugate $\bmod 3$ and $\bmod 9$, it is self-conjugate modulo $\exp G$. Theorem 5.1 implies that Sylow 2-subgroup of G is not cyclic if G supports an HDS. Thus, $p = 2$ rules out groups $C_{16} \times C_9 \cong [144, 2]$ and $C_{16} \times C_3^2 \cong [144, 30]$. Similarly, because 3 is self-conjugate $\bmod 2$ and $\bmod 4$, Sylow 3-subgroup of G supporting an HDS is not cyclic if $\exp G = 2 \cdot 3, 2 \cdot 9, 4 \cdot 3$ or $4 \cdot 9$. Now $p = 3$ rules out groups $C_9 \times C_2^2 \times C_4 \cong [144, 47]$, $C_9 \times C_4^2 \cong [144, 20]$, and $C_9 \times C_2^4 \cong [144, 113]$.

Regarding group $[144, 23]$, we take into consideration the following statement.

Theorem 5.2 ([1, p. 425]). *Let D be a (v, k, λ) difference set in an abelian group G, let H be a subgroup of G of order s and index u, and denote the exponent of G/H by u^*. Moreover, assume the existence of a positive integer m with $(m, n) \neq 1$ which is self-conjugate modulo u^* and for which m^2 divides n. If the Sylow p-subgroup of G/H is cyclic for every prime p dividing m and u, then one has $m \leq 2^{r-1}s$, where r is the number of distinct primes dividing (m, u).*

Following the notation of this theorem let us put $G = [144, 23] \cong C_9 \times C_2 \times C_8 = \langle x\rangle \times \langle y\rangle \times \langle z\rangle$ and $H = \left\langle z^4 \right\rangle$. Then $s = 2$ and $u = 72$; $u^* = \exp(G/H) = \exp(C_9 \times C_2 \times C_4) = 9 \cdot 4$. Moreover, $m = 3$ satisfies the conditions of the theorem and $p = 3$ is the only divisor of m and u. Sylow 3-subgroup of G/H is cyclic and the theorem implies $3 \leq 2^{r-1}s = 2$ (because $r = 1$), which is a contradiction.

The same result for the abelian case is obtained in [12] using the contrapositive of the fact that if a group contains a difference set, then any homomorphic image of that group contains an image of the difference set.

6. Preliminaries to PDSes and Cayley graphs construction

We start with defining combinatorial objects that we construct next.

Definition 6.1. *Let H be a group of order v. A k-subset $S \subset H$ is called a (v, k, λ, μ)* partial difference set *if the multiset $\left\{xy^{-1} \mid x, y \in S, x \neq y\right\}$ contains each nonidentity element of S exactly λ times and it contains each nonidentity element of $H \setminus S$ exactly μ times.*

Using the notation of the group ring $\mathbb{Z}H$ (where $S = \sum_{s\in S} s$), a (v, k, λ, μ) partial difference set $S \subset H$ in group H can be defined as a subset for which the equation

$$S \cdot S^{(-1)} = k1_H + \lambda(S \setminus \{1_H\}) + \mu((H \setminus S) \setminus \{1_H\})$$

holds; $S^{(-1)} = \sum_{s\in S} s^{-1}$.

The notion of a partial difference set (PDS) generalizes that of a difference set. It is obvious that any (v, k, λ) difference set is a (v, k, λ, λ) partial difference set.

PDSes S_1 and S_2 in groups H_1 and H_2, respectively, we call *equivalent* if there exists a group isomorphism $\varphi : H_1 \to H_2$ which maps S_1 onto S_2.

A partial difference set $S \subset H$ is called *reversible* if $S = S^{(-1)}$. A reversible partial difference set $S \subset H$ is *regular* if $1_H \notin S$. Our further interest sticks only to regular PDSes. It is easy to see (cf. [14]) that the following assertions hold.

Proposition 6.2. *Suppose that S is a reversible (v, k, λ, μ) PDS in a group H, such that $1_H \in S$. Then $S \setminus \{1_H\}$ is a regular $(v, k-1, \lambda-2, \mu)$ PDS in H. Conversely, if S is a regular PDS in H, then $S \cup \{1_H\}$ is a reversible PDS with corresponding parameters.*

Proposition 6.3. *Suppose that Δ is a (v, k, λ) difference set in H, $x \in H$. Then*

(i) Δx is a regular (v, k, λ, λ) PDS if and only if $x^{-1} \notin \Delta$ and Δx is a reversible set;

(ii) $\Delta x \setminus \{1_H\}$ *is a regular* $(v, k-1, \lambda-2, \lambda)$ *PDS if and only if* $x^{-1} \in \Delta$ *and* Δx *is a reversible set.*

The notion of a PDS is connected to graph theory. A *finite graph* $\Gamma = (\Omega, E)$ consists of a finite set Ω of points, called vertices, and a subset E of unordered pairs from Ω called edges.

Definition 6.4. *A strongly regular graph (SRG) with parameters* (v, k, λ, μ) *is a graph with* v *vertices which is regular of valency* k*, i.e. every vertex is incident with* k *edges, such that any pair of adjacent vertices have exactly* λ *common neighbours and any pair of non-adjacent vertices have exactly* μ *common neighbours.*

Two graphs are isomorphic if there is a bijection between their vertex sets that preserves adjacency. Regular partial difference sets and strongly regular graphs are closely related through the concept of the Cayley graph. This relation we employ for constructions in Section 7.

Definition 6.5. *For a group* H *and a set* $S \subset H$ *with the property that* $1_H \notin S$ *and* $S = S^{(-1)}$*, the Cayley graph* $\Gamma = Cay(H, S)$ *over* H *with connection set* S *is the graph with vertex set* H *so that the vertices* x *and* y *are adjacent if and only if* $x^{-1}y \in S$*.*

Accordingly, the set of edges of a Cayley graph $\Gamma = Cay(H, S)$ over H with connection set S is $E := \{\{x, xs\} \mid x \in H,\, s \in S\}$. Our construction of strongly regular graphs (cf. [10]) will be based on the following important assertion about Cayley graphs, [1, p. 230] or [13].

Theorem 6.6. *A Cayley graph* $Cay(H, S)$ *is a* (v, k, λ, μ) *strongly regular graph if and only if* S *is a* (v, k, λ, μ) *regular partial difference set in* H*.*

Obviously, equivalent regular PDSes correspond to isomorphic strongly regular Cayley graphs. Moreover, for two inequivalent partial difference sets S_1 and S_2 in a group H, the graphs $Cay(H, S_1)$ and $Cay(H, S_2)$ can be isomorphic. Similarly, for two inequivalent partial difference sets S_1 and S_2 in groups H_1 and H_2, $|H_1| = |H_2|$, the graphs $Cay(H_1, S_1)$ and $Cay(H_2, S_2)$ can be isomorphic. The examples of both such cases are present in our construction described and analyzed in the next section.

7. Construction of regular PDSes and SRGs

We use $(144, 66, 30)$ difference sets to construct regular $(144, 66, 30, 30)$ and $(144, 65, 28, 30)$ partial difference sets. Following the theoretical background highlighted in Section 6, it is easily verified that a procedure for the search of regular partial difference sets, starting from a known difference set $\Delta \subseteq H$, can be performed in the next two steps:

(i) construction of all shifts Δx of Δ, $x \in H$;

(ii) selection of those shifts which are reversible sets in H.

Then, each reversible shift which does not contain 1_H is a regular (v, k, λ, λ) PDS, while each reversible shift that contains 1_H yields a regular $(v, k-1, \lambda-2, \lambda)$ PDS $\Delta x \setminus \{1_H\}$.

To this “shifting procedure” we have submitted the constructed 5765 inequivalent difference sets in 131 groups listed in (4.1). Reversible shifts are singled out and then tested upon group automorphisms by Magma. The final result is obtaining 3452 inequivalent reversible $(144, 66, 30)$ difference sets in 53 groups, two of them ($[144, 178]$ and $[144, 197]$) being abelian. The next table shows the exact number of obtained regular PDSes of both types in the specified group $[144, cn]$. It is given in the form $r_1 + r_2$, where r_1 is the number of obtained $(144, 66, 30, 30)$ PDSes and r_2 is the number of obtained $(144, 65, 28, 30)$ PDSes. For instance, group $[144, 186]$ contains the greatest number $(196 + 212 = 408)$ of regular PDSes.

$[144, cn]$ ↓	rPDS ↓	$[144, cn]$ ↓	rPDS ↓	$[144, cn]$ ↓	rPDS ↓	$[144, cn]$ ↓	rPDS ↓
63	8+8	132	30+38	160	8+8	186	196+212
64	26+34	133	26+26	162	34+38	188	5+2
65	50+54	136	42+50	166	10+10	189	7+3
66	12+12	143	28+28	167	86+102	190	3+1
67	8+8	144	40+44	169	20+20	191	52+52
76	8+8	145	28+28	170	23+27	192	60+79
77	12+12	146	8+8	172	74+94	193	4+3
78	8+8	149	20+20	176	5+5	194	0+1
79	26+34	150	8+8	177	46+54	195	9+11
84	50+54	151	86+102	$\underline{178}$	5+5	196	48+64
115	108+124	153	74+82	179	23+27	$\underline{197}$	6+7
116	30+30	154	136+168	182	1+1		
123	3+3	155	1+1	183	9+3		
129	2+2	159	8+8	184	0+1		

The number of obtained regular PDSes with parameters $(144, 66, 30, 30)$ is 1620. Their existence is confirmed in 51 groups of order 144; in groups $[144, 184]$ and $[144, 194]$ PDSes of cardinality 66 have not been found.

The next table shows the number of non-isomorphic SRGs of both valencies that correspond to the constructed regular PDSes, group by group. Like in the previous table, it is given in the form of a sum of the numbers related to valencies 66 and 65, respectively.

$[144, cn]$ ↓	SRG ↓	$[144, cn]$ ↓	SRG ↓	$[144, cn]$ ↓	SRG ↓	$[144, cn]$ ↓	SRG ↓
63	4+4	132	10+12	160	5+5	186	11+13
64	12+16	133	8+8	162	6+7	188	2+2
65	12+14	136	14+16	166	5+5	189	1+1
66	6+6	143	8+8	167	24+32	190	1+1
67	4+4	144	9+10	169	5+5	191	11+11
76	4+4	145	8+8	170	8+12	192	9+11
77	6+6	146	5+5	172	10+18	193	2+1
78	4+4	149	5+5	176	5+5	194	0+1
79	12+16	150	5+5	177	8+12	195	6+7
84	12+14	151	24+32	$\underline{178}$	5+5	196	6+7
115	16+20	153	9+10	179	8+12	$\underline{197}$	6+7
116	10+10	154	27+35	182	1+1		
123	2+1	155	1+1	183	2+2		
129	1+1	159	5+5	184	0+1		

A comparison of the last two tables reveals numerous examples of nonabelian groups in which inequivalent PDSes correspond to isomorphic Cayley graphs.

Regarding isomorphism of the corresponding strongly regular Cayley graphs, our 3452 regular PDSes split into 121 non-isomorphic SRG classes; they are presented in Magma file “SRG144”, [17]. On the same site we provide the file “Graphs144Analysis” with the graphs' automorphism groups data obtained using Magma. The files show that 1620 constructed inequivalent PDSes of cardinality 66 correspond to 43 non-isomorphic strongly regular graphs of valency 66. The next table contains the orders of their full automorphism groups and the number of non-isomorphic graphs Γ having the full automorphism group of the given order.

$\vert Aut\Gamma\vert$	144	288	576	1152	1728	3456	5184	10368	190080
No. of graphs	2	2	26	4	2	2	2	2	1

It is interesting that the largest automorphism group ($|Aut\Gamma| = 190080$) has $[144, 182]$ as the only regular subgroup. On the other side, the majority of full automorphism groups has many regular subgroups. For example, in both cases with $|Aut\Gamma| = 3456$, the full group has 28 regular subgroups. Thus, inequivalent PDSes from non-isomorphic groups correspond to isomorphic Cayley graphs.

The existence of regular PDSes of cardinality 65 is confirmed in 53 groups. The constructed 1832 inequivalent such PDSes correspond to 78 non-isomorphic strongly regular graphs of valency 65. The next table contains the orders of the full automorphism groups and the number of non-isomorphic graphs Γ having the full automorphism group of the given order.

$\lvert Aut\Gamma\rvert$	No. of nonisom. graphs
144	7
288	29
576	26
864	3
1152	5
1440	1
1728	3
3456	1
10368	1
15552	1
31104	1

Again, $[144, 182]$ is the only regular subgroup of $Aut\Gamma$ in case of the single graph Γ with $|Aut\Gamma| = 1440$. As for the last four graphs in the table, their full automorphism groups have many regular subgroups. For instance, even 32 in case $|Aut\Gamma| = 10368$.

It is of interest also to present the set of the obtained non-isomorphic strongly regular Cayley graphs hosted by each of 51 (53) groups. As it would be space consuming to do it in the paper, we present instead a selection of interesting results for both valencies in the next two tables. The complete distribution is available in the files "Cayley (144,66,30,30) by groups" and "Cayley (144,65,28,30) by groups" at [17].

Parameters $(144, 66, 30, 30)$ i.e. VALENCY 66

$\lvert Aut\Gamma\rvert \downarrow \ddots\ [144, cn] \rightarrow$	$\cdots$	151	154	167	172	182	$\cdots$
144					2		
288			1		1		
576		15	15	15	3		
1152		4	4	4	2		
1728		1	1	1			
3456		2	2	2	2		
5184			2				
10368		2	2	2			
190080						1	
No. of graphs	$\cdots$	24	27	24	10	1	$\cdots$

Groups $[144, 151]$, $[144, 154]$, and $[144, 167]$ are selected since hosting a respectable number of non-isomorphic graphs. Group $[144, 172]$ is selected because the two obtained graphs of valency 66 with $|Aut\Gamma| = 144$ are presented only through regular PDSes in that group. The characteristic feature of group $[144, 182]$ is already mentioned.

Parameters $(144, 65, 28, 30)$ i.e. VALENCY 65

$\lvert Aut\Gamma\rvert \downarrow \iddots [144, cn] \rightarrow$	$\cdots$	154	172	182	192	$\cdots$
144			6		1	
288		8	5		2	
576		15	3		2	
864		1				
1152		5	3		2	
1440				1		
1728		2			1	
3456		1			1	
10368		1	1			
15552		1			1	
31104		1			1	
No. of graphs	$\cdots$	35	18	1	11	$\cdots$

Once again group $[144, 182]$ is the only group that hosts strongly regular Cayley graph Γ of valency 65, $|Aut\Gamma| = 1440$, through a PDS. Seven obtained non-isomorphic graphs of valency 65 with full group of order 144 appear in groups $[144, 172]$ and $[144, 192]$ as presented in the table.

We see that even $27 + 35 = 62$ non-isomorphic strongly regular Cayley graphs of valencies 66 and 65 can be represented through regular PDSes in group $[144, 154]$. Among them one finds representatives of all obtained graphs Γ of valency 66 with $|Aut\Gamma| = 1152$, 3456, 5184 and 10368, as well as representatives of all obtained graphs Γ of valency 65 with $|Aut\Gamma| = 1152$, 3456, 10368, 15552 and 31104.

Acknowledgements.

The author wishes to thank her colleague Joško Mandić for his help with both calculations and valuable discussions. Thanks also to Christopher P. Mooney for providing us with a copy of the NSF-REU undergraduate research project report [12], further to our personal communication.

References

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

[2] C. Bhattacharya and K. W. Smith, *Factoring* $(16, 6, 2)$ *Hadamard difference sets,* Electron. J. Combin. **15** (2008), #R112.

[3] W. Bosma, J. J. Cannon, C. Fieker and A. Steel (eds.), Handbook of Magma functions, Edition 2.16, 2010.

[4] S. Braić, A. Golemac, J. Mandić and T. Vučičić, *Primitive Symmetric Designs with up to* 2500 *Points,* J. Combin. Des. **19** (2011), 463–474.

[5] C. J. Colbourn and J. H. Dinitz, Eds., Handbook of combinatorial designs, Second Edition, CRC Press, New York, 2007.

[6] P. J. Cameron and C. E. Praeger, *Block-transitive t-designs I: point-imprimitive designs,* Discrete Math. **118** (1993), 33–43.

[7] J. A. Davis and J. Jedwab, *A survey of Hadamard difference sets,* in: Groups, Difference Sets and the Monster (eds. K. T. Arasu et al.), de Gruyter, Berlin-New York, 1996, pp. 145–156.

[8] J. F. Dillon, *Variations on a scheme of McFarland for noncyclic difference sets,* J. Combin. Theory Ser. A **40** (1985), 9–21.

[9] J. F. Dillon, *Some REALLY beautiful Hadamard matrices,* Cryptogr. Commun. **2** (2010), 271–292.

[10] A. Golemac, J. Mandić and T. Vučičić, *New regular partial difference sets and strongly regular graphs with parameters* $(96, 20, 4, 4)$ *and* $(96, 19, 2, 4)$*,* Electron. J. Combin. **13** (2006), #R88.

[11] Y. J. Ionin and M. S. Shrikhande, Combinatorics of Symmetric Designs, Cambridge University Press, New York, 2006.

[12] N. Kroeger, M. Miller, C. P. Mooney, K. Shepard and K. W. Smith, Determining Existence of Hadamard Difference Sets in Groups of Order 144, NSF-REU research report, Central Michigan University, 2007.

[13] S. L. Ma, *Partial difference sets,* Discrete Math. **52** 1984, 75–89.

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

[15] J. Mandić and T. Vučičić, *On the existence of Hadamard difference sets in groups of order* 400*,* Adv. Math. Commun. **10** (2016), 547–554.

[16] P. K. Menon, *On difference sets whose parameters satisfy a certain relation,* Proc. Amer. Math. Soc. **13** (1962), 739–745.

[17] `http://www.pmfst.hr/∼vucicic/MAGMA_REC144/`

Hadamardovi diferencijski skupovi i s njima povezani kombinatorni objekti u grupama reda 144

Tanja Vučičić

Sažetak. U ovom radu bavimo se kombinatorički zanimljivim i zahtjevnim problemom egzistencije diferencijskih skupova u grupama reda 144 koji do sada nije riješen u potpunosti. Primijenjena konstruktivna metoda, uvedena u našim nedavnim istraživanjima, pokazala se veoma učinkovitom. Rezultat je više od 5000 neekvivalentnih (144,66,30) diferencijskih skupova konstruiranih u 131-oj grupi reda 144. Broj njima odgovarajućih neizomorfnih simetričnih dizajna je 1364.

Dobivene diferencijske skupove smo upotrijebili za konstrukciju novih regularnih (144,66,30,30) i (144,65,28,30) parcijalnih diferencijskih skupova, kao i pridruženih jako regularnih grafova. Konstruirana su 43 takva neizomorfna grafa valencije 66 te 78 njih valencije 65. Pune grupe automorfizama dobivenih grafova i simetričnih dizajna istražene su pomoću softverskog paketa Magma.

Tanja Vučičić
Faculty of Science
University of Split
Ruđera Boškovića 33
21 000 Split, Croatia
E-mail: vucicic@pmfst.hr

Received: 18.10.2018.
Revised: 20.12.2018.
Accepted: 22.1.2019.