

Hadamard difference sets and corresponding regular partial difference sets in groups of order 144

Tanja Vučičić

University of Split, Croatia

March 17, 2015

Hadamard difference sets and corresponding regular partial difference sets in groups of order 144

This is a joint research with Joško Mandić.

Hadamard difference sets and corresponding regular partial difference sets in groups of order 144

There are 197 groups of order 144. Solving the problem of difference set (DS) existence in these groups has not been completed yet.

In focus: $(144,66,30)$ DSs construction by the new method we here describe.

We also show the construction of **regular partial difference sets** (PDSs) and **strongly regular graphs** (SRGs) with parameters $(144,66,30,30)$ and $(144,65,28,30)$.

A (v, k, λ) **difference set** Δ is a subset of size k in a group G of order v with the property that the multiset of products $\{xy^{-1} \mid x, y \in \Delta, x \neq y\}$ contains exactly λ copies of each non-identity element of G .

A (v, k, λ) **difference set** Δ is a subset of size k in a group G of order v with the property that the multiset of products $\{xy^{-1} \mid x, y \in \Delta, x \neq y\}$ contains exactly λ copies of each non-identity element of G .

The **development** of a difference set $\Delta \subseteq G$ is the incidence structure

$$\text{dev}\Delta = (G, \{\Delta g \mid g \in G\}).$$

It relates difference sets (DSs) to symmetric designs (SDs) in the following way:

Theorem

Let $\Delta \subseteq G$ be a (v, k, λ) difference set. Then $\text{dev}\Delta$ is a symmetric (v, k, λ) design with $G \leq \text{Aut}(\text{dev}\Delta)$. Group G acts regularly on points and blocks of $\text{dev}\Delta$.

Theorem

Let $\Delta \subseteq G$ be a (v, k, λ) difference set. Then $\text{dev}\Delta$ is a symmetric (v, k, λ) design with $G \leq \text{Aut}(\text{dev}\Delta)$. Group G acts regularly on points and blocks of $\text{dev}\Delta$.

Theorem

Let $D = (\mathcal{P}, \mathcal{B})$ be a symmetric (v, k, λ) -design with regular automorphism group G . 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 .

Theorem

Let $\Delta \subseteq G$ be a (v, k, λ) difference set. Then $\text{dev}\Delta$ is a symmetric (v, k, λ) design with $G \leq \text{Aut}(\text{dev}\Delta)$. Group G acts regularly on points and blocks of $\text{dev}\Delta$.

Theorem

Let $D = (\mathcal{P}, \mathcal{B})$ be a symmetric (v, k, λ) -design with regular automorphism group G . 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 .

Parameter triples of the form

$$(4u^2, 2u^2 - u, u^2 - u), \quad u \in \mathbb{N}, \quad (1)$$

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

It is well-known that two Hadamard difference sets (HDSs) yield a new HDS by the 'product' method according to the following theorem.

Theorem (Product method, Menon)

Let $G = G_1 \times G_2$ be the direct product of groups G_1 and G_2 . If difference sets with parameters of type (1) exist in G_1 and G_2 for $u = u_1$ and $u = u_2$ respectively, then group G contains a difference set with parameters (1) for $u = 2u_1 u_2$.

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

$$\Delta := (\Delta_1 \times \overline{\Delta}_2) \cup (\overline{\Delta}_1 \times \Delta_2), \quad (2)$$

where $\overline{\Delta}_i = G_i \setminus \Delta_i$, $i = 1, 2$.

Product construction of $(144, 66, 30)$ difference sets

Our considered $(144, 66, 30)$ HDSs with $u = 6$ can obviously be obtained by the product method **from** $(36, 15, 6)$ **HDSs and a trivial HDS in group of order 4**, consisting of a single point.

There exist exactly 9 nonisomorphic (35 inequivalent) $(36, 15, 6)$ HDSs and two trivial $(4, 1, 0)$ HDSs.

$(144, 66, 30)$ HDSs obtained as their product serve as the initial set of DSs needed to launch our new construction method.

Our construction method

Our construction method is applicable to transitive incidence structures.
A transitive incidence structure we denote by

$$I(\Omega, G, B), \quad (3)$$

where Ω is the point set, G is an automorphism group acting transitively on Ω and $B = \{B^g \mid g \in G\}$, $B \subseteq \Omega$, the block set.

Regular symmetric designs (block designs) corresponding to our aimed DSs will be obtained as transitive substructures of the overstructures that we develop in the construction procedure.

Our construction method: basic theorem

From the following well-known theorem by Cameron and Praeger¹

Theorem (1)

If $I(\Omega, H, B)$ is a $t - (v, k, \lambda)$ design and $H \leq G \leq \text{Sym}(\Omega)$ holds, then $I(\Omega, G, B)$ is a $t - (v, k, \lambda^*)$ design with $\lambda^* \geq \lambda$.

we conclude that block design as a transitive substructure can appear only in transitive overstructure which is block design itself.

¹P.J. Cameron and C.E. Praeger, *Block-transitive t -designs I: point-imprimitive designs*, Discrete Mathematics **118** (1993), 33-43.

Our construction method in two steps

In that sense, starting from a known difference set, say Δ , we accomplish the construction of new DSs with the same parameters by proceeding in the following two steps:

Our construction method in two steps

In that sense, starting from a known difference set, say Δ , we accomplish the construction of new DSs with the same parameters by proceeding in the following two steps:

- developing a transitive overstructure (of the regular symmetric design corresponding to Δ) which is block design,

Our construction method in two steps

In that sense, starting from a known difference set, say Δ , we accomplish the construction of new DSs with the same parameters by proceeding in the following two steps:

- developing a transitive overstructure (of the regular symmetric design corresponding to Δ) which is block design,
- exploring the developed block design for desirable regular subdesigns.

Construction method - step one: developing an overstructure

Let Δ be a difference set in group H and let G be its overgroup, $H \leq G \leq \text{Sym}(\Omega)$.

Construction method - step one: developing an overstructure

Let Δ be a difference set in group H and let G be its overgroup, $H \leq G \leq \text{Sym}(\Omega)$.

For any point $\omega \in \Omega$ let $B = \{\omega^g \mid g \in \Delta\}$.

Construction method - step one: developing an overstructure

Let Δ be a difference set in group H and let G be its overgroup, $H \leq G \leq \text{Sym}(\Omega)$.

For any point $\omega \in \Omega$ let $B = \{\omega^g \mid g \in \Delta\}$.

Then, $I(\Omega, G, B)$ is a block design (Theorem (1)), an overstructure to be explored for regular subdesigns.

Construction method - step one: developing an overstructure

Let Δ be a difference set in group H and let G be its overgroup, $H \leq G \leq \text{Sym}(\Omega)$.

For any point $\omega \in \Omega$ let $B = \{\omega^g \mid g \in \Delta\}$.

Then, $I(\Omega, G, B)$ is a block design (Theorem (1)), an overstructure to be explored for regular subdesigns.

This investigation we perform with the help of software MAGMA. If G is of appropriate size, then a simple command in MAGMA returns all regular subgroups $R \leq G$ up to conjugation.

Construction method - step two: obtaining transitive substructures

First, let's consider obtaining substructures of a given transitive design $D = I(\Omega, G, B)$ related to a subgroup $H \leq G$ transitive on Ω .

Let B_1, \dots, B_l be representatives of all H -orbits on B .

Then

$$\{I(\Omega, H, B_i), i = 1, \dots, l\} \quad (4)$$

is the set of all transitive incidence substructures of D with an automorphism group H .

Obviously, there exist $g_i \in G, i = 1, \dots, l$ so that $B_i = B^{g_i}$. Accordingly, (4) becomes

$$\{I(\Omega, H, B^{g_i}), i = 1, \dots, l\}. \quad (5)$$

Construction method - step two: obtaining transitive substructures

Applying the following simple fact about transitive incidence structures:

Lemma

Incidence structures $I(\Omega, G, B^\pi)$ and $I(\Omega, G^{\pi^{-1}}, B)$ are isomorphic for every $\pi \in \text{Sym}(\Omega)$.

gives that the set (5), up to isomorphism, is

$$\{I(\Omega, H^{g_i^{-1}}, B), i = 1, \dots, l\}, \quad (6)$$

which is technically convenient for a software search.

Construction method - step two: filtering

Consequently, **exploring incidence structures**

$$I(\Omega, H^g, B), \text{ with } g \text{ from the (right) transversal of } H \text{ in } G, \quad (7)$$

suffice **to obtain all transitive substructures of the starting structure D related to the subgroup $H \leq G$.**

Construction method - step two: filtering

Consequently, **exploring incidence structures**

$$I(\Omega, H^g, B), \text{ with } g \text{ from the (right) transversal of } H \text{ in } G, \quad (7)$$

suffice **to obtain all transitive substructures of the starting structure D related to the subgroup $H \leq G$.**

We choose H to be **regular subgroup**.

Construction method - step two: filtering

Consequently, **exploring incidence structures**

$$I(\Omega, H^g, B), \text{ with } g \text{ from the (right) transversal of } H \text{ in } G, \quad (7)$$

suffice **to obtain all transitive substructures of the starting structure D related to the subgroup $H \leq G$.**

We choose H to be **regular subgroup**.

What **we** do is **check**,

Construction method - step two: filtering

Consequently, **exploring incidence structures**

$$I(\Omega, H^g, B), \text{ with } g \text{ from the (right) transversal of } H \text{ in } G, \quad (7)$$

suffice **to obtain all transitive substructures of the starting structure D related to the subgroup $H \leq G$.**

We choose H to be **regular subgroup**.

What **we** do is **check**,
for each regular subgroup $R \leq G$

Construction method - step two: filtering

Consequently, **exploring incidence structures**

$$I(\Omega, H^g, B), \text{ with } g \text{ from the (right) transversal of } H \text{ in } G, \quad (7)$$

suffice **to obtain all transitive substructures of the starting structure D related to the subgroup $H \leq G$.**

We choose H to be **regular subgroup**.

What **we** do is **check**,

for each regular subgroup $R \leq G$

and for every \tilde{R} from the conjugacy class of R in G ,

Construction method - step two: filtering

Consequently, **exploring incidence structures**

$$I(\Omega, H^g, B), \text{ with } g \text{ from the (right) transversal of } H \text{ in } G, \quad (7)$$

suffice **to obtain all transitive substructures of the starting structure D related to the subgroup $H \leq G$.**

We choose H to be **regular subgroup**.

What **we** do is **check**,

for each regular subgroup $R \leq G$

and for every \tilde{R} from the conjugacy class of R in G ,

which among the structures $I(\Omega, \tilde{R}, B)$ (if any) are block designs.

Construction method - step two: filtering

Consequently, **exploring incidence structures**

$$I(\Omega, H^g, B), \text{ with } g \text{ from the (right) transversal of } H \text{ in } G, \quad (7)$$

suffice **to obtain all transitive substructures of the starting structure D related to the subgroup $H \leq G$.**

We choose H to be **regular subgroup**.

What **we** do is **check**,

for each regular subgroup $R \leq G$

and for every \tilde{R} from the conjugacy class of R in G ,

which among the structures $I(\Omega, \tilde{R}, B)$ (if any) are block designs.

Thus obtained designs $I(\Omega, \tilde{R}, B)$ are symmetric. The corresponding difference sets in underlying groups \tilde{R} are easily read off.

Look back on an overgroup choice

The chosen overgroup G in step one should not be too large so as to insure that its regular subgroups stay within the reach of MAGMA.

Look back on an overgroup choice

The chosen overgroup G in step one should not be too large so as to insure that its regular subgroups stay within the reach of MAGMA.

It is also desirable that overgroup G contains a considerable number of regular subgroups.

Look back on an overgroup choice

The chosen overgroup G in step one should not be too large so as to insure that its regular subgroups stay within the reach of MAGMA.

It is also desirable that overgroup G contains a considerable number of regular subgroups.

It turned out that **holomorph of H** , denoted by $Hol(H)$, was an appropriate choice for G .

$Hol(H)$ is a semidirect product of H by $Aut(H)$, where the action of $Aut(H)$ is natural.

Outcome of the construction procedure

Without having exhausted all construction possibilities, we stopped the procedure at the stage when the number of constructed inequivalent (144, 66, 30) difference sets rose to **5765** and the absence of new groups appearing in the process was indicative. Thereby the problem of existence is solved for **131** groups $[144, id]$, '*id*' belonging to the list:

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

Group index is written in red if DS in that group cannot be obtained by any product construction.

Constructed difference sets are distributed in these 131 groups as show the exponents of the group *id*-numbers in the following list:

[52¹⁵, 53⁵, 54², 55⁵, 58⁷, 59⁹, 60⁷, 61⁷, 62¹³, 63⁸⁶, **64**¹⁹⁵, 65¹⁰¹, 66¹⁶³, 67⁹⁹, 70, 71⁸, 73⁸, 74⁵, 75⁴, 76⁸², 77¹⁴⁸, 78⁹¹, **79**¹⁹⁸, 81⁸, 82¹⁰, 83¹⁴, 84¹¹², 85⁵, 86⁴, 87⁴, 89⁴, 90⁴, 91, 92³⁶, 93⁶³, 94³⁹, 95⁶⁵, 97⁴, 98², 99⁶, 100⁴¹, 101¹¹, 102²⁹, 103²⁵, 104⁵, 105, 107⁴, 108⁴, **115**²⁰⁹, 116⁹⁸, 118⁶, 119², 120²³, 121³, 122⁶, 123¹³, 124³, 125³, 126³, 127⁹, 128⁹, 129⁶, 130⁷, 131, 132⁶⁵, 133⁶¹, 134⁵, 135, 136⁶¹, 137⁶⁷, 138⁵², 139⁴⁹, 140⁶⁴, 141⁵⁰, 142⁵⁸, 143¹⁴⁵, 144⁸¹, 145⁸⁹, 146¹¹⁶, 147¹¹⁹, 148⁵⁵, 149¹¹¹, 150⁷⁴, 151¹⁴², 152⁵², 153¹⁷⁴, 154¹⁷³, 155¹⁶, 156¹⁹, 157¹⁹, 158⁴⁶, 159¹⁰⁸, 160⁷⁵, 161⁵⁰, 162⁸⁰, 163⁶⁰, 164²⁷, 165²⁰, 166⁵⁷, 167¹⁵², 168⁴², 169⁷⁵, 170²⁸, 171⁵¹, 172⁴⁹, 173⁵⁰, 174⁴⁴, 175²², 176²⁹, 177⁵⁷, 178²⁷, 179³², 180²⁰, 181²⁷, 182, 183⁸, 184⁴, 185⁵, 186¹⁵⁴, 187¹², 188¹³, 189³, 190⁶, 191⁶⁸, 192¹⁰⁸, 193¹⁰, 194³, 195²⁷, 196¹⁶, 197⁵]

Symmetric designs

The developments of the constructed difference sets split into **1364** isomorphism classes of symmetric designs.

The next table contains the orders of the full automorphism groups and the number of nonisomorphic designs having the full automorphism group of the given order.

As expected, designs with small automorphism groups are numerous, while few of them have large automorphism groups.

Symmetric designs

$ 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 ²
1440	1	93312	1 ³
1728	16	190080	1 ⁴

²Design obtainable by the product method

³Design obtainable by the product method

⁴ $AutD$ is a primitive group containing M_{12} . Corr. DS is in [144,182].

Regular partial difference sets with parameters (144,66,30,30) and (144,65,28,30)

The notion of a difference set is generalized by that of a partial difference set (PDS).

Four parameters determine a PDS.

A (v, k, λ, μ) *partial difference set* S in a group G of order v is a subset $S \subseteq G$ of size k such that every nonidentity element $g \in S$ has exactly λ representations as a quotient $g = xy^{-1}$ using distinct elements x, y of S , and every nonidentity element $g \in G \setminus S$ has exactly μ such representations.

- Any (v, k, λ) difference set is a (v, k, λ, λ) partial difference set.

Partial differential sets S_1 and S_2 in groups G_1 and G_2 , respectively, we will call *equivalent* if there exists a group isomorphism $\varphi : G_1 \rightarrow G_2$ which maps S_1 onto S_2 .

Regular partial difference sets with parameters (144,66,30,30) and (144,65,28,30)

Our further interest sticks only to regular PDSs.

- A partial difference set S is called *reversible* if $S = S^{(-1)} = \{s^{-1} \mid s \in S\}$.
- A reversible partial difference set S is called *regular* if $e \notin S$.

A simple and efficient procedure for the search of regular partial difference sets, starting from a known difference set $\Delta \subseteq G$, consists of the following steps:

Regular partial difference sets with parameters (144,66,30,30) and (144,65,28,30)

Our further interest sticks only to regular PDSs.

- A partial difference set S is called *reversible* if $S = S^{(-1)} = \{s^{-1} \mid s \in S\}$.
- A reversible partial difference set S is called *regular* if $e \notin S$.

A simple and efficient procedure for the search of regular partial difference sets, starting from a known difference set $\Delta \subseteq G$, consists of the following steps:

- construction of all shifts Δx of Δ , $x \in G$,

Regular partial difference sets with parameters (144,66,30,30) and (144,65,28,30)

Our further interest sticks only to regular PDSs.

- A partial difference set S is called *reversible* if $S = S^{(-1)} = \{s^{-1} \mid s \in S\}$.
- A reversible partial difference set S is called *regular* if $e \notin S$.

A simple and efficient procedure for the search of regular partial difference sets, starting from a known difference set $\Delta \subseteq G$, consists of the following steps:

- construction of all shifts Δx of Δ , $x \in G$,
- selection of those shifts which are reversible sets in G ,

Regular partial difference sets with parameters (144,66,30,30) and (144,65,28,30)

Our further interest sticks only to regular PDSs.

- A partial difference set S is called *reversible* if $S = S^{(-1)} = \{s^{-1} \mid s \in S\}$.
- A reversible partial difference set S is called *regular* if $e \notin S$.

A simple and efficient procedure for the search of regular partial difference sets, starting from a known difference set $\Delta \subseteq G$, consists of the following steps:

- construction of all shifts Δx of Δ , $x \in G$,
- selection of those shifts which are reversible sets in G ,
- each shift which does not contain e is a regular (v, k, λ, λ) PDS,

Regular partial difference sets with parameters (144,66,30,30) and (144,65,28,30)

Our further interest sticks only to regular PDSs.

- A partial difference set S is called *reversible* if $S = S^{(-1)} = \{s^{-1} \mid s \in S\}$.
- A reversible partial difference set S is called *regular* if $e \notin S$.

A simple and efficient procedure for the search of regular partial difference sets, starting from a known difference set $\Delta \subseteq G$, consists of the following steps:

- construction of all shifts Δx of Δ , $x \in G$,
- selection of those shifts which are reversible sets in G ,
- each shift which does not contain e is a regular (v, k, λ, λ) PDS,
- each shift which contains e yields a regular $(v, k - 1, \lambda - 2, \lambda)$ PDS $\Delta x \setminus \{e\}$.

Regular partial difference sets with parameters (144,66,30,30) and (144,65,28,30)

To this procedure of "surveyed shifting" we have submitted the constructed difference sets. After MAGMA-testing on group automorphisms, the final result is

2334 inequivalent regular PDSs in 53 groups: $\left\{ \begin{array}{l} \mathbf{1125} \rightsquigarrow (144,66,30,30) \\ \quad \quad \quad + \\ \mathbf{1209} \rightsquigarrow (144,65,28,30) \end{array} \right.$

$[144, id]$ ↓	rPDS ↓	$[144, id]$ ↓	rPDS ↓	$[144, id]$ ↓	rPDS ↓	$[144, id]$ ↓	rPDS ↓
63	6+4	132	16+24	160	6+7	186	124+165
64	15+15	133	14+18	162	26+34	188	5+2
65	33+27	136	24+32	166	8+6	189	7+3
66	8+6	143	20+24	167	59+54	190	3+1
67	6+4	144	32+40	169	16+12	191	30+36
76	6+4	145	20+24	170	18+14	192	44+71
77	8+6	146	6+7	172	59+47	193	4+3
78	6+4	149	16+12	176	4+3	194	0+1
79	15+15	150	6+7	177	36+28	195	7+10
84	33+27	151	59+54	178	4+3	196	40+48
115	60+80	153	58+74	179	18+14	197	5+5
116	16+20	154	97+96	182	1+1		
123	3+3	155	1+1	183	9+3		
129	2+2	159	6+7	184	0+1		

Strongly regular graphs with parameters $(144,66,30,30)$ and $(144,65,28,30)$

For a group G and a set $S \subset G$ with the property that $e \notin S$ and $S = S^{(-1)}$, the Cayley graph $\Gamma = \text{Cay}(G, S)$ over G with connection set S is the graph with vertex set G so that the vertices x and y are adjacent if and only if $x^{-1}y \in S$. Then Γ is undirected graph without loops.

The following assertion⁵ about Cayley graphs holds.

A Cayley graph $\text{Cay}(G, S)$ 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 G .

⁵S.L. Ma, Partial Difference Sets, Discrete Mathematics, 52 (1984), 75-89.

Strongly regular graphs with parameters $(144,66,30,30)$ and $(144,65,28,30)$

- For two inequivalent partial difference sets S_1 and S_2 in a group G , the graphs $\text{Cay}(G, S_1)$ and $\text{Cay}(G, S_2)$ can be isomorphic.
- Similarly, for two inequivalent partial difference sets S_1 and S_2 in groups G_1 and G_2 , $|G_1| = |G_2|$, the graphs $\text{Cay}(G_1, S_1)$ and $\text{Cay}(G_2, S_2)$ can be isomorphic.

The examples of both such cases appeared in our analysis.

Regarding (graph) isomorphism of the corresponding strongly regular Cayley graphs, our regular PDSs split into **121 nonisomorphic SRG-classes**.

43 graphs are with parameters $(144,66,30,30)$ and **78** with parameters $(144,65,28,30)$.

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

$ Aut\Gamma \downarrow \cdot \cdot [144, id] \rightarrow$...	154	182	...	No. of nonisom.
144					2
288		1			2
576		15			26
1152		4			4
1728		1			2
3456		2			2
5184		2			2
10368		2			2
190080			1		1
	...	27	1	...	Total: 43

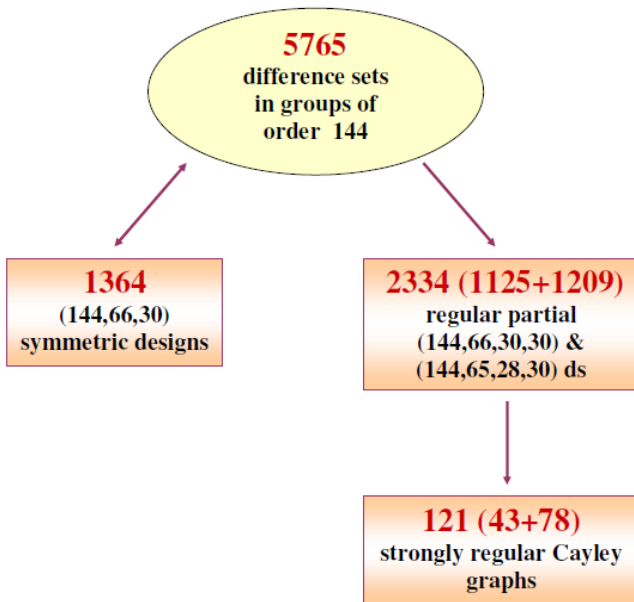
Parameters (144,65,28,30) i.e. VALENCY 65

$ Aut\Gamma \downarrow \cdot \cdot [144, id] \rightarrow$...	154	182	...	No. of nonisom.
144					7
288		8			29
576		15			26
864		1			3
1152		5			5
1440			1		1
1728		2			3
3456		1			1
10368		1			1
15552		1			1
31104		1			1
	...	35	1	...	Total: 78

For instance, even $62=27+35$ nonisomorphic graphs of valencies 66 and 65 can be represented as regular PDSs in the group [144,154].

The MAGMA-files containing records of the constructed nonisomorphic SDs and SRGs are available at the site

http://www.pmfst.hr/~vucicic/MAGMA_REC144/



Thank you!