

COMBINATORICS 2010, Verbania - Italy, June 27 - July 03, 2010

PRIMITIVE SYMMETRIC DESIGNS HAVING UP TO 2500 POINTS

Tanja Vučičić
University of Split, Croatia

June 28, 2010

This is a joint research with S. Braić, A. Golemac and J. Mandić.

S. Braić, A. Golemac, J. Mandić and T. Vučićić, *Primitive Symmetric Designs with Prime Power Number of Points*, Journal of Combinatorial Designs 18 (2010), 141–154.

1 Main result

All symmetric designs with up to 2500 points which admit a point-primitive group of automorphisms (prime number of points excluded) are classified up to a few undecided cases by giving the non-existence proofs or explicit constructions.

There are:

- **60** designs with **affine type** primitive full automorphism group;
- **54** designs with **almost simple** primitive full automorphism group;
- **2** designs with **product** action type primitive full automorphism group.

All designs are **self-dual** and the group action is **block-primitive** as well.

The corresponding DESIGN¹ records are available at the site:

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

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

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

¹ L.H. Soicher, The DESIGN package for GAP, Version 1.3, 2006,
http://designtheory.org/software/gap_design/

2 Preliminaries

The research includes group theory, design theory, theory of difference sets (multiplier theorems), wide-range computer computations in GAP² and the GAP library of primitive permutation groups.

Up to permutation isomorphism, a primitive group in this library is determined by its two parameters:

- v — degree of action;
- nr — the position of the group in the list of primitive groups for degree v .

Our notation: $G(v, nr)$.

² The GAP Group, GAP- groups, algorithms and programming, version 4.4; Aachen, St Andrews, 2006. (<http://www.gap-system.org>)

GAP-command	GAP-output
<code>NrPrimitiveGroups (v)</code>	The number of primitive permutation groups of degree v .
<code>PrimitiveGroup (v, nr)</code>	Primitive permutation group on the position nr for degree v , $1 \leq nr \leq \text{NrPrimitiveGroups}(v)$.

A (v, k, λ) **symmetric design** is a finite incidence structure $D = (P, B)$ consisting of $|P| = v$ points and $|B| = v$ blocks, where each block is incident with k points and any two distinct points are incident with exactly λ common blocks.

An *automorphism* of a symmetric design D is a permutation on P which sends blocks to blocks.

The set of all automorphisms of D forms its full automorphism group commonly denoted by $AutD$.

In geometrical sense, symmetric designs with **transitive** automorphism groups are considerably rich structures.

Here we have been focusing on a subclass of such designs with automorphism groups acting primitively on the point set, called **primitive symmetric designs**.

Our notation:

PSD – primitive symmetric design

3 Primitive group action; examples

Let G denote a transitive permutation group acting on a set X .

A **block** for G is a nonempty subset $\Delta \subseteq X$ with the property that

$$(\forall g \in G) \text{ either } \Delta = \Delta^g \text{ or } \Delta \cap \Delta^g = \emptyset. \quad (1)$$

X itself and all the singletons $\{x\} \subseteq X$ are *trivial* blocks for G . Any other block is called *nontrivial*.

G is called **primitive** if no nontrivial block for G exists in X .

Proposition 3.1 Let G be a permutation group acting transitively on a set X with at least two points. G is primitive if and only if each point stabilizer $G_x, x \in X$, is a maximal subgroup of G .

Proposition 3.2 Let G be a 2-homogeneous permutation group of degree greater than 2. Then G is primitive.

Thus symmetric designs with 2-transitive automorphism groups are examples of primitive designs. These designs are classified by Kantor and they are called **Kantor designs**.

Theorem 3.1 (Kantor³) If D is a (v, k, λ) symmetric design with $v > 2k$ and a 2-transitive automorphism group, then D is one of the following:

- a) $PG(d, q)$,
- b) a unique $(11, 5, 2)$ symmetric design,
- c) a unique $(176, 50, 14)$ symmetric design or
- d) a $(2^{2m}, 2^{m-1}(2^m - 1), 2^{m-1}(2^{m-1} - 1))$ symmetric design, of which there is one for each $m \geq 2$.

³ W. M. Kantor, *Classification of 2-transitive symmetric designs*, Graphs and Combinatorics **1** (1985), 165 – 166.

Another example is provided by Paley difference sets which consist of non-zero squares in $(F_q, +)$, $q = p^m$, $q \equiv 3 \pmod{4}$.

They yield a series of primitive symmetric designs with parameters $(q, \frac{q-1}{2}, \frac{q-3}{4})$ called **Paley designs**.

4 Approach to the problem

We consider all triples (v, k, λ) , $2k < v$ and $v \leq 2499$, which satisfy the well-known necessary conditions for parameters of a symmetric design:

- (1) $\lambda(v - 1) = k(k - 1)$ (Fisher's equality);
- (2) if v is even then $n = k - \lambda$ is a square (Schutzenberger's theorem),
- (3) if v is odd then diophantine equation $x^2 = ny^2 + (-1)^{\frac{v}{2}}\lambda z$ has a non-trivial solution in integers (Bruck-Ryser-Chowla theorem).

We associate each admissible triple with all primitive groups of degree v and explore the possibility of individual group action on a corresponding design. What we examine are couples

$$[(v, k, \lambda), nr].$$

admissible parameters
of a symmetric design

the hypothetical primitive automorphism
group $G = G(v, nr) :=$
 $:= \text{PrimitiveGroup}(v, nr)$ of (v, k, λ) design

Each couple $[(v, k, \lambda), nr]$ we call '**a case**'.

Consideration range:

v range / type	(v, k, λ) total	$[(v, k, \lambda), nr]$ total
$7 \leq v \leq 2499$	2183	29534
$v = p^m, p$ prime , $m \geq 2$	71	14031
$v = p, p$ prime	624	10758
$v \neq p^m, p$ prime , $m \geq 1$	1488	4745

The beginning of our research: we know of the existence of Kantor and Paley primitive symmetric designs with well-known full automorphism groups. In our range of consideration: 41 Kantor-type and 5 Paley-type parameter triples.

KANTOR-type parameter triples:

$35 \times \mathbf{PG}$, (11, 5, 2), (176, 50, 14)
 (16, 6, 2)
 (64, 28, 12)
 (256, 120, 56)
 (1024, 496, 240)

One 2-transitive PSD exists for each parameter triple.

PALEY-type parameter triples:

(27, 13, 6)
 (243, 121, 60)
 (343, 171, 85)
 (1331, 665, 332)
 (2187, 1093, 546)

One 2-homogeneous PSD exists for each parameter triple.

Regarding these parameter triples the question is whether there exist corresponding primitive symmetric designs other than Paley and Kantor designs.

For the remaining parameter triples we have to solve the problem of the *PSDs* existence.

5 Eliminations

5.1 : due to properties of automorphisms of a symmetric design in general

- upper bounds for the fixed points number of a nontrivial automorphism
- the size of orbits of an automorphism group

5.2 : due to regularity

These are characteristic eliminations for **affine type primitive groups**.

In 13135 cases, out of 14031 with prime power number of points, the underlying group is of affine type.

Affine type primitive permutation groups have regular elementary abelian subgroup (the socle), so the theory of difference sets in abelian groups can be applied. From the link between difference sets and symmetric designs we conclude the following.

If in the observed case $[(v, k, \lambda), nr]$ underlying group $G(v, nr)$ is of affine type and (v, k, λ) elementary abelian difference set does not exist then primitive (v, k, λ) symmetric design with automorphism group $G(v, nr)$ does not exist, so we can eliminate the case.

To decide on the existence status of elementary abelian (v, k, λ) difference sets we used:

- numerous **tables of existence**,
- different **necessary existence criteria** (to prove the non-existence of difference sets),
- the theory of multipliers of difference sets, in particular **numerical multipliers**.

Through finding a group of numerical multipliers and by using properties of general multipliers we managed to eliminate many cases with underlying group of affine type.

The well-known First multiplier theorem and Second multiplier theorem give sufficient conditions for positive integer m to be a multiplier of a difference set. They lead to the formula for numerical multiplier m :

$$m \in \bigcap_{\substack{p \\ p|d}} \{p^f \pmod{e} \mid f = 1, \dots, |p|\}, \quad (2)$$

where p and m are coprime with v , and $|p|$ is the multiplicative order of p modulo v . We obtain $m \in \mathbb{Z}$ satisfying the given conditions using programming in GAP.

6 Design construction attempt

To all the cases that survived the described eliminations we applied "*design construction attempt*".

This procedure can be treated as both a general elimination method and a construction method.

Its application in examining the case $[(v, k, \lambda), nr]$ is the following.

We look for a subgroup $H \leq G = G(v, nr)$ which, if $G \leq \text{Aut}D$, fixes at least one block of D . Then H -fixed block, say b , is a union of H -orbits and $\{b^g \mid g \in G\}$ is the set of blocks of D .

Given a subgroup H , one of these two possibilities occur:

- I) For all possible blocks b composed from H -orbits $(\{1, \dots, v\}, \{b^g \mid g \in G\})$ proves not to be a (v, k, λ) symmetric design. Then the particular case $[(v, k, \lambda), nr]$ can be ruled out.
- II) The procedure produces all designs with these data.

Checking in procedure I) can be time and memory consuming computer task so as to grow beyond our computational reach. For our unsolved cases (to be displayed later) it was not feasible and, at the present time, this method is not applicable.

A "good" choice of H , if possible, should ensure that we either rule out the case or perform design constructions in reasonable time.

A choice of a p -group H with $p \nmid v$ ensures that H has a fixed block. Exactly one such block is the most desirable situation.

Therefore, when looking for H , Sylow p -subgroups of G are of our interest. If for a prime $p, p \nmid v$, and $A \in \text{Syl}_p(G)$ there exists an element $g \in A \leq G$ fixing exactly one point, then we easily prove that $N_G(A)$ fixes exactly one block.

Choosing $H = N_G(A)$ is usually sufficient for our methods.

However, some more complicated situations occurred in H -choices which we managed to solve theoretically.

Also, for some groups $G = G(v, nr)$ **GAP-Tables of Marks** contain the necessary data so that we can call in GAP the representatives of all conjugacy classes of G -subgroups of index v which are the candidates for H .

6.1 RESULTS FOR $v = p^m, m > 1$

Positive results are obtained only for Paley and Kantor-type parameters. The results suggest for instance that primitive symmetric designs with p^m points, $m \geq 2$, which are not projective geometries, should either have the parameters of Paley designs or p should be 2.

Except for projective geometry $(121, 40, 13)$, the full automorphism groups of all the designs obtained are of affine type.

- **Paley type parameters** - **31** selfdual designs are constructed.

parameters	cases total	designs total	not solved " nr "
$(27, 13, 6)$	15	1	\emptyset
$(243, 121, 60)$	36	2	\emptyset
$(343, 171, 85)$	90	14	\emptyset
$(1331, 665, 332)$	92	13	1
$(2187, 1093, 546)$	73	1	\emptyset

A brief structural description of full automorphism groups of the obtained designs other than Paley ones is given in the following table. The designs are denoted as in web files.

design D	$Aut D$ id.	S	S -orbit lengths	S_b -orbit lengths
$D243[1]$	$G(3^5, 3)$	$C_{11} \rtimes C_5$	$1^1 11^2 55^4$	$11^1 55^2$
$D343[1] - [2]$	$G(7^3, 38)$	$C_3 wr C_3$	$1^1 9^2 27^6 81^2$	$9^1 27^3 81^1$
$D343[4]$	$G(7^3, 23)$	$C_9 \rtimes C_3$	$1^1 9^2 27^{12}$	$9^1 27^6$
$D343[5] - [14]$	$G(7^3, 15)$	C_9	$1^1 9^{38}$	9^{19}
$D1331[1] - [2]$	$G(11^3, 34)$	$C_5 \times (C_5^2 \rtimes C_3)$	$1^1 15^2 75^4 125^2 375^2$	$15^1 75^2 125^1 375^1$
$D1331[4] - [6]$	$G(11^3, 31)$	$C_5 \times (C_{19} \rtimes C_3)$	$1^1 95^2 285^4$	$95^1 285^2$
$D1331[7] - [11]$	$G(11^3, 18)$	$C_5 \times (C_7 \rtimes C_3)$	$1^1 35^2 105^{12}$	$35^1 105^6$
$D1331[12] - [13]$	$G(11^3, 112)$	C_{95}	$1^1 95^{14}$	95^7

Conjecture. If D is a primitive design with Paley type parameters, then there exist integers d_1, \dots, d_t and k_1, \dots, k_t , $d_i > 1$, $k_i \geq 1$, such that orbit structure of point stabilizer $S \leq Aut D$ is $1^1 d_1^{2k_1} \dots d_t^{2k_t}$, and block stabilizer $S_b \leq Aut D$ orbit structure on block points is $d_1^{k_1} \dots d_t^{k_t}$.

- **Kantor-type parameters** - **30** selfdual designs are constructed.

parameters	cases total	designs total	Not solved
(16, 6, 2)	22	1	\emptyset
(64, 28, 12)	74	1	\emptyset
(121, 40, 13)	57	1	\emptyset
(256, 120, 56)	244	5	\emptyset
(1024, 496, 240)	115	22	1, 2, 3, 5, 6

For Kantor designs with $v = 2^m$, $m = 4, 6, 8$, and 10 the full group structure is $F_2^m \rtimes Sp_m(F_2)$, where $Sp_m(F_2)$ is a symplectic group.

For Kantor design with $v = 121$ the full group is $PSL_5(3)$.

An analysis of the full group structure of the other obtained designs is given in the following tables.

design D	$Aut D$ id.	S	S -orbit lengths	S_b -orb. lengths
$D256[2]$	$G(2^8, 80)$	$D_{10} wr C_2$	$1^1 10^3 25^3 50^3$	$10^2 25^2 50^1$
$D256[3]$	$G(2^8, 63)$	$ S = 2^4 \cdot 3^4$	$1^1 12^1 27^1 54^2 108^1$	$12^1 54^2$
$D256[4]$	$G(2^8, 119)$	$(C_5 \rtimes C_4) \times D_6$	$1^1 15^1 30^2 60^3$	$30^2 60^1$
$D256[5]$	$G(2^8, 112)$	$C_3 \times D_{10} \times D_6$	$1^1 30^1 45^1 90^2$	$30^1 90^1$

design D	$Aut D$ id.	S	S -orbit lengths	S_b -orbit lengths
$D1024[2]$	$G(2^{10}, 54)$	$PSL_2(11) \rtimes C_2$	$1^1 22^1 55^2 66^1 110^1 165^1 220^1 330^1$	$1^1 55^1 110^1 330^1$
$D1024[3] - [6]$	$G(2^{10}, 8)$	$(C_{11} \rtimes C_5) \rtimes C_2$	$1^1 11^1 22^1 55^6 110^6$	$1^1 55^3 110^3$
$D1024[7] - [22]$	$G(2^{10}, 4)$	$C_{11} \rtimes C_5$	$1^1 11^3 55^{18}$	$1^1 55^9$

6.2 RESULTS FOR $v \neq p^m$

53 des. with almost simple primitive gr. + **2** des. with product type primitive gr.

I. 53 designs with almost simple primitive groups: **47** in **5** series + **6** designs

parameters of D / (number of D_s)	$AutD$	rank	description and properties
$\left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right) / (34)$	$P\Gamma L_{d+1}(q)$	2	$PG(d, q)$, $d \geq 2$, flag and antiflag-tr.
$\left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right) / (7)$	$P\Gamma O_{d+2}(q)$	3	Orthogonal SD of Higman, d, q odd, $d \geq 3$, antiflag-tr.
$\left(\frac{3^m(3^m-1)}{2}, \frac{3^{m-1}(3^m+1)}{2}, \frac{3^{m-1}(3^{m-1}+1)}{2}\right) / (2)$	$PO_{2m+1}(3)$	3	$m > 1$, flag-tr.
$\left(\frac{3^m(3^m+1)}{2}, \frac{3^{m-1}(3^m-1)}{2}, \frac{3^{m-1}(3^{m-1}-1)}{2}\right) / (2)$	$PO_{2m+1}(3)$	3	$m > 1$, flag-tr.
$\left(\frac{q^6-1}{q-1}, \frac{q^5-1}{q-1}, \frac{q^4-1}{q-1}\right) / (2)$	$AutG_2(q)$	4	$D(H(q)^*)$ from general. hexagons, $q = p^\alpha$, $p \neq 3$, antiflag-tr.

- Hadamard design $(35, 17, 8)$, antiflag,

3	4	1	2
A_7	S_7	A_8	S_8
4	4	3	3

- Menon design $(36, 15, 6)$, antiflag,

6	7
$PSU_3(3)$	$PSU_3(3) \cdot 2$
4	3

- Biplane $(56, 11, 2)$, antiflag,

1	2	3	4	5
$PSL_3(4)$	$PSL_3(4) \cdot 2$	$PSL_3(4) \cdot 2$	$PSL_3(4) \cdot 2$	$PSL_3(4) \cdot 2^2$
3	3	3	3	3

- Menon design $(144, 66, 30)$, flag,

3	4
M_{12}	$M_{12}.2$
5	4

.

$AutD_{144}[1]$ has two regular subgroups.

Besides projective geometries this is the only design with almost simple primitive automorphism group that has regular subgroup;

- Menon design $(144, 66, 30)$, flag,

5
$M_{12}.2$
4

;

- $(176, 50, 14)$ design with Kantor-type parameters, flag and antiflag,

3	4
M_{22}	HS
3	2

.

II. 2 Menon designs with 1296 points

Symmetric designs of Menon family have parameters of the form $(4t^2, 2t^2 - t, t^2 - t)$. We constructed

- two $(36, 15, 6)$ Menon designs ($t = 3$);
- two $(144, 66, 30)$ Menon designs ($t = 6$).

"Product" of Menon designs $D_i = (P_i, B_i)$, $i = 1, 2$ with $t = t_i$ is a new Menon design $D_1 \otimes D_2 = (P, B)$ with $t = 2t_1t_2$, where $P = P_1 \times P_2$ and $B = \{(B_1 \times B_2^c) \cup (B_1^c \times B_2) \mid B_1 \in B_1, B_2 \in B_2\}$. If $G_1 \leq \text{Aut}D_1$ and $G_2 \leq \text{Aut}D_2$ then $G_1 \times G_2 \leq \text{Aut}(D_1 \otimes D_2)$.

Product $D^{\otimes n} = D \otimes D \otimes \cdots \otimes D$ of n copies of a primitive Menon design $D = (P, B)$ is primitive as well. Namely, if G acts primitively on P then wreath product $G \text{ wr } S_n = (G \times \cdots \times G) \rtimes S_n$ is a subgroup of $\text{Aut}D^{\otimes n}$ with product type primitive action on $P \times \cdots \times P$ (primitive type III(b)).

Therefore each of our four constructed Menon designs yields an infinite series ($n \geq 2$) of Menon designs with product type primitive automorphism groups.

Applying "design construction attempt" we obtained exactly two nonisomorphic Menon designs with 1296 points ($t = 18$) and product type primitive groups. These are "squares" of Menon designs with 36 points, the first designs of the cited series. So we indirectly proved that the product of two different primitive Menon designs is not necessarily primitive.

The number of points of the next designs in these series ($n = 3$) exceeds the range of our research. The same happens with the first designs in two series originated by Menon designs with 144 points. Precisely, if D has $v = 4t^2$ points then the number of points of $D^{\otimes n}$ is $4(2^{n-1}t^n)^2$.

All primitive group actions on these designs we present by the following two tables:

	27	36	37	47
$D1296[1]$:	$PSU_3(3)^2 .2$	$PSU_3(3)^2 .4$	$PSU_3(3)^2 .2^2$	$PSU_3(3)^2 .D_8$,
	10	6	7	6

$$AutD1296[1] \cong G(36, 7) \text{ wr } S_2, G(36, 7) \cong AutD36[1].$$

	69	74	75	77
$D1296[2]$:	$PSp_4(3)^2 .2$	$PSp_4(3)^2 .4$	$PSp_4(3)^2 .2^2$	$PSp_4(3)^2 .D_8$,
	6	6	6	6

$$AutD1296[2] \cong G(36, 9) \text{ wr } S_2, G(36, 9) \cong AutD36[2].$$

Designs $D1296[1]$ and $D1296[2]$ are neither flag nor antiflag-transitive.

7 Undecided cases

In the sense that we could not rule them out and that design constructions are not feasible as yet, unsolved remain:

1⁰) 5 cases with affine type primitive groups ($v = p^m, m > 1$)

$$(729, 273, 102), nr = 330;$$

$$(2197, 793, 286), nr = 1, 2, 8, 20.$$

The reduction with minimal primitive groups is applied.

2⁰) 12 cases with almost simple type primitive groups ($v \neq p^m$)

case: $[(v, k, \lambda), nr]$	$G(v, nr)$	case: $[(v, k, \lambda), nr]$	$G(v, nr)$
$[(1600, 780, 380), 17]$	$G(1600, 17) = PSU(3, 4)$	$[(1431, 495, 171), 1]$	$G(1431, 1) = PSL(2, 53)$
$[(1456, 195, 26), 1]$	$G(1456, 1) = Suz(8)$	$[(1711, 855, 427), 2]$	$G(1711, 2) = PSL(2, 59)$
$[(1456, 162, 324), 1]$	$G(1456, 1) = Suz(8)$	$[(1770, 610, 210), 1]$	$G(1770, 1) = PSL(2, 59)$
$[(2080, 540, 140), 1]$	$G(2080, 1) = Suz(8)$	$[(1830, 590, 190), 1]$	$G(1830, 1) = PSL(2, 61)$
$[(1128, 392, 136), 1]$	$G(1128, 1) = PSL(2, 47)$	$[(2016, 651, 210), 1]$	$G(2016, 1) = PSL(2, 64)$
$[(1176, 376, 120), 1]$	$G(1176, 1) = PSL(2, 49)$	$[(2211, 715, 231), 1]$	$G(2211, 1) = PSL(2, 67)$

It is easily checked that flag or antiflag-transitivity is not possible in any of the unsolved cases. This means that we have constructed and described all flag and antiflag-transitive primitive symmetric designs with $v < 2500$.

Many successful constructions led to isomorphic designs. For isomorphic structures reduction we used DESIGN package.

The files with DESIGN-records of 116 constructed nonisomorphic designs are available at the site:

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

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

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

where there is an "info" file with instructions how to use the data.