GLASNIK MATEMATIČKI
Vol. 45(65)(2010), 291 – 305

PRIMITIVE SYMMETRIC DESIGNS WITH AT MOST 255 POINTS

Snježana Braić
University of Split, Croatia

Abstract. In this paper we either prove the non-existence or give explicit construction of all (v, k, λ) symmetric designs with primitive automorphism groups of degree $v \leq 255$. We prove that, up to isomorphism, there exist exactly 142 such designs. The research involves programming and wide-range computations. We make use of software package GAP and the library of primitive groups which it contains.

1. Introduction

Primitive symmetric designs, meaning symmetric designs with automorphism groups acting primitively on the point set, form one important subclass of transitive symmetric designs. It is known that 2-transitive symmetric designs are classified by Kantor ([11]). These designs are called Kantor designs. They are examples of primitive designs because 2-transitive groups are primitive. Another example is provided by Paley difference sets; they yield a series of primitive symmetric designs called Paley designs. The parameter triples of Paley and Kantor designs we call Paley type and Kantor type parameters, respectively.

This research considers (v, k, λ) symmetric designs with primitive automorphism groups of degree $v \leq 255$. All designs with this property are constructed and classified. We confine ourselves to $v > 2k$ because the complement of a primitive design is also primitive with the same full automorphism group. The final result is:

2010 *Mathematics Subject Classification.* 05B05, 05B10.
Key words and phrases. Symmetric design, primitive automorphism group, difference set.

THEOREM 1.1. *Up to isomorphism, there exist exactly* 71 *primitive* (v, k, λ) *symmetric designs with* 57 *different parameter triples for* $2k < v \leq 255$. *The full automorphism groups of all obtained designs are of affine or almost simple primitive type. All designs are selfdual and the full automorphism group also acts primitively on blocks.*

Detailed results are presented in Section 6.

2. Notation and preliminaries

In this section we recall just a few definitions and facts from group theory and design theory that are relevant for our study. We assume that the reader is acquainted with the basic facts of design theory ([1, 4]), group theory ([3, 8]), and theory of difference sets, with the emphasis on multiplier theorems ([1, 12]). Our notation and terminology is common, in accordance with the cited literature.

2.1. *Primitive group action.* The analysis of primitive groups in terms of their socles provides a natural approach to their classification. Generally, the *socle* of a finite nontrivial group G, denoted by $soc(G)$, is the subgroup generated by the set of all minimal normal subgroups of G. If G is a primitive group then socle of G is the direct product of m copies of some simple group T, i.e., $soc(G) \cong T^m$. According to O'Nan-Scott Theorem ([8]), all finite primitive groups can be classified into the five following types: affine type, regular nonabelian type, almost simple type, diagonal type and product type. For our research only primitive groups of affine and almost simple type are important because they appear as full automorphism groups of our obtained designs.

2.2. *Symmetric designs.* A (v, k, λ) *symmetric design* is a finite incidence structure $D = (V, \mathcal{B})$ consisting of $|V| = v$ points and $|\mathcal{B}| = v$ blocks, where each block is incident with k points and any two distinct points are incident with exactly λ common blocks. The value $n = k - \lambda$ is the *order* of D. An *automorphism* of D is a permutation on V which sends blocks to blocks. The full automorphism group of D, denoted by $Aut\ D$, is the group of all automorphisms of D. Throughout the paper we denote a point stabilizer by $S \leq Aut\ D$.

The following theorem gives a complete classification of symmetric designs with 2-transitive automorphism groups.

THEOREM 2.1 (Kantor, [11]). *If D is a (v, k, λ) symmetric design with $2-$transitive automorphism group and $v > 2k$, then D is one of the following:*

a) $PG(n, q)$,
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* $m \geq 2$.

Note that Kantor's theorem also describes all primitive k-transitive symmetric designs for all $k > 2$.

DEFINITION 2.2. *Let* G *be a finite group of order* v. *A* (v, k, λ) ***difference set*** *in* G *is a* k*-subset* Ω *of* G *provided that the multiset* $\{xy^{-1} \mid x, y \in \Omega, x \neq y\}$ *contains each nonidentity element of* G *exactly* λ *times. The* ***development*** *of* Ω *is the incidence structure dev* $\Omega = (G, \{\Omega g \mid g \in G\})$.

The following theorem describes the relation between symmetric designs and the development of difference sets.

THEOREM 2.3 ([1, p. 299]). *Let* G *be a finite group of order* v *and* Ω *a proper, non-empty* k*-subset of* G. *Then* Ω *is a* (v, k, λ) *difference set in* G *if and only if dev* Ω *is a* (v, k, λ) *symmetric design on which* G *acts regularly.*

EXAMPLE 2.4. Let q be a prime power and $q \equiv 3 (\mathrm{mod}\, 4)$. Then quadratic residues $\{x^2 : x \in F_q \setminus \{0\}\}$ in additive group of the finite field F_q form the well-known Paley difference set with the parameter triple $(q, \frac{q-1}{2}, \frac{q-3}{4})$. The development of Paley difference set is a symmetric design with the 2-homogeneous full automorphism group. This group is precisely described in subsection 6.1. Note that Paley designs, yielded by Paley difference sets, are primitive.

3. Approach to the problem

In our study we make use of the software package GAP ([9]), the well-known system for computational group theory, especially the GAP-library of primitive groups. In the library, groups are arranged according to the degree v of group action on the set $\{1, \ldots, v\}$ and no two groups of the same degree are conjugate. The GAP-command `NrPrimitiveGroups(`v`)` returns the number of primitive groups of degree v. Note that `NrPrimitiveGroups(`v`)`≥ 2 for all $v \geq 3$ (namely, A_v and S_v are primitive groups of degree v). The command `PrimitiveGroup(`v, nr`)`for $1 \leq nr \leq$ `NrPrimitiveGroups(`v`)`, returns the primitive group of degree v with number nr from the library's list; the returned group is unique up to permutation isomorphism.

At the start of the research we find all triples (v, k, λ), $2k < v \leq 255$, which satisfy the following 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 the diophantine equation $x^2 = ny^2 + (-1)^{\frac{v-1}{2}} \lambda z$ has a non-trivial solution in integers (Bruck-Ryser-Chowla theorem).

There are 179 such parameter triples obtained by GAP-programming. The corresponding code can be found at the following site

(∗) `http://www.pmfst.hr/~sbraic/PrimitiveSD_at_most_255/`

in the file *Program_for_necessary_conditions*. Next, we eliminate 39 parameter triples with `NrPrimitiveGroups(`v`)`$= 2$ because A_v and S_v cannot act as automorphism groups of a symmetric design with v points ([1, p. 174]). The remaining 140 parameter triples are given in Table 1. There are 30 Paley type and 22 Kantor type parameter triples in our range of consideration; 4 of them are both Paley and Kantor type. In Table 1 they are labelled by the superscripts "P" and "K", respectively. For them we have to check whether there exist corresponding primitive symmetric designs other than Paley and Kantor designs, while for the other parameters we have to solve the question of the existence of corresponding primitive symmetric designs. For 31 parameters labelled in Table 1 by the subscript "E" we prove that primitive symmetric designs do not exist; this elimination will be explained in subsection 4.3.

$(7,3,1)^{K,P}$,	$(11,5,2)^{K,P}$,	$(13,4,1)^{K}$,	$(15,7,3)^{K}$,	$(16,6,2)^{K}$,
$(19,9,4)^{P}$,	$(21,5,1)^{K}$,	$(23,11,5)^{P}$,	$(25,9,3)$,	$(27,13,6)^{P}$,
$(31,6,1)^{K}$,	$(31,10,3)_{E}$,	$(31,15,7)^{K,P}$,	$(35,17,8)$,	$(36,15,6)$,
$(37,9,2)$,	$(40,13,4)^{K}$,	$(41,16,6)_{E}$,	$(43,21,10)^{P}$,	$(45,12,3)$,
$(47,23,11)^{P}$,	$(49,16,5)$,	$(55,27,13)$,	$(56,11,2)$,	$(57,8,1)^{K}$,
$(59,29,14)^{P}$,	$(61,16,4)_{E}$,	$(61,25,10)_{E}$,	$(63,31,15)^{K}$,	$(64,28,12)^{K}$,
$(66,26,10)$,	$(67,33,16)^{P}$,	$(71,15,3)_{E}$,	$(71,21,6)_{E}$,	$(71,35,17)^{P}$,
$(73,9,1)^{K}$,	$(78,22,6)$,	$(79,13,2)_{E}$,	$(79,27,9)_{E}$,	$(79,39,19)^{P}$,
$(81,16,3)$,	$(83,41,20)^{P}$,	$(85,21,5)^{K}$,	$(85,28,9)$,	$(85,36,15)$,
$(91,10,1)^{K}$,	$(91,45,22)$,	$(97,33,11)_{E}$,	$(100,45,20)$,	$(101,25,6)$,
$(103,34,11)_{E}$,	$(103,51,25)^{P}$,	$(105,40,15)$,	$(107,53,26)^{P}$,	$(109,28,7)$,
$(112,37,12)$,	$(113,49,21)_{E}$,	$(119,59,29)$,	$(120,35,10)$,	$(121,16,2)$,
$(121,25,5)$,	$(121,40,13)^{K}$,	$(127,28,6)_{E}$,	$(127,36,10)_{E}$,	$(127,63,31)^{K,P}$,
$(131,26,5)_{E}$,	$(131,40,12)_{E}$,	$(131,65,32)^{P}$,	$(133,12,1)^{K}$,	$(133,33,8)$,
$(135,67,33)$,	$(139,24,4)_{E}$,	$(139,46,15)_{E}$,	$(139,69,34)^{P}$,	$(144,66,30)$,
$(149,37,9)_{E}$,	$(151,51,17)$,	$(151,75,37)^{P}$,	$(153,57,21)$,	$(155,22,3)$,
$(155,56,20)$,	$(155,77,38)$,	$(156,31,6)^{K}$,	$(157,13,1)_{E}$,	$(163,81,40)^{P}$,
$(165,41,10)$,	$(167,83,41)^{P}$,	$(169,49,14)$,	$(169,57,19)$,	$(169,64,24)$,
$(171,35,7)$,	$(171,51,15)$,	$(171,85,42)$,	$(175,30,5)$,	$(175,87,43)$,
$(176,50,14)^{K}$,	$(179,89,44)^{P}$,	$(181,36,7)_{E}$,	$(181,81,36)$,	$(183,14,1)^{K}$,
$(183,91,45)$,	$(191,20,2)_{E}$,	$(191,76,30)$,	$(191,95,47)^{P}$,	$(193,64,21)_{E}$,
$(196,91,42)$,	$(197,49,12)$,	$(199,45,10)_{E}$,	$(199,55,15)$,	$(199,99,49)^{P}$,
$(203,101,50)$,	$(208,46,10)$,	$(210,77,28)$,	$(211,21,2)_{E}$,	$(211,70,23)$,
$(211,91,39)_{E}$,	$(211,105,52)^{P}$,	$(220,73,24)$,	$(223,37,6)_{E}$,	$(223,75,25)_{E}$,
$(223,111,55)^{P}$,	$(225,64,18)$,	$(227,113,56)^{P}$,	$(229,57,14)$,	$(229,76,25)$,
$(231,46,9)$,	$(231,70,21)$,	$(231,115,57)$,	$(239,35,5)_{E}$,	$(239,85,30)$,
$(239,119,59)^{P}$,	$(241,16,1)_{E}$,	$(241,81,27)_{E}$,	$(241,96,38)_{E}$,	$(243,121,60)^{P}$,
$(251,125,62)^{P}$,	$(253,28,3)$,	$(253,36,5)$,	$(253,64,16)$,	$(255,127,63)^{K}$

TABLE 1

In the next step we associate every triple (v,k,λ) from Table 1 with all primitive groups of degree v. In other words, we go through the values of couples $[(v,k,\lambda),nr]$ where parameter triple (v,k,λ) is taken from Table 1 and nr stands for the hypothetical primitive automorphism group $G(v,nr)$:=`PrimitiveGroup`(v,nr) of a (v,k,λ) design. Each such couple we call 'a case'. Using GAP-programming we obtain 2061 cases $[(v,k,\lambda),nr]$ to examine. The record of all these cases is available at the site $(*)$ in the file *All_cases*.

The starting point for solving these large number of cases is the Kantor's result. If the primitive group $G(v,nr)$, related to case $[(v,k,\lambda),nr]$, is t-transitive with $t\geq 2$, that case is analysed in accordance with Kantor's theorem.

v range / type	(v,k,λ) total	$[(v,k,\lambda),nr]$ total	
$2k<v\leq 255$	140	$t=1:1512$ $t\geq 2:\ 549$	2061 total

TABLE 2.

4. Elimination

We continue our research with elimination attempts. Some cases can be eliminated immediately. Namely, cases with at least 2-transitive groups corresponding to the parameters which are not Kantor type can be discarded from further consideration. Furthermore, we rule out the cases where $G(v,nr)$ is A_v or S_v. Thus we eliminate 468 out of 549 cases with at least 2-transitive groups.

We use three elimination criteria on 1512 cases $[(v,k,\lambda),nr]$, where related primitive group $G(v,nr)$ is exactly 1-transitive. The first two criteria refer to the properties of automorphisms of a symmetric design. In the first criterion we check the bounds for the fixed points number of a nontrivial automorphism (Proposition 4.1 and Proposition 4.2) and, in the second, the size of orbits of an automorphism group (Theorem 4.3). The third elimination criterion is based on the link between difference sets and symmetric designs (Theorem 2.3).

Compared to the other criteria applied, elimination through checking the number of fixed points proves to be the most efficient.

4.1. *Elimination due to the number of fixed points.* We use the following facts.

PROPOSITION 4.1 ([12, p. 82], [13, p. 33]). *Let D be a (v,k,λ) symmetric design of order n and let $g\in Aut\ D$ be a nonidentity automorphism with the*

set $Fix(g)$ of the points it fixes. Then

$$|Fix(g)| \leq v - 2n \quad \text{and} \quad |Fix(g)| \leq k + \sqrt{n}.$$

If $|Fix(g)| = v - 2n$ or $|Fix(g)| = k + \sqrt{n}$, then g is an involution and each non-fixed block contains exactly λ fixed points.

PROPOSITION 4.2 ([12, p. 155]). *Let D be a (v, k, λ) symmetric design and $g \in Aut\ D$ an involution. Then*

$$|Fix(g)| = 0 \quad or \quad |Fix(g)| \geq \begin{cases} 1 + \dfrac{k}{\lambda}, & k, \lambda \quad both\ even \\ 1 + \dfrac{k-1}{\lambda}, & otherwise. \end{cases}$$

The number of fixed points of some automorphism of prime order is greater than the number of fixed points of any nonidentity automorphism, so the above conditions is enough to check for automorphisms of prime order. Further, if $|Fix(g)| = 0$ the propositions hold. Therefore, we check the conditions for prime order automorphisms $g \in S \leq Aut\,(D)$. Moreover, due to the transitivity it is enough to consider the stabilizer of some special point, say 1.

The list of thus eliminated cases is given at the site $(*)$ in the file *Fixed_points*.

4.2. *Elimination due to the size of point and block orbits.*

THEOREM 4.3 ([12, p. 98]). *Let D be a symmetric (v, k, λ) design of order n and let $H \leq Aut\ D$ be its automorphism group. Let H have the orbits of size $s_1, \ldots, s_m$ on points and of size $t_1, \ldots, t_m$ on blocks. Then*

$$\frac{n^{m+1} t_1 \cdot \ \cdots \ \cdot t_m}{s_1 \cdot \ \cdots \ \cdot s_m}$$

is the square of an integer.

We make use the above theorem by applying its statement in an equivalent form. Namely, whenever it is possible to find a subgroup $H \leq G = G\,(v, nr) \leq Aut\ D$ with an even number of orbits on V, for which there exist a prime p and $l \in N \cup \{0\}$ such that $p^{2l+1} \mid n$, $p^{2l+2} \nmid n$, and $p \nmid |H|$, then Theorem 4.3 ensures that (v, k, λ) symmetric design D with the automorphism group G does not exist, so we can rule out the case $[(v, k, \lambda), nr]$. The cases eliminated in this way are stored at the site $(*)$ in the file *Size_of_orbits*.

4.3. *Elimination due to regularity.* From Theorem 2.3 we conclude that if a primitive group $G = G\,(v, nr)$ has a regular subgroup H and a (v, k, λ) difference set in H does not exist then primitive (v, k, λ) symmetric design having G as automorphism group does not exist so we can eliminate the case $[(v, k, \lambda), nr]$.

Generally, it is not easy to check whether a group has a regular subgroup or not. However, it is known that groups which have a prime degree contain

a regular subgroup. Hence, for a prime v, we can eliminate the parameter triple (v, k, λ) if (v, k, λ) difference set does not exist.

Furthermore, for $v = p^m$ every affine type group $G(v, nr)$ contains regular elementary abelian subgroup F_p^m, so the non-existence of the corresponding elementary abelian difference set eliminates the case $[(v, k, \lambda), nr]$.

The existence status of abelian (v, k, λ) difference sets is rather well documented in numerous tables of existence in literature ([1, 4, 12]). Besides, we made use of the following necessary existence criterion to prove the non-existence of difference sets.

THEOREM 4.4 ([12, p. 131 and 134]). *Let Ω be a (v, k, λ) difference set in a group G. If for some divisor w of v, $w \in \mathbb{N}$, $w > 1$, and some prime p there exists an integer $j \in \mathbb{Z}$ such that $p^j \equiv -1 \pmod{w}$, then p does not divide the squarefree part of n.*

Moreover, if G is abelian with $w = \exp(G)$ and p does not divide w, then p does not divide the order n.

Hence, if a prime p divides the squarefree part of n, if w divides v and also $p^j \equiv -1 \pmod{w}$ for some integer j, then (v, k, λ) difference set in groups of order v does not exist.

By applying Theorem 4.4 or the aforementioned tables we proved the non-existence of difference sets for 31 out of 73 parameter triples (v, k, λ) which have a prime v. Consequently, all these parameters are ruled out. In the Table 1 they are labelled by the subscript "E". Furthermore, the non-existence of difference sets with parameters $(25, 9, 3)$, $(55, 27, 13)$, $(121, 16, 2)$, $(121, 25, 5)$, $(169, 49, 14)$, $(169, 57, 19)$ and $(169, 64, 24)$ was determined, as well as the non-existence of the elementary abelian $(81, 16, 3)$ difference set. For each of these parameters we determined that their remaining corresponding primitive groups have a regular elementary abelian subgroup; so we eliminated all these parameters.

The $(121, 40, 13)$ difference set in elementary abelian group F_{11}^2 does not exist ([1]). This fact directly eliminated three cases $[(121, 40, 13), nr]$, $nr = 1$,12 and 47 because the corresponding primitive groups have the regular elementary abelian subgroup F_{11}^2 (we checked that $G(121, 47) = PSL(2, 11)$ has the regular subgroup F_{11}^2, whereas $G(121, 1)$ and $G(121, 12)$ are of affine type).

The parameter triple $(100, 45, 20)$ includes four cases in which primitive groups are not of affine type, but we checked that these groups have a regular subgroup H and a difference set in H does not exist; so we can rule out these cases.

The all eliminated cases are stored at the site $(*)$ in the file *Regularity*.

After all elimination criteria is applied, 1097 cases are eliminated.

5. Design construction attempts

Using our computer programs for design construction we solved 496 remaining cases. We use one of two algorithms for construction of (v, k, λ) symmetric design with an automorphism group $G := G(v, nr)$ depending on wherther v is a prime or not. If v is not a prime, the algorithm is based on finding a suitable cyclic subgroup of a point stabilizer in G. Otherwise, the algorithm is based on the results of difference set theory, more precisely, on the theory of multipliers. We used the DESIGN package ([14]) to reduce the obtained designs up to isomorphism.

5.1. *Design construction based on a subgroup of a point stabilizer.* This construction is applied on all 308 cases $[(v, k, \lambda), nr]$ for which v is not a prime. The procedure is the following: we look for a subgroup $H \leq G := G(v, nr)$ which, if $G \leq Aut\ D$, fixes at least one block of D. Then a H-fixed block B of length k is a union of H-orbits and $\mathcal{B} = \{B^g \mid g \in G\}$ is the set of blocks of D. If for an intended block B composed from H-orbits the corresponding $\mathcal{B}$ satisfies the conditions:

1. $|\mathcal{B}| = v$,
2. $|B_i \cap B_j| = \lambda$ for all $B_i, B_j \in \mathcal{B}$, $B_i \neq B_j$ (λ balance),
3. $|\{B_i \in \mathcal{B} \mid 1 \in B_i\}| = k$,

the structure $(\{1, \ldots, v\}, \mathcal{B})$ is a (v, k, λ) symmetric design with automorphism group G. Thus we obtain all (v, k, λ) symmetric designs which have the group G as the automorphism group. Otherwise, if for all possible blocks B the above conditions do not hold, the structure $(\{1, \ldots, v\}, \mathcal{B})$ is not a (v, k, λ) symmetric design and the case $[(v, k, \lambda), nr]$ can be ruled out.

The existence of at least one fixed block for a chosen subgroup $H \leq G$ is the starting point for applying this method. A choice of a cyclic group $H = \langle g \rangle$, $1 \neq g \in S$ ensures that H has a fixed block because a cyclic automorphism group fixes equal number of points and blocks. Hence, it can be a "good" choice of H. But, the efficiency in the application of this method depends on the number of H-orbits, i.e., on H-orbit lengths. A "good" choice of H, if possible, should ensure that we either rule out the case or perform design constructions in reasonable time. It is not convenient for H to have a large number of small orbits. In that case we deal with a huge number of possibilities for forming a H-fixed block B from H-orbits. Checking for all possible B that $\mathcal{B}$ is not the set of design blocks, so as to rule out the case, is both a time and memory consuming computer task. If it is not feasible, this method is not applicable. Alternatively, we use the following fact.

Lemma 5.1. *Let H be a p-group acting on a set X. Then for the set $X_0 \subset X$ of its fixed elements we have $|X| \equiv |X_0| \pmod{p}$.*

From this lemma we conclude that p-group $H < G$ with $p \nmid v$ surely has a fixed block. Consequently, when looking for H, Sylow p-subgroups of G, $p \nmid v$, can be used as H.

Applying this method of construction, 73 out of 308 cases are eliminated and exactly 28 nonisomorphic primitive symmetric designs with 22 different parameter triples are constructed.

5.2. *Design construction based on a difference set.* The method of design construction described above is useless when the point stabilizer is of small order or trivial which occurs when v is a prime. In these 188 cases, algorithm of construction involves the theory of multipliers of a difference set.

For a chosen prime v, all primitive groups of degree v have, up to permutation isomorphism, the same regular subgroup C_v, which is also primitive. This fact boils down our search for all primitive symmetric designs with prime number of points v to construction of (v, k, λ) symmetric designs under the action of regular group C_v only; i.e., to 44 cases. The full automorphism group of each thus obtained design will have all other primitive groups of degree v acting on (v, k, λ) symmetric designs as its subgroups. Hence, we confine the research to looking for cyclic difference sets in group C_v. In effort to solve 44 cases with v prime and $G(v, nr) = C_v$, we applied the theory of multipliers of difference sets, in particular we used numerical multipliers.

DEFINITION 5.2. *Let Ω be a (v, k, λ) difference set in a group G. An automorphism $\alpha \in \mathrm{Aut}(G)$ is called a* ***multiplier*** *of Ω if there exist $a, b \in G$ with $\Omega^\alpha = a\Omega b$. If a multiplier $\alpha \in \mathrm{Aut}(G)$ is of the form $x \overset{\alpha}{\mapsto} x^m$ for some $m \in \mathbb{Z}$, then α is called a* ***numerical multiplier*** *of Ω.*

Regarding the last definition, sometimes the integer m is then also called a numerical multiplier of Ω. The meaning is always clear from the context. All multipliers of a difference set form a group. In a cyclic group each multiplier is obviously numerical. The following property of multipliers of a cyclic difference set prove to be useful for our construction of difference set Ω in C_v, or for showing that difference set in that group does not exist.

THEOREM 5.3 ([1, p. 307]). *Let Ω be an abelian (v, k, λ) difference set in a group G. Then there exists a translate Ωa, $a \in G$, fixed by every numerical multiplier of Ω. In particular, for a cyclic difference set there exists its translate fixed by every multiplier.*

On the basis of Theorem 5.3, without loss of generality, we can take that the cyclic (v, k, λ) difference set in construction is fixed by the related group of all multipliers and by any of its subgroups. Given a group M of multipliers of a (v, k, λ) difference set Ω in C_v, we consider Ω as a union of certain M-orbits on C_v, i.e., $\Omega = \bigcup a_i^M$ for some $a_i \in C_v$, where $k = \sum_i \left|a_i^M\right|$ holds.

In order to find a group M of multipliers of an intended cyclic difference set Ω, we need the conditions on a positive integer m that are sufficient for m to be a numerical multiplier of Ω. These conditions should refer only to parameters v, k, λ, and n of Ω. There are several theorems on multipliers dealing with this problem ([1, p. 323]). We use the following.

THEOREM 5.4 (Second multiplier theorem). *Let Ω be an abelian (v, k, λ) difference set in a group G, and let $d > \lambda$ be a divisor of n which is coprime with v. Moreover, let m be an integer coprime with v satisfying the following condition: for every prime p dividing d there exists $f \in \mathbb{N}$ with $m \equiv p^f \pmod{e}$, where e denotes the exponent of G. Then m is a numerical multiplier for Ω.*

Accordingly, for numerical multiplier m we have

$$m \in \bigcap_{\substack{p \\ p|d}} \left\{ p^f \pmod{e} \mid f = 1, \ldots, |p| \right\},$$

where p and m are coprime with v, and $|p|$ is the multiplicative order of p modulo v. The last formula for $m \in \mathbb{Z}$ is easily GAP-programmed.

The most desirable situation is when $|M|$ is big enough to ensure the feasibility of our computation. In some of our cases we had the problem with a small M and the huge number of possibilities for forming a difference set from M-orbits on C_v; however, all cases are solved. There exist exactly 43 nonisomorphic primitive symmetric designs with 35 different parameter triples.

EXAMPLE 5.5. By Theorem 5.4 we find that a group of numerical multipliers of a $(127, 63, 31)$ difference set Ω in group C_{127} is $M = \{1, 2, 4, 8, 16, 32, 64\} \cong C_7$. Ω is a union of some M-orbits on C_{127}, them being $0M = \{0\}$ and 18 orbits of length 7:

$1M = \{1, 2, 4, 8, 16, 32, 64\}$, $3M = \{3, 6, 12, 24, 48, 65, 96\}$,
$5M = \{5, 10, 20, 33, 40, 66, 80\}$, $7M = \{7, 14, 28, 56, 67, 97, 112\}$,
$9M = \{9, 17, 18, 34, 36, 68, 72\}$, $11M = \{11, 22, 44, 49, 69, 88, 98\}$,
$13M = \{13, 26, 35, 52, 70, 81, 104\}$, $15M = \{15, 30, 60, 71, 99, 113, 120\}$,
$19M = \{19, 25, 38, 50, 73, 76, 100\}$, $21M = \{21, 37, 41, 42, 74, 82, 84\}$,
$23M = \{23, 46, 57, 75, 92, 101, 114\}$, $27M = \{27, 51, 54, 77, 89, 102, 108\}$,
$29M = \{29, 39, 58, 78, 83, 105, 116\}$, $31M = \{31, 62, 79, 103, 115, 121, 124\}$,
$43M = \{43, 45, 53, 85, 86, 90, 106\}$, $47M = \{47, 61, 87, 94, 107, 117, 122\}$,
$55M = \{55, 59, 91, 93, 109, 110, 118\}$, $63M = \{63, 95, 111, 119, 123, 125, 126\}$.

Besides $M = \{1, 2, 4, 8, 16, 32, 64\}$, difference set Ω contains 8 orbits of length 7. There are $\binom{17}{8} = 24310$ possibilities to form a set of cardinality 63 from these orbits. After computer checking all of them to λ-balancing we obtain 40 solutions. These resulting difference sets give six nonisomorphic $(127, 63, 31)$ symmetric designs with regular primitive automorphism group C_{127}.

6. Description of the constructed designs

There exist exactly 71 primitive (v, k, λ) symmetric designs for $2k < v \leq 255$ with 57 different parameter triples. We distinguish four different parameter types of obtained designs: only Paley type (P), only Kantor type (K), both Paley and Kantor type (P and K) and parameters which are neither Paley nor Kantor type (not P or K). Some numerical data for each of these types of parameters are given in the following table:

type of parameter:	P	K	P and K	not P or K	total
Number of obtained designs:	29	21	10	11	71
Number of different parameters:	26	18	4	9	57
Number of designs not P or K:	3	3	4	11	21

Table 3.

The files with DESIGN-records of 21 constructed nonisomorphic designs which are neither Paley nor Kantor designs are stored in a separate file on the web site $(*)$ for each v. In Tables 4, 5, 7 and 8 these designs and their corresponding full automorphism groups are described. They are denoted in the same way in the tables and web files. The record of each design D contains a permutation representation of $Aut\ D$ and all blocks of the design.

6.1. *Primitive symmetric designs with Paley type parameters.* We obtained 29 primitive symmetric designs with 26 Paley type parameters.

If $q > 19$, 2-homogeneous full automorphism group of $(q, \frac{q-1}{2}, \frac{q-3}{4})$ Paley design $P(q)$ comprises all permutations π of the points given by

$$\pi : x \longrightarrow a\sigma(x) + b,$$

where a is a nonzero square in F_q, $b \in F_q$, and σ is an automorphism of the field F_q ([12]). Thus, regarding the structure, $Aut\,(P(q)) \cong F_q \rtimes \left(F_q^{(2)} \rtimes Aut(F_q)\right)$ and $|Aut\,(P(q))| = q \cdot \frac{q-1}{2} \cdot m$. The subgroup of $Aut\,(P(q))$ consisting of permutations of the points given by $x \longrightarrow x + b$ acts regularly. $Aut\,(P(q))$ is an affine rank 3-group with orbit lengths of point stabilizer S: $1^1, \left(\frac{q-1}{2}\right)^2$ ([7]). Block stabilizer acts transitively on a fixed block.

A brief structural description of full automorphism groups of the three obtained designs with Paley type parameters which are not Paley designs is given in the Table 4.

Theorem 6.1. *There exist exactly two primitive symmetric designs for each of Paley type parameters* $(43, 21, 10)$, $(223, 111, 55)$ *and* $(243, 121, 60)$.

parameter	design stored as	type, $Aut\ D$ id.	S	S-orbit lengths
$(43, 21, 10)$	$43[2]$	affine $G(43, 5)$	C_7	$1^1 7^6$
$(223, 111, 55)$	$D223[2]$	affine $G(223, 5)$	C_{37}	$1^1 37^6$
$(243, 121, 60)$	$D243[2]$	affine $G(243, 3)$	$C_{11}{:}\, C_5$	$1^1 11^2 55^4$

TABLE 4.

For the other 23 *Paley type parameters there exists a unique primitive symmetric design with each of these parameters, the Paley one. All these designs have full automorphism groups of affine type.*

6.2. *Primitive symmetric designs with Kantor type parameters.* We obtained 21 primitive symmetric designs with 18 Kantor type parameters. For each Kantor design D, $Aut\ D$ is a rank 2 group with point stabilizer not stabilizing any block. If D is a $(2^{2m}, 2^{m-1}(2^m - 1), 2^{m-1}(2^{m-1} - 1))$ symmetric design, then $Aut\ D$ has many affine rank 3 primitive subgroups ([7]). In particular, for $m = 2$ and 3, the full group structure is $F_2^{2m} \rtimes Sp_{2m}(F_2)$, where $Sp_{2m}(F_2)$ is a symplectic group. For $D = PG(n, q)$, $q = p^m$ is a prime power, the full automorphism group is a projective general semilinear group $P\Gamma L_{n+1}(q)$ (fundamental theorem of projective geometry ([1])).

Some information about the full automorphism groups of the three designs with Kantor type parameters which are not Kanor designs is summarized in the following table.

parameter	design stored as	$Aut\ D$ id.	type of $Aut\ D$:
$(40, 13, 4)$	$D40[2]$	$G(40, 4)$	almost simple $PSp(4, 3) : C_2$
$(63, 31, 15)$	$D63[2]$	$G(63, 2)$	almost simple $PSU(3, 3).C_2$
$(156, 31, 15)$	$D156[2]$	$G(156, 4)$	almost simple $PSp(4, 5).C_2$

TABLE 5.

THEOREM 6.2. *There exist exactly two primitive symmetric designs for each of Kantor type parameters* $(40, 13, 4)$,$(63, 31, 15)$ *and* $(156, 31, 6)$. *For the other* 15 *Kantor type parameters there exists a unique primitive symmetric design with each of these parameters, the Kantor one. For designs* $(16, 6, 2)$ *and* $(64, 28, 12)$ *the full automorphism groups are of affine type; in all other cases the full automorphism groups are of almost simple type.*

6.3. *Primitive symmetric designs with Paley and Kantor type parameters.* There exist 10 primitive symmetric designs with 4 parameters which are both Paley and Kantor type.

parameter	Number of designs:	design type
$(7, 3, 1)$	1	$P = PG(2, 2)$
$(11, 5, 2)$	1	$P = K$
$(31, 15, 7)$	2	$P, PG(4, 2)$
$(127, 63, 31)$	6	$P, PG(6, 2)$ and 4 other designs

TABLE 6.

The Table 7 gives some information about the structure of the full automorphism groups of $(127, 63, 31)$ symmetric designs which are neither Paley nor Kantor designs.

design stored as	type, *Aut* D id.	S	S-orbit lengths
$D127[3], D127[4], D127[5]$	affine $G(127, 5)$	C_7	$1^1 7^{18}$
$D127[6]$	affine $G(127, 9)$	C_{21}	$1^1 21^6$

TABLE 7.

THEOREM 6.3. *There exists exactly one primitive symmetric design for each of the parameters* $(7, 3, 1)$ *and* $(11, 5, 2)$. *There exist exactly two* $(31, 15, 7)$ *primitive symmetric designs:* $PG(4, 2)$ *and* $P(31)$. *There exist exactly six* $(127, 63, 31)$ *primitive symmetric designs:* $PG(6, 2)$, $P(127)$ *and* 4 *designs which are neither Paley nor Kantor designs. The full automorphism groups of projective geometries are of almost simple type. The full automorphism groups of all other designs are of affine type.*

6.4. *Parameters neither Paley nor Kantor type.* Out of 57 parameter triples related to obtained designs, 9 parameters are neither Paley nor Kantor type.

THEOREM 6.4. *There exist exactly* 11 *primitive symmetric designs for the parameters which are neither Paley nor Kantor type. The full automorphism groups of the designs with a prime* v *are of affine type; if* v *is not a prime, the full automorphism groups are of almost simple type.*

The Table 8 presents some information about the structure of full automorphism groups of these 11 designs.

REMARK 6.5. The first and last design in Table 5 have been described by Higman ([10]) while the second design of Table 5 belongs to the series described in [6]. The design with *Aut* $D \cong P\Gamma U(3, 3)$ from the Table 8 was found by Crnković ([5]), the designs with *Aut* $D \cong PSp(4, 3) : C_2$ are described in [7] while the designs with $v = 144$ can be found in the PhD-thesis of W. Wirth ([15]).

parameter	design stored as	$Aut\ D$ id.	type of $Aut\ D$:
$(35, 17, 8)$	$D35[1]$	$G(35, 2)$	almost simple S_8
$(36, 15, 6)$	$D36[1]$	$G(36, 7)$	almost simple $P\Gamma U(3, 3)$
	$D36[2]$	$G(36, 9)$	almost simple $PSp(4, 3) : C_2$
$(37, 9, 2)$	$D37[1]$	$G(37, 6)$	affine $C_{37} : C_9$
$(45, 12, 3)$	$D45[1]$	$G(45, 5)$	almost simple $PSp(4, 3) : C_2$
$(56, 11, 2)$	$D56[1]$	$G(56, 5)$	almost simple $PSL(3, 4).C_2\hat{}2$
$(101, 25, 6)$	$D101[1]$	$G(101, 7)$	affine $C_{101} : C_{25}$
$(109, 28, 7)$	$D109[1]$	$G(109, 9)$	affine $C_{109} : C_{27}$
$(144, 66, 30)$	$D144[1]$	$G(144, 5)$	almost simple $M\_12.2$
	$D144[2]$	$G(144, 4)$	almost simple $M\_12.2$
$(197, 49, 12)$	$D197[1]$	$G(197, 7)$	affine $C_{197} : C_{49}$

TABLE 8.

REFERENCES

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

[2] S. Braić, Symmetric designs with primitive automorphism groups, PhD-thesis, University of Zagreb, 2007.

[3] P. J. Cameron, Permutation groups, Cambridge University Press, Cambridge, 1999.

[4] C. J. Colbourn and J. H. Dinitz, Eds., Handbook of combinatorial designs, Second Edition, CRC Press, Boca Raton, 2007.

[5] D. Crnković, *Symmetric* $(36, 15, 6)$ *design having* $U(3, 3)$ *as an automorphism group*, Glas. Mat. Ser. III **34(54)** (1999), 1–3.

[6] U. Dempwolff and W. M. Kantor, *Symmetric designs from the* $G_2(q)$ *generalized hexagons,* J. Combin. Theory Ser. A **98** (2002), 410–415.

[7] U. Dempwolff, *Affine rank 3 groups on symmetric designs*, Des. Codes Cryptogr. **31** (2004), 159–168.

[8] J. D. Dixon and B. Mortimer, Permutation groups, Springer, New York, 1996.

[9] The GAP Group, GAP – groups, algorithms, and programming, version 4.4; Aachen, St. Andrews, 2006, `http://www.gap-system.org`.

[10] D. G. Higman, *Finite permutation groups of rank 3,* Math. Z. **86** (1964), 145–156.

[11] W. M. Kantor, *Classification of* 2*-transitive symmetric designs*, Graphs Combin. **1** (1985), 165–166.

[12] E. S. Lander, Symmetric designs: an algebraic approach, London Mathematical Society Lecture Note Series **74**, Cambridge University Press, London, 1983.

[13] J. J. Seidel, A. Blokhuis and H. A. Wilbrink, Graphs and Association Schemes, Algebra and Geometry, EUT-Report 83-WSK-02, 1983.

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

[15] W. Wirth, Konstruktion symmetrischer Designs, PhD-thesis, University of Mainz, 2000.

S. Braić
Department of Mathematics
University of Split
Teslina 12/III, 21 000 Split
Croatia

Received: 8.9.2009.
Revised: 16.1.2010.