On the existence of block-transitive combinatorial designs
Michael Huber

To cite this version:

HAL Id: hal-00990459
https://hal.inria.fr/hal-00990459
Submitted on 13 May 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
On the existence of block-transitive combinatorial designs

Michael Huber

Wilhelm-Schickard-Institute for Computer Science, University of Tübingen, Sand 13, D-72076 Tübingen, Germany
E-mail michael.huber@uni-tuebingen.de


Block-transitive Steiner $t$-designs form a central part of the study of highly symmetric combinatorial configurations at the interface of several disciplines, including group theory, geometry, combinatorics, coding and information theory, and cryptography. The main result of the paper settles an important open question: There exist no non-trivial examples with $t = 7$ (or larger). The proof is based on the classification of the finite 3-homogeneous permutation groups, itself relying on the finite simple group classification.

Keywords: Combinatorial design, block-transitive group of automorphisms, 3-homogeneous permutation group

1 Introduction

One of the outstanding problems in combinatorial design theory concerns the existence of Steiner $t$-designs (i.e., $t$-$(v,k,1)$ designs) with $t > 5$. In particular the existence of Steiner $t$-designs admitting an interesting group of automorphisms is of great interest. The known examples for $t \leq 5$ often encompass a high degree of regularity and establish deep connections to permutation group theory, geometry, combinatorics, coding and information theory, and cryptography.

There has been recent progress on the existence problem by characterizing Steiner $t$-designs which admit a flag-transitive group of automorphisms (cf. [20]). In this paper, we focus on the existence problem of Steiner $t$-designs under the weaker condition of block-transitivity. P. Cameron and C. Praeger [7] proved the non-existence of block-transitive (Steiner) $t$-designs for $t > 7$. Moreover, they conjectured that there are no non-trivial examples for $t = 6$. Recently, the author [19, 22] essentially confirmed the non-existence of block-transitive Steiner 6-designs. The main result of the present paper settles now the challenging remaining question for $t = 7$.

Main Theorem There is no non-trivial Steiner 7-design $D$ admitting a block-transitive group $G \leq \text{Aut}(D)$ of automorphisms.

The paper is organized as follows: Preliminary results which are important for the remainder of the paper are collected in Section 2. In Section 3 a detailed account on previous and related work is presented. In Section 4 the proof of the Main Theorem will be given. It is based on the classification of the finite 3-homogeneous permutation groups, itself relying on the classification of the finite simple groups.
2 Preliminary Results

2.1 $t$-Designs

Combinatorial design theory is a fascinating subject on the interface of several disciplines, including group theory, geometry, combinatorics, coding and information theory, and cryptography. In particular, the study of designs with high symmetry properties has a very long history and establishes deep connections between these areas. One of its highlights surely is the remarkable interrelation between the Mathieu–Witt designs, Golay codes, sporadic simple Mathieu groups, Leech lattice, and Kissing Numbers and Sphere Packing problems (cf., e.g., [2] [23] [32]). A recent connection with cryptography is given in [21].

Combinatorial designs may be regarded as generalizations of finite projective planes. More formally: For positive integers $t \leq k \leq v$ and $\lambda$, we define a $t$-$(v, k, \lambda)$ design to be a finite incidence structure $\mathcal{D} = (X, B, I)$, where $X$ denotes a set of points, $|X| = v$, and $B$ a set of blocks, $|B| = b$, satisfying the following regularity properties: each block $B \in B$ is incident with $k$ points, and each $t$-subset of $X$ is incident with $\lambda$ blocks. A flag of $\mathcal{D}$ is an incident point-block pair $(x, B) \in I$ with $x \in X$ and $B \in B$.

For historical reasons, a $t$-$(v, k, \lambda)$ design with $\lambda = 1$ is called a Steiner $t$-design (sometimes also a Steiner system). We note that in this case each block is determined by the set of points which are incident with it, and thus can be identified with a $k$-subset of $X$ in a unique way. If $t < k < v$, then we speak of a non-trivial Steiner $t$-design. As a simple example, the vector space $\mathbb{F}_2^n$ ($n \geq 3$) with block set $\mathcal{B}$ taken to be the set of all subsets of four distinct elements of $\mathbb{F}_2^n$ whose vector sum is zero is a (boolean) Steiner $3$-$(2^n, 4, 1)$ design. There are many infinite classes of Steiner $t$-designs for $t = 2$ and $3$, however for $t = 4$ and $5$ only a finite number are known. For a detailed treatment of combinatorial designs, we refer to [1] [8] [24] [35]. In particular, [1] [3] provide encyclopedic accounts of key results and contain existence tables with known parameter sets.

We consider automorphisms of a $t$-design $\mathcal{D}$ as pairs of permutations on $X$ and $B$ which preserve incidence, and call a group $G \leq \text{Aut}(\mathcal{D})$ of automorphisms of $\mathcal{D}$ block-transitive (respectively flag-transitive, point $t$-transitive, point $t$-homogeneous) if $G$ acts transitively on the blocks (respectively transitively on the flags, $t$-transitively on the points, $t$-homogeneously on the points) of $\mathcal{D}$. For short, $\mathcal{D}$ is said to be, e.g., block-transitive if $\mathcal{D}$ admits a block-transitive group of automorphisms.

For $\mathcal{D} = (X, B, I)$ a Steiner $t$-design with $G \leq \text{Aut}(\mathcal{D})$, let $G_x$ denote the stabilizer of a point $x \in X$, and $G_B$ the setwise stabilizer of a block $B \in B$. For $x, y \in X$ and $B \in B$, we define $G_{xy} = G_x \cap G_y$.

For any $x \in \mathbb{R}$, let $\lfloor x \rfloor$ denote the greatest positive integer which is at most $x$.

All other notation is standard.

2.2 Combinatorial Existence Results

We recall some standard combinatorial results which we use in this paper. For the existence of $t$-designs, basic necessary conditions can be obtained via elementary counting arguments (see, for instance, [1]):

**Proposition 1** Let $\mathcal{D} = (X, B, I)$ be a $t$-$(v, k, \lambda)$ design, and for a positive integer $s \leq t$, let $S \subseteq X$ with $|S| = s$. Then the total number of blocks incident with each element of $S$ is given by

$$
\lambda_s = \lambda \frac{v-s}{t-s}. 
$$

In particular, for $t \geq 2$, a $t$-$(v, k, \lambda)$ design is also an $s$-$(v, k, \lambda_s)$ design.
It is customary to set \( r := \lambda_1 \) denoting the total number of blocks incident with a given point (referring to the ‘replication number’ from statistical design of experiments, one of the origins of design theory).

**Corollary 2**  Let \( \mathcal{D} = (X, B, I) \) be a \( t-(v, k, \lambda) \) design. Then the following holds:

(a) \( bk = vr \).

(b) \( \binom{v}{t} \lambda = b \binom{k}{t} \).

(c) \( r(k-1) = \lambda_2(v-1) \) for \( t \geq 2 \).

**Corollary 3**  Let \( \mathcal{D} = (X, B, I) \) be a \( t-(v, k, \lambda) \) design. Then

\[
\lambda \left( \frac{v-s}{t-s} \right) \equiv 0 \pmod{\binom{k-s}{t-s}}
\]

for each positive integer \( s \leq t \).

For non-trivial Steiner \( t \)-designs lower bounds for \( v \) in terms of \( k \) and \( t \) can be given (see P. Cameron \[5\] Thm. 3A.4, and J. Tits \[37\] Prop. 2.2):

**Proposition 4**  If \( \mathcal{D} = (X, B, I) \) is a non-trivial Steiner \( t \)-design, then the following holds:

(a) (Tits 1964): \( v \geq (t+1)(k-t+1) \).

(b) (Cameron 1976): \( v - t + 1 \geq (k-t+2)(k-t+1) \) for \( t > 2 \). If equality holds, then \((t, k, v) = (3, 4, 8), (3, 6, 22), (3, 12, 112), (4, 7, 23), \) or \((5, 8, 24)\).

We note that in general Part \( \text{[a]} \) is stronger for \( k < 2(t-1) \), while Part \( \text{[b]} \) is stronger for \( k > 2(t-1) \). For \( k = 2(t-1) \) both assert that \( v \geq t^2 - 1 \). As we are in particular interested in the case when \( t = 7 \), we deduce from Part \( \text{[b]} \) the following upper bound for the positive integer \( k \).

**Corollary 5**  Let \( \mathcal{D} = (X, B, I) \) be a non-trivial Steiner \( 7 \)-design. Then

\[
k \leq \left\lfloor \sqrt{v + \frac{11}{2}} \right\rfloor.
\]

We finally state two classical results on the existence of \( t \)-designs. The first is due to D. Ray-Chaudhuri and R. Wilson \[33\] Thm. 1], and the second is by L. Teirlinck \[36\]:

**Theorem 6** (Ray-Chaudhuri & Wilson 1975). Let \( \mathcal{D} = (X, B, I) \) be a \( t-(v, k, \lambda) \) design. If \( t \) is even, say \( t = 2s \), and \( v \geq k + s \), then \( b \geq \binom{v}{s} \). If \( t \) is odd, say \( t = 2s + 1 \), and \( v - 1 \geq k + s \), then \( b \geq 2 \binom{v-1}{s} \).

**Theorem 7** (Teirlinck 1987). For every positive integer value of \( t \), there exists a non-trivial \( t \)-design.

However, although Teirlinck’s recursive methods are constructive, they only produce examples with tremendously large values of \( \lambda \). Via computer search, \( t-(v, k, \lambda) \) designs with \( t \geq 6 \) and smaller values of \( \lambda \) (where \( \lambda \) is at least 4) have been constructed in recent years by the method of orbiting under a group (see \[26\] for an overview). Until now no non-trivial Steiner \( t \)-design with \( t \geq 6 \) is known.

**Problem 8**  Does there exist any non-trivial Steiner \( t \)-design with \( t \geq 6 \)?
3 Previous and Related Work

We focus on $t$-designs which admit groups of automorphisms with high symmetry properties. One of the early important results is due to R. Block [2 Thm. 2]:

**Proposition 9** (Block 1965). Let $D = (X, B, I)$ be a non-trivial $t$-$(v, k, \lambda)$ design with $t \geq 2$. If $G \leq \text{Aut}(D)$ acts block-transitively on $D$, then $G$ acts point-transitively on $D$.

For a $2$-$(v, k, 1)$ design $D$, it is elementary that the point 2-transitivity of $G \leq \text{Aut}(D)$ implies its flag-transitivity. For $2$-$(v, k, \lambda)$ designs, this implication remains true if $r$ and $\lambda$ are relatively prime (see, for instance, [12 Chap. 2.3, Lemma 8]). However, for $t$-$(v, k, \lambda)$ designs with $t \geq 3$, it can be deduced from Proposition 9 that always the converse holds (see [3] or [14 Lemma 2]):

**Proposition 10** Let $D = (X, B, I)$ be a non-trivial $t$-$(v, k, \lambda)$ design with $t \geq 3$. If $G \leq \text{Aut}(D)$ acts flag-transitively on $D$, then $G$ acts point 2-transitively on $D$.

Investigating highly symmetric $t$-designs for large values of $t$, P. Cameron and C. Praeger [7 Thm. 2.1] deduced from Theorem 6 and Proposition 9 the following assertion:

**Proposition 11** (Cameron & Praeger 1993). Let $D = (X, B, I)$ be a $t$-$(v, k, \lambda)$ design with $t \geq 2$. Then, the following holds:

(a) If $G \leq \text{Aut}(D)$ acts block-transitively on $D$, then $G$ also acts point $[t/2]$-homogeneously on $D$.

(b) If $G \leq \text{Aut}(D)$ acts flag-transitively on $D$, then $G$ also acts point $(t + 1)/2$-homogeneously on $D$.

As for $t \geq 7$ the flag-transitivity, respectively for $t \geq 8$ the block-transitivity of $G \leq \text{Aut}(D)$ implies at least its point 4-homogeneity, they obtained the following restrictions as a consequence of the finite simple group classification (cf. [7 Thm. 1.1]):

**Theorem 12** (Cameron & Praeger 1993). Let $D = (X, B, I)$ be a $t$-$(v, k, \lambda)$ design. If $G \leq \text{Aut}(D)$ acts block-transitively on $D$ then $t \leq 7$, while if $G \leq \text{Aut}(D)$ acts flag-transitively on $D$ then $t \leq 6$.

Moreover, they formulated the following far-reaching conjecture (cf. [7 Conj. 1.2]):

**Conjecture 13** (Cameron & Praeger 1993). There are no non-trivial block-transitive 6-designs.

The author [19, 22] recently confirmed the non-existence of block-transitive Steiner 6-designs, modulo two special cases that remain elusive.

**Theorem 14** (Huber 2010). Let $D = (X, B, I)$ be a non-trivial Steiner 6-design. Then $G \leq \text{Aut}(D)$ cannot act block-transitively on $D$, except possibly when $G = P\Gamma L(2, p^e)$ with $p = 2$ or 3 and $e$ is an odd prime power.

Previously, the author classified all flag-transitive Steiner $t$-designs with $t > 2$ (see [14, 15, 16, 17, 18] and [20] for a monograph). These results answered a series of 40-year-old problems and generalized theorems of J. Tits [37] and H. Lüneburg [31]. Earlier, F. Buekenhout, A. Delandtsheer, J. Doyen, P. Kleidman, M. Liebeck, and J. Saxl [4, 10, 27, 29, 34] had essentially characterized all flag-transitive Steiner 2-designs. All these classification results rely on the classification of the finite simple groups. As flag-transitivity clearly implies block-transitivity, these results provide nice examples of block-transitive Steiner designs. An encyclopedic survey of further results, in particular on point-imprimitive block-transitive $t$-designs, is given by [11].
4 Proof of the Main Theorem

We prove in this section our Main Theorem stated in Section 1. In order to investigate the existence problem of non-trivial block-transitive Steiner 7-designs, we can as a consequence of Proposition 11 (a) make use of the classification of all finite 3-homogeneous permutation groups, which itself relies on the classification of all finite simple groups (cf. [6, 13, 25, 28, 30]). We remark that the list given in [7] List 2.2] is slightly incomplete.

4.1 Finite 3-homogeneous Permutation Groups

The list of groups is as follows: Let $G$ be a finite 3-homogeneous permutation group on a set $X$ with $|X| \geq 4$. Then $G$ is either of

(A) Affine Type: $G$ contains a regular normal subgroup $T$ which is elementary Abelian of order $v = 2^d$.

If we identify $G$ with a group of affine transformations $x \mapsto x^g + u$ of $V = V(d, 2)$, where $g \in G_0$ and $u \in V$, then particularly one of the following occurs:

1. $G \cong AGL(1, 8)$, $A\Gamma L(1, 8)$, or $A\Gamma L(1, 32)$
2. $G_0 \cong SL(d, 2)$, $d \geq 2$
3. $G_0 \cong A_7$, $v = 2^4$

or

(B) Almost Simple Type: $G$ contains a simple normal subgroup $N$, and $N \leq G \leq \text{Aut}(N)$. In particular, one of the following holds, where $N$ and $v = |X|$ are given as follows:

1. $A_v$, $v \geq 5$
2. $PSL(2, q)$, $q > 3$, $v = q + 1$
3. $M_v$, $v = 11, 12, 22, 23, 24$ (Mathieu groups)
4. $M_{11}$, $v = 12$

We note that if $q$ is odd, then $PSL(2, q)$ is 3-homogeneous for $q \equiv 3 \pmod{4}$, but not for $q \equiv 1 \pmod{4}$, and hence not every group $G$ of almost simple type satisfying $[\square]$ is 3-homogeneous on $X$.

**Remark 15** If $G \leq \text{Aut}(D)$ acts block-transitively on any Steiner $t$-design $D$ with $t \geq 6$, then by Proposition 11 (a), $G$ acts point 3-homogeneously and in particular point 2-transitively on $D$. Applying Corollary 2 yields the equation

$$b = \binom{n}{k} = \frac{v(v-1)|G_{xy}|}{|G_B|},$$

where $x$ and $y$ are two distinct points in $X$ and $B$ is a block in $D$. We will see that this arithmetical condition in combination with the combinatorial tools from Section 2 gives immediately strong results for some of the cases to be examined.
4.2 Groups of Automorphisms of Affine Type

Using the notation as before, let us assume for the rest of the section that $\mathcal{D} = (X, \mathcal{B}, I)$ is a non-trivial Steiner 7-design with $G \leq \text{Aut}(\mathcal{D})$ acting block-transitively on $\mathcal{D}$. Clearly, we may assume that $k > 7$ as we do not consider trivial designs. We will examine in this subsection those cases where $G$ is of affine type.

Case (1): $G \cong AGL(1, 8)$, $AGL(1, 8)$, or $AGL(1, 32)$.

As $k > 7$, the case $v = 8$ is not possible. For $v = 32$, we have $|G| = 5v(v - 1)$ and $k \leq 11$ by Corollary 5. The few possibilities can easily be ruled out using Corollary 2 together with Remark 15.

Case (2): $G \cong SL(d, 2)$, $d \geq 2$.

Let $e_i$ denote the $i$-th standard basis vector of the vector space $V = V(d, 2)$, and $(e_i)$ the 1-dimensional vector subspace spanned by $e_i$. We will prove by contradiction that $G \leq \text{Aut}(\mathcal{D})$ cannot act block-transitively on any non-trivial Steiner 7-design $\mathcal{D}$.

We may assume that $v = 2^d > k > 7$. We remark that clearly any seven distinct points are non-coplanar in $AG(d, 2)$ and hence generate an affine subspace of dimension at least 3. Let $\mathcal{E} = (e_1, e_2, e_3)$ denote the 3-dimensional vector subspace spanned by $e_1, e_2, e_3$. Then $SL(d, 2)|\mathcal{E}$, and therefore also $G_0, e$, acts point-transitively on $V \setminus \mathcal{E}$. If the unique block $B \in \mathcal{B}$ which is incident with the 7-subset \( \{0, e_1, e_2, e_3, e_1 + e_2, e_2 + e_3, e_1 + e_3\} \) contains some point outside $\mathcal{E}$, then it would already contain all points of $V \setminus \mathcal{E}$. But then $k \geq 2^d - 8 + 7 = 2^d - 1$, a contradiction to Corollary 5. Hence, $B$ lies completely in $\mathcal{E}$. The block-transitivity of $G$ now implies that each block must be contained in a 3-dimensional affine subspace. On the other hand, any seven distinct points that do not lie in a 3-dimensional affine subspace must also be incident with a unique block by the definition of Steiner designs, a contradiction.

Case (3): $G_0 \cong A_7$, $v = 2^4$.

As $v = 2^4$, we have $k \leq 9$ by Corollary 5. But, Corollary 2(e) obviously eliminates the cases when $k = 8$ or 9.

4.3 Groups of Automorphisms of Almost Simple Type

When $G$ is of almost simple type, then the Cases (B) 1, 3 and 4 of Section 4.1 cannot occur as elementarily proved in [7, Sect. 2, mainly Prop. 2.4]. Hence, we only have to consider

Case (2): $N = PSL(2, q)$, $v = q + 1$, $p^r > 3$.

Here $\text{Aut}(N) = PGL(2, q)$, and $|G| = (q + 1)q^{\frac{(q - 1)}{n}}$ with $n = (2, q - 1)$ and $a \mid ne$. We may assume that $q \geq 8$. We will show that $G \leq \text{Aut}(\mathcal{D})$ cannot act block-transitively on any non-trivial Steiner 7-design $\mathcal{D}$.

From Remark 15, we obtain

\[
(q - 2)(q - 3)(q - 4)(q - 5)|G_B| \cdot n = k(k - 1)(k - 2)(k - 3)(k - 4)(k - 5)(k - 6) \cdot a. \tag{1}
\]

Due to Proposition 4, we have

\[
q - 5 \geq (k - 5)(k - 6). \tag{2}
\]

Hence, from Equation (1) follows

\[
(q - 2)(q - 3)(q - 4)|G_B| \cdot n \leq k(k - 1)(k - 2)(k - 3)(k - 4) \cdot a. \tag{3}
\]
If we assume that $k \geq 27$, then obviously

$$k(k - 1)(k - 2)(k - 3) < 2[(k - 5)(k - 6)]^2,$$

and hence

$$(q - 2)(q - 3)(q - 4) | G_B| \cdot n < 2(q - 5)^2(k - 4) \cdot a \leq 2(q - 5)^2 \lceil \sqrt{q + 1} + \frac{3}{2} \rceil \cdot a$$

in view of Inequality (3) and Corollary 5. Taking into account that always $a \leq \log_2 q$, it follows immediately that $|G_B| \cdot n = 1$ for each possible value of $q \neq 32$. Hence, in particular $q$ must be even. But then the right hand side of Equation (1) is always divisible by 16 but never the left hand side, a contradiction. The case $q = 32$ as well as the few remaining possibilities for $k < 27$ can easily be ruled out by hand using Equation (1) and Inequality (2).

This completes the proof of the Main Theorem. \qed

**Acknowledgements**

The author gratefully acknowledges support by the Deutsche Forschungsgemeinschaft (DFG) via a Heisenberg grant (Hu954/4).
References


