A family of 4-designs with block size 9

Jürgen Bierbrauer
Mathematisches Institut der Universität
Im Neuenheimer Feld 288
69 Heidelberg
Germany

December 2, 1999

Abstract

We construct a family of simple 4-designs with parameters

$$4-(2^f+1,9,84),\ (f,6)=1, f\geq 5.$$

Introduction

The construction of *infinite series of (nontrivial) t-designs* with constant λ is one of the hardest and most important problems of design theory. By this we mean a family $\{\mathcal{D}_i\}, i=1,2,\dots$ of designs with parameters $t-(v_i,k,\lambda)$, where $v_i\rightarrow\infty$ and such that none of the $\mathcal{D}_i$ is the complete design. When t and k are given, we wish to minimize λ. Teirlinck [6] constructed such series for every natural number t. The parameters of his families are
$t-(v,t+1,l(t))$, where $\lambda(t)=lcm(\binom{t}{m}|m=1,2,\dots t)$, $\lambda^*(t)=lcm(1,2,\dots t+1)$, $l(t)=\prod_{i=1}^t\lambda(i)\cdot\lambda^*(i)$, $v\equiv t\ (\ l(t)), v>t$. Here $l(t)$ is the smallest value of λ which is achievable with Teirlinck's method.
The difficulty of constructing such series increases of course with t. To the author's best knowledge only two series of t-designs with constant λ and $t\geq 4$ have hitherto been known aside from Teirlinck's series: Alltop's series

[1] with parameters $4-(2^{2f+1}+1,5,5),\ f\geq 2$ and a series of non-simple designs $5-(2^f+2,6,15), f\geq 4$ as constructed in [5] by Jungnickel and Vanstone.
In a short series of papers we set out to construct more such families of 4-designs, where λ is constant and small. In [2] we constructed a family of simple designs with parameters $4-(2^{2f+1}+1,6,10), f\geq 2$. The main result of the present paper is the following:

Theorem 1 *Let $q=2^f, (f,6)=1, f\geq 5$. Then there is a simple design with parameters $4-(q+1,9,84)$ whose full automorphism group is $P\Gamma L_2(q)$.*

In a subsequent paper [3] some more infinite series of 4-designs with constant λ are constructed on the projective line in characteristic 2. Here $k\in\{6,8,9\}$.
Let notation be like in the statement of the theorem. Consider the field $\mathbb{F}_q$ of q elements and the projective line $\mathcal{P}_1(q)=\mathbb{F}_q\cup\{\infty\}$. The group $G=PGL_2(q)$ has order $(q+1)q(q-1)$ and operates as a group of permutations on $\mathcal{P}_1(q)$. The elements $g\in G$ are the linear fractional operations

$$\tau\mapsto\frac{a\cdot\tau+c}{b\cdot\tau+d}=\tau^g.$$

Here $g\in G$ may be represented by the nonsingular matrix $\begin{pmatrix} a & b\\ c & d\end{pmatrix}$, which is determined by g up to multiplication by scalar matrices. Here the usual conventions concerning the symbol ∞ are to be used ($\frac{1}{\infty}=0,\frac{1}{0}=\infty,\frac{a\cdot\infty+c}{b\cdot\infty+d}=\frac{a}{b}$). Recall that G is sharply triply transitive in its action on $\mathcal{P}_1(q)$. The group $P\Gamma L_2(q)$ appearing in the statement of the Theorem is the extension of $G=PGL_2(q)$ by the (cyclic) group of field automorphisms of $\mathbb{F}_q$ over $\mathbb{F}_2$. The stabilizer $Stab_G(X)$ of a subset $X\subset\mathcal{P}_1(q)$ is the subgroup, which consists of all the elements of G mapping X onto X. Choose $\{\infty,0,1\}\subset\mathcal{P}_1(q)$ and let H be the stabilizer in G of $\{\infty,0,1\}$. Then $H=<\chi,\eta>\cong S_3$, where

$$\chi(a)=a+1,\ \eta(a)=1/a\ (a\in\mathcal{P}_1(q)).$$

Here S_3 denotes the symmetric group on three letters. H acts semi-regularly on $\mathcal{P}_1(q)-\{\infty,0,1\}$. Its orbits are

$B_u = \{u, u+1, 1/u, (u+1)/u, 1/(u+1), u/(u+1)\}$, where $u \in \mathbb{F}_q - \{0,1\}$. It has been shown in [2] that the G-orbits of the B_u form a design $\mathcal{B}'$ with parameters $4-(q+1, 6, 10)$.

The construction

We use the notation introduced in the Introduction and work under the assumptions of Theorem 1.

Lemma 1 *Let $X \subset \mathcal{P}_1(q), K = Stab_G(X), |X| = k$. Then $|K|$ divides $k(k-1)(k-2)$.*

Proof: The G-orbit containing X forms a design $3-(q+1, k, \lambda)$ with $\lambda = k(k-1)(k-2)/|K|$. ■

We define the blocks $\mathcal{B}$ of our design as the union of the G-orbits of the sets

$$\{\infty, 0, 1\} \cup B_u,\ u \in \mathbb{F}_q - \{0,1\}.$$

By definition each block is stabilized by a subgroup S_3 of G.

Lemma 2 *Let B be a block of the design $\mathcal{B}$ as defined above. Then the G-stabilizer of B is isomorphic to S_3.*

Proof: By Lemma 1 the order of $Stab_G(B)$ divides 9.8.7. The restrictions on the exponent f guarantee that 7 and 9 do not divide the order of G. Thus $|Stab_G(B)| = 3.2^i, i = 1, 2, 3$. As G does not contain elements of orders 4 or 6, we are done. ■

The stabilizer (in G) of a block B has two orbits of points in B. The sizes of the orbits are 3 and 6. Thus a block remembers the way it was constructed. We conclude that the number of blocks is the same as in $\mathcal{B}'$:

$$b = (q+1)q(q-1)(q-2)/36.$$

Lemma 3 *A 9-subset of $\mathcal{P}_1(q)$ is a block of $\mathcal{B}$ if and only if it is the union of the non-regular and some regular orbit of some subgroup S_3 of G.*

Proof: G has exactly $q(q-1)/2$ subgroups of order 3. As the normalizer of a group of order 3 is a dihedral group of order $2(q+1)$, the number of subgroups S_3 of G is $\frac{q(q-1)}{2} \cdot \frac{q+1}{3}$. Each such group has $(q-2)/6$ regular orbits. The Lemma follows. ■

We now proceed to show that $\mathcal{B}$ is indeed a 4-design. Recall that G is 3-transitive. Thus it suffices, to show that every 4-element set containing $\{\infty, 0, 1\}$ is contained in exactly 84 blocks of $\mathcal{B}$. Let $\mathcal{S} = \{\infty, 0, 1, a\}$ for some $a \in \mathbb{F}_q - \{0, 1\}$ and suppose B is a block containing $\mathcal{S}$. Let B_0 be the orbit of length 3 of $Stab_G(B)$ and consider $d = |\mathcal{S} \cap B_0|$. Obviously there are exactly 4 blocks $B \supset \mathcal{S}$ with $d = 3$. The design $\mathcal{B}'$ shows that there are exactly 10 such blocks with $d = 0$.
Let $d = 2$. As $\mathcal{S}$ is invariant under a four-group, we need consider only half of the cases, namely without restriction

$$B_0 \cap \mathcal{S} = \{\infty, s\}, \text{ where } s \in \{0, 1, a\}.$$

For each s we are looking for the number of elements $x \in \mathbb{F}_q - \mathcal{S}$ such that the elements in $\{0, 1, a\} - \{s\}$ are in the same orbit under the stabilizer of $\{\infty, s, x\}$. We use the element $\tau \longrightarrow (\tau + s)/(x + s)$ of G to map $\{\infty, s, x\}$ onto $\{0, 1\}$. The conditions for x are then the following:

- $a/x \in B_x$ in case $s = 0$.
- $(a+1)/(x+1) \in B_x$ in case $s = 1$.
- $(a+1)/(x+a) \in B_{a/(x+a)}$ in case $s = a$.

Thus 18 equations for x have to be considered. In case $s = 0$ these are the following:

$$a/x \in \{x, x+1, 1/x, (x+1)/x, 1/(x+1), x/(x+1)\}.$$

The third of these equations has no solution, the first, fourth and fifth equation have a unique solution each. The solvability of the remaining two equations depends on the conditions $tr(a) = 0$ and $tr(1/a) = 0$, respectively, where $tr : \mathbb{F}_q \longrightarrow \mathbb{F}_2$ is the *trace* with values in the prime field. It follows from Hilbert's Theorem 90 that in characteristic 2 the quadratic equation $x^2 + v \cdot x + u = 0$ (where $v \neq 0$) has exactly 2 or 0 solutions if $tr(u/v^2) = 0$,

or $tr(u/v^2) = 1$, respectively. The two remaining cases $s = 1$ and $s = a$ are handled in an analogous way. In each case one of the six equations has no solutions, three equations possess unique solutions and the solvability of the remaining two equations depends on a trace-condition. Fortunately the six trace-conditions occur in pairs, i.e. for fixed u the condition $tr(u) = 0$ occurs as often as $tr(u) = 1$. We count 15 solutions. Consequently there are precisely 30 blocks $B \supset \mathcal{S}$ satisfying $d = 2$.
Let $d = 1$. As the stabilizer of $\mathcal{S}$ acts transitively on $\mathcal{S}$ we can assume $B_0 \cap \mathcal{S} = \{\infty\}$. We are looking for the number of unordered pairs $\{x, y\}$ such that $\{0, 1, a\}$ is contained in an orbit of the stabilizer of $\{\infty, x, y\}$. Consider the linear fractional substitution $\rho \in G$, where

$$\rho(\tau) = (\tau + x)/(x + y).$$

Then $\rho : \{\infty, x, y\} \longrightarrow \{\infty, 0, 1\}$. Further $\rho : (0, 1, a) \longrightarrow (u, u_1, u_2)$, where

$$u = x/(x + y), u_1 = (x + 1)/(x + y), u_2 = (x + a)/(x + y).$$

The condition on x, y is then transformed into the following:

$$\{u_1, u_2\} \subset B_u - \{u\}.$$

This yields 20 systems of two equations each for x, y. The equations and the numbers of their solutions are given in Table 1.

We work out the case corresponding to the first row of Table 1. We have to consider the following system of two equations for x,y:

$$(x + 1)/(x + y) = y/(x + y)$$
$$(x + a)/(x + y) = (x + y)/x$$

The first equation shows $x + y = 1$. The second equation is then equivalent to $x + a = 1/x$ and to $x^2 + a \cdot x + 1 = 0$. We get 2 solutions if $tr(1/a) = 0$, no solution otherwise.
The entry 1 in the last column stands for a unique solution. The other equations have two solutions if the trace-condition in the last column is satisfied, no solution otherwise. We observe that the trace-conditions occur in pairs again. The total number of solutions is 20. Bearing in mind that

Table 1

u_1	u_2	solutions
$u+1$	$1/u$	$tr(1/a)=0$
$u+1$	$(u+1)/u$	$tr(1/(a+1))=0$
$u+1$	$1/(u+1)$	$tr(1/(a+1))=0$
$u+1$	$u/(u+1)$	$tr(1/a)=0$
$1/u$	$u+1$	$tr(a)=0$
$1/u$	$(u+1)/u$	$tr(a)=1$
$1/u$	$1/(u+1)$	1
$1/u$	$u/(u+1)$	1
$(u+1)/u$	$u+1$	$tr(1/(a+1))=1$
$(u+1)/u$	$1/u$	$tr(1/a)=1$
$(u+1)/u$	$1/(u+1)$	1
$(u+1)/u$	$u/(u+1)$	1
$1/(u+1)$	$u+1$	$tr(1/(a+1))=1$
$1/(u+1)$	$1/u$	1
$1/(u+1)$	$(u+1)/u$	1
$1/(u+1)$	$u/(u+1)$	$tr(1/a))=1$
$u/(u+1)$	$u+1$	$tr(a)=0$
$u/(u+1)$	$1/u$	1
$u/(u+1)$	$(u+1)/u$	1
$u/(u+1)$	$1/(u+1)$	$tr(a)=1$

- we have considered only one fourth of the cases occuring under $d = 1$, and
- we have considered ordered pairs (x, y) where we should have considered unordered pairs,

we see that there are exactly 40 blocks $B \supset \mathcal{S}$ satisfying $d = 1$. Thus the total number of blocks containing $\mathcal{S}$ is $4 + 10 + 30 + 40 = 84$.
A glance at the list of 3-transitive permutation groups (see [4]) shows that the automorphism group of $\mathcal{B}$ cannot be larger than $P\Gamma L_2(q)$.

References

[1] W.O.Alltop: *An infinite class of 4-designs,* Journal of Combinatorial Theory 6(1969),320-322.

[2] J.Bierbrauer: *A new family of 4-designs,* submitted for publication to Graphs and Combinatorics.

[3] J.Bierbrauer: *Some friends of Alltop's designs* $4-(2^f+1, 5, 5)$, submitted for publication to Journal of Statistical Planning and Inference.

[4] P.J.Cameron: *Finite permutation groups and finite simple groups,* Bull.London Math.Soc. 13(1981),1-22.

[5] D.Jungnickel,S.A.Vanstone: *Hyperfactorizations of graphs and 5-designs,* J.Univ.Kuwait (Sci.) 14(1987),213-223.

[6] L.Teirlinck: *Locally trivial t-designs and t-designs without repeated blocks,* Discrete Mathematics 77(1989), 345-356.