A new family of 4-designs

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

$$4-(2^f+1, 6, 10),\ \text{f odd.}$$

The construction

For design-theoretic notation the reader should consult [1]. A related paper [2] appeared recently in this journal. We prove the following theorem:

Theorem 1 *Let $q=2^f$, f odd, $f\geq 5$. Then there is a simple design with parameters $4-(q+1,6,10)$ whose full automorphism group is $P\Gamma L_2(q)$.*

Proof: Let $G=PGL_2(q)$ in its natural action on the projective line $\mathcal{P}_1(q)$. Then $|G|=(q+1)q(q-1)$ and G acts sharply triply transitively. Fix $\{\infty,0,1\}\subset\mathcal{P}_1(q)$. The stabilizer H of $\{\infty,0,1\}$ in G is isomorphic to the symmetric group S_3, generated by involutions τ and η, where

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

H acts semi-regularly on $\mathcal{P}_1(q)-\{\infty,0,1\}$. Its orbits are the 6-sets

$B_a = \{a, a+1, 1/a, (a+1)/a, 1/(a+1), a/(a+1)\}$, where $a \in \mathbb{F}_q - \{0,1\}$. We define the blocks of our design as the set of images under G of the different B_a.

Lemma 1 *Let $X \subset \mathcal{P}_1(q), |X| = 6$ under the assumptions of the Theorem. Then the stabilizer of X in G has order 1,2,3 or 6.*

Proof: This is an immediate consequence of the following facts:

- G is sharply 3-transitive on $\mathcal{P}_1(q)$.
- 5 does not divide the order of G.
- The Sylow-2-subgroups of G are elementary abelian.

■

It follows that each block of our design has S_3 as stabilizer in G.

Lemma 2 *If $B_a \neq B_b$ (equivalently $a, b \in \mathbb{F}_q - \{0,1\}, b \notin B_a$), then B_a and B_b are in different G-orbits. In particular G has exactly $(q-2)/6$ orbits of blocks.*

Proof: Assume $g : B_a \longrightarrow B_b, g \in G$. Then g normalizes H. The union of the fixed points of the involutions in H is exactly $\{\infty, 0, 1\}$. Thus $g \in H$, contradiction. ■

We calculate the number of blocks:

$$b = \frac{q-2}{6} \cdot |G|/6 = (q+1)q(q-1)(q-2)/36.$$

Lemma 3 *The blocks are exactly the unions of two 3-cycles of elements of order 3 in G.*

Proof: As every block is S_3-invariant, it has the required form. On the other hand there are exactly $(q-1)q/2$ subgroups of order three in G. As $q+1$ is a multiple of 3, elements of order three are fixedpointfree. Thus the number of 6-subsets of the required form is $\frac{(q-1)q}{2} \cdot \binom{(q+1)/3}{2}$, and this happens to equal the number b of blocks. ∎

We proceed to the proof of the Theorem. Let $\mathcal{S} = \{\infty, 0, 1, a\}$. We have to prove that $\mathcal{S}$ is in exactly 10 blocks. By Lemma 3 this is equivalent to the statement that there are exactly 10 subgroups U of order three in G such that $\mathcal{S}$ is in the union of two U-orbits. As an element of order three in G is uniquely determined by a 3-cycle, there are exactly four such groups U having an entire 3-cycle in $\mathcal{S}$. It remains to prove that there are exactly six elements of order three in G affording one of the following six operations:

1. $\infty \longrightarrow 0,\ 1 \longrightarrow a.$
2. $\infty \longrightarrow 1,\ 0 \longrightarrow a.$
3. $\infty \longrightarrow a,\ 0 \longrightarrow 1.$
4. $\infty \longrightarrow 0,\ a \longrightarrow 1.$
5. $\infty \longrightarrow 1,\ a \longrightarrow 0.$
6. $\infty \longrightarrow a,\ 1 \longrightarrow 0.$

Consider the first case above. An element $g \in G$ mapping $\infty \longrightarrow 0,\ 1 \longrightarrow a$ has the form $g(x) = a(1+d)/(x+d)$ for some field-element d. The element g has order three if and only $a(1+d)/d = d$, equivalently if and only if

$$d^2 + ad + a = 0.$$

The substitution $x = d/a$ shows: the number of elements of order three in G satisfying the first case above is the number of solutions x of the equation

$$x^2 + x + 1/a = 0.$$

If we consider any of the remaining five cases, we are led to the same type of equation, where the constant term varies over B_a. Thus we have to prove the following:
The equation

$$\prod_{u \in B_a} (x^2 + x + u) = 0$$

has exactly six solutions $x \in I\!F_q$. It is a simple fact that $x^2 + x + u = 0$ has two solutions if $tr(u) = 0$, no solution if $tr(u) = 1$, where tr is the trace $: I\!F_q \longrightarrow I\!F_2$. As B_a is closed under translation with 1 and as $tr(1) = 1$, each factor $(x^2+x+u)(x^2+x+u+1) = 0$ $(u \in B_a)$ has exactly two solutions and $\prod_{u \in B_a}(x^2 + x + u) = 0$ has six solutions, as required. We have shown that our designs has the parameters as given in the statement of the Theorem. This works for $f = 3$ too, but we get the complete design in this case. For $f \geq 5$ the construction shows that $P\Gamma L_2(q)$ is contained in the automorphism group of the design. A short glance at the list of 3-transitive permutation groups (see [3]) shows that the full automorphism group cannot be larger. For $f = 5$ this design was already known as $P\Gamma L_2(32)$ is 4-homogeneous on the projective line.

References

[1] T.Beth,D.Jungnickel,H.Lenz: *Design Theory,* Bibliographisches Institut, Zürich 1985.

[2] J.Bierbrauer: *Designs with block-size 6 in projective planes of characteristic 2,* Graphs and Combinatorics 8(1992), 207-224.

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