Shadow and Shade of Designs $4-(2^{\mathsf{f}}+1,6,10)$

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

Tran van Trung
Institut für Experimentelle Mathematik
Universität Essen
Ellernstrasse 29
4300 Essen 12, Germany

1 Introduction

Let $\mathsf{q}=2^{\mathsf{f}}$, f odd. Define blocks to be the 6-subsets of $\mathsf{PG}(1,\mathsf{q})$ having stabilizer S_3 in $\mathsf{PGL}(2,\mathsf{q})$. It has been shown in [3] that this yields a block design $\mathcal{B}$ with parameters $4-(\mathsf{q}+1,6,10)$. We shall prove the following:

Theorem 1.1 *If* $(\mathsf{f},6)=1$*, then block intersection number 5 does not occur in the block design* $\mathcal{B}$*.*

As is usual in combinatorics of finite sets (see [2]), we consider the *shadow* $\Delta\mathcal{B}$ and the *shade* $\nabla\mathcal{B}$ of $\mathcal{B}$. Here $\Delta\mathcal{B}$ is the family of those 5-subsets of $\mathsf{PG}(1,\mathsf{q})$ which are contained in some member of $\mathcal{B}$, $\nabla\mathcal{B}$ consists of the 7-subsets of $\mathsf{PG}(1,\mathsf{q})$ which contain some member of $\mathcal{B}$.

Corollary 1.2 *If* $(\mathsf{f},6)=1$*, then* $\Delta\mathcal{B}$ *is a block design with parameters* $4-(\mathsf{q}+1,5,20)$*,* $\nabla\mathcal{B}$ *is a block design with parameters* $4-(\mathsf{q}+1,7,70(\mathsf{q}-5)/3)$*. The full automorphism group of* $\Delta\mathcal{B}$ *and of* $\nabla\mathcal{B}$ *is* $\mathsf{P\Gamma L}(2,\mathsf{q})$*.*

Proof of the Corollary. The parameters of $\Delta\mathcal{B}$ follows directly from Theorem 1.1 and the parameters of $\mathcal{B}$. As for $\nabla\mathcal{B}$, each block of $\nabla\mathcal{B}$ contains exactly one block of $\mathcal{B}$. We get $\lambda_4(\nabla\mathcal{B})=10(\mathsf{q}-5)+4(\lambda_3(\mathcal{B})-10)$. As $\lambda_3(\mathcal{B})=10(\mathsf{q}-2)/3$, we can calculate $\lambda_4(\nabla\mathcal{B})$. By construction all of our designs admit $\mathsf{P\Gamma L}(2,\mathsf{q})$ as an automorphism group. A short glance at the list of 3-transitive permutation groups shows that the full automorphism group of our designs cannot be larger. □

Theorem 1.3 *If* $(\mathsf{f},6)=1$*, then* $\Delta\mathcal{B}$ *is disjoint from Alltop's design with parameters* $4-(\mathsf{q}+1,5,5)$ *as constructed in [1]. Thus the union of these designs has parameters* $4-(\mathsf{q}+1,5,25)$ *and full automorphism group* $\mathsf{P\Gamma L}(2,\mathsf{q})$*.*

2 The proofs

Proof of Theorem 1.1. It has been proved in [3] that blocks of $\mathcal{B}$ are exactly the unions of two orbits of elements of order 3 in $\mathsf{PGL}(2,q)$.

Let $S \subset \mathsf{PG}(1,q)$, $|S| = 4$. Then S is in 10 blocks. Four of these arise from elements of order 3 having one orbit completely in S. These are the *block of type I*, and points $\notin S$ on one of these blocks are *neighbours of type I* of S:

$N_I(S) = \{P | P \notin S,$ there is an element of order 3 such that $S \cup \{P\}$ is in the union of two orbits and one of these orbits is contained in $S\}$.

The remaining 6 blocks through S have *type II*. They yield *neighbours of type II* of S:

$N_{II}(S) = \{P | P \notin S,$ there is an element of order 3 such that $S \cup \{P\}$ is in the union of two orbits and none of these orbits is contained in $S\}$.

Assume now there are blocks B_1, B_2 of $\mathcal{B}$ satisfying $|B_1 \cap B_2| = 5$. Let $B_1 = D_1 \cup D_1'$, $B_2 = D_2 \cup D_2'$ be the subdivision of our blocks into orbits of a subgroup $Z_3 < \mathsf{PGL}(2,q)$, say $D_1 = \{1,2,3\}$, $D_1' = \{4,5,6\}$. Without restriction $B_1 \cap B_2 = \{1,2,3,4,5\} \supset D_1$. If we choose $S = D_1 \cup \{4\}$ or $S = D_1 \cup \{5\}$, then B_1 will be of type I with respect to S. We have $B_2 = \{1,2,3,4,5,x\}$, and without restriction either $D_2 = \{1,2,x\}$, $D_2' = \{3,4,5\}$ or $D_2 = \{1,2,4\}$, $D_2' = \{3,5,x\}$. In both cases the choice $S = \{1,2,3,5\}$ guarantees that B_2 has type II with respect to S.

Choose now $S = \{\infty, 0, 1, a\}$. We have just seen that we can assume B_1 to be of type I and B_2 to be of type II with respect to S. Let us denote the element $(\tau \longmapsto (a\tau + b)/(c\tau + d))$ either $(a\tau + b)/(c\tau + d)$ or by the corresponding matrix. The elements

$1/(\tau + 1) \ : \ (\infty, 0, 1)(a, 1/(a+1), (a+1)/a),$

$a^2/(\tau + a) \ : \ (\infty, 0, a)(1, a^2/(a+1), a(a+1)),$

$(\tau + a^2 + a + 1)/(\tau + a) \ : \ (\infty, 1, a)(0, (a^2+a+1)/a, a^2+a+1),$

$a(\tau + a)/((a^2+a+1)\tau + a^2) \ : \ (0, 1, a)(\infty, a/(a^2+a+1), a^2/(a^2+a+1))$

shows

$$N_I(S) = \{1/(a+1), (a+1)/a, a(a+1), a^2/(a+1), (a^2+a+1)/a, a^2/(a^2+a+1), a^2+a+1, a/(a^2+a+1)\}.$$

This set is invariant under $\mathsf{Stab}(S) = \{a/\tau,\ (\tau + a)/(\tau + 1)\} \cong E_4$.

The neighbours of type II are furnished by elements of order 3 in $\mathsf{PGL}(2,q)$ affording one of six possible operations:

$(1) \infty \mapsto 0,\ 1 \mapsto a,$

$(2) \infty \mapsto 0,\ a \mapsto 1, \ldots,$

$(6) \infty \mapsto a,\ 1 \mapsto 0$

The existence of such an element depends on a trace-condition in each of the six cases. If the codition is satisfied, there are exactly two elements of order 3 which afford this operation. This defines then a set $N_{II,i}(S)$ of 4 elements, $i = 1, 2, \ldots, 6$. The two elements of order 3 defining II, i can be written in the form $\tau \longmapsto (\alpha\tau + \beta)/(\gamma\tau + d)$, where α, β, γ are determined and d is one of the two solutions of a quadratic equation. In each of these cases we shall list the data just mentioned. We have to prove then $N_{II,i}(S) \cap N_I(S) = \emptyset$

(provided the trace condition is satisfied). We still have the group $\mathtt{Stab}(S) \cong E_4$ at our disposition. It has the nice property of permuting transitively the elements of $N_{II,i}(S)$ for very i. Thus it suffices to fix one elements $e \in N_{II,i}(S)$ and to check that $e \notin N_I(S)$, for every $i = 1, 2, \ldots, 6$. By our assumption $(f, 6) = 1$, no elements of $\mathbb{F}_q - \{0, 1\}$ can satisfy a polynomial equation of degree smaller than 5. We shall use this fact all the time.

$(II, 1) \quad \sigma_1 : \infty \mapsto 0,\ 1 \mapsto a, \quad$ condition $\quad \mathrm{tr}(1/a) = 0,$

$\sigma_1 = a(1 + d)/(\tau + d)$, where $d^2 = a(d + 1), \quad e = d.$

$d = 1/(a + 1) \Rightarrow 1/(a^2 + 1) = a.a/(a + 1) \Rightarrow a^2(a + 1) = 1.$

$d = (a + 1)/a \Rightarrow (a^2 + 1)/a^2 = a.1/a = 1 \Rightarrow 1 = 0.$

$d = a(a + 1) \Rightarrow a^2(a^2 + 1) = a(a^2 + a + 1) \Rightarrow a^3 + a^2 + 1 = 0.$

$d = a^2/(a + 1) \Rightarrow a^4/(a^2 + 1) = a(a^2 + a + 1)/(a + 1) \Rightarrow a = 0.$

$d = (a^2 + a + 1)/a \Rightarrow (a^4 + a^2 + 1)/a^2 = a(a^2 + 1)/a = a^2 + 1 \Rightarrow 1 = 0.$

$d = a^2/(a^2 + a + 1) \Rightarrow a^4/(a^2 + a + 1)^2 = a(a + 1)/(a^2 + a + 1) \Rightarrow 1 = 0.$

$d = a^2 + a + 1 \Rightarrow a^4 + a^2 + 1 = a(a^2 + a) \Rightarrow a^4 + a^3 + 1 = 0.$

$d = a/(a^2 + a + 1) \Rightarrow a^2/(a^2 + a + 1)^2 = a(a^2 + 1)/(a^2 + a + 1) \Rightarrow a^4 + a^3 + 1 = 0.$

$(II, 2) \quad \sigma_2 : \infty \mapsto 0,\ 1 \mapsto a, \quad$ condition $\quad \mathrm{tr}(a) = 0,$

$\sigma_2 = (a + d)/(\tau + d)$, where $d^2 = d + a, \quad e = (a + d)/d.$

$e = 1/(a + 1) \Rightarrow d = a + 1 \Rightarrow a^2 + 1 = (a + 1) + a = 1 \Rightarrow a = 0.$

$e = (a + 1)/a \Rightarrow d = a^2 \Rightarrow a^4 = a^2 + a.$

$e = a(a+1) \Rightarrow d = a/(a^2+a+1) \Rightarrow a^2/(a^2+a+1)^2+a/(a^2+a+1)+a = 0 \Rightarrow a = 0.$

$e = a^2/(a + 1) \Rightarrow d = a(a + 1)/(a^2 + a + 1) \Rightarrow a^3 + a + 1 = 0.$

$e = (a^2+a+1)/a \Rightarrow d = a^2/(a^2+1) \Rightarrow a^4/(a^4+1)+a^2/(a^2+1)+a = 0 \Rightarrow a^4+a+1 = 0.$

$e = a^2/(a^2 + a + 1) \Rightarrow d = a(a^2 + a + 1)/(a + 1) \Rightarrow a^4 + a + 1 = 0.$

$e = a^2 + a + 1 \Rightarrow d = 1/(a + 1) \Rightarrow 1/(a^2 + 1) + 1/(a + 1) + a = 0 \Rightarrow a = 0.$

$e = a/(a^2 + a + 1) \Rightarrow d = a(a^2 + a + 1)/(a^2 + 1) \Rightarrow a = 0.$

$(II, 3) \quad \sigma_3 : \infty \mapsto 1,\ 0 \mapsto a, \quad$ condition $\quad \mathrm{tr}(1/(a + 1)) = 0,$

$\sigma_3 = (\tau + ad)/(\tau + d)$, where $d^2 + (a + 1)d + 1 = 0, \quad e = (ad + 1)/(d + 1).$

$e = 1/(a + 1) \Rightarrow d = a/(a^2 + a + 1) \Rightarrow a^2/(a^2 + a + 1)^2 + (a + 1)a/(a^2 + a + 1) + 1 = 0 \Rightarrow a = 1.$

$e = (a + 1)/a \Rightarrow d = 1/(a^2 + a + 1) \Rightarrow 0 = a^4 + a^3 + a^2 + 1 = (a + 1)(a^3 + a + 1).$

$e = a(a + 1) \Rightarrow d = (a^2 + a + 1)/a^2 \Rightarrow a^5 = 1 \Rightarrow f \equiv 0 \pmod 4.$

$e = a^2/(a + 1) \Rightarrow d = (a^2 + a + 1)/a \Rightarrow a = 1.$

$e = (a^2 + a + 1)/a \Rightarrow d = (a + 1) \Rightarrow (a^2 + 1) + (a + 1)(a + 1) + 1 = 0 \Rightarrow 1 = 0.$

$e = a^2/(a^2 + a + 1) \Rightarrow d = 1/(a(a + 1)) \Rightarrow a^5 = 1 \Rightarrow f \equiv 0 \pmod 4$.

$e = a^2 + a + 1 \Rightarrow d = a/(a + 1) \Rightarrow a^2/(a^2 + 1) + a + 1 = 0 \Rightarrow a^3 + a + 1 = 0$.

$e = a/(a^2 + a + 1) \Rightarrow d = (a + 1)/a^2 \Rightarrow (a^2 + 1)/a^4 + (a^2 + 1)/a^2 + 1 = 0 \Rightarrow 1 = 0$.

$(\mathrm{II}, 4)$ $\sigma_4 : \infty \mapsto 1,\ a \mapsto 0,$ condition $\mathrm{tr}(a) = 1$,

$\sigma_4 = (\tau + a)/(\tau + d)$, where $d^2 + d + a + 1 = 0,\quad e = a/d$.

$e = 1/(a + 1) \Rightarrow d = a(a + 1) \Rightarrow a^2(a^2 + 1) + a(a + 1) + a + 1 = 0 \Rightarrow a^4 = 1$.

$e = (a + 1)/a \Rightarrow d = a^2/(a + 1) \Rightarrow a^4 + a + 1 = 0$.

$e = a(a + 1) \Rightarrow d = 1/(a + 1) \Rightarrow a^3 + a^2 + 1 = 0$.

$e = a^2/(a + 1) \Rightarrow d = (a + 1)/a \Rightarrow (a^2 + 1)/a^2 + (a + 1)/a + a + 1 = 0 \Rightarrow a^4 = 1$.

$e = (a^2 + a + 1)/a \Rightarrow d = a^2/(a^2 + a + 1) \Rightarrow (a + 1) + (a^4 + 1) = 0$.

$e = a^2/(a^2 + a + 1) \Rightarrow d = (a^2 + a + 1)/a \Rightarrow (a + 1)(a^3 + a^2 + 1) = 0$.

$e = a^2 + a + 1 \Rightarrow d = a/(a^2 + a + 1) \Rightarrow (a + 1)(a^4 + a + 1) = 0$.

$e = a/(a^2 + a + 1) \Rightarrow d = a^2 + a + 1 \Rightarrow 0 = (a^4 + a^2 + 1) + (a^2 + a + 1) + a + 1 \Rightarrow a^4 = 1$.

$(\mathrm{II}, 5)$ $\sigma_5 : \infty \mapsto a,\ 0 \mapsto 1,$ condition $\mathrm{tr}(1/(a + 1)) = 1$,

$\sigma_5 = (a\tau + d)/(\tau + d)$, where $d^2 + (a + 1)d + a^2 = 0,\quad e = (a + d)/(1 + d)$.

$e = 1/(a + 1) \Rightarrow d = (a^2 + a + 1)/a \Rightarrow (a + 1)(a^3 + a^2 + 1) = 0$.

$e = (a + 1)/a \Rightarrow d = a^2 + a + 1 \Rightarrow 0 = a^4 + a^2 + 1 + (a^3 + 1) + a^2 \Rightarrow a^3(a + 1) = 0$.

$e = a(a + 1) \Rightarrow d = a^2/(a^2 + a + 1) \Rightarrow (a + 1)(a^4 + a^3 + 1) = 0$.

$e = a^2/(a + 1) \Rightarrow d = a/(a^2 + a + 1) \Rightarrow a^5 = 1 \Rightarrow f \equiv 0 \pmod 4$.

$e = (a^2 + a + 1)/a \Rightarrow d = 1/(a + 1) \Rightarrow 0 = 1/(a^2 + 1) + 1 + a^2 \Rightarrow a = 0$.

$e = a^2/(a^2 + a + 1) \Rightarrow d = a(a + 1) \Rightarrow 0 = a^2(a^2 + 1) + a(a^2 + 1) + a^2 = a^4 + a^3 + a$.

$e = a^2 + a + 1 \Rightarrow d = (a + 1)/a \Rightarrow 0 = (a^2 + 1)/a^2 + (a^2 + 1)/a + a^2 \Rightarrow a^5 = 1 \Rightarrow f \equiv 0 \pmod 4$.

$e = a/(a^2 + a + 1) \Rightarrow d = a^2/(a + 1) \Rightarrow 0 = a^4/(a^2 + 1) + a^2 + a^2 \Rightarrow a = 0$.

$(\mathrm{II}, 6)$ $\sigma_6 : \infty \mapsto a,\ 1 \mapsto 0,$ condition $\mathrm{tr}(1/a) = 1$,

$\sigma_6 = a(\tau + 1)/(\tau + d)$, where $d^2 + ad + a(a + 1) = 0,\quad e = a/d$.

$e = 1/(a + 1) \Rightarrow d = a(a + 1) \Rightarrow a(a + 1)(a^2 + 1) = 0$.

$e = (a + 1)/a \Rightarrow d = a^2/(a + 1) \Rightarrow a^3 + a + 1 = 0$.

$e = a(a + 1) \Rightarrow d = 1/(a + 1) \Rightarrow a^4 + a^3 + 1 = 0$.

$e = a^2/(a + 1) \Rightarrow d = (a + 1)/a \Rightarrow a^2 = 1$.

$e = (a^2 + a + 1)/a \Rightarrow d = a^2/(a^2 + a + 1) \Rightarrow (a + 1)(a^4 + a^3 + 1) = 0$.

$e = a^2/(a^2 + a + 1) \Rightarrow d = (a^2 + a + 1)/a \Rightarrow a^2 = 1$.

$e = a^2 + a + 1 \Rightarrow d = a/(a^2 + a + 1) \Rightarrow a = 1.$

$e = a/(a^2+a+1) \Rightarrow d = a^2+a+1 \Rightarrow (a^4+a^2+1)+(a^3+a^2+a)+a^2+a = 0 \Rightarrow a = 1.$

We get a contradiction in each case. Theorem 1.1 is proved. □

Proof of Theorem 1.3. Let X be a block of Alltop's design, i.e. $|X| = 5$ and $\mathsf{Stab}(X) \cap \mathsf{PGL}(2, q) \cong E_4$. We can choose without restriction $X = \{\infty, 0, 1, a, a + 1\}$ for some $a \in |\mathsf{GF}_q - \{0, 1\}$. Assume $X \in \Delta\mathcal{B}$. This means there is an element ρ of order 3 in $\mathsf{PGL}(2, q)$ having X in the union of two orbits. By using $\mathsf{Stab}(X)$ we can assume that one of the following holds:

$(i) \quad <\rho>=<(\infty, 0, 1)>, \quad (ii) \quad <\rho>=<(\infty, 0, a)>,$

$(iii) \quad <\rho>=<(\infty, 0, a + 1)>, \quad (iv) \quad <\rho>=<(0, 1, a)>.$

Assume (i) holds. Then $\rho = (\tau \mapsto 1/(\tau + 1))$. The orbit of a under ρ contains $1/(a + 1)$ and $(a + 1)/a$. Thus $a + 1$ is not in this orbit, contradiction. Similar considerations lead to contradictions in the remaining cases. The statement concerning automorphism group follows as in the proof of the Corollary.

References

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

[2] Ian Anderson, Combinatorics of finite sets, Clarendon Press, Oxford 1987.

[3] J. Bierbrauer, A new family of 4-designs, to appear in *Journal of Comb. Theory A.*