Discrete Mathematics 342 (2019) 2886–2892

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Automorphism groups of designs with $\lambda = 1$

William M. Kantor *

University of Oregon, Eugene, OR 97403, United States
Northeastern University, Boston, MA 02115, United States

ARTICLE INFO

Article history:
Received 4 April 2018
Accepted 30 January 2019
Available online 9 March 2019

Keywords:
Automorphism group
Design

ABSTRACT

If G is a finite group and $k = q > 2$ or $k = q + 1$ for a prime power q then, for infinitely many integers v, there is a 2-$(v, k, 1)$-design $\mathbf{D}$ for which $\mathrm{Aut}\mathbf{D} \cong G$.

1. Introduction

Starting with Frucht's theorem on graphs [7], there have been many papers proving that any finite group is isomorphic to the full automorphism group of some specific type of combinatorial object. Babai surveyed this topic [3], and in [3, p. 8] stated that in [1] he had proved that 2-designs with $\lambda = 1$ are such objects when $k = q > 2$ or $k = q+1$ for a prime power q. (The case of Steiner triple systems was handled in [13].) The purpose of this note is to provide a proof of Babai's result[1]:

Theorem 1.1. *Let G be a finite group and q a prime power.*

(i) *There are infinitely many integers v such that there is a* 2-$(v, q + 1, 1)$-*design* $\mathbf{D}$ *for which* $\mathrm{Aut}\mathbf{D} \cong G$.
(ii) *If $q > 2$ then there are infinitely many integers v such that there is a* 2-$(v, q, 1)$-*design* $\mathbf{D}$ *for which* $\mathrm{Aut}\mathbf{D} \cong G$.

Parts of our proof mimic [5, Sec. 5] and [9, Sec. 4], but the present situation is much simpler. We modify a small number of subspaces of a projective or affine space in such a way that the projective or affine space can be recovered from the resulting design by elementary geometric arguments. Further geometric arguments determine the automorphism group.

Section 7 contains further properties of the design $\mathbf{D}$ in the theorem, some of which are needed in future research [6].

Notation: We use standard permutation group notation, such as x^π for the image of a point x under a permutation π and $g^h = h^{-1}gh$ for conjugation. The group of automorphisms of a projective space $Y = \mathrm{PG}(V)$ defined by a vector space V is denoted by $\mathrm{P\Gamma L}(V) = \mathrm{P\Gamma L}(Y)$; this is induced by the group $\Gamma\mathrm{L}(V)$ of invertible semilinear transformations on V. Also $\mathrm{A\Gamma L}(V)$ denotes the group of automorphisms of the affine space $\mathrm{AG}(V)$ defined by V.

2. A simple projective construction

Let G be a finite group. Let Γ be a simple, undirected, connected graph on $\{1, \ldots, n\}$ such that $\mathrm{Aut}\Gamma \cong G$ and G acts semiregularly on the vertices. There is such a graph for each $n \geq 6|G|$ that is a multiple of $|G|$ (using [2]).

* Correspondence to: University of Oregon, Eugene, OR 97403, United States.
E-mail address: kantor@uoregon.edu.

[1] This theorem was proved before I knew of Babai's result.

https://doi.org/10.1016/j.disc.2019.01.030

Let $K=\mathbf{F}_q\subset F=\mathbf{F}_{q^4}$, and let θ generate F^*. Let V_F be an n-dimensional vector space over F, with basis $v_1,\ldots,v_n$. View G as acting on V_F, permuting $\{v_1,\ldots,v_n\}$ as it does $\{1,\ldots,n\}$. View V_F as a vector space V over K. If Y is a set of points of $\mathbf{P}=\mathrm{PG}(V)$ then $\langle Y\rangle$ denotes the smallest subspace of $\mathbf{P}$ containing Y.

We will modify the point-line design $\mathrm{PG}_1(V)$ of $\mathbf{P}$, using nonisomorphic designs Δ_1 and Δ_2 whose parameters are those of $\mathrm{PG}_1(K^4)=\mathrm{PG}_1(3,q)$ but are not isomorphic to that design, chosen so that $\mathrm{Aut}\Delta_1$ fixes a point (Proposition 3.5).

Our design $\mathbf{D}$ has the set $\mathfrak{P}$ of points of $\mathbf{P}$ as its set of points. Most blocks of $\mathbf{D}$ are lines of $\mathbf{P}$, with the following exceptions involving some of the subspaces Fv, $0\neq v\in V$, viewed as subsets of $\mathfrak{P}$. For orbit representatives i and ij of G on the vertices and ordered edges of Γ,

(I) replace the set of lines of $\mathrm{PG}_1(Fv_i)$ by a copy of the set of blocks of Δ_1, subject only to the condition

(#) there are distinct blocks, neither of which is a line of $\mathbf{P}$, whose span in $\mathbf{P}$ is $\mathrm{PG}_1(Fv_i)$,

and then apply all $g\in G$ to these sets of blocks in order to obtain the blocks in $\mathrm{PG}_1((Fv_i)^g)$, $g\in G$; and

(II) replace the set of lines of $\mathrm{PG}_1(F(v_i+\theta v_j))$ by a copy of the set of blocks of Δ_2, subject only to (#), and then apply all $g\in G$ to these sets of blocks in order to obtain the blocks in $\mathrm{PG}_1(F(v_i+\theta v_j)^g)$, $g\in G$.

We need to check that these requirements can be met.

(i) *Satisfying* (#): Let $\bar\Delta_s$ be an isomorphic copy of Δ_s, $s=1$ or 2, whose set of points is that of $\mathrm{PG}_1(Fv)=\mathrm{PG}_1(Fv_i)$ or $\mathrm{PG}_1(F(v_i+\theta v_j))$. Let B_1 and B_2 be any distinct blocks of $\bar\Delta_s$. Choose any permutation π of the points of $\mathrm{PG}_1(Fv)$ such that the sets B_1^π and B_2^π are not lines of $\mathrm{PG}_1(Fv)$ and together span $\mathrm{PG}_1(Fv)$. Using $\bar\Delta_s^\pi$ in place of $\bar\Delta_s$ satisfies (#). (If $q+1\geq 4$ then B_2 is not needed.)

(ii) *These replacements are well-defined*: For (II), if $F(v_i+\theta v_j)^g\cap F(v_i+\theta v_j)^{g'}\neq 0$ for some $g,g'\in G$, then $v_{i^{g'}}+\theta v_{j^{g'}}\in F(v_{i^g}+\theta v_{j^g})$. Then either $v_{i^{g'}}=v_{i^g}$ and $v_{j^{g'}}=v_{j^g}$, or $v_{i^{g'}}=\alpha\theta v_{j^g}$ and $\theta v_{j^{g'}}=\alpha v_{i^g}$ for some $\alpha\in F^*$; but in the latter case we obtain $1=\alpha\theta$ and $\theta=\alpha$, whereas θ generates F^*. Thus, $v_{i^{g'}}=v_{i^g}$, so the semiregularity of G on $\{1,\ldots,n\}$ implies that $g'=g$, as required.

It is trivial to see that $\mathbf{D}$ *is a design having the same parameters as* $\mathrm{PG}_1(V)$. Clearly G acts on the collection of subsets of $\mathfrak{P}$ occurring in (I) or (II): we can view G as a subgroup of both $\mathrm{Aut}\mathbf{D}$ and $\mathrm{PGL}(V)$.

We emphasize that the sets in (I) and (II) occupy a tiny portion of the underlying projective space: most sets Fv are unchanged. More precisely, in view of the definition of $\mathbf{D}$:

$$\begin{array}{l}\textit{Every block of } \mathbf{D} \textit{ not contained in a set (I) or (II) is a line of } \mathbf{P}.\\ \textit{Every line of } \mathbf{P} \textit{ not contained in set (I) or (II) is a block of } \mathbf{D}.\end{array}\tag{2.1}$$

Nevertheless, we will distinguish between the *lines of* $\mathbf{P}$ and the *blocks of* $\mathbf{D}$, even when the blocks happen to be lines. A *subspace* of $\mathbf{D}$ is a set of points that contains the block joining any pair of its points. (Examples: (I) and (II) involve subspaces of $\mathbf{D}$.) A *hyperplane* of $\mathbf{D}$ is a subspace of $\mathbf{D}$ that meets every block but does not contain every point. We need further notation:

$$\textit{Distinct } y,z\in\mathfrak{P} \textit{ determine a block } yz \textit{ of } \mathbf{D} \textit{ and a line } \langle y,z\rangle \textit{ of } \mathbf{P}.\tag{2.2}$$

$$\begin{array}{l}\textit{For distinct } y,z\in\mathfrak{P} \textit{ and } x\in\mathfrak{P}-yz,\\ \langle x|y,z\rangle=\bigcup\big\{xp\mid p\in y'z',\,y'\in xy-\{x\},\,z'\in xz-\{x\},\,\{y,z\}\neq\{y',z'\}\big\}.\end{array}\tag{2.3}$$

Here (2.3) depends only on $\mathbf{D}$ not on $\mathbf{P}$, which will allow us to recover $\mathbf{P}$ from $\mathbf{D}$.

Lemma 2.4. *If $y,z\in\mathfrak{P}$ are distinct, then there are more than $\frac{1}{2}|\mathfrak{P}|$ points $x\in\mathfrak{P}-yz$ such that*

(1) *$\langle x,y,z\rangle$ is a plane of $\mathbf{P}$ every line of which, except possibly $\langle y,z\rangle$, is a block of $\mathbf{D}$,*
(2) *$\langle x|y,z\rangle=\langle x,y,z\rangle$,*
(3) *if $yz\subseteq\langle x|y,z\rangle$ then $\langle y,z\rangle=yz$, and*
(4) *if $yz\not\subseteq\langle x|y,z\rangle$ then $\langle y,z\rangle$ is the union of the pairs $\{y_1,z_1\}\subset\langle x|y,z\rangle$ such that $y_1z_1\not\subseteq\langle x|y,z\rangle$.*

Proof. Let

$$x\notin yz\cup\bigcup\big\{\langle y,z,Fv\rangle\mid Fv \text{ in (I) or (II)}\big\}.\tag{2.5}$$

There are more than $(q^{4n}-1)/(q-1)-n^2(q^6-1)/(q-1)-(q+1)>\frac{1}{2}|\mathfrak{P}|$ such points x. Clearly $\langle x,y,z\rangle$ is a plane of $\mathbf{P}$.

(1) Let $L\neq\langle y,z\rangle$ be a line of $\langle x,y,z\rangle$, so $\langle x,y,z\rangle=\langle y,z,L\rangle$. If L is not a block of $\mathbf{D}$ then, by (2.1), L is contained in some set Fv in (I) or (II), so $x\in\langle y,z,L\rangle\subseteq\langle y,z,Fv\rangle$ contradicts (2.5).

(2) By (1), $\langle x,y\rangle$ and $\langle x,z\rangle$ are blocks of $\mathbf{D}$. Let $\{y',z'\}$ be as in (2.3). Then $\{y',z'\}\subset\langle x,y,z\rangle$ and $\langle y',z'\rangle\neq\langle y,z\rangle$. By (1), $y'z'=\langle y',z'\rangle\subseteq\langle x,y,z\rangle$ and $xp=\langle x,p\rangle\subseteq\langle x,y,z\rangle$ for each point p of $\langle y',z'\rangle$. Then $\langle x|y,z\rangle\subseteq\langle x,y,z\rangle$. Each point of $\langle x,y,z\rangle$ lies in such a line $\langle x,p\rangle$; since that line is a block by (1), $\langle x,y,z\rangle\subseteq\langle x|y,z\rangle$.

(3) If $yz\neq\langle y,z\rangle$ then, by (2.1), yz lies in some set Fv in (I) or (II). By hypothesis and (2), $yz\subseteq\langle x|y,z\rangle\cap Fv=\langle x,y,z\rangle\cap Fv=\langle y,z\rangle$. Thus, $yz=\langle y,z\rangle$.

(4) We have $yz \neq \langle y, z\rangle$ since $\langle y, z\rangle \subseteq \langle x, y, z\rangle = \langle x|y, z\rangle$ by (2). By (2.1), since $\langle y, z\rangle$ is not a block it is contained in some set Fv in (I) or (II).

For any $\{y_1, z_1\}$ in (4) we have $\{y_1, z_1\} \subseteq \langle x|y, z\rangle = \langle x, y, z\rangle$ by (2), and $y_1z_1 \not\subseteq \langle x, y, z\rangle$, so $\langle y_1, z_1\rangle$ is not a block of **D** and hence $\langle y_1, z_1\rangle = \langle y, z\rangle$ by (1).

On the other hand, consider an arbitrary pair $\{y_1, z_1\} \subset \langle y, z\rangle \subset Fv$. Then $y_1z_1 \subset Fv$ by the definition of **D**. Since $\langle y, z\rangle$ is not a block, $y_1z_1 \not\subseteq \langle y, z\rangle = \langle x|y, z\rangle \cap Fv$ by (2), so $y_1z_1 \not\subseteq \langle x|y, z\rangle$. Thus, $\langle y, z\rangle$ is the union of the pairs $\{y_1, z_1\}$ in (4). □

Proof of Theorem 1.1(i). We first recover the lines of **P** from **D**. For distinct $y, z \in \mathfrak{P}$, use each $x \notin yz$ in Lemma 2.4(3) or (4) in order to obtain, more than $\frac{1}{2}|\mathfrak{P}|$ times, the same set of points that must be $\langle y, z\rangle$.

We have now reconstructed all lines of **P** *as subsets of* $\mathfrak{P}$. Then we have also recovered **P**, V, $\Gamma L(V)$ and $P\Gamma L(V)$, so that Aut**D** is induced by a subgroup of Aut**P** $= P\Gamma L(V)$, and hence by a subgroup H of $\Gamma L(V)$ such that Aut**D** $\cong H/K^*$.

Any block of **D** that is not a line of **P** spans a 2-space or 3-space of **P** occurring in some 3-space $PG_1(Fv)$ in (I) or (II), and spans at least a 4-space of **P** together with any block in any $PG_1(Fv') \neq PG_1(Fv)$. Any two blocks of **D** that are not lines of **P** and lie in the same set in (I) or (II) span at most a 3-space of **P**; by (#) each set in (I) or (II) is spanned by two such blocks.

This recovers all subsets (I) *and* (II) *of* $\mathfrak{P}$ from **D** and **P**. Moreover, the fact that $\Delta_1 \not\cong \Delta_2$ specifies which of these subspaces of **D** have type (I) (or (II)).

We next determine the F-structure of V using **D**. We claim that *the subgroup of* $GL(V)$ *fixing each set in* (I) *or* (II) *consists of scalar multiplications by members of* F^*. Clearly such scalar multiplications behave this way. Let $h \in GL(V)$ behave as stated. Then $h: xv_i \mapsto (xA_i)v_i$ for each $x \in F$, each i and a 4×4 invertible matrix A_i over K. If ij is an ordered edge of Γ and $x \in F$, then $(x(v_i + \theta v_j))^h = (xA_i)v_i + ((x\theta)A_j)v_j$ is in $F(v_i + \theta v_j)$, so $(xA_i)\theta = (x\theta)A_j$. Since ji is an ordered edge, also $(xA_j)\theta = (x\theta)A_i$, so $(x\theta\theta)A_i = ((x\theta)A_j)\theta = (xA_i)\theta\theta$, and A_i commutes with multiplication by θ^2. By Schur's Lemma, $xA_i = xa_i$ for all $x \in F$ and some $a_i \in F^*$. Then $xa_i\theta = x\theta a_j$, so $a_i = a_j$. Since Γ is connected, all a_i are equal, proving our claim.

In particular, the field F and the F-space V_F can be reconstructed from **D**. Then $H \leq \Gamma L(V_F)$ since H normalizes F^*, while G lies in H. Since the sets in (II) correspond to (ordered) edges of Γ, H induces Aut$\Gamma \cong G$ on the collection of sets in (I). It remains to show that the kernel of this action is K^*.

Let $h \in H \leq \Gamma L(V_F)$. Multiply h by an element of G in order to have h fix all Fv_i. Let $\sigma \in$ Aut$F$ be the field automorphism associated with h. For each i we have $v_i^h = a_iv_i$ for some $a_i \in F^*$. Let ij be an ordered edge of Γ and write $b = a_j/a_i$. As above, $F(v_i + \theta v_j)^h = F(a_iv_i + \theta^\sigma a_jv_j) = F(v_i + \theta^\sigma bv_j)$ and $F(\theta v_i + v_j)^h = F(\theta^\sigma a_iv_i + a_jv_j) = F(v_i + \theta^{-\sigma}bv_j)$ both have type (II), so $\theta^\sigma b = \theta^{\pm 1}$ and $\theta^{-\sigma}b = \theta^{\mp 1}$. Then $b^2 = 1$, $\theta^\sigma = \pm\theta^{\pm 1}$, and hence $\sigma = 1$ and $b = 1$ since θ generates F^*. The connectedness of Γ implies that all a_i are equal: h is scalar multiplication by $a_1 \in F^*$.

Since h fixes Fv_1 it induces an automorphism of the subspace of **D** determined by Fv_1. By (I) and our condition on Δ_1, h fixes a point Kcv_1 of Fv_1, where $c \in F^*$. Then $Kcv_1 = (Kcv_1)^h = Kca_1v_1$, so $a_1 \in K$. Thus, $h \in K^*$ and Aut**D** $\cong G$. □

3. A simpler projective construction

We need a fairly weak result (Proposition 3.5) concerning designs with the parameters of $PG_1(3, q)$. We know of two published constructions for designs having those parameters, due to Skolem [15, p. 268] and Lorimer [12]. However, isomorphism questions seem difficult using their descriptions. Instead, we will use a method that imitates [9,14] (but which was hinted at by Skolem's idea).

Consider a hyperplane X of **P** $= PG(d, q)$, $d \geq 3$; we identify **P** with $PG_1(d, q)$. Let π be any permutation of the points of X. Define a geometry $\mathbf{D}_\pi$ as follows:

the set $\mathfrak{P}$ of points is the set of points of **P**, and
blocks are of two sorts:
- the lines of **P** not in X, and
- the sets L^π for lines $L \subset X$.

Once again it is trivial to see that $\mathbf{D}_\pi$ is a design having the same parameters as **P**. Note that π has nothing to do with the incidences between points and the blocks not in X.

We have a hyperplane X of $\mathbf{D}_\pi$ such that the blocks of $\mathbf{D}_\pi$ not in X are lines of a projective space **P** for which $\mathfrak{P}$ is the set of points. We claim that *the lines of this projective space can be recovered from* $\mathbf{D}_\pi$ *and* X. Namely, we have all points and lines of **P** not in X. For distinct $y, z \in X$ and $x \notin X$, the set $\langle x|y, z\rangle$ in (2.3) consists of the points of the plane $\langle x, y, z\rangle$ of **P**, and $\langle x|y, z\rangle \cap X$ is the line $\langle y, z\rangle$. We have now obtained all lines of the original projective space **P**, as claimed. It follows that

$$\mathrm{Aut}\mathbf{D}_\pi \leq \mathrm{Aut}\mathbf{P}. \tag{3.1}$$

The symbol X is ambiguous: it will now mean either a set of points or a hyperplane of the underlying *projective space* (as in the next result). It will not refer to X together with a different set of lines produced by a permutation π.

Proposition 3.2. *The designs* $\mathbf{D}_\pi$ *and* $\mathbf{D}_{\pi'}$ *are isomorphic by an isomorphism sending* X *to itself if and only if* π *and* π' *are in the same* $P\Gamma L(X)$, $P\Gamma L(X)$ *double coset in* Sym(X).

Moreover, the pointwise stabilizer of X *in* Aut$\mathbf{D}_\pi$ *is transitive on the points outside of* X, *and the stabilizer* $(\mathrm{Aut}\mathbf{D}_\pi)_X$ *of* X *induces* $P\Gamma L(X) \cap P\Gamma L(X)^\pi$ *on* X.

Proof. Let $g:\mathbf{D}_\pi \to \mathbf{D}_{\pi'}$ be such an isomorphism. We just saw that $\mathbf{P}$ is naturally reconstructible from either design. It follows that g is a collineation of $\mathbf{P}$; its restriction $\bar{g}$ to X is in $\mathrm{P\Gamma L}(X)$.

If $L \subset X$ is a line of $\mathbf{P}$ then g sends the block $L^\pi \subset X$ of $\mathbf{D}_\pi$ to a block $L^{\pi g} \subset X$ of $\mathbf{D}_{\pi'}$. Then $L^{\pi g \pi'^{-1}}$ is a line of $\mathbf{P}$, so that $\pi\bar{g}\pi'^{-1}$ is a permutation of the points of the hyperplane X of $\mathbf{P}$ sending lines to lines, and hence is an element $h \in \mathrm{P\Gamma L}(X)$. Thus, π and π' are in the same $\mathrm{P\Gamma L}(X)$, $\mathrm{P\Gamma L}(X)$ double coset.

Conversely, if π and π' are in the same $\mathrm{P\Gamma L}(X)$, $\mathrm{P\Gamma L}(X)$ double coset let $\bar{g}, h \in \mathrm{P\Gamma L}(X)$ with $\pi\bar{g}\pi'^{-1} = h$. Extend $\bar{g}$ to $g \in \mathrm{Aut}\mathbf{P}$ in any way. We claim that g is an isomorphism $\mathbf{D}_\pi \to \mathbf{D}_{\pi'}$. It preserves incidences between blocks not in X and points of $\mathbf{P}$ since $g \in \mathrm{Aut}\mathbf{P}$ and those incidences have nothing to do with π and π'. Consider an incidence $x \in B \subset X$ for a block B of $\mathbf{D}_\pi$. Then $B = L^\pi$ for a line $L \subset X$. Since $g \in \mathrm{Aut}\mathbf{P}$, $x^g \in B^g = B^{\bar{g}} = L^{\pi\bar{g}} = (L^h)^{\pi'}$, which is a block of $\mathbf{D}_{\pi'}$, as required.

For the final assertion, the pointwise stabilizer of X in $\mathrm{Aut}\mathbf{P}$ is in $\mathrm{Aut}\mathbf{D}_\pi$ by the definition of $\mathbf{D}_\pi$. We have seen that the group induced on X by $\mathrm{Aut}\mathbf{D}_\pi$ corresponds to the pairs $(\bar{g}, h) \in \mathrm{P\Gamma L}(X) \times \mathrm{P\Gamma L}(X)$ satisfying $\pi\bar{g}\pi^{-1} = h$. □

Note that there are many extensions g of $\bar{g}$ since the designs $\mathbf{D}_\pi$ have many automorphisms inducing the identity on X. Double cosets arise naturally in this type of result; compare [9, Theorem 4.4].

Let $v_i = (q^i - 1)/(q - 1)$.

Corollary 3.3. *There are at least $v_d!/(v_{d+1}|\mathrm{P\Gamma L}(d, q)|^2)$ pairwise nonisomorphic designs having the same parameters as* $\mathbf{P}$.

Proof. Fix π in the proposition. There are at most v_{d+1} hyperplanes Y of $\mathbf{D}_\pi$ (as in [8, Theorem 2.2]). By the proposition there are then at most $|\mathrm{P\Gamma L}(X)|^2$ choices for π' such that $\mathbf{D}_\pi \cong \mathbf{D}_{\pi'}$ by an isomorphism sending Y to X. Since there are $v_d!$ choices for π we obtain the stated lower bound. □

Remark 3.4. We describe a useful trick. *A transposition σ and a 3-cycle τ are in different* $\mathrm{P\Gamma L}(d, q)$, $\mathrm{P\Gamma L}(d, q)$ *double cosets in* $\mathrm{Sym}(N)$, *$N = (q^d - 1)/(q - 1)$, if $d \geq 3$ and we exclude the case $d = 3, q = 2$.* For, if $\sigma g = h\tau$ with $g, h \in \mathrm{P\Gamma L}(d, q)$ then $g^{-1}h = g^{-1}\cdot\sigma g\tau^{-1} = \sigma^g\tau^{-1} \in \mathrm{P\Gamma L}(d, q)$ fixes at least $N - 5$ points, and hence is 1 by our restriction on d, whereas $\sigma^g \neq \tau$.

Proposition 3.5. *For any q there are two designs having the parameters of $\mathbf{P} = \mathrm{PG}_1(3, q)$ and not isomorphic to one another or to $\mathbf{P}$, for one of which the automorphism group fixes a point.*

Proof. If $q = 2$ then there are even such designs with trivial automorphism group [4]. (Undoubtedly such designs exist for all q.)

Assume that $q > 2$. The preceding corollary and remark provide us with two nonisomorphic designs. It remains to deal with the final assertion constructively.

Let π be a transposition (x_1, x_2) of X. We will show that $\mathbf{D}_\pi$ behaves as stated.

First note that each $g \in \mathrm{Aut}\mathbf{D}_\pi$ fixes X. For, suppose that $Y = X^g \neq X$ for some g, where $g \in \mathrm{Aut}\mathbf{P}$ by (3.1). The blocks in Y not in X are lines of $\mathbf{P}$. Then the same is true of the blocks in $Y^{g^{-1}} = X$ not in $X^{g^{-1}}$. This contradicts the fact that π sends all lines $\neq \langle x_1, x_2\rangle$ of $\mathbf{P}$ inside X and on x to sets that are not lines of $\mathbf{P}$.

By Proposition 3.2, $\mathrm{Aut}\mathbf{D}_\pi = (\mathrm{Aut}\mathbf{D}_\pi)_X$ induces $\mathrm{P\Gamma L}(X) \cap \mathrm{P\Gamma L}(X)^\pi$ on X. Let $\pi\bar{g}\pi^{-1} = h$ for $\bar{g}, h \in \mathrm{P\Gamma L}(X)$. Then $\bar{g}^{-1}h = \pi^{\bar{g}}\pi^{-1}$ is a collineation of X that moves at most $2\cdot 2$ points of X and hence fixes at least $(q^2+q+1)-2\cdot 2 > q+\sqrt{q}+1$ points. By elementary (semi)linear algebra, the only such collineation is 1, so that $\bar{g} = h$ commutes with π and hence fixes the line $\langle x_1, x_2\rangle$. Then $\bar{g}$ also fixes a point of X and hence of $\mathbf{D}_\pi$. □

Remark 3.6. By excluding the possibilities $q \leq 8$ and q prime in the previous section we could have used nondesarguesian projective planes (and $[F:K] = 3$).

4. A simple affine construction

We now consider Theorem 1.1(ii). The proof is similar to that of Theorem 1.1(i). That result handles the cases $q = 3$, 4 or 5, but we ignore this and only assume that $q > 2$.

Let G and Γ be as in Section 2. This time we use $K = \mathbf{F}_q \subset F = \mathbf{F}_{q^3}$; once again θ generates F^*. Let V_F be an n-dimensional vector space over F, with basis $v_1, \ldots, v_n$. View V_F as a vector space V over K. If Y is a set of points of $\mathbf{A}$ then $\langle Y\rangle$ denotes the smallest affine subspace containing Y.

We will modify the point-line design $\mathrm{AG}_1(V)$ of $\mathbf{A} = \mathrm{AG}(V)$, using nonisomorphic designs Δ_1, Δ_2 whose parameters are those of $\mathrm{AG}_1(3, q)$ but are not isomorphic to that design, chosen so that $\mathrm{Aut}\Delta_1$ fixes at least two points (Proposition 5.2).

Our design $\mathbf{D}$ has V as its set of points. Most blocks of $\mathbf{D}$ are lines of $\mathbf{A}$, with exceptions involving the sets Fv, $0 \neq v \in V$, in Section 2(I, II), where now *Fv is viewed as a 3-dimensional affine space.*

As before, the set of lines of $\mathrm{AG}_1(Fv_i)$ or $\mathrm{AG}_1(F(v_i + \theta v_j))$ is replaced by a copy of the set of blocks of Δ_1 or Δ_2. This time, for each of these we require

(#′) there are distinct blocks, each of which spans a plane of $\mathbf{A}$, such that the intersection of those planes is a line.

Clearly, these two blocks span a 3-space. (When $q > 3$ it would be marginally easier to require that there is a single block that spans a 3-space.) Condition (#′) can be satisfied exactly as in *Satisfying* (#) in Section 2. Since different sets Fv meet only in a single point, the modifications made inside them are unrelated. Once again it is easy to check that this produces a design **D** with the desired parameters for which $G \le \mathrm{Aut}\mathbf{D}$.

As in Section 2, most sets Fv are unchanged. In view of the definition of **D**, the analogue of (2.1) holds. We use the natural analogues of definitions (2.2) and (2.3), using **A** in place of **P** and V in place of $\mathfrak{P}$.

Lemma 4.1. *If $y, z \in V$ are distinct, then there are more than $\frac{1}{2}|V|$ points $x \in V - yz$ such that*

(1) *every line of the plane $\langle x, y, z\rangle$ of* **A***, except possibly $\langle y, z\rangle$, is a block of* **D***,*
(2) $\langle x|y, z\rangle = \langle x, y, z\rangle$,
(3) *if $yz \subseteq \langle x|y, z\rangle$ then $\langle y, z\rangle = yz$, and*
(4) *if $yz \not\subseteq \langle x|y, z\rangle$ then $\langle y, z\rangle$ is the union of the pairs $\{y_1, z_1\} \subset \langle x|y, z\rangle$ such that $y_1z_1 \not\subseteq \langle x|y, z\rangle$.*

Proof. Using x in (2.5), this is proved exactly as in Lemma 2.4 except for (2), where we need to consider parallel lines using blocks that are lines by (1). Clearly $\langle x|y, z\rangle \subseteq \langle x, y, z\rangle$; we must show that $\langle x, y, z\rangle \subseteq \langle x|y, z\rangle$. In (2.3), for p in the line $y'z' = \langle y', z'\rangle$ of $\langle x, y, z\rangle$ parallel to $\langle y, z\rangle$, the blocks $xp \subset \langle x|y, z\rangle$ cover all points of the plane $\langle x, y, z\rangle$ except for those in the line L on x parallel to $\langle y, z\rangle$. If $y' \in xy - \{x, y\}$ and $p' = y'z \cap L$, then $L = xp' \subset \langle x|y, z\rangle$, so $\langle x, y, z\rangle \subseteq \langle x|y, z\rangle$. □

Proof of Theorem 1.1(ii). First recover all lines of **A** from **D** exactly as in the proof of Theorem 1.1(i). This also produces both the K-space V and $\mathrm{A\Gamma L}(V)$ from **D**.

We recover all subsets (I) and (II) essentially as before. Consider a pair B, B' of blocks of **D** behaving as in (#′): $\langle B\rangle$ and $\langle B'\rangle$ are planes and $\langle B\rangle \cap \langle B'\rangle$ is a line. Since distinct subsets in (I) or (II) do not have a common line, each such pair B, B' spans a subset in (I) or (II). Thus, by (#′) we have obtained each subset in (I) or (II) from **D** and **A** using some pair B, B'. Once again, the fact that $\Delta_1 \ncong \Delta_2$ specifies which of these subspaces of **D** have type (I) (or (II)).

The subsets (I) all contain 0, and Aut**D** fixes their intersection, so Aut**D** is induced by a subgroup of $\mathrm{A\Gamma L}(V)_0 = \Gamma\mathrm{L}(V)$.

Recover the field F exactly as in the proof of Theorem 1.1(i). Once again, Aut**D** is a subgroup of $\Gamma\mathrm{L}(V_F)$ that induces $\mathrm{Aut}\Gamma \cong G$ on the collection of sets in (I).

By repeating the argument at the end of the proof of Theorem 1.1(i) we reduce to the case of $h \in \mathrm{Aut}\mathbf{D}$ fixing all sets in (I) and acting on V as $v \mapsto av$ for some $a \in F^*$. We chose Δ_1 so that $\mathrm{Aut}\Delta_1$ fixes at least two of its points. It follows that $a = 1$, so that $h = 1$ and $\mathrm{Aut}\mathbf{D} \cong G$. □

5. A simpler affine construction

Consider a plane X of $\mathbf{A} = \mathrm{AG}(3, q) = \mathrm{AG}(V)$, $q > 2$; we identify **A** with $\mathrm{AG}_1(3, q)$. Let π be any permutation of the points of X. Define a geometry $\mathbf{D}_\pi$ as follows:

the set V of points is the set of points of **A**, and
blocks are of two sorts:
- the lines of **A** not in X, and
- the sets L^π for lines $L \subset X$.

Once again it is trivial to see that $\mathbf{D}_\pi$ is a design having the same parameters as **A**.

As in Section 3, the blocks of $\mathbf{D}_\pi$ not in X are lines of an affine space **A** for which V is the set of points. As in Sections 3 and 4, *the lines of this affine space can be recovered from* $\mathbf{D}_\pi$ using the analogue of (2.3).

Proposition 5.1. *The designs $\mathbf{D}_\pi$ and $\mathbf{D}_{\pi'}$ are isomorphic by an isomorphism sending X to itself if and only if π and π' are in the same $\mathrm{A\Gamma L}(X)$, $\mathrm{A\Gamma L}(X)$ double coset in $\mathrm{Sym}(X)$. This produces at least $q^2!/(q(q^2+q+1)|\mathrm{A\Gamma L}(2, q)|^2)$ pairwise nonisomorphic designs having the same parameters as $\mathrm{AG}_1(3, q)$.*

Moreover, the pointwise stabilizer of X in $\mathrm{Aut}\mathbf{D}_\pi$ is transitive on the points outside of X, and $(\mathrm{Aut}\mathbf{D}_\pi)_X$ induces $\mathrm{A\Gamma L}(X) \cap \mathrm{A\Gamma L}(X)^\pi$ on X.

Proof. This is the same as for Proposition 3.2 and Corollary 3.3. □

Proposition 5.2. *For any $q \ge 3$ there are at least two designs having the parameters of $\mathbf{A} = \mathrm{AG}_1(3, q)$, not isomorphic to one another or to* **A***, such that the automorphism group of one of them fixes at least two points.*

Proof. The bound in the preceding proposition provides us with many nonisomorphic designs. We need to deal with the requirement concerning automorphism groups. By [11] we may assume that $q \ge 4$.

Let $\pi \in \mathrm{Sym}(X)$ be a 4-cycle (x, x_1, x_2, x_3), where x_1, x_2, x_3 are on a line not containing x. We will show that $\mathbf{D}_\pi$ behaves as required.

Let $g \in \mathrm{Aut}\mathbf{D}_\pi$. As in the proof of Proposition 3.5, g fixes X and induces a collineation $\bar{g}$ of the subspace X of $\mathbf{A}$. By Proposition 5.1, $\pi\bar{g} = h\pi$ with $\bar{g}, h \in \mathrm{A\Gamma L}(X)$. As before, $\bar{g}^{-1}h = \pi^{\bar{g}}\pi^{-1}$ is a collineation of X that fixes at least $q^2 - 2\cdot 4 > q$ points as $q \geq 4$. Then $\bar{g} = h$ and $\pi^{\bar{g}} = \pi$. Since the collineation $\bar{g}$ commutes with π it fixes $\{x, x_1, x_2, x_3\}$ and hence also x, and so is the identity on the support of π. Thus, $\mathrm{Aut}\mathbf{D}_\pi$ is the identity on that support. □

6. Steiner quadruple systems

We have avoided $\mathrm{AG}(d, 2)$ in the preceding two sections. Here we briefly comment about those spaces in the context of 3-$(v, 4, 1)$-designs (Steiner quadruple systems), outlining a proof of the following result in [13].

Theorem 6.1. *If G is a finite group then there are infinitely many integers v such that there is a 3-$(v, 4, 1)$-design $\mathbf{D}$ for which* $\mathrm{Aut}\mathbf{D} \cong G$.

Proof. Let $K = \mathbf{F}_2 \subset F = \mathbf{F}_{16}$ and Γ be as in Section 2, with θ a generator of F^*. Let V_F be a vector space over F with basis $v_1, \ldots, v_n$, viewed as a K-space V. This time we modify the 3-design $\mathrm{AG}_2(V)$ of points and (affine) planes of V. We use nonisomorphic designs Δ_1, Δ_2 having the parameters of $\mathrm{AG}_2(4, 2)$ but not isomorphic to that design, and such that $\mathrm{Aut}\Delta_1 = 1$ [10].

Once again our design $\mathbf{D}$ has V as its set of points. Most blocks of $\mathbf{D}$ are planes of $\mathbf{A}$, with exceptions involving the sets Fv, $0 \neq v \in V$, in Section 2(I, II), where now Fv *is viewed as a 4-dimensional affine space.* As before, the set of planes of $\mathrm{AG}_2(Fv_i)$ or $\mathrm{AG}_2(F(v_i + \theta v_j))$ is replaced by a copy of the set of blocks of Δ_1 or Δ_2. This time, for each of these we require

(#″) there are distinct blocks, each of which spans a 3-space of $\mathbf{A}$, such that the intersection of those 3-spaces is a plane.

Once again it is easy to check that this produces a design $\mathbf{D}$ with the desired parameters for which $G \leq \mathrm{Aut}\mathbf{D}$.

Distinct $x, y, z \in V$ determine a block xyz of $\mathbf{D}$ and a plane $\langle x, y, z\rangle$ of $\mathbf{A}$. For distinct x, y, z and $w \notin xyz$, instead of (2.3) we use $\langle w|x, y, z\rangle = \bigcup \big\{abc \mid a \in wxy - \{w\}, b \in wxz - \{w\}, c \in wyz - \{w\}$, with a, b, c distinct and not all in $\{x, y, z\}\big\}$.

As before, all planes of $\mathbf{A}$ can be recovered from $\mathbf{D}$, this time using various sets $\langle w|x, y, z\rangle$. Also the sets in (I) and (II) can be recovered, as can F, and the argument at the end of Section 4 goes through as before. □

7. Concluding remarks

Remark 7.1. When considering possible consequences of this paper it became clear that additional properties of our designs should also be mentioned.

(1) Additional properties of the design $\mathbf{D}$ in Theorem 1.1(i).

- (a) $\mathrm{PG}(3, q)$-*connectedness*. The following graph is connected: the vertices are the subspaces of $\mathbf{D}$ isomorphic to $\mathrm{PG}_1(3, q)$, with two joined when they meet.
- (b) $\mathrm{PG}(n-1, q)$ *generation*. $\mathbf{D}$ is generated by its subspaces isomorphic to $\mathrm{PG}_1(n-1, q)$.
- (c) Every point of $\mathbf{D}$ is in a subspace isomorphic to $\mathrm{PG}_1(n-1, q)$ (in fact, many of these).
- (d) More than q^n points are moved by every nontrivial automorphism of $\mathbf{D}$.

(2) Additional properties of the design $\mathbf{D}$ in Theorem 1.1(ii).

- (a) $\mathrm{AG}(3, q)$-*connectedness*. The following graph is connected: the vertices are the subspaces of $\mathbf{D}$ isomorphic to $\mathrm{AG}_1(3, q)$, with two joined when they meet.
- (b) $\mathrm{AG}(n, q)$ *generation*. $\mathbf{D}$ is generated by its subspaces isomorphic to $\mathrm{AG}_1(n, q)$.
- (c) Every point of $\mathbf{D}$ is in a subspace isomorphic to $\mathrm{AG}_1(n, q)$ (in fact, many of these).
- (d) More than q^n points are moved by every nontrivial automorphism of $\mathbf{D}$.

(3) Additional properties of the design $\mathbf{D}$ in Theorem 6.1. This time versions of (2a) (using $\mathrm{AG}_2(4, 2)$-connectedness), (2b), (2c), (2d) (2e) hold.

These reflect the fact that the sets of points in (I) or (II) cover a tiny portion of the underlying projective or affine space: a subset of the points determined by F-linear combinations of at most two of the v_i. For (1a), it is easy to see that any point in $\mathfrak{P}$ lies in a 4-space of V that contains some point $K\beta\sum_i v_i$, $\beta \in F^*$, and meets each set in (I) or (II) in at most a point; by (2.1) this produces a subspace of $\mathbf{D}$ isomorphic to $\mathrm{PG}_1(3, q)$. Moreover, all $K\beta\sum_i v_i$ lie in $F(\sum_i v_i)$, which also produces a subspace of $\mathbf{D}$ isomorphic to $\mathrm{PG}_1(3, q)$.

For (1b) we give examples of subspaces of V:

$$\langle v_1 + \theta^2 v_2, v_2 + \theta^2 v_3 + \theta^i v_4, \ldots, v_{n-2} + \theta^2 v_{n-1} + \theta^i v_n, v_1 + v_2 + v_4 + v_5, \theta(v_1 + v_2 + v_4 + v_5)\rangle$$

for $2 < i < q^4 - 1$. Each of these misses all sets in (I) or (II), and hence determines a subspace of $\mathbf{D}$ isomorphic to $\mathrm{PG}_1(n-1, q)$. These subspaces generate a subspace of $\mathbf{D}$ containing the points $K(\theta^i - \theta^3)v_n$, $3 < i < q^4 - 1$, and hence also $\mathrm{PG}_1(Fv_n)$. Now permute the subscripts to generate $\mathbf{D}$.

Part (1c) holds by using K-subspaces similar to the above ones. There are clearly projective spaces of larger dimension that are subdesigns of **D**.

Part (1d) depends on the semiregularity of G on $\{v_1, \ldots, v_n\}$. Use the points $K\sum_i \alpha_i v_i$ with $\alpha_1 = 1$ and $\alpha_i \in F - \{1\}$ for $i > 1$, where each $\alpha \in F - \{1\}$ occurs either for 0 or at least two basis vectors v_i. The lower bound q^n is easy to obtain but very poor.

Both (2) and (3) are handled as in (1).

Remark 7.2. In (II) we used the K-subspaces $F(v_i + \theta v_j)$. We could have used subspaces $F(v_i + \theta_r v_j)$, $r = 1, \ldots, s$, for various θ_r, together with further nonisomorphic designs $\Delta_{2,r}$ (which are needed to distinguish among the $F(v_i + \theta_r v_j)$). All proofs go through without difficulty, as do the additional properties in the preceding remark.

Remark 7.3. Each of our designs has the same parameters as some $\mathrm{PG}_1(V)$ or $\mathrm{AG}_1(V)$. What is needed is a much better type of result, such as: *for each finite group G there is an integer $f(|G|)$ such that, if q is a prime power and if $v > f(|G|)$ satisfies the necessary conditions for the existence of a* 2-$(v, q+1, 1)$-*design, then there is such a design* **D** *for which* Aut**D** $\cong G$. When $q = 2$ this result is proved in a sequel to the present paper [6].

Acknowledgments

I am grateful to Jean Doyen for providing me with a clear description of Skolem's construction and for helpful comments concerning this research. I am also grateful to a referee for many helpful comments. This research was supported in part by a grant from the Simons Foundation.

References

[1] L. Babai, BIBD's with given automorphism groups, (unpublished); see [3, p. 8].
[2] L. Babai, On the minimum order of graphs with given group, Can. Math. Bull. 17 (1974) 467–470.
[3] L. Babai, On the abstract group of automorphisms, in: Combinatorics (Swansea, 1981), in: LMS Lecture Notes, vol. 52, Cambridge U. Press, Cambridge-New York, 1981, pp. 1–40.
[4] F.N. Cole, L.D. Cummings, H.S. White, The complete enumeration of triad systems in 15 elements, Proc. Natl. Acad. Sci. 3 (1917) 197–199.
[5] U. Dempwolff, W.M. Kantor, Distorting symmetric designs, Des. Codes Cryptogr. 48 (2008) 307–322.
[6] J. Doyen, W.M. Kantor, Automorphism groups of Steiner triple systems. http://arxiv.org/abs/1808.03615.
[7] R. Frucht, Herstellung von Graphen mit vorgegebener abstrakter Gruppe, Compos. Math. 6 (1938) 239–250.
[8] D. Jungnickel, V.D. Tonchev, The number of designs with geometric parameters grows exponentially, Des. Codes Cryptogr. 55 (2010) 131–140.
[9] W.M. Kantor, Automorphisms and isomorphisms of symmetric and affine designs, J. Algebr. Comb. 3 (1994) 307–338.
[10] P. Kaski, P. Östergård, O. Pottonen, The Steiner quadruple systems of order 16, J. Combin. Theory Ser. A 113 (2006) 1764–1770.
[11] C.C. Lindner, A. Rosa, On the existence of automorphism free Steiner triple systems, J. Algebra 34 (1975) 430–443.
[12] P. Lorimer, A class of block designs having the same parameters as the design of points and lines in a projective 3-space, in: Combinatorial Mathematics (Proc. Second Australian Conf. Univ. Melbourne, Melbourne, 1973), in: Lecture Notes in Math., vol. 403, Springer, Berlin, 1974, pp. 73–78.
[13] E. Mendelsohn, On the groups of automorphisms of Steiner triple and quadruple systems, J. Combin. Theory Ser. A 25 (1978) 97–104.
[14] S.S. Shrikhande, On the nonexistence of affine resolvable balanced incomplete block designs, Sankhyā 11 (1951) 185–186.
[15] E. Witt, Über Steinersche Systeme, Abh. Math. Sem. Hamburg 12 (1938) 265–275.