J Algebr Comb (2008) 28: 351–363
DOI 10.1007/s10801-007-0105-0

Universal families of permutation groups

William M. Kantor

Received: 21 May 2007 / Accepted: 25 October 2007 / Published online: 20 November 2007

Abstract For several families $\mathcal{F}$ of finite transitive permutation groups it is shown that each finite group is isomorphic to a 2-point stabilizer of infinitely many members of $\mathcal{F}$.

Keywords Permutation groups · 2-point stabilizer

1 Introduction

Graphs, strongly regular graphs, finite distributive lattices and many other combinatorial objects are *universal* [1] in the sense that each finite group is isomorphic to the *full* automorphism group of one of these objects. In this note we consider a group-theoretic version of this notion. A family $\mathcal{F}$ of finite permutation groups will be called *universal* if each finite group is isomorphic to a 2–point stabilizer of a member of $\mathcal{F}$.

We describe a transitive permutation group as A/B, the set of cosets of a subgroup B of A with the usual action. In each of the following families, the subgroup B is embedded in A in a "natural" manner, specified more precisely in Sect. 2.

Theorem 1.1 *Each of the following families of permutation groups is universal, where q is any given prime power and n ranges over all positive integers*:

(i) $S_{\binom{n}{k}}/S_n$ *for fixed* $k \geq 2$;

(ii) $S_{\binom{n}{k}_q}/P\Gamma L(n,q)$ *for fixed* $k \geq 1$ *and* q, *where the Gaussian coefficient* $\binom{n}{k}_q$ *is the number of* k*-dimensional subspaces of* $\mathbb{F}_q^n$;

This research was supported in part by NSF grants DMS 9301308 and DMS 0242983.

W.M. Kantor (✉)
University of Oregon, Eugene, OR 97403, USA
e-mail: kantor@uoregon.edu

(iii) *$S_{a(n,k)_q}/A\Gamma L(n,q)$ for fixed $k \geq 0$ and q, where $a(n,k)_q$ denotes the number of k-dimensional affine subspaces of $\mathbb{F}_q^n$;*
(iv) *$S_N/P\Gamma I(V)$ for any fixed isometry type $\mathcal{I}_k$ of $N = |\mathcal{I}_k(V)|$ totally singular or nondegenerate k–dimensional subspaces of an n–dimensional symplectic, orthogonal or unitary vector space V, over a given finite field, with projective semilinear isometry group $P\Gamma I(V)$; and*
(v) $\mathrm{PGL}(n,q)/N(n,q)$ *for each q, where $N(n,q)$ is the group of $n \times n$ monomial matrices over $\mathbb{F}_q$ modulo scalars.*

In Sect. 2 we will show that, whenever n is sufficiently large with respect to $|G|$, in each case there is a 2–point stabilizer isomorphic to G. The group-theoretic structure of G does not enter at all: our arguments are the same for cyclic groups and simple groups.

This type of question arose in [6], where a stronger version of (ii) in the case $k = 1$ was used to show that the set of symmetric designs with the parameters of a projective space $\mathrm{PG}(d,q)$ is universal for each $q \geq 3$. (The same was accomplished for Hadamard designs much later in [7], again using a version of (ii) with $k = 1$.) A general conjecture concerning universality appeared in [2] (see below). The preceding examples were obtained soon afterwards, but universality seemed and still seems an entertaining rather than a useful property. Nevertheless, our results and related ones [4, 5] suggest that this notion needs to be examined further.

Each of the permutation groups in the theorem has base size 2 for large n. In fact, a simple counting argument [2] shows that "almost all" pairs of points are bases. Our arguments show that there are large numbers of orbits of pairs of points with stabilizers isomorphic to G (cf. Theorem 2.1′). It is difficult to imagine how mere counting could prove this.

What these results need is a general theory. Is there a general result that includes all of the above permutation groups? One possibility is

> [2, Conjecture 2.4]: Let $G_1, G_2, \ldots$ be primitive groups of degrees $n_1, n_2, \ldots$, where $n_i \to \infty$ and $G_i \neq S_{n_i}$ or A_{n_i} for all i. Let X be an abstract group which is embeddable in G_i for infinitely many values of i. Then, for some i, and some permutation $g \in S_{n_i}$, we have $G_i \cap G_i^g = X$.

It might be more reasonable to assume, in addition, that there are "natural" injections $G_i \to G_{i+1}$ for all i, as in all known examples of this phenomenon.

Proof outline All of the proofs are elementary. The idea is as follows. In each case we have a permutation action A/B of a symmetric or linear group A on a large set. We construct a rather boring faithful permutation action of the target group G on A/B: a small number of regular orbits together with a very large number of fixed points. We then construct a permutation or linear transformation $\alpha \in A$ that commutes with G and whose cycles are very restricted. The goal is then to show that, if $\sigma \in B$ and $\sigma^\alpha = \tau \in B \cap B^\alpha$, then $\sigma = \tau \in G$. In general, this is accomplished in two steps.

(1) We prove that $\alpha^{-1}\alpha^\sigma = \tau^{-1}\sigma$ is 1 by playing information concerning the supports of α and α^σ against the fact that $\tau^{-1}\sigma \in B$.

(2) Once σ commutes with α we use the nontrivial cycles of α to restrict σ and eventually to deduce that $\sigma \in G$. These cycles are designed to be of different lengths

whenever this is allowed by the requirement that α commutes with G; and the supports of these cycles must overlap somewhat when viewed in the underlying set or vector space.

In order for both (1) and (2) to work we need to have a highly structured set, or basis of a vector space, underlying A; and a detailed description of the desired element α, including the lengths and supports its different cycles. Nevertheless, there is a great deal of freedom in our constructions. Our choices for α are certainly far from optimal.

We emphasize that our elementary arguments are far more combinatorial than they are group-theoretic.

2 Proofs

There is an obvious permutation action of S_n on the set $\binom{X}{k}$ of all k-subsets of the n-set X underlying S_n. We begin with the case $k = 2$:

Theorem 2.1 *If G is a finite group and $n > (2|G| + 1)[\log |G| + 3] + 4$, then G is isomorphic to a 2–point stabilizer in the permutation group $S_{\binom{n}{2}}/S_n$.*[1]

Proof Let $G = \langle g_1, \dots, g_d\rangle$ with d minimal, so that all $g_j \neq 1$ and $d \leq \log |G|$; let $d = 0$ if $G = 1$. We will use the following n–set X:

$$X := (G \times M)\dot{\cup}\{u\}\dot{\cup}Y \text{ with } M := \{1, \dots, m\} \text{ for } m := d + 3$$

for some set $\{u\}\dot{\cup}Y$, where $g \in G$ acts faithfully on X by inducing 1 on $\{u\} \cup Y$ and sending $(h, i) \mapsto (hg, i)$ for $h \in G, i \in M$. Thus, we can view G as a subgroup of S_n. Note that

$$|Y| - 2 = n - |G|m - 3 > |G|m + m + 1 > m \tag{1}$$

by hypothesis.

Choose distinct points $y_0, \dots, y_m \in Y$.

Let $\{Z, u\} := \{\{z, u\} \mid z \in Z\} \subseteq \binom{X}{2}$ whenever $Z \subseteq X\backslash\{u\}$.

Let $\gamma(k)$ denote the k–cycle $(1, \dots, k)$ of M; we will use various k.

We will show that, for the permutation $\alpha \in S_{\binom{n}{2}}$ defined as follows, *$S_n \cap S_n^\alpha$ and $C_{S_n}(\alpha)$ both turn out to be G*:

- $\alpha\colon \{(g, i), u\} \mapsto \{(g, i^{\gamma(m)}), u\}$ for all $g \in G, i \in M$,
- $\alpha\colon \{(g, i), y_0\} \leftrightarrow \{(g, i), y_i\}$ for all $g \in G, i \in M$,
- $\alpha\colon \{(g, i), (g_j g, i^{\gamma(j+2)})\} \mapsto \{(g, i^{\gamma(j+2)}), (g_j g, i^{\gamma(j+2)^2})\}$
  for all $g \in G$, $1 \leq j \leq d$, $1 \leq i \leq j + 2$, and
- α is a $(|Y| + 1)$–cycle on $\{Y, u\} \cup \big\{\{y_0, y_1\}\big\}$.

[1] Logarithms will be to the base 2.

(We assume that σ fixes every 2-subset not mentioned. We will adopt this convention in all descriptions of permutations in later proofs.) To see that this is well-defined, suppose that $\{(g,i),(g_jg,i^{\gamma(j+2)})\}=\{(g',i'),(g_{j'}g',i'^{\gamma(j'+2)})\}$ for some g,i,j,g',i',j' with $j\geq j'$ (so that $i\leq j+2$). The possibility $i=i'^{\gamma(j'+2)}$, $i^{\gamma(j+2)}=i'$, cannot occur: the support of the product of $\gamma(j+2)=(1,\dots,j+2)$ and $\gamma(j'+2)=(1,\dots,j'+2)$ is $\{1,\dots,j+2\}$ since $j+2\geq j'+2\geq 3$. It follows that $g=g'$, $i=i'$ and $g_jg=g_{j'}g$, so that $j=j'$.

Note that $\gamma(j+2)$ is not used when $G=1$ (i.e., $d=0$). Also note that every pair containing u is in the support of α.

Clearly G centralizes α.

Consider $\sigma,\tau\in S_n$ such that $\sigma^\alpha=\tau$. We must show that $\sigma=\tau\in G$.

Claim 1 *α centralizes σ.*

Otherwise, $1\neq\rho:=\alpha^{-1}\alpha^\sigma=\alpha^{-1}\sigma^{-1}\alpha\sigma=\tau^{-1}\sigma\in S_n$. The only pairs in $\binom{X}{2}$ that might be moved by ρ are those in the support of α or α^σ, namely

$$\begin{aligned}&\{(g,i),u\},\ \{(g,i),y_0\},\ \{(g,i),y_i\},\\&\quad\{(g,i),(g_jg,i^{\gamma(j+2)})\},\ \{y,u\},\ \{y_0,y_1\},\\&\{(g,i),u\}^\sigma,\ \{(g,i),y_0\}^\sigma,\ \{(g,i),y_i\}^\sigma,\\&\quad\{(g,i),(g_jg,i^{\gamma(j+2)})\}^\sigma,\ \{y,u\}^\sigma,\ \{y_0,y_1\}^\sigma,\end{aligned}$$

for some g,i,j,y. If ρ moves some $x\in X$ then it moves all $n-2$ pairs $\{x,x'\}$ with $x'\in X-\{x,x^\rho\}$. Since $n-2>2(|G|m+2)$ by hypothesis, the only members of X occurring in (at least) $n-2$ members of the above list are u and u^σ. It follows that these are the only points moved by ρ, and hence $\rho=(u,u^\sigma)$.

There are at least $|Y|-2$ choices for $z_1\in Y$ such that $\{z_1,u\}^{\alpha^{-1}}\neq\{y_0,y_1\},\{u,u^\sigma\}$, and then $\{z_1,u\}^{\alpha^{-1}}=\{z_2,u\}$ with $z_2\in Y$ and $z_2\neq u^\sigma=u^\rho$. For each such z_1 we have $\{z_2,u\}^{\alpha^\sigma}=\{z_1,u\}^{\alpha^{-1}\alpha^\sigma}=\{z_1^\rho,u^\rho\}=\{z_1,u^\sigma\}\neq\{z_2,u\}$, so that $\{z_2,u\}$ lies in the support of α^σ and hence must be a pair of the form $\{(g,i)^\sigma,u^\sigma\}$, $\{(g,i)^\sigma,y_0^\sigma\}$, $\{(g,i)^\sigma,y_i^\sigma\}$, $\{(g,i)^\sigma,(g_jg,i^{\gamma(j+2)})^\sigma\}$, $\{y^\sigma,u^\sigma\}$ or $\{y_0^\sigma,y_1^\sigma\}$. Since $u^\sigma\neq z_2,u$, no pair $\{y^\sigma,u^\sigma\}$ can occur here. Thus, for each of (at least) $|Y|-2$ choices for z_1, we have $z_2\in(G\times M)^\sigma\cup\{y_i^\sigma\mid 0\leq i\leq m\}$. Then $|Y|-2\leq|G|m+m+1$, which contradicts (1). This proves our claim.

Claim 2 $\sigma\in G$.

Clearly $\sigma=\tau$ permutes the cycles of α. Since α has a unique $(|Y|+1)$–cycle (as $n<2|Y|+1$), $\sigma\in S_n$ centralizes the $(|Y|+1)$–cycle on $\{Y,u\}\cup\{\{y_0,y_1\}\}$, hence fixes $\{y_0,y_1\}$ and thus is 1 on $Y\cup\{u\}$.

Since $j+2\leq d+2=m-1$, each m–cycle of α has support $\{g\times M,u\}$ for some $g\in G$, so that these sets are permuted by σ. Since σ fixes u, it permutes the subsets of X of the form $g\times M$, $g\in G$: there is a permutation $g\mapsto\bar g$ of G such that $(g\times M)^\sigma=\bar g\times M$ for all $g\in G$.

If $i \in M$, then σ permutes the transpositions of α involving $y_i = y_i^{\sigma}$, and hence sends $G \times i$ to itself. Thus, $(g, i)^{\sigma} = (\bar{g}, i)$ for all g, i.

This completes the proof if $G = 1$. Thus, we now assume that $G \neq 1$. In view of the action of G on X, by replacing σ by $\sigma \bar{1}^{-1}$ we may assume that $\bar{1} = 1$. We must show that $\sigma = 1$.

Fix g and j. Then the pairs $\{(g, i), (g_j g, i^{\gamma(j+2)})\}$, $1 \le i \le j+2$, lie in a $(j+2)$-cycle of α that is sent by σ to another $(j+2)$-cycle. Thus, $\big\{\{(g, i), (g_j g, i^{\gamma(j+2)})\} \mid 1 \le i \le j+2\big\}^{\sigma} = \big\{\{(\bar{g}, i), (\overline{g_j g}, i^{\gamma(j+2)}) \mid 1 \le i \le j+2\}\big\}$ must have the form $\big\{\{(g', i'), (g_j g', i'^{\gamma(j+2)})\} \mid 1 \le i' \le j+2\big\}$ for some g'. As before, there cannot be a pair $i, i' \in \{1, \dots, j+2\}$ such that $(\bar{g}, i) = (g_j g', i'^{\gamma(j+2)})$ and $(g_j g, i^{\gamma(j+2)}) = (g', i')$. Consequently, $\bar{g} = g'$ and $\overline{g_j g} = g_j g' = g_j \bar{g}$ for each j.

Since the g_j generate G it follows that $\overline{hg} = h\bar{g}$ for all $h, g \in G$. Letting $g = 1$ we see that $\bar{h} = h\bar{1} = h$ for all $h \in G$, and hence $(g, i)^{\sigma} = (g, i)$ for all g, i, as claimed. □

There are many choices for α in the above simple construction. Perhaps more interesting is the observation that there are so many choices that the number of nonconjugate pairs $\{S_n, S_n^{\alpha}\}$ with $G = S_n \cap S_n^{\alpha}$ is enormous:

Theorem 2.1′ *In* Theorem 2.1, *if also $n \ge 40$ then there are more than $n^{n^2/10}$ orbits of $S_{\binom{n}{2}}$ on the pairs of points whose stabilizers are isomorphic to G.*

Proof We let X and G be the same as before, and construct permutations α as above for a given choice $y_0, \dots, y_m \in Y$ such that α also has one further cycle of length $\binom{|Y|-1}{2}$ using all of $Y \backslash \{y_0\}$. The same argument as above shows that we still have $S_n \cap S_n^{\alpha} = G$. The number of α obtained in this manner is the number of choices for our additional cycle, namely $N := \left(\binom{|Y|-1}{2} - 1\right)!$, where $|Y| > 1 + n/2$.

The subgroup S_n of $S_{\binom{n}{2}}$ is self-normalizing, and each orbit of S_n on $S_{\binom{n}{2}}/S_n$ has size at most $n!$. Thus, the number of inequivalent pairs $S_n, S_n\alpha$ of points for which $S_n \cap S_n^{\alpha} = G$ is at least

$$N/n! > (n^2/8) \cdots (n+1) > n^{(n^2-8n)/8} \ge n^{n^2/10}. \qquad \square$$

The above lower bound estimate is clearly very crude. Similar addenda are easily obtained for our remaining theorems.

Theorem 2.2 *If G is a finite group, $k \ge 3$ and $n \ge 2|G|[\log|G| + k]^2$, then G is isomorphic to a 2–point stabilizer in the permutation group $S_{\binom{n}{k}}/S_n$.*

Proof Let $G = \langle g_1, \dots, g_d \rangle$ be as before, where $d \le \log|G|$, and let $m := d + k$ and $M := \{1, \dots, m\}$. This time let our n-set be the disjoint union

$$X = (G \times M) \dot{\cup} \{u\} \dot{\cup} W \dot{\cup} Y,$$

where G acts on $G \times M$ as before, inducing 1 on $\{u\} \cup W \cup Y$, and where $|W| = k - 2$. Note that $|Y| = n - |G|m - 1 - (k-2) > |G|mk$ by hypothesis.

Let $y_0, \dots, y_m \in Y$ and $\gamma(k)$ be as before. Let $Y_{k-2} = \{y_2, \dots, y_{k-1}\}$, and let Y^* be any set of $(m+1)-(k-2)$ members of $\binom{Y}{k}$.

If K is any $(k-2)-$subset of X, for any distinct $a, b \in X \backslash K$ write

$$\{a, b, K\} := \{a, b\} \cup K \in \binom{X}{k}, \text{ and}$$

$$\{A; b, K\} := \big\{\{a, b, K\} \mid a \in A\big\} \subseteq \binom{X}{k} \quad \text{if } A \subseteq X \backslash (K \cup \{b\}).$$

Define $\alpha \in S_{\binom{n}{k}}$ as follows:

- α: $\{(g, i), u, W\} \mapsto \{(g, i^{\gamma(m)}), u, W\}$ for all $g \in G, i \in M$,
- α: $\{(g, i), y_0, W\} \leftrightarrow \{(g, i), y_i, W\}$ for all $g \in G, i \in M$,
- α: $\{(g, i), (g_j g, i^{\gamma(j+2)}), W\} \mapsto \{(g, i^{\gamma(j+2)}), (g_j g, i^{\gamma(j+2)^2}), W\}$ for all $g \in G$, $1 \le j \le d$, $1 \le i \le j+2$,
- α is a $(|Y|+1)$–cycle on all $|Y|+1$ members of $\{Y; u, W\} \cup \big\{\{y_0, y_1, W\}\big\}$, and
- α is an $(m+1)$–cycle on all $m+1$ members of $\{W; y_0, Y_{k-2}\} \cup Y^*$.

Note that $j+2 \le d+2 < m$, so that $1 \le i \le j+2$ implies that $i \in M$. Once again, α is well-defined and centralizes G.

Let $\sigma, \tau \in S_n$ and $\sigma^\alpha = \tau$. Once again we claim that α centralizes σ. This time, the only k–sets that might be moved by $\rho := \alpha^{-1}\alpha^\sigma = \tau^{-1}\sigma \in S_n$ are

$$\begin{aligned} &\{(g, i), u, W\},\ \{(g, i), y_0, W\},\ \{(g, i), y_i, W\} \\ &\quad \{(g, i), (g_j g, i^{\gamma(j+2)}), W\},\ \{y; u, W\},\ \{y_0, y_1, W\}, \{w; y_0, Y_{k-2}\},\ \text{in } Y^*, \\ &\{(g, i), u, W\}^\sigma,\ \{(g, i), y_0, W\}^\sigma,\ \{(g, i), y_i, W\}^\sigma, \\ &\quad \{(g, i), (g_j g, i^{\gamma(j+2)}), W\}^\sigma,\ \{y; u, W\}^\sigma,\ \{y_0, y_1, W\}^\sigma,\ \{w; y_0, Y_{k-2}\}^\sigma,\ \text{in } Y^{*\sigma}, \end{aligned}$$

for some j, g, i, y, w. If ρ moves some $x \in X$ then it moves all $\binom{n-2}{k-1}$ of the k–sets containing x but not x^ρ. However, it follows from the above list that fewer than $4n$ of the k–sets moved by ρ contain any given member of X, where $4n \le \binom{n-2}{2} \le \binom{n-2}{k-1}$. Thus, $\rho = 1$, as claimed. (N.B.–Thus, the case $k \ge 3$ is somewhat easier than the case $k = 2$ was.)

Consequently, $\sigma = \tau$ permutes the cycles of α, which have lengths m, 2, $j+2$, $m+1$ or $|Y|+1$, where $2 < j+2 \le d+2 < m < m+1 < |Y|+1$. Since $\sigma \in S_n$ centralizes the $(|Y|+1)$–cycle on $\{Y; u, W\} \cup \big\{\{y_0, y_1, W\}\big\}$, it sends this set to itself, hence fixes u, $\{y_0, y_1\}$, Y and W, and then is 1 on Y. Also σ centralizes the $(m+1)$–cycle of α and is 1 on $\{u\} \cup Y_{k-2}$ and Y^*, and hence it is also 1 on W.

Since σ permutes the m–cycles of α it permutes the sets $\{g \times M; u, W\}$, $g \in G$, and hence also the sets $g \times M$. Then there is a permutation $g \mapsto \bar{g}$ of G such that $(g \times M)^\sigma = \bar{g} \times M$ for all g. Moreover, since σ permutes the transpositions in α it fixes each subset $G \times i$, $i \in M$, and we obtain $\sigma \in G$ precisely as in the proof of Theorem 2.1. □

Theorem 2.3 *If G is a finite group, $k \ge 1$, $n > 4k|G| + 2k$ and q is any prime power, then G is isomorphic to a 2–point stabilizer in the permutation group $S_{\binom{n}{k}_q}/\mathrm{P\Gamma L}(n,q)$.*

Notation The indicated symmetric group acts on the set $\mathcal{S}_k(\mathbb{F}_q^n)$ of all k–spaces of $\mathbb{F}_q^n$, and $\mathrm{P\Gamma L}(n,q)$ is the group of all invertible projective semilinear transformations of that vector space.

Proof We will use $2k$ copies of the regular representation of G. Namely, write $K = \mathbb{F}_{q^{2k}}$ and

$$\mathbb{F}_q^n = (\bigoplus_{g\in G} Kx_g) \oplus Ku \oplus \langle Y\rangle$$

for vectors u and x_g, $g \in G$, that are linearly independent over K, and where $\langle Y\rangle$ denotes the $\mathbb{F}_q$–span of the linearly independent set Y. Let each $h \in G$ act linearly on $\mathbb{F}_q^n$, fixing each member of Y and acting on $(\oplus_{g\in G} Kx_g) \oplus Ku$ as a K–linear transformation sending $x_g \mapsto x_{gh}$ while fixing u. Note that $|Y| > 2k|G|$, by hypothesis.

We will construct a permutation $\alpha \in S_{\binom{n}{k}_q}$ such that $\mathrm{P\Gamma L}(n,q) \cap \mathrm{P\Gamma L}(n,q)^\alpha$ *and* $C_{\mathrm{P\Gamma L}(n,q)}(\alpha)$ *both turn out to be* G. Once again let $G = \langle g_1, \dots, g_d\rangle$ with minimal $d \le \log|G|$. We use several permutations:

- π, a cycle of length $\left(\binom{2k+|Y|}{k}_q - \binom{2k}{k}_q - \binom{|Y|}{k}_q - 2\right)$ on $\mathcal{S}_k(Ku + \langle Y\rangle)\backslash\left(\mathcal{S}_k(Ku) \cup \mathcal{S}_k(\langle Y\rangle)\right)$ to be defined below;
- π_*, a cycle of length $\binom{2k}{k}_q$ on $\mathcal{S}_k(Kx_1)$; and
- π_j, $1 \le j \le d$, a permutation of $\mathcal{S}_k(Kx_1 + \langle x_{g_j}\rangle + \langle Y\rangle)\backslash\mathcal{S}_k(Kx_1)$ that has a single nontrivial cycle of k–spaces, and these span $Kx_1 + \langle x_{g_j}\rangle + \langle Y\rangle$, where the lengths of the nontrivial cycles differ for different j. Such permutations exist since $\binom{2k+1+|Y|}{k}_q - \binom{2k}{k}_q - d > \binom{2k+|Y|}{k}_q$, the number of k–spaces in a hyperplane of $Kx_1 + \langle x_g\rangle + \langle Y\rangle$.

Note that the nontrivial cycles of all of the above permutations have different lengths.

We still need to define the permutation π. Write $A = Ku$ and $B = \langle Y\rangle$. Choose any k-spaces X_1, X_2 in $A + B$ such that $\dim A \cap X_1 = 1$, $\dim B \cap X_2 = k - 1$ and $B \cap X_1 = A \cap X_2 = 0$. Let π be a cycle of length $|\mathcal{S}_k(A+B)| - |\mathcal{S}_k(A)| - |\mathcal{S}_k(B)| - 2$ of $\mathcal{S}_k(A + B)\backslash\left(\mathcal{S}_k(A) \cup \mathcal{S}_k(B)\right)$ that fixes X_1 and X_2. The crucial property of π is that *no* $\gamma \in \mathrm{P\Gamma L}(n,q)$ *can induce a non-scalar transformation of* $A + B$ *that fixes* A *and* B *and commutes with* π. For, suppose that there is such a γ. Then γ induces a nontrivial power π^j on $\mathcal{S}_k(A + B)\backslash\left(\mathcal{S}_k(A) \cup \mathcal{S}_k(B)\right)$, fixing only X_1 and X_2 there. Since $(A \cap X_1) + (B \cap X_2)$ is another k-space fixed by π^j, this is impossible.

Define α as follows (where h ranges through G):

- a cycle of length $\binom{2k}{k}_q - 1$ on $\mathcal{S}_k(Ku)$;
- a cycle of length $\binom{2k}{k}_q - 2$ on $\mathcal{S}_k\left(K(u + \sum_{g\in G} x_g)\right)$;
- a cycle of length $\binom{\langle Y\rangle}{k}_q$ on $\mathcal{S}_k(\langle Y\rangle)$;
- π on $\mathcal{S}_k(Ku + \langle Y\rangle)\backslash(\mathcal{S}_k(Ku) \cup \mathcal{S}_k(\langle Y\rangle))$;
- π_*^h on $\mathcal{S}_k(Kx_1)^h = \mathcal{S}_k(Kx_h)$; and

- π_j^h on $\big(\mathcal{S}_k(Kx_1+\langle x_{g_j}\rangle+\langle Y\rangle)\backslash\mathcal{S}_k(Kx_1)\big)^h$ whenever $1\le j\le d$.

Since $g_j^{-1}\neq g_i$ for $j\neq i$, $(Kx_1+\langle x_{g_j}\rangle+\langle Y\rangle)\cap(Kx_h+\langle x_{g_jh}\rangle+\langle Y\rangle)=0$ for $h\neq 1$, and hence the permutation α is well-defined.

Once again G commutes with α. Once again consider $\sigma,\tau\in \mathrm{P\Gamma L}(n,q)$ such that $\sigma^\alpha=\tau$; later we will view these as elements of $\Gamma\mathrm{L}(n,q)$. Since $n=2k|G|+2k+|Y|$ and $|G|<|Y|/2k$, it follows that $\tau^{-1}\sigma=\alpha^{-1}\alpha^\sigma$ moves at most

$$2(|G|+2)\binom{2k}{k}_q+2(d|G|+2)\binom{2k+1+|Y|}{k}_q<\frac{1}{2}\binom{n}{k}_q$$

members of $\mathcal{S}_k(\mathbb{F}_q^n)$. However, every nontrivial element of $\mathrm{P\Gamma L}(n,q)$ moves at least $\frac{1}{2}\binom{n}{k}_q$ members of $\mathcal{S}_k(\mathbb{F}_q^n)$ (see, for example, [3, Proposition 3.1]). Consequently, $\tau^{-1}\sigma=1$ and σ centralizes α. (N.B.–This restriction on the possible number of moved points makes this part of the proof easier than before.)

Thus, σ permutes the nontrivial cycles of α. Since the permutations π, π_* and π_j, were constructed so as to be pairwise not conjugate under the action of $\mathrm{P\Gamma L}(n,q)$, σ permutes the nontrivial cycles of α lying in each of the following sets: $\mathcal{S}_k(Ku+\langle Y\rangle)$, $\mathcal{S}_k(Ku)$, $\mathcal{S}_k(\langle Y\rangle)$, $\mathcal{S}_k(K(u+\sum_{g\in G}x_g))$, $\cup_{h\in G}\mathcal{S}_k(Kx_h)\mid h\in G)$, and $\cup_{h\in G}\mathcal{S}_k(Kx_1+\langle x_g\rangle+\langle Y\rangle)^h$ whenever $1\le j\le d$. Each such cycle of k–spaces spans a subspace of $\mathbb{F}_q^n$, so that σ *fixes* $Ku+\langle Y\rangle$, Ku, $\langle Y\rangle$ *and* $K(u+\sum_{g\in G}x_g)$, *and acts on each of the following sets of subspaces*:

$$\{Kx_h\mid h\in G\}\quad\text{and}\quad\{Kx_h+\langle x_{g_jh}\rangle+\langle Y\rangle\mid h\in G\}\quad\text{for } 1\le j\le d.$$

For each $h\in G$ let $\bar h\in G$ satisfy $(Kx_h)^\sigma=Kx_{\bar h}$. By replacing σ by some σh with $h\in G$ we may assume that $\bar 1=1$.

Since σ fixes Ku and $\langle Y\rangle$ and commutes with the unique longest cycle on $\mathcal{S}_k(Ku+\langle Y\rangle)$, the crucial property of π states that σ is a scalar on $Ku+\langle Y\rangle$. We may assume that $\sigma=1$ on $Ku+\langle Y\rangle$.

If $a\in K$ let $a'\in K$ with $a'(u+\sum_{g\in G}x_g)=(a(u+\sum_{g\in G}x_g))^\sigma=au+\sum_{g\in G}(ax_g)^\sigma$, where $(ax_g)^\sigma\in Kx_{\bar g}$. Then $a'=a$ and $(ax_g)^\sigma=ax_{\bar g}$.

In particular, if $G=1$ then this shows that $\sigma=1$, as required. Now assume that $G\neq 1$.

Fix $g=g_j$. If $h\in G$ let $h'\in G$ with $(Kx_h+\langle x_{gh}\rangle+\langle Y\rangle)^\sigma=Kx_{h'}+\langle x_{gh'}\rangle+\langle Y\rangle$. Then $Kx_{\bar h}\subseteq Kx_{h'}+\langle x_{gh'}\rangle+\langle Y\rangle$, so that $h'=\bar h$ does not depend on g. Now $Kx_{\bar h}+\langle x_{gh}\rangle^\sigma\subseteq Kx_{\bar h}+\langle x_{g\bar h}\rangle+\langle Y\rangle$, where $\langle x_{gh}\rangle^\sigma\subseteq(Kx_{gh})^\sigma=Kx_{\overline{gh}}$.

Thus, $g_j\bar h=\overline{g_jh}$ for all j and h. As before it follows that $\bar g=g$ for all g. Consequently, $(ax_g)^\sigma=ax_{\bar g}=ax_g$ for all $a\in K$, $g\in G$, so that $\sigma=1$. □

Remark When $k=1$ the above result is already "better" than [6, Proposition 10.2], where it was assumed that $n>20|G|^2$ in a similar argument. However, that paper needed to impose many additional restrictions on α for its applications to symmetric designs. Moreover, we also needed a version of Theorem 2.3: there are exponentially many different orbits of pairs of points even with the aforementioned additional restrictions.

We turn next to the symmetric group on the set of affine subspaces of a vector space. Recall that $\mathrm{A\Gamma L}(n,q)$ denotes the group of all invertible semilinear affine transformations of $\mathbb{F}_q^n$, and that $S_{\mathrm{a}(n,k)_q}$ acts on the set of all $\mathrm{a}(n,k)_q$ affine k–spaces of $\mathbb{F}_q^n$.

Theorem 2.4 *If G is a finite group, $k \geq 0$, $n > 4(k+1)|G| + 2k + 2$ and q is any prime power, then G is isomorphic to a 2–point stabilizer in the permutation group $S_{\mathrm{a}(n,k)_q}/\mathrm{A\Gamma L}(n,q)$.*

Sketch While it is straightforward to imitate previous proofs, it is easier to modify the proof of Theorem 2.3 slightly. In that proof, use $K = \mathbb{F}_{q^{2(k+1)}}$ and let H be a hyperplane of $\mathbb{F}_q^n$ fixed by G and containing no member of $\{x_g \mid g \in G\} \cup \{u\} \cup Y \cup \{u + \sum_{g\in G} x_g\}$. Choose α to be 1 on $\mathcal{S}_k(H)$ and to have one very large cycle on each subset $\mathcal{S}_k(Ku)$, $\mathcal{S}_k\big(K(u + \sum_{g\in G} x_g)\big)$, $\mathcal{S}_k(\langle Y\rangle)$, $\mathcal{S}_k(Ku + \langle Y\rangle)$, $\mathcal{S}_k(Kx_h)$, and $\mathcal{S}_k(Kx_1 + \langle x_{g_j}\rangle + \langle Y_0\rangle)^h$ for $h \in G$, $1 \leq j \leq d$, as before.

Complete the proof of Theorem 2.3 as before. Then restrict from $\mathrm{P\Gamma L}(n,q)$ to $\mathrm{A\Gamma L}(n,q)$ by fixing H and using the same G and α. Then $G \leq \mathrm{A\Gamma L}(n,q) \cap \mathrm{A\Gamma L}(n,q)^\alpha \leq \mathrm{P\Gamma L}(n,q) \cap \mathrm{P\Gamma L}(n,q)^\alpha = G$. □

Notation Let V be a vector space equipped with a nondegenerate quadratic, alternating or hermitian form. Let $\mathrm{P\Gamma I}(V)$ denote the projectivized version of the group of all semilinear transformations of V that preserve the form up to a field automorphism and a scalar. Fix an isometry type $\mathcal{I}_k$ of totally singular or nondegenerate k–dimensional subspaces of V. For any subspace W let $\mathcal{I}_k(W)$ denote the set of all subspaces of type $\mathcal{I}_k$ in W.

Theorem 2.5 *If G is a finite group, $k \geq 1$, $n > 8k|G| + 8k$, q is any prime power and V is an n–dimensional $\mathbb{F}_q$–space equipped as above, then G is isomorphic to a 2–point stabilizer in the permutation group $S_N/\mathrm{P\Gamma I}(V)$, where $N = |\mathcal{I}_k(V)|$.*

Proof This time we use $4k$ copies of the regular representation of G. Namely, write $K = \mathbb{F}_{q^{2k}}$, let $T\colon K \to \mathbb{F}_q$ denote the trace map, and let

$$V = \big(\big(\bigoplus_{g\in G} Ke_g\big) \oplus \big(\bigoplus_{g\in G} Kf_g\big)\big) \perp \big(Ku \oplus \langle Y\rangle\big).$$

Here e_g, f_g, for $g \in G$, are singular vectors that are linearly independent over K such that $(\alpha e_g, \beta f_g) = T(\alpha\beta)$ for all $\alpha, \beta \in \mathbb{F}_q$ (or $T(\alpha\bar{\beta})$ when V is unitary with associated involutory field automorphism $\beta \mapsto \bar{\beta}$), $(e_g, e_h) = (f_g, f_h) = (e_g, f_h) = 0$ for $g \neq h$, and $Ku \oplus \langle Y\rangle$ is a nondegenerate $\mathbb{F}_q$-subspace perpendicular to $(\oplus_{g\in G} Ke_g) \oplus (\oplus_{g\in G} Kf_g)$.

The remainder of the proof is very similar to that of Theorem 2.3. □

This theorem can also be proved by restricting from the groups $\mathrm{P\Gamma L}(V)$ and G to the subgroup $\mathrm{P\Gamma I}(V)$ and essentially the same G.

The preceding results all used permutation representations of the symmetric group in order to handle 2–point stabilizers. The next result uses a permutation representation of $\mathrm{PGL}(n,q)$, with stabilizer the group $N=N(n,q)$ of all $n\times n$ monomial matrices over $\mathbb{F}_q$, modulo scalar matrices.

Theorem 2.6 *If G is a finite group, $n>|G|[\log|G|+6]$, and q is any prime power, then G is isomorphic to a 2–point stabilizer in the permutation representation $\mathrm{PGL}(n,q)/N(n,q)$.*

Proof Let $G=\langle g_1,\dots,g_d\rangle$ with d minimal, so that $d\le\log|G|$ and $d=0$ if $G=1$. Write $D:=\{1,\dots,d\}$ and $M:=\{1,\dots,m\}$, where $m:=n-2|G|-d|G|-1\ge 4|G|$ by hypothesis. Let $\mathbb{F}_q^n$ have the following basis:

$$\{x(g),\ y(g),\ w(j,g),u,\ z(k)\mid g\in G, j\in D, k\in M\},$$

and let each $h\in G$ act on this basis by fixing u and each $z(k)$ and sending $x(g)\mapsto x(gh)$, $y(g)\mapsto y(gh)$ and $w(j,g)\mapsto w(j,gh)$ for $g\in G$, $j\in D$. Thus, we can view G as a subgroup of $\mathrm{PGL}(n,q)$. Note that there are no basis vectors $w(j,g)$ if $G=1$.

View N as the group of monomial transformations with respect to the above basis.

Define $\alpha\in\mathrm{GL}(n,q)$ as follows, where $g\in G$, $j\in D$, $k\in M$, $s_x:=\sum_g x(g)$, $s_y:=\sum_g y(g)$ and $s_z:=\sum_k z(k)$:

$$\begin{aligned}
x(g)&\mapsto x(g)\\
y(g)&\mapsto y(g)+x(g)\\
w(j,g)&\mapsto w(j,g)+x(g)+\sum_1^j y(g_ig)+s_z\\
u&\mapsto u+s_y\\
z(k)&\mapsto \sum_1^k z(i)+u+s_x+s_y.
\end{aligned}$$

In order to see that α is invertible, note that $\mathrm{Im}\,\alpha$ contains all $x(g)$ and $y(g)$, then also u and all $z(k)$, and finally all $w(j,g)$.

As usual α centralizes G. As usual we consider $\sigma,\tau,\rho\in N$ such that $\tau=\sigma^\alpha$ and $\rho=\tau^{-1}\sigma=\alpha^{-1}\alpha^\sigma$. Using the definition of α, there are two ways to describe the action of $\alpha^\sigma=\alpha\rho$:

$$\begin{aligned}
x(g)^\sigma&\mapsto x(g)^\sigma\\
y(g)^\sigma&\mapsto y(g)^\sigma+x(g)^\sigma\\
w(j,g)^\sigma&\mapsto w(j,g)^\sigma+x(g)^\sigma+\sum_1^j y(g_ig)^\sigma+s_z^\sigma\\
u^\sigma&\mapsto u^\sigma+s_y^\sigma\\
z(k)^\sigma&\mapsto \sum_1^k z(i)^\sigma+u^\sigma+s_x^\sigma+s_y^\sigma
\end{aligned}$$

and

$$\begin{aligned} x(g) &\mapsto x(g)^\rho \\ y(g) &\mapsto y(g)^\rho + x(g)^\rho \\ w(j,g) &\mapsto w(j,g)^\rho + x(g)^\rho + \sum_1^j y(g_i g)^\rho + s_z^\rho \\ u &\mapsto u^\rho + s_y^\rho \\ z(k) &\mapsto \sum_1^k z(i)^\rho + u^\rho + s_x^\rho + s_y^\rho . \end{aligned}$$

The rest of the argument consists of a straightforward comparison of these different descriptions of $\alpha^\sigma = \alpha\rho$.

As σ, $\rho \in N$, each image of a basis vector under either of these linear transformations is a scalar multiple of a basis vector.

Define the *weight* of a vector to be the number of nonzero coordinates when it is written in our basis. The weights of $\alpha\rho$-images for different "types" of basis vectors are as follows:

type	$x(g)$	$y(g)$	$w(j,g)$	u	$z(k)$
weight	1	2	$2+j+m$	$1+\lvert G\rvert$	$1+k+2\lvert G\rvert$

where $j \in D, k \in M$. We will also use a slight refinement of weight: the number of nonzero coordinates of a given type (hence, for example, x-*weight* and xy-*weight*). Note that some coincidences are possible for the above weights, for example if $G = 1$. However, in general all of the above weights are different (recall that $m \geq 4|G|$), and hence our two descriptions of the action of $\alpha\rho$ imply that σ maps each basis vector to a scalar multiple of one of the same type.

The only basis vectors whose $\alpha\rho$-images have weight 1 are the $x(g)$. Hence, $x(g)^\sigma = a_g x(\bar{g})$ with $a_g \in \mathbb{F}$, $\bar{g} \in G$, and $\alpha\rho$ sends

$$\begin{aligned} a_g x(\bar{g}) &\mapsto a_g x(\bar{g}) \\ a_g x(\bar{g}) &\mapsto a_g x(\bar{g})^\rho . \end{aligned}$$

Then $x(g) = x(g)^\rho$ for all g.

Replace σ by $\sigma \bar{1}^{-1}$ in order to have $\bar{1} = 1$.

The only basis vectors whose $\alpha\rho$-images have weight 2 and x-weight 1 are the $y(g)$ (this uses the fact that $x(g) = x(g)^\rho$). Since we already know that $x(g)^\sigma$ has x-weight 1, it follows from the above description of the behavior of $y(g)^\sigma$ that $y(g)^\sigma = b_g y(g')$ with $b_g \in \mathbb{F}$, $g' \in G$, and

$$\begin{aligned} b_g y(g') &\mapsto b_g y(g') + a_g x(\bar{g}) \\ b_g y(g') &\mapsto b_g \Big[y(g')^\rho + x(g') \Big] . \end{aligned}$$

Then $a_g = b_g$, $\bar{g} = g'$, $y(g) = y(g)^\rho$ and $y(g)^\sigma = a_g y(\bar{g})$ for all g.

The only basis vector whose $\alpha\rho$-image has weight $1+|G|$, with x-weight 0, is u. Since we already know that $u^\sigma + s_y^\sigma$ has x-weight 0, it follows that $u^\sigma = fu$ with $f \in \mathbb{F}$, and $fu \mapsto fu + s_y^\sigma$, $fu \mapsto f[u^\rho + s_y]$. Then $u = u^\rho$ and all $a_g = f$.

The only basis vector whose $\alpha\rho$-image has weight $1+k+2|G|$, with xy-weight $2|G|$, is $z(k)$. This time $z(k)^\sigma = f_k z(k)$ with $f_k \in \mathbb{F}$, and

$$f_k z(k) \mapsto \sum_1^k f_i z(i) + fu + s_x^\sigma + s_y^\sigma$$

$$f_k z(k) \mapsto f_k\Big[\sum_1^k z(i)^\rho + u + s_x + s_y\Big].$$

Then all $f_k = f$, $z(i) = z(i)^\rho$, $z(k)^\sigma = fz(k)$, $s_z^\sigma = fs_z$ and $s_z^\rho = s_z$.

Thus, if $G = 1$ then σ is the scalar transformation f on all basis vectors $x(g), y(g), u, z(k)$, and we are finished. Now assume that $G \neq 1$.

The only basis vectors whose $\alpha\rho$-images have weight $2+j+m$, with y-weight j, are the $w(j,g)$. This time $w(j,g)^\sigma = c_{j,g} w(j, \psi(j,g))$ with $c_{j,g} \in \mathbb{F}$, $\psi(j,g) \in G$, and (abbreviating $\psi = \psi(j,g)$)

$$c_{j,g} w(j,\psi) \mapsto c_{j,g} w(j,\psi) + fx(\bar{g}) + \sum_1^j fy(\overline{g_i g}) + fs_z$$

$$c_{j,g} w(j,\psi) \mapsto c_{j,g}\Big[w(j,\psi)^\rho + x(\psi) + \sum_1^j y(g_i\psi) + s_z\Big].$$

Then all $c_{j,g} = f$, $\bar{g} = \psi$ and $\overline{g_i g} = g_i\psi = g_i\bar{g}$ for all j, g, i.

As usual, $\overline{hg} = h\bar{g}$ for all h, g, and then $\bar{h} = h$. Thus, σ induces f on each of the basis vectors, so that $\sigma = 1$ in $\mathrm{PGL}(n,q)$. □

Remark Of course, the corresponding result and proof hold for $\mathrm{PSL}(n,q)$ and $\mathrm{P\Gamma L}(n,q)$ with very minor modifications.

The action in the preceding theorem has a building-theoretic description: for each q and varying n, the permutation representation of $\mathrm{PGL}(n,q)$ on the set of apartments of the underlying building yields a universal family. A similar argument shows that the corresponding result holds for the buildings of each type of classical group for each choice of field.

References

1. Babai, L.: Automorphism groups, isomorphism, reconstruction. In: Graham, R.L., Grötschel, M., Lovász, L. (eds.) Handbook of Combinatorics, vol. 1, pp. 1447–1540. Elsevier, Amsterdam (1995)
2. Cameron, P.J., Kantor, W.M.: Random permutations: Some group–theoretic aspects. Comb. Probab. Comput. **2**, 257–262 (1993)
3. Guralnick, R.M., Kantor, W.M.: Probabilistic generation of finite simple groups. J. Algebra **234**, 743–792 (2000)

4. James, J.P.: Two point stabilisers of partition actions of linear groups. J. Algebra **297**, 453–469 (2006)
5. James, J.P.: Arbitrary groups as two-point stabilisers of symmetric groups acting on partitions. J. Algebr. Comb. **24**, 355–360 (2006)
6. Kantor, W.M.: Automorphisms and isomorphisms of symmetric and affine designs. J. Algebr. Comb. **3**, 307–338 (1994)
7. Merchant, E.: Structure and automorphism groups of Hadamard designs. J. Algebr. Comb. **24**, 137–155 (2006)