

## Finite geometry for a generation

William M. Kantor\*

University of Oregon

For Joe Thas on the occasion of his fiftieth birthday

There are a number of results concerning the generation of a collineation group by two of its elements. A. A. Albert and J. Thompson [1] were the first to exhibit two elements generating the little projective group  $\text{PSL}(d, q)$  of  $\text{PG}(d-1, q)$  (for each  $d$  and  $q$ ). According to a theorem of W. M. Kantor and A. Lubotzky [8], “almost every” pair of its elements generates  $\text{PSL}(d, q)$  as  $qd \rightarrow \infty$  (asymptotically precise bounds on this probability are obtained in W. M. Kantor [6]). Given  $1 \neq g \in \text{PSL}(d, q)$ , the probability that  $h \in \text{PSL}(d, q)$  satisfies  $\langle g, h \rangle = \text{PSL}(d, q)$  was studied by R. M. Guralnick, W. M. Kantor and J. Saxl [3], and its behavior was found to depend on how  $qd \rightarrow \infty$ . Yet another variation that has been proposed is “ $1\frac{1}{2}$ ”-generation: if  $1 \neq g \in \text{PSL}(d, q)$  then *some*  $h \in \text{PSL}(d, q)$  satisfies  $\langle g, h \rangle = \text{PSL}(d, q)$ . This note concerns a stronger version of this notion:

**Theorem.** *For any  $d \geq 4$  and any  $q$ , there is a conjugacy class  $\mathcal{C}$  of cyclic subgroups of  $\text{PSL}(d, q)$  such that, if  $1 \neq g \in \text{PSL}(d, q)$ , then  $\langle g, C \rangle = \text{PSL}(d, q)$  for more than  $\left(1 - \frac{1}{q} - \frac{1}{q^{d-1}}\right)^2 |\mathcal{C}|$  elements  $C \in \mathcal{C}$ . In particular, there are more than  $0.4|\mathcal{C}|$  such elements if  $q > 2$ .*

While this does not look at all like a geometric theorem, the proof is entirely geometric. The same type of result holds when  $d = 2$  or  $3$  (and is easy), as well as for all the classical groups. The proof by W. M. Kantor [7] for the latter groups is still reasonably geometric, but is harder than the situation of the Theorem.

Let  $V$  be the vector space underlying  $\text{PG}(d-1, q)$ . The following is a simple observation concerning the set  $\text{Fix}(g)$  of fixed points (in  $\text{PG}(d-1, q)$ ) of a collineation  $g$ :

**Lemma 1.** *Let  $g \in \text{PSL}(V)$  have prime order.*

- (i) *If  $|g| \nmid q$  then, for some point  $z$  and hyperplane  $Z$  fixed by  $g$ ,  $z$  lies in every hyperplane fixed by  $g$ .*
- (ii) *If  $|g| \nmid q$  then  $\text{Fix}(g) \subseteq A \cup B$  for nonzero subspaces  $A$  and  $B$  such that  $V = A \oplus B$  and each hyperplane fixed by  $g$  contains  $A$  or  $B$ .*

**Proof.** Let  $\hat{g}$  be a linear transformation inducing  $g$ .

(i) We may assume that  $|\hat{g}| = |g|$ . Since  $|\hat{g}| \nmid q$ ,  $\text{Fix}(g)$  is the set of points in the null space of  $\hat{g} - I$ , and this subspace is nonzero and proper in  $V$ . Let  $Z$

---

\*Research supported in part by the NSF.

be any hyperplane containing  $\text{Fix}(g)$ . Dually, the intersection of the set of fixed hyperplanes is nonzero, is fixed by  $g$ , and hence contains a nonzero point  $z$  fixed by  $g$ .

(ii) This time  $\text{Fix}(g)$  is the union of eigenspaces of  $\hat{g}$  whose corresponding eigenvalues are in  $GF(q)$ . The span of these eigenspaces is their direct sum. Hence, let  $B$  be any such (nonzero) eigenspace of smallest dimension, and let  $A$  be a complement to  $B$  containing all remaining eigenspaces; if there are no such nonzero eigenspaces then there are no fixed points, and  $B$  can be chosen to be an arbitrary point.  $\square$

Let  $C$  be a cyclic subgroup of  $\text{PSL}(d, q)$  of order  $q^{d-1} - 1$  that splits  $V$  as  $V = x \oplus X$  for a non-incident point  $x$  and hyperplane  $X$  (i.e., antiflag) of  $\text{PG}(d-1, q)$ , where  $C$  is transitive on the sets of points and hyperplanes of  $X$ . Let  $\mathcal{C}$  denote the conjugacy class  $C^{\text{PSL}(d, q)}$  of  $C$ . In view of the transitivity of  $\text{PSL}(d, q)$  on the antiflags of  $\text{PG}(d-1, q)$ , each antiflag is fixed by the same number of members of  $\mathcal{C}$ .

**Lemma 2.** *Assume that  $d \geq 4$  and  $\text{PSL}(d, q) \neq \text{PSL}(4, 2)$ . If  $C \leq J \leq \text{PSL}(d, q)$ , where  $J$  moves both  $x$  and  $X$ , then  $J = \text{PSL}(d, q)$ .*

**Proof.** Since  $C$  is transitive on both the points and hyperplanes of  $V/x$ ,  $J$  is transitive on the set of those hyperplanes not disjoint from  $\Omega := x^J$ , and also on the set of those lines not disjoint from  $\Omega$ . In particular, all hyperplanes not disjoint from  $\Omega$  meet  $\Omega$  in the same number of points; and the same is true for the lines not disjoint from  $\Omega$ . Since  $J$  moves the only point fixed by  $C$ ,  $|\Omega| > 1$ . It follows that  $\Omega$  is either the complement of a hyperplane or consists of all points (this simple result uses the fact that  $d \geq 4$ , and is proved on the bottom of p. 68 of W. M. Kantor [4]). Since  $J$  moves the only hyperplane fixed by  $C$ ,  $\Omega$  must consist of all points.

Thus,  $J$  is transitive on the set of points of  $\text{PG}(d-1, q)$ , and hence also on the set of incident point-line pairs. By a result of W. M. Kantor [5],  $J$  is 2-transitive on points. Now a theorem of P. J. Cameron and W. M. Kantor [2] implies that  $J = \text{PSL}(d, q)$ .  $\square$

The case  $\text{PSL}(4, 2) \cong A_8$  of the Theorem will be left to the reader, and hence is excluded here. Fix  $1 \neq g \in \text{PSL}(d, q)$ , where  $|g|$  is prime. Call  $C \in \mathcal{C}$  “good” if  $\langle g, C \rangle = \text{PSL}(d, q)$ .

(i) Suppose that  $|g| \nmid q$ . Let  $z, Z$  be as in Lemma 1(i). By Lemma 2, if  $C \in \mathcal{C}$  is chosen so that its unique fixed point  $x$  and hyperplane  $X$  satisfy  $x \notin Z$  and  $z \notin X$ , then  $\langle g, C \rangle = \text{PSL}(d, q)$ . The number of antiflags  $x, X$  behaving in this manner is  $q^{d-1}(q^{d-1} - q^{d-2})$ , and all such antiflags are fixed by the same number of members of  $\mathcal{C}$ . Consequently, the proportion of good members of  $\mathcal{C}$  is at least

$$\frac{q^{d-1}(q^{d-1} - q^{d-2})}{[(q^d - 1)/(q - 1)]q^{d-1}} > \frac{1}{2}.$$

(ii) Suppose that  $|g| \nmid q$ . Let  $A$  and  $B$  be as in Lemma 1(ii), where  $A$  is a subspace  $\text{PG}(a-1, q)$  and  $B$  is a subspace  $\text{PG}(b-1, q)$  with  $a+b = d$  and  $a \geq b$ . Let  $\mathcal{N}$  be the number of antiflags  $x, X$  such that  $x \notin A \cup B$  and  $X \not\supseteq A, B$ . Then the proportion of good members of  $\mathcal{C}$  is at least

$$\frac{\mathcal{N}}{[(q^d - 1)/(q - 1)]q^{d-1}} = \frac{\left[ \frac{q^d - 1}{q - 1} - \frac{q^{d-a} - 1}{q - 1} - \frac{q^{d-b} - 1}{q - 1} \right] (q^{d-1} - q^{a-1} - q^{b-1})}{[(q^d - 1)/(q - 1)]q^{d-1}} \\ \geq \frac{q^d - q - q^{d-1} + 1}{q^d - 1} \frac{q^{d-1} - 1 - q^{d-2}}{q^{d-1}}.$$

The right hand side is always  $> \left(1 - \frac{1}{q} - \frac{1}{q^{d-1}}\right)^2$ ; if  $q \geq 3$  then it is at least  $(52/80)(17/27) > 0.4$ . This proves the Theorem.

**Remark.** If  $q$  is fixed and  $d \rightarrow \infty$ , and if  $g$  is always chosen to be a perspectivity in (i) or (ii), then the desired probability  $\rightarrow (1 - 1/q)^2$ .

## References

- [1] A. A. Albert and J. Thompson, Two-element generation of the projective unimodular group. *Ill. J. Math.* 3 (1959) 421–439.
- [2] P. J. Cameron and W. M. Kantor, 2-Transitive and antiflag transitive collineation groups of finite projective and polar spaces. *J. Algebra* 60 (1979) 384–422.
- [3] R. M. Guralnick, W. M. Kantor and J. Saxl, The probability of generating a classical group (to appear in *Comm. in Algebra*).
- [4] W. M. Kantor, Characterizations of finite projective and affine spaces. *Can. J. Math.* 21 (1969) 64–75.
- [5] W. M. Kantor, Line-transitive collineation groups of finite projective spaces. *Israel J. Math.* 14 (1973) 229–235.
- [6] W. M. Kantor, Some topics in asymptotic group theory, pp. 403–421 in *Groups, Combinatorics and Geometry* (eds. M. W. Liebeck and J. Saxl), LMS Lecture Notes 165, 1992.
- [7] W. M. Kantor,  $1\&\frac{1}{4}$ -generation of finite classical groups (in preparation).
- [8] W. M. Kantor and A. Lubotzky, The probability of generating a finite classical group. *Geom. Ded.* 36 (1990) 67–87.