$(2, p)$-generation of finite simple groups

Carlisle S. H. King Supervisor: Prof. Martin W. Liebeck

Question

Is every non-abelian finite simple group generated by an involution and an element of prime order?

Introduction

Let G be a finite simple group. A result of Steinberg proves that every finite simple group is generated by a pair of elements. Given a pair of positive integers a and b, we say G is (a, b)-generated if G is generated by a pair of elements of orders a and b.

As two involutions generate a dihedral group, the smallest pair of interest is $(2, 3)$. The question of which finite simple groups are $(2, 3)$-generated has been studied extensively. A sample of results is listed below.

Table: $(2, 3)$-generation of finite simple groups

Family	Result	Reference
Alternating groups	All except A_3, A_6, A_7, A_8	[4]
Classical groups	All but finitely many not equal to $PSp_4(2^f), PSp_4(3^f)$	[2]
Exceptional groups	All except ${}^2B_2(2^{2f+1})$	[3]
Sporadic groups	All except $M_{11}, M_{22}, M_{23}, McL$	[5]

The problem of determining exactly which finite simple groups are $(2, 3)$-generated, or more generally $(2, p)$-generated for some prime p, remains open.

General method

Let G be any finite group. Let $M <_{\max} G$ denote a maximal subgroup. For a group H let $i_m(H)$ denote the number of elements of order m in H. Let $x \in G$ be an element of order p. Let $P_2(G, x)$ denote the probability that G is generated by x and a random involution, and let $Q_2(G, x) = 1 - P_2(G, x)$. We have

$$Q_2(G, x) \leq \sum_{x \in M <_{\max} G} \frac{i_2(M)}{i_2(G)}. \qquad (1)$$

To prove G is $(2, p)$-generated, it suffices to prove $Q_2(G, x) < 1$.

For the classical groups, our method in most cases is as follows:

1. Choose a prime p dividing the order of G such that p does not divide the order of many maximal subgroups;
2. For $x \in G$ of order p, determine the maximal subgroups containing x using Aschbacher's theorem;
3. Bound $i_2(M)$ and $i_2(G)$ in terms of n and q such that for n, q sufficiently large we have $Q_2(G, x) < 1$ using (1), and hence G is $(2, p)$-generated.

For the remaining cases with small n and q we improve the bounds case by case.

Primitive prime divisors

Let $q, e > 1$ be positive integers with $(q, e) \neq (2^a - 1, 2), (2, 6)$. By Zsigmondy's theorem, there exists a prime divisor $r_{q,e}$ of $q^e - 1$ such that $r_{q,e}$ does not divide $q^i - 1$ for $i < e$. We call $r_{q,e}$ a primitive prime divisor of $q^e - 1$.

If G is a finite simple classical group with natural module V of dimension n over the field $\mathbb{F}_{q^\delta}$, where $\delta = 2$ if G is unitary and $\delta = 1$ otherwise, let p be a primitive prime divisor $p = r_{q,e}$, where e is listed below.

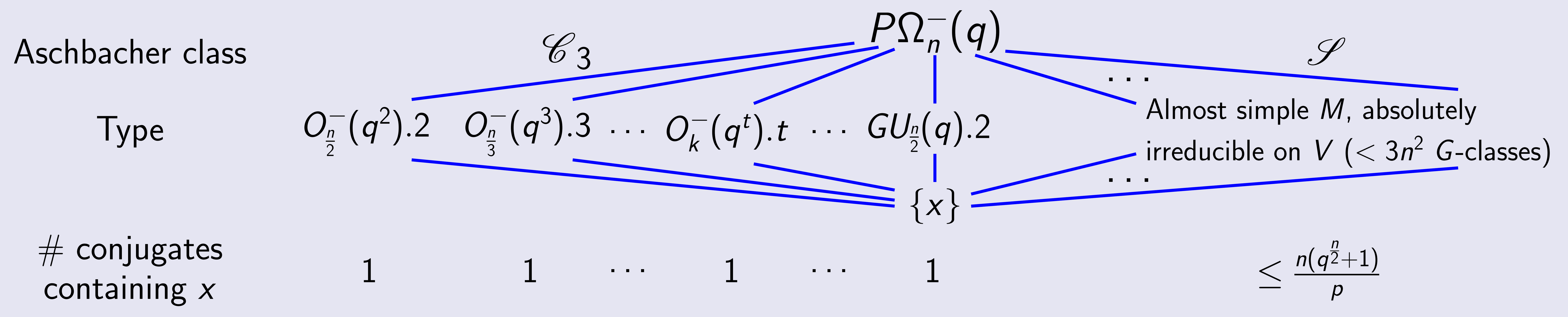
Table: Values of e

G	e
$PSL_n(q), PSp_n(q), P\Omega_n^-(q)$	n
$P\Omega_n^+(q)$	$n-2$
$P\Omega_n(q)$ (nq odd)	$n-1$
$PSU_n(q)$ (n odd)	$2n$
$PSU_n(q)$ (n even)	$2n-2$

Example: $P\Omega_n^-(q)$

Let $G = P\Omega_n^-(q)$. We prove G is $(2, p)$-generated for some prime p as follows:

1. Let $p = r_{q,n}$ as above, and let $x \in G$ be an element of order p.
2. By Aschbacher's theorem, the G-classes of maximal subgroups M possibly containing x are as follows:



3. We bound the number of involutions $i_2(M)$ of M as

$$i_2(M) \leq \quad \cdots \quad 2(q^t+1)q^{\frac{n^2}{4t}-t} \quad \cdots \quad 2(q+1)^2 q^{\frac{n^2}{8}+\frac{n}{4}-2} \quad \begin{cases} q^{2n+4} & \text{if } \mathrm{soc}(M) \neq A_{n'}, \\ (n+2)! & \text{otherwise,} \end{cases}$$

and we have $i_2(G) \geq \frac{1}{8}q^{\frac{n^2}{4}-1}$. Therefore, using (1), we have $Q_2(G, x) < 1$ for $n \geq 18$, and so G is $(2, p)$-generated for $n \geq 18$.

Theorem

Let G be a finite simple classical group with natural module of dimension n over $\mathbb{F}_{q^\delta}$, where $\delta = 2$ if G is unitary and $\delta = 1$ otherwise. Assume $n \geq 8$ and $G \neq P\Omega_8^+(2)$. Let p be a primitive prime divisor of $q^e - 1$, where e is listed above. Then G is $(2, p)$-generated.

Theorem

Every non-abelian finite simple group G is generated by an involution and an element of prime order.

References

[1] C. S. H. King, Generation of finite simple groups by an involution and an element of prime order. https://arxiv.org/abs/1603.04717.

[2] M. W. Liebeck, A. Shalev, Classical groups, probabilistic methods and the $(2, 3)$-generation problem. *Ann. Math.* **144** (1996), 77-125.

[3] F. Lübeck, G. Malle, $(2, 3)$-generation of exceptional groups. *J. London. Math. Soc.* **59** (1999), 101-122.

[4] G. A. Miller, On the groups generated by two operators. *Bull. Am. Math. Soc.* **7** (1901), 424-426.

[5] A. J. Woldar, On Hurwitz generation and genus actions of sporadic groups. *Ill. J. Math.* **33** (1989), 416-437.