# Generating sets of finite groups

## Joint work with Peter Cameron and Andrea Lucchini

Colva M. Roney-Dougal

12 January 2017

# Random generation

Fact 1: For many interesting groups

$$\mathbb{P}(\langle x_1, x_2 \rangle = G \mid x_i \text{ uniform random in } G)$$

is very close to 1.

Fact 2: Inside these same groups, there exist quite a few $x_1 \in G$ such that

$$\mathbb{P}(\langle x_1, x_2 \rangle = G \mid x_2 \text{ uniform random})$$

is very close to 0.

So would like to understand the structure of generating sets.

# Easier algebraic objects

$V = \mathbb{F}^d$ – finite dimensional vector space.

Then

1. Any two irredundant generating sets have the same size.
2. Let $v, w \in V$. Then

$$(\langle v, X \rangle = V \Leftrightarrow \langle w, X \rangle = V) \quad \forall X \subset V$$

   if and only if $\langle v \rangle = \langle w \rangle$.

# $p$-groups

Throughout rest of talk, let $G$ be a finite group.

$\Phi(G)$ – Frattini subgroup: intersection of all maximal subgps of $G$.

$\Phi(G) = \{g \in G \ : \ g$ belongs to no irredundant gen set for $G\}$.

**Theorem (Burnside's basis theorem)**

*$P$ – $p$-group, with $|P : \Phi(P)| = p^d$.*
*[Then $P/\Phi(P) \cong (\mathbb{F}_p^d, +)$.]*

*$P/\Phi(P) = \langle \Phi(P)x_i : 1 \leq i \leq n \rangle$ if and only if $P = \langle x_1, \ldots, x_n \rangle$.*

*Furthermore, $P = \langle x_1, \ldots, x_n \rangle$ if and only if there exists a subset $Y$ of $x_1, \ldots, x_n$ of size $d$ such that $P = \langle Y \rangle$.*

# $p$-groups, ctd

**Corollary**

1. *Any two irredundant generating sets of a finite $P$-group have the same size.*
2. *If $x, y \in P$, then*

$$(\langle x, X\rangle = P \Leftrightarrow \langle y, X\rangle = P) \quad \forall X \subseteq P$$

*if and only if $\langle \Phi(P)x\rangle = \langle \Phi(P)y\rangle$.*

So in these two cases, we have a good understanding of the structure of generating sets.

# Minimal generating sets for finite groups

Final reminder: $G$ is always a finite group.

Write $d(G)$ for smallest number of generators of $G$.

Lots known about $d(G)$, e.g.

1. $G$ almost simple $\Rightarrow d(G) \leq 3$.
2. If each Sylow subgroup of $G$ can be generated by $n$ elts, then $d(G) \leq n + 1$. Lucchini '89; Guralnick '89.
3. $G \leq \mathrm{S}_n$: see Gareth Tracey's talk (11.15 today)!
4. $G \leq \mathrm{GL}_n(F)$: Kovacs & Robinson 91; Holt & CMRD 13.
5. . . . much much more

# Maximal irredundant generating sets for finite groups

$\mu(G)$:= maximal size of an irredundant generating set for $G$.

Diaconis & Saloff-Coste '98: $n-1 \leq \mu(S_n) \leq 2n$.

Whiston '00: $\mu(S_n) = n-1$.
Whiston & Saxl '02: $3 \leq \mu(\mathrm{PSL}_2(p)) \leq 4$.

Jambor '13: $\mu(\mathrm{PSL}_2(p)) = 4 \Leftrightarrow p \in \{7, 11, 19, 31\}$.

**Theorem (Apisa & Klopsch '14)**

*If $d(G) = \mu(G)$, then every quotient $\overline{G}$ of $G$ satisfies $d(\overline{G}) = \mu(\overline{G})$ and $G$ is solvable.*

**Theorem (Lucchini '13)**

*$G$ – soluble. $\pi(G)$ – number of prime divisors of $|G|$.*
*Then $\mu(G) - d(G) \geq \pi(G) - 2$.*

# A new family of relations

In the rest of the talk, we look at how elements can be interchanged between generating sets.

For $x, y \in G$, say $x \equiv_{\mathrm{m}}^{(r)} y$ if $\forall z_1, \ldots, z_{r-1} \in G$

$$(\langle x, z_1, \ldots, z_{r-1} \rangle = G \quad \Leftrightarrow \quad \langle y, z_1, \ldots, z_{r-1} \rangle = G)$$

(So $x$ and $y$ can be interchanged in any $r$-element generating set.)

**Lemma**

1. *Equiv relations* $\equiv_{\mathrm{m}}^{(r)}$ *get finer as* $r \to \infty$.
2. $\equiv_{\mathrm{m}}^{(r)}$ *is universal for* $r < d(G)$.
3. $\equiv_{\mathrm{m}}^{(d(G))}$ *has at least* $r + 1$ *equivalence classes.*

# The limit of the family, and a new group invariant

For $x, y \in G$, define $x \equiv_{\mathrm{m}} y$ if $x$ and $y$ lie in the same maximal subgroups of $G$.

- $x \equiv_{\mathrm{m}} y$ is the limit of $\equiv_{\mathrm{m}}^{(r)}$.

Define $\psi(G)$ to be smallest $r$ for which $\equiv_{\mathrm{m}}$ coincides with $\equiv_{\mathrm{m}}^{(r)}$.

**Example ($G = \mathrm{S}_4$)**

- The relation $\equiv_{\mathrm{m}}^{(1)}$ is universal.
- The double-transpositions lie in no 2-elt gen set, so are $\equiv_{\mathrm{m}}^{(2)}$-equivalent to $1_G$. Otherwise $x \equiv_{\mathrm{m}}^{(2)} y \Leftrightarrow \langle x \rangle = \langle y \rangle$. So 14 classes.
- For $r \geq 3$ the double-transpositions form one $\equiv_{\mathrm{m}}^{(r)}$-class; the other classes don't change. So 15 classes.
- So $\psi(\mathrm{S}_4) = 3$.

# Some bounds on $\psi(G)$

**Lemma**

*$\psi(G) \geq d(G)$, and if $G$ has a normal subgroup $N$ s.t. $N \not\leq \Phi(G)$ and $d(G/N) = d(G)$, then $\psi(G) \geq d(G) + 1$.*

**Theorem**

*If $G$ is soluble, then $\psi(G) \leq d(G) + 1$.*

**Theorem**

*For all finite $G$, $\psi(G) \leq d(G) + 5$.*
*$G$ simple $\Rightarrow \psi(G) \leq 5$. $G$ almost simple $\Rightarrow \psi(G) \leq 7$.*

**Theorem**

*$\psi(G) \leq \mu(G)$. So if $G = \mathrm{PSL}_2(p)$ then $\psi(G) \leq 4$.*

Question Does there exist a $G$ for which $\psi(G) > d(G) + 1$?

# Efficient generation

Say that $G$ is efficiently generated if for all $x \in G$, if $d_{\{x\}}(G) = d(G)$ then $x \in \Phi(G)$.

**Lemma**

*If $\psi(G) = d(G)$ then $G$ is efficiently generated.*

**Lemma**

*If $d(M) < d(G)$ for every maximal subgroup $M$ of $G$, then $\psi(G) = d(G)$.*

We have a precise description of the soluble groups that are efficiently generated.
$S_4$ is the smallest soluble group that is not efficiently generated.

**Problem**

*Characterise the insoluble groups that are efficiently generated.*

# A finer relation

We define $x \equiv_{\mathrm{c}} y \Leftrightarrow \langle x \rangle = \langle y \rangle$.
Then

$$x \equiv_{\mathrm{c}} y \Leftrightarrow \quad (\langle x, X \rangle = \langle y, X \rangle \quad (\forall X \subseteq G)).$$

Hence if $x \equiv_{\mathrm{c}} y$ then $x \equiv_{\mathrm{m}} y$.

**Theorem**

*Let $G$ be a group for which $\equiv_{\mathrm{c}}$ coincides with $\equiv_{\mathrm{m}}$.*

1. *We have a (messy) characterisation of such soluble $G$.*
2. $\Phi(G) = 1$.
3. *$G/\mathrm{Soc}(G)$ is soluble, and if $G$ has a nonabelian minimal normal subgroup $N \cong S_1 \times \cdots \times S_t$ then either $t = 1$ or $t = 2$ and $S_1 \cong \mathrm{P}\Omega_8^+(q)$ with $q \leq 3$.*

Problem: Characterise the insoluble $G$ for which $\equiv_{\mathrm{c}}$ coincides with $\equiv_{\mathrm{m}}$.

# Some asymptotics

**Theorem (Łuczak & Pyber '93)**

$G - \mathrm{S}_n$ or $\mathrm{A}_n$. *Then for almost all $x \in G$, the only transitive subgroups of $\mathrm{S}_n$ containing $x$ are $\mathrm{S}_n$ and (possibly) $\mathrm{A}_n$.*

**Corollary**

$G - \mathrm{S}_n$ or $\mathrm{A}_n$. *For almost all $x, y \in G$, the following are equivalent*

1. $x \equiv_{\mathrm{m}} y$.
2. $x \equiv_{\mathrm{m}}^{(2)} y$.
3. *the cycles of $x$ and $y$ induce the same partition of $\{1, \ldots, n\}$.*

**Theorem (Shalev '98)**

*A random element of $\mathrm{GL}_n(q)$ lies in no proper irreducible subgroup not containing $\mathrm{SL}_n(q)$.*

So something similar should be true for linear groups.

# The generating graph $\Gamma(G)$

Define $\Gamma := \Gamma(G)$ by
$V(\Gamma) = G, \qquad x \sim y \Leftrightarrow \langle x, y \rangle = G.$
Assume from now on that $d(G) \leq 2$.

Structure of $\Gamma$ often corresponds to nice group-theoretic properties.

- Clique number
- Colouring number
- Total domination number
- Determines $G$ up to isomorphism?

This project actually began with us looking at $\mathrm{Aut}(\Gamma(G))$ for various almost simple $G$.

# Automorphism group of $\Gamma(G)$

First observation: $\mathrm{Aut}(\Gamma(G))$ is MASSIVE!

e.g. $|\mathrm{A}_5| = 60$, $\mathrm{Aut}(\Gamma(\mathrm{A}_5)) = 2^{31} \cdot 3^7 \cdot 5$.

A graph reduction: For vertices $x, y$, say $x \equiv_\Gamma y$ if $x$ and $y$ have the same neighbours. Identify equivalence classes, get quotient graph $\overline{\Gamma}$.

Notice if $\Gamma = \Gamma(G)$ then $\equiv_\Gamma$ is $\equiv_{\mathrm{m}}^{(2)}$.

Can weight $V(\overline{\Gamma})$ by number of vertices of $\Gamma$ they represent: $\overline{\Gamma}_w$.

$\Gamma$ and $\overline{\Gamma}$ have same clique nr, chromatic nr, total domination nr.

**Example ($G = \mathrm{A}_5$)**

$\psi(G) = 2$. The relations $\equiv_{\mathrm{m}}$, $\equiv_\Gamma$ and $\equiv_{\mathrm{c}}$ are all equal.
6 $\equiv_\Gamma$-classes of elts of order 5, 10 of order 3, and 16 singletons.
Kernel of action on $\equiv_\Gamma$-classes has order $(4!)^6(2!)^{10}$.
$\mathrm{Aut}(\overline{\Gamma}_w(\mathrm{A}_5)) = \mathrm{Aut}(\overline{\Gamma}(\mathrm{A}_5)) = \mathrm{S}_5$.

# Spread

Spread of $G$ is $k$ if for all $x_1, \ldots, x_k \in G \setminus \{1\}$ there exists a $y \in G$ s.t. $\langle x_i, y \rangle = G$ for all $i$, and $k$ is the maximal such integer.
Spread $k \Rightarrow$ every $k$ verts of $\Gamma \setminus 1$ have a common neighbour.
$\Gamma$ and $\overline{\Gamma}$ have same spread.

**Conjecture (Breuer, Guralnick, Kantor)**

$|G| \geq 3$. *The following are equivalent:*

1. *spread of $G \geq 1$*
2. *spread of $G \geq 2$*
3. *all proper quotients of $G$ are cyclic*

Work in progress of Burness, Guralnick, many others ...

**Theorem**

*If $G$ is soluble and has nonzero spread, then $\psi(G) \leq 2$.*

Conjecture: If $G$ has nonzero spread then $\psi(G) \leq 2$.

# $\mathrm{Aut}(\Gamma(G))$ for $G$ of nonzero spread

**Theorem**

*Let the $\Gamma$-classes of $G$ have sizes $k_1, \ldots, k_n$. Then* $\mathrm{Aut}(\Gamma(G)) = (\mathrm{S}_{k_1} \times \cdots \times \mathrm{S}_{k_n}) : \mathrm{Aut}(\overline{\Gamma}_w(G))$.

Let $\mathrm{Aut}^*(G)$ be action of $\mathrm{Aut}(G)$ on $\overline{\Gamma}_w(G)$.

Then $\mathrm{Aut}^*(G) \leq \mathrm{Aut}(\overline{\Gamma}_w(G)) \leq \mathrm{Aut}(\overline{\Gamma}(G))$.

**Theorem**

*$G$ – group with nonzero spread. Then $\mathrm{Aut}^*(G) = \mathrm{Aut}(G)$ if and only if $G$ is nonabelian.*

Not always the case that $\mathrm{Aut}(\overline{\Gamma}_w(G)) = \mathrm{Aut}(\overline{\Gamma}(G))$.

# Soluble groups of nonzero spread

Let $G$ be a soluble group of nonzero spread. Then $G$ is one of

1. Cyclic
2. $C_p \times C_p$, with $p$ prime
3. Semidirect product of an elementary abelian group with an irreducible subgroup of its Singer cycle.

**Proposition**

1. *Let $G = C_n$, where $r = \pi(n)$. Then $\overline{\Gamma}(G)$ has $2^r$ vertices, and* $\mathrm{Aut}(\overline{\Gamma}_w(G)) = 1$.
2. *Let $G = C_p^2$. Then $\overline{\Gamma}(G)$ has $p + 2$ vertices, and* $\mathrm{Aut}(\overline{\Gamma}_w(G)) \cong \mathrm{S}_{p+1}$.
3. *Let $G = C_p^k : C_n$ be nonabelian with all proper quotients cyclic, and let $r = \pi(n)$.*
   *Then $\overline{\Gamma}(G)$ has $(2^r - 1)p^k + 2$ vertices if $n$ is squarefree, and $2^r p^k + 2$ otherwise.* $\mathrm{Aut}(\overline{\Gamma}_w(G)) \cong \mathrm{S}_{p^k}$.

# Some thought-provoking calculations

The *m*-universal action of $G$ is the perm action made by taking the disjoint union of the actions on cosets of maximal subgroups, one for each conj class.

**Lemma**

1. $x \equiv_{\mathrm{m}} y$ *iff* $\mathrm{Fix}(x) = \mathrm{Fix}(y)$ *in m-universal action.*
2. $\langle x, y \rangle = G$ *iff* $\mathrm{Fix}(x) \cap \mathrm{Fix}(y) = \emptyset$*.*

Using this we found:

**Theorem**

*$G$ – almost simple group with socle of order $< 1000$ s.t. all proper quotients are cyclic. Then* $\mathrm{Aut}(\overline{\Gamma}_w(G)) = \mathrm{Aut}(G)$.

Question: Does this pattern continue?