

# Minimal and probabilistic generation of finite groups

Joint with Derek Holt

Colva Roney-Dougal

4 May 2010

## Some motivation

Let  $x_1, \dots, x_k$  either be permutations of  $\{1, \dots, n\}$  or  $n \times n$  invertible matrices.

**Assume** we can produce random elements of  $G = \langle x_1, \dots, x_k \rangle$ .  
( $G$  is the group **generated** by  $x_1, \dots, x_k$ : all possible products of the  $x_i$ s and their inverses)

### Question

*Given  $\delta \in (0, 1)$  and  $x_1, \dots, x_k$ , how many elements of  $G$  are needed to generate  $G$  with probability at least  $\delta$ ?*

Denote this number by  $d^\delta(G)$ .

Denote the **minimum** number of elts that generate  $G$  by  $d(G)$ .

## Definitions for permutation groups

$G \leq S_n$  is **transitive** if for all  $\alpha, \beta \in \{1, \dots, n\}$  there exists  $g \in G$  such that  $\alpha^g = \beta$ .

$$\begin{aligned} G &= \langle (1, 2, 3, 4), (2, 4) \rangle \leq S_4 && \text{transitive} \\ H &= \langle (1, 2, 3, 4)(5, 6), (2, 4) \rangle \leq S_6 && \text{intransitive} \end{aligned}$$

A subset  $\Delta \subset \{1, \dots, n\}$  is a **block** for  $G$  if  $1 < |\Delta| < n$  and for all  $g \in G$  either  $\Delta^g = \Delta$  or  $\Delta^g \cap \Delta = \emptyset$ .

A transitive  $G \leq S_n$  is **primitive** if  $G$  has no blocks; otherwise  $G$  is **imprimitive**.

- $G = \langle (1, 2, 3, 4, 5, 6) \rangle \leq S_6$  is transitive.
  - $\{1, 4\}$  is a block for  $G$ , so  $G$  is imprimitive.
- $G = \langle (1, 2, 3, 4), (1, 2) \rangle = S_4$  is primitive.

# Minimal generation of permutation groups

## Lemma (Wielandt)

Let  $P \leq S_{p^m}$  be a transitive  $p$ -group. Then  $d(P) \leq 1 + \sum_{i=0}^{m-2} p^i$ .

## Corollary

If  $P \leq S_n$  is a  $p$ -group, then  $d(P) \leq n/2$ .

## Theorem (Cameron, Solomon & Turull 89; Neumann)

Let  $G \leq S_n$ . Then  $d(G) \leq \max\{2, n/2\}$ .

**Bound is tight:**

- If  $n$  is even then  $C_2^{n/2} \leq S_n$ , and  $d(C_2^{n/2}) = n/2$ .
- $S_3$  needs two generators.

# Primitive permutation groups

Can we do better if we assume extra facts about  $G$ ?

$G$  transitive – not much tighter bound (Cameron, Solomon & Turull 89).

Theorem (Lucchini, Menegazzo & Morigi 01)

*There exists a constant  $c$  such that if  $G \leq S_n$  is primitive then*

$$d(G) \leq \frac{c \log n}{\sqrt{\log \log n}}.$$

Not clear what  $c$  is.

# Subgroups of primitive permutation groups

Let  $G \leq H$ . Then  $G$  is a **subnormal** subgroup of  $H$  if there exist  $H_1, \dots, H_k$  such that  $G \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_k \trianglelefteq H$ .

## Theorem (Holt/CMRD 10?)

*Let  $G \leq S_n$  be a subnormal subgroup of a primitive group. Then  $d(G) \leq \log n$ .*

(all logs are to base 2.)

**Bound is tight:** The group  $K = (\mathbb{F}_2^m, +) \trianglelefteq \text{AGL}(m, 2) \leq S_{2^m}$ .

Here  $\text{AGL}(m, 2)$  is primitive, and  $d(K) = m = \log(2^m)$ .

# Minimal generation of finite matrix groups

Let

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} : a \in \mathbb{F}_{p^e} \right\} \leq \mathrm{GL}(2, \mathbb{F}_{p^e}).$$

Then  $G \cong (\mathbb{F}_{p^e}, +)$ , so  $d(G) = e$ . Similar version in  $\mathrm{GL}(n, \mathbb{F}_{p^e})$  has  $d(G) = n^2 e/4$ .

So for arbitrary fields, no upper limit on number of generators!

From now on,  $F$  is any field.  $G \leq \mathrm{GL}(n, F)$  is **irreducible** if  $G$  stabilises no proper nontrivial subspace of  $F^n$ .

$G$  is **completely reducible** if  $F^n$  is a direct sum of subspaces, on each of which  $G$  acts irreducibly.

## Completely reducible matrix groups

### Theorem (Isaacs 72)

*If  $G \leq \text{GL}(n, F)$  is a comp red, finite  $p$ -group, then  $d(G) \leq 3n/2$ .*

### Theorem (Guralnick 89, Lucchini 89)

*Let  $G$  be a finite group. If each Sylow subgroup of  $G$  can be generated by  $\leq t$  elements, then  $d(G) \leq t + 1$ .*

### Theorem (Kovács & Robinson 91)

*If  $G \leq \text{GL}(n, F)$  is finite, completely reducible, then  $d(G) \leq 3n/2$ .*

**Bound is tight:** If  $F$  contains a fourth root of 1, then there exists an irreducible  $K \leq \text{GL}(2, F)$  such that  $d(K) = 3$ .

$K^{n/2} \leq \text{GL}(n, F)$  is completely reducible and  $d(K^{n/2}) = 3n/2$ .

# New results on completely reducible groups

## Theorem (Holt & CMRD 10)

Let  $G \leq \text{GL}(n, F)$  be finite and completely reducible.

- If  $F$  contains no fourth root of 1, then  $d(G) \leq n$ .
- If  $|F| = 2$  and  $n \geq 4$  then either  $d(G) = n/2 + 1$  with  $G \cong C_3^{n/2} : 2$  or  $d(G) \leq n/2$ .

**Bounds are tight:**

- If  $q \equiv 3 \pmod{4}$  and  $G \cong Q_8^{n/2} \leq \text{GL}(n, q)$  then  $d(G) = n$ .
- If  $|F| = 2$  and  $G \cong S_3^{n/2} \cong \text{GL}(2, 2)^{n/2} \leq \text{GL}(n, 2)$  then  $d(G) = n/2$ .

# Quasiprimitive matrix groups

## Question

*Can we do better if we make extra assumptions about the group?*

$G \leq \text{GL}(n, F)$  acts **homogeneously** if  $F^n$  is a direct sum of isomorphic submodules.

$G$  is **quasiprimitive** if every normal subgroup of  $G$  acts homogeneously.

## Theorem (Lucchini, Menegazzo & Morigi 01)

*There exists a constant  $c$  such that if  $n \geq 2$  and  $G \leq \text{GL}(n, F)$  is finite and quasiprimitive, then  $d(G) \leq c \log n$ .*

We get that  $c$  is around **6**.

# Subgroups of weakly quasiprimitive matrix groups

$G$  is **weakly quasiprimitive** if every characteristic subgroup of  $G$  acts homogeneously.

(characteristic: fixed by every automorphism of  $G$ .)

## Theorem (Holt & CMRD 10)

*Let  $G \leq \text{GL}(n, F)$ ,  $Z = Z(\text{GL}(n, F))$ . If  $G$  is a subnormal subgroup of a finite weakly quasiprimitive group, then  $d(GZ/Z) \leq 2 \log n$ .*

**Bound is tight:** If  $q$  is odd then there exists an extraspecial group  $G = 2^{1+2m} \leq \text{GL}(2^m, q)$ , with  $d(G) = 2m = 2 \log n$ , that's a normal subgroup of a quasiprimitive group.

$G$  **not** quasiprimitive: might be a better bound for quasiprimitives. We know a primitive  $G$  with  $d(G) = 2(\log_3 2) \log n \sim 1.262 \log n$ .

# Random generation

Recall -  $d^\delta(G)$  is the minimum number of random elements needed to generate  $G$  with probability at least  $\delta$ .

## Theorem (Lubotsky 02)

$$d^{1/e}(G) \leq d(G) + 2 \log \log |G| + 4.02.$$

A minor adjustment of Lubotsky's proof gives

## Theorem

*Let  $\delta \in (0, 1)$  be given, and let  $t$  be such that  $\zeta(t) \leq 2 - \delta$ . Then*

$$d^\delta(G) \leq d(G) + 2 \log \log |G| + 2 + t.$$

$\zeta(t)$  is Euler's zeta function; for  $t > 1$  it's monotonically decreasing, and tending to 1.

# Random generation of permutation groups

If  $G \leq S_n$  then  $\log \log |G| < \log n + \log \log n$ .

## Theorem (Holt & CMRD ?10)

Let  $\delta \in (0, 1)$ , and let  $t$  be such that  $\zeta(t) \leq 2 - \delta$ . Let  $G \leq S_n$ .

- $d^\delta(G) < n/2 + 2(\log n + \log \log n) + t + 2$ .
- If  $G$  is a subnormal subgroup of a primitive group, then  $d^\delta(G) < 3 \log n + 2 \log \log n + t + 2$ .

## Computational applications:

- If  $H \leq S_n$ , we can efficiently test whether  $H$  is primitive.
- Given  $x_1, \dots, x_k \in H$ , we know how to compute random elements of  $G = \langle x_1, \dots, x_k \rangle^H \trianglelefteq H$ .
- Now know how many needed to generate  $G$  with probability  $\geq \delta$ .

# Random generation of matrix groups

If  $G \leq \text{GL}(n, q)$  then  $\log \log |G| < 2 \log n + \log \log q$ .

## Theorem (Holt & CMRD 10)

Let  $G \leq \text{GL}(n, q)$  be completely reducible,  $\delta$  and  $t$  as before.

- $d^\delta(G) < 3n/2 + 4 \log n + 2 \log \log q + t + 2$ .
- If  $q \not\equiv 1 \pmod{4}$  then  $d^\delta(G) < n + 4 \log n + 2 \log \log q + t + 2$ .
- If  $q = 2$  then  $d^\delta(G) < n/2 + 4 \log n + t + 2$ .
- If  $G$  is a subnormal subgroup of a weakly quasiprimitive group then  $d^\delta(G) < 5 \log n + 2 \log \log n + t + 3$ .

## Computational applications:

- Can efficiently test whether a group is irreducible. If so, then normal subgroup is completely reducible.
- Can also often efficiently determine whether group is primitive.