Random Generation and Chief Lengths of Permutation Groups

Nina Menezes
University of St Andrews

Joint work with Martyn Quick & Colva Roney-Dougal

Nikolaus Conference, December 2011

Motivation

Throughout let G be a finite group, and let log denote $\log_2$.

Given $\epsilon \in (0,1)$, how many elements are needed to generate G with failure probability at most ϵ? Call this number $d^{\epsilon}(G)$.

Can be used for the matrix group recognition project. When constructing composition trees we construct homomorphisms ϕ and generate $\mathrm{im}\phi$ and $\ker\phi$.
How many random elements do we need to generate all of $\ker\phi$?

Chief Lengths

Definition

A *chief series* for G is a series $1 = N_0 \lhd N_1 \lhd \ldots \lhd N_l = G$ where each $N_i \trianglelefteq G$ and N_{i+1}/N_i is minimal normal in G/N_i. The quotient groups N_{i+1}/N_i are the *chief factors*.

Any two chief series of G have the same length and the same multiset of isomorphism types of chief factors.

Definition

The *chief length*, $l(G)$, of G is the length of a chief series of G.

For any G, $l(G) \leq \log |G|$.

Random Generation

A slight modification of a result of Lubotzky gives the following.

Theorem (Lubotzky, 2002)

Let $\epsilon \in (0,1)$ and let t be such that $\zeta(t) \leq 1+\epsilon$. Then

$$d^{\epsilon}(G) \leq d(G) + 2\log l(G) + t + 2.$$

Here ζ is the Riemann zeta function, $\zeta(t) = \sum_{n=1}^{\infty} 1/n^t$ and $d(G)$ is the minumum number of generators for G.

Generation of Permutation Groups

Lubotzky's theorem can be combined with the following bounds on $d(G)$.

Theorem (Neumann)

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

Theorem (Holt & Roney-Dougal, 2011)

Let H be a subnormal subgroup of a primitive permutation group G of degree n. Then $d(H) \leq \log n$ unless $n = 3$ and $H \cong S_3$.

We wish to bound the chief length of $G \leq S_n$.

O'Nan–Scott Theorem

Let G be a permutation group of degree n. Then one of the following cases holds.

1. G is intransitive.
2. G is imprimitive.
3. G is primitive and of one of the following types.
   - Affine type, $G = \mathbb{F}_p^k \rtimes H$ for $H \in \mathrm{GL}_k(p)$.
   - Twisted wreath product.
   - Diagonal type.
   - Product type.
   - Almost simple type, $S \leq G \leq \mathrm{Aut(S)}$ where S is non-abelian simple.

Chief Lengths of Permutation Groups

Theorem (NEM, MRQ, CMRD 2011)

Let $G \leq S_n$ have s orbits. Then

$$l(G) \leq n - s.$$

Theorem (NEM, MRQ, CMRD 2011)

If $G \leq S_n$ is primitive then one of the following holds.

1. *G is of affine type and $l(G) \leq 4 \log n$.*
2. *G is a twisted wreath product and $l(G) \leq \log_{60} n$.*
3. *G is of diagonal type and $l(G) \leq 1 + \log_{60} n + \log \log n$.*
4. *G is of product type and $l(G) \leq \log n$.*
5. *G is an almost simple group and $l(G) \leq 1 + \log 3 + \log \log n$.*

Let $H \trianglelefteq G$. Then we have a chief series for G passing through H. The length of the part of the chief series of G from 1 up to H is denoted $l_G(H)$. Note that $l_G(H) \leq l(H)$.

Lemma

Let $H \trianglelefteq G$. Then $l(G) = l_G(H) + l(G/H)$.

Lemma

Let G be a subdirect product of H_1 and H_2. Then $l(G) \leq l(H_1) + l(H_2)$.

Chief Lengths of Permutation Groups

Example (Diagonal Type)

By definition, $G = T^k.H \leq S_n$, T non-abelian simple, $H \leq S_k \times \mathrm{Out}(T)$, $n = |T|^{k-1}$. Assume $k \geq 3$.

$l(G) = l_G(T^k) + l(H)$.
$\mathrm{Soc}(G) = T^k$, so $l_G(T^k) = 1$

H a subdirect product of $H_1 \leq S_k$ and $H_2 \leq \mathrm{Out}(T)$, so $l(H) \leq l(H_1) + l(H_2)$.
By induction, $l(H_1) \leq k - 1 \leq \log_{60} n$ and $l(H_2) \leq \log |H_2| \leq \log |\mathrm{Out}(T)| \leq \log\log |T| \leq \log\log n$. So

$$l(G) \leq 1 + \log_{60} n + \log\log n.$$

Chief Lengths of Permutation Groups

These bounds can be achieved in the imprimitive and intransitive cases.

Example

Let $W_k = \underbrace{C_2 \text{ wr } C_2 \text{ wr} \ldots \text{wr } C_2}_{k \text{ times}} \leq S_n = S_{2^k}$.

Then $|W_k| = 2^{2^{k-1}+2^{k-2}+\ldots+1}$.

As W_k is a 2-group its chief length is

$$l(W_k) = \log_2 |W_k| = 2^{k-1} + 2^{k-2} + \ldots + 1 = n - 1.$$

If we take a direct product of s groups of this form (we may take different values of k) we get an intransitive group with s orbits which achieves the bound $l(G) \leq n - s$.

Random Generation of Permutation Groups

Combining Lubotzky's result for $d^\epsilon(G)$, Neumann's result for $d(G)$ and our result for $l(G)$ gives the following.

Theorem (NEM, MRQ, CMRD, 2011)

Let $G \leq S_n$, and let G have s orbits. Let $\epsilon \in (0,1)$, and let t be such that $\zeta(t) \leq 1+\epsilon$. Then

$$d^\epsilon(G) \leq n/2 + 2\log(n-s) + t + 2.$$

Random Generation of Permutation Groups

Combine bounds with those of Holt & Roney-Dougal. If G is almost simple, $d(G) \leq 3$ (Dalla Volta & Lucchini 1995).

Theorem (NEM, MRQ, CMRD 2011)

Let $\epsilon \in (0,1)$ be given, and let t be such that $\zeta(t) \leq 1+\epsilon$. If $G \leq S_n$ is primitive, then one of the following holds.

1. *G is of affine type and $d^\epsilon(G) \leq \log n + 2\log\log n + t + 6$.*
2. *G is a twisted wreath product and $d^\epsilon(G) \leq \log n + 2\log(\log_{60} n) + t + 2$.*
3. *G is of diagonal type and $d^\epsilon(G) \leq \log n + 2\log(1 + \log_{60} n + \log\log n) + t + 2$.*
4. *G is of product type and $d^\epsilon(G) \leq \log n + 2\log\log n + t + 2$.*
5. *G is almost simple and $d^\epsilon(G) \leq 2\log\log\log n + t + 5 + \log(1 + \log 3)$.*

What Next?

Let $G \leq \mathrm{GL}_n(q)$ be completely reducible. Then

$$l(G) \leq 4n + n\log(q-1) - 1.$$

In addition, if G is primitive,

$$l(G) \leq 2(\log n)^2 + 3\log n + \log n \log\log q + \log(q-1).$$

Hope to improve these bounds.

Thank you for listening!