

Probabilistic Generation of Profinite Groups

Martyn Quick

University of St. Andrews

<http://www-groups.mcs.st-and.ac.uk/~martyn/>

11th March 2004

Finiteness Conditions

Infinite group theory at the time of Kurosh and P. Hall (c. 1940s) asked the following type of question:

Let \mathcal{P} be a property satisfied by all finite groups. If G is any (finitely generated) group satisfying \mathcal{P} , is it necessarily finite?

The Burnside Problem. Let G be a finitely generated group of finite exponent. Is G finite?

Tarski–Ol’shanskii Monsters: For sufficiently large primes p , there exist infinite groups G such that every proper subgroup is cyclic of order p .
(Ol’shanskii 1980)

Residual Finiteness

Definition. A group G is *residually finite* if for every non-identity element g of G there exists a normal subgroup N of finite index in G such that $g \notin N$.

IDEA: In a residually finite group, the elements can be distinguished between in the finite quotients.

Zelmanov's Solution to the Restricted Burnside Problem (1990/1991). *For each n and d , there is a largest finite group with d generators and exponent n .*

Equivalently

A finitely generated residually finite group of finite exponent is finite.

Profinite Groups

Let G be a residually finite group.

Form the inverse limit of the finite quotients of G
(the *profinite completion* of G):

$$\hat{G} = \varprojlim G/N$$

Then \hat{G} is a *profinite group*:

- a topological group which is
- compact and Hausdorff
- the open sets are unions of cosets of open subgroups
- G is dense in \hat{G} .

Probability and Generation

A profinite group Γ has a (normalised) *Haar measure* μ :

- $0 \leq \mu(X) \leq 1$ for all (measurable) subsets of Γ
- $\mu(\emptyset) = 0, \quad \mu(\Gamma) = 1.$

We use μ to define probability on Γ .

The probability that d randomly chosen elements generate Γ is

$$p_d(\Gamma) = \mu(S_d)$$

where

$$S_d = \{ (x_1, \dots, x_d) \in \Gamma^d \mid \overline{\langle x_1, \dots, x_d \rangle} = \Gamma \}.$$

Definition. A profinite group Γ is *positively finitely generated (PFG)* if there exists d such that $p_d(\Gamma) > 0$.

Theorem. [Mann–Shalev 1997] *A profinite group Γ is PFG if and only if it has polynomial maximal subgroup growth.*

$$m_n(\Gamma) = \#\{ M \leq_o \Gamma \mid M \text{ is a maximal subgroup of } \Gamma \text{ with } |\Gamma : M| = n \}.$$

Polynomial maximal subgroup growth: There exists γ with

$$m_n(\Gamma) \leq n^\gamma.$$

Theorem. [Borovik–Pyber–Shalev 1996]

Let Γ be a finitely generated profinite group and suppose there is a finite group F which does not occur as a subgroup of some quotient of Γ by an open subgroup. Then Γ is PFG.

Iterated Wreath Products

Let m_1, m_2, \dots be a sequence of integers with $m_r \geq 5$ for all r . Let

$$W_1 = \text{Alt}(m_1) \text{ acting on } \Omega_1 = \{1, 2, \dots, m_1\}$$

$$W_2 = \text{Alt}(m_2) \text{ wr}_{\Omega_1} W_1 \\ \text{acting on } \Omega_2 = \{1, 2, \dots, m_2\} \times \Omega_1$$

\vdots

$$W_r = \text{Alt}(m_r) \text{ wr}_{\Omega_{r-1}} W_{r-1} \\ \text{acting on } \Omega_r = \{1, 2, \dots, m_r\} \times \Omega_{r-1}$$

\vdots

Form

$$\hat{W} = \varprojlim W_r.$$

Theorem. [Bhattacharjee 1994]

$$p_2(\hat{W}) \geq (1 - \varepsilon) \cdot p_2(\text{Alt}(m_1))$$

where $\varepsilon \rightarrow 0$ as $m_1 \rightarrow \infty$.

Dixon (1969): $p_2(\text{Alt}(m_1)) \rightarrow 1$ as $m_1 \rightarrow \infty$.

Corollary. $p_2(\hat{W}) \rightarrow 1$ as $m_1 \rightarrow \infty$.

Dixon (1969), Kantor–Lubotzky (1990) and Liebeck–Shalev (1995) show:

Theorem. *If G is a finite simple group then $p_2(G) \rightarrow 1$ as $|G| \rightarrow \infty$.*

Let G_1, G_2, \dots be a sequence of non-abelian finite simple groups. Let

$$\begin{array}{ll} W_1 = G_1 & \text{acting on } \Omega_1 \\ W_2 = G_2 \text{ wr}_{\Omega_1} W_1 & \text{acting on } \Omega_2 \\ \vdots & \\ W_r = G_r \text{ wr}_{\Omega_{r-1}} W_{r-1} & \text{acting on } \Omega_r \\ \vdots & \end{array}$$

Form

$$\hat{W} = \varprojlim W_r.$$

Theorem. [MQ, *Comm. Algebra*, to appear]
If the above actions are regular, then

$$p_2(\hat{W}) \geq (1 - \varepsilon) \cdot p_2(G_1)$$

where $\varepsilon \rightarrow 0$ as $|G_1| \rightarrow \infty$.

Parker–MQ (*J. Algebra*, 2003): parametrise (conjugacy classes of) maximal subgroups of a wreath product which complement the base group.

Theorem. [MQ 2003/4] *If the above actions are transitive and faithful, then*

$$p_2(\hat{W}) \geq (1 - \varepsilon) \cdot p_2(G_1)$$

where $\varepsilon \rightarrow 0$ as $|G_1| \rightarrow \infty$.