The number of maximal subgroups and probabilistic generation of finite groups[1]

Ramón Esteban-Romero[1 2]

[1]Departament de Matemàtiques
Universitat de València

[2]Institut Universitari de Matemàtica Pura i Aplicada
Universitat Politècnica de València

Ischia (NA), March, 2018 / Ischia Group Theory 2018

[1]Joint work with A. Ballester-Bolinches, P. Jiménez-Seral and H. Meng

Outline

Outline

Introduction
Probabilistic generation

All groups in this talk will be finite.

Motivating question

Let G be a d-generated group. How many elements one should expect to choose uniformly and randomly to generate G? $\varepsilon(G)$

Introduction
Probabilistic generation

Netto, 1880:

- The probability that a randomly chosen pair of elements of $\mathrm{Alt}(n)$ generates $\mathrm{Alt}(n)$ tends to 1 as $n \to \infty$ (conjecture).
- The probability that a randomly chosen pair of elements of $\mathrm{Sym}(n)$ generates $\mathrm{Sym}(n)$ tends to $3/4$ as $n \to \infty$ (conjecture).

E. Netto.
The theory of substitutions and its applications to Algebra.
Register Publ. Co., Inland Press, Ann Arbor, Michigan, USA, 1892.
Translation from the original (1880) in German.

Introduction
Probabilistic generation

Dixon, 1969:

- Netto's conjecture is true: the proportion of generating pairs for $\mathrm{Alt}(n)$ or $\mathrm{Sym}(n)$ is greater than $1 - 2/(\ln \ln n)^2$ for sufficiently large n.
- He conjectures that the same happens for simple groups.

J. D. Dixon.
The probability of generating the symmetric group.
Math. Z., 110(3):199–205, 1969.

Introduction

Probabilistic generation

Kantor, Lubotzky, 1990; Liebeck, Shalev, 1995: Dixon's conjecture is valid: If G is almost simple with socle S, the probability that a pair of elements of G generates a subgroup containing S tends to 1 as $|G| \to \infty$.

W. M. Kantor and A. Lubotzky.
The probability of generating a finite classical group.
Geom. Dedicata, 36(1):67–87, 1990.

M. W. Liebeck and A. Shalev.
The probability of generating a finite simple group.
Geom. Dedicata, 56(1):103–113, 1995.

Introduction
Probabilistic generation

Pomerance, 2001: If G is abelian, then

$$\varepsilon(G) \leq \mathrm{d}(G) + \sigma,$$

where $\sigma = 2.118456563\dots$ is obtained from Riemann zeta function (best possible for abelian groups) and $\mathrm{d}(G)$ is the minimum number of generators of G.

C. Pomerance.
The expected number of random elements to generate a finite abelian group.
Period. Math. Hungar., 43(1-2):191–198, 2001.

Introduction
Probabilistic generation

Definition (Pak)

G group.
$\nu(G)$: least positive integer k such that G is generated by k random elements with probability at least $1/e$.

Theorem (Pak)

$$\frac{1}{e}\varepsilon(G) \leq \nu(G) \leq \frac{e}{e-1}\varepsilon(G).$$

I. Pak.
On probability of generating a finite group.
Preprint, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.43.7319.

Introduction
Probabilistic generation

Since

$$\langle x_1, \dots, x_k \rangle \neq G \iff \exists M \lessdot G \text{ such that } \langle x_1, \dots, x_k \rangle \leq M,$$

the maximal subgroups are relevant in the scope of probabilistic generation. In fact,

$$\begin{aligned} \operatorname{Prob}(\langle x_1, \dots, x_k \rangle \leq M) &= \prod_{i=1}^{k} \operatorname{Prob}(x_i \in M) \\ &= \left(\frac{|M|}{|G|}\right)^k = \frac{1}{|G:M|^k} \end{aligned}$$

The number $\mathrm{m}_n(G)$ of maximal subgroups of G of a given index n is also relevant.

Introduction
Probabilistic generation

Theorem (Lubotzky, 2002)

If G is a group with r chief factors in a given chief series, then

$$\mathrm{m}_n(G) \leq r(r + n^{\mathrm{d}(G)})n^2 \leq r^2 n^{\mathrm{d}(G)+2}.$$

Furthermore,

$$\nu(G) \leq \frac{1 + \log\log|G|}{\log \mathrm{i}(G)} + \max\left(\mathrm{d}(G), \frac{\log\log|G|}{\log \mathrm{i}(G)}\right) + 2.02,$$

$\mathrm{i}(G)$: smallest index of a proper subgroup of G

log: logarithm to the base 2

A. Lubotzky.
The expected number of random elements to generate a finite group.
J. Algebra, 257:452–459, 2002.

Introduction

Probabilistic generation

Theorem (Detomi and Lucchini, 2003)

There exists a constant c such that, for any group G, $\nu(G) \leq \lfloor \mathrm{d}(G) + c \log \lambda(G) \rfloor$ if $\lambda(G) > 1$, otherwise, $\nu(G) \leq \lfloor \mathrm{d}(G) + c \rfloor$, where $\lambda(G)$ denotes the number of non-Frattini chief factors in a given chief series of G.

$\lfloor x \rfloor$: defect integer part of x.

E. Detomi and A. Lucchini.
Crowns and factorization of the probabilistic zeta function of a finite group.
J. Algebra, 265(2):651–668, 2003.

Introduction
Probabilistic generation

Definition

For a group G, let us call

$$\mathcal{M}(G) = \max_{n\geq 2} \log_n \mathrm{m}_n(G) = \max_{n\geq 2} \frac{\log \mathrm{m}_n(G)}{\log n}.$$

$\log_n x$: logarithm to the base n of x, that is, $\log_n x = \log x / \log n = \ln x / \ln n$.

Theorem (Lubotzky, 2002)

$$\mathcal{M}(G) - 3.5 \leq \nu(G) \leq \mathcal{M}(G) + 2.02.$$

Outline

Introduction
Bounds of Jaikin-Zapirain and Pyber

Definition

Let G be a group, A a characteristically simple group.

- $\mathrm{rk}_A(G)$: largest number r such that G has a normal section that is the direct product of r non-Frattini chief factors of G that are isomorphic (not necessarily G-isomorphic) to A.
- $\mathrm{l}(G)$: least degree of a faithful transitive permutation representation of G, i.e., the smallest index of a core-free subgroup of G.

A. Jaikin-Zapirain and L. Pyber.
Random generation of finite and profinite groups and group enumeration.
Ann. Math., 173:769–814, 2011.

Introduction
Bounds of Jaikin-Zapirain and Pyber

Theorem (Jaikin-Zapirain, Pyber, 2011, Theorem 1)

There exist two absolute constants $0 < \alpha < \beta$ *such that for every group* G *we have*

$$\alpha\left(\mathrm{d}(G) + \max_A \left\{\frac{\log \mathrm{rk}_A(G)}{\log \mathrm{l}(A)}\right\}\right) < \nu(G) < \beta\, \mathrm{d}(G) + \max_A \left\{\frac{\log \mathrm{rk}_A(G)}{\log \mathrm{l}(A)}\right\},$$

where A *runs through the non-abelian chief factors of* G*.*

The max on the RHS is 0 if G is soluble (JZ-P, private communications).

Introduction
Bounds of Jaikin-Zapirain and Pyber

Theorem (Jaikin-Zapirain, Pyber, 2011, Theorem 9.5)

Let G be a d-generated group. Then

$$\max\left\{d, \max_{n\geq 5}\frac{\log \operatorname{rk}_n(G)}{c_7 \log n} - 4\right\} \leq \nu(G)$$
$$\leq cd + \max_{n\geq 5}\frac{\log \max\{1, \operatorname{rk}_n(G)\}}{\log n} + 3,$$

where c and c_7 are two absolute constants.

$\operatorname{rk}_n(G)$: maximum of $\operatorname{rk}_A(G)$, where A runs over the non-abelian characteristically simple groups A with $\operatorname{l}(A) \leq n$.

Outline

Introduction
Aims of this talk

Aims:

- To give an interpretation of the invariant $\mathrm{rk}_A(G)$ for a non-abelian characteristically simple group A.
- To improve the upper bound for $\mathrm{m}_n(G)$ and, hence, for $\nu(G)$.
- To estimate the values of the constants in Theorem 9.5 of Jaikin-Zapirain and Pyber, 2011.

Outline

Large characteristically simple sections of a group

Primitive groups

Definition

A primitive group is a group with a core-free maximal subgroup.

If M is a maximal subgroup of G, then M/M_G is a core-free maximal subgroup of G/M_G and so G/M_G is primitive.

Large characteristically simple sections of a group
Primitive groups

Theorem (Baer, 1957)

Let G be a primitive group and let U be a core-free maximal subgroup of G. Exactly one of the following statements holds:

1. $\mathrm{Soc}(G) = S$ *is a self-centralising abelian minimal normal subgroup of* G, $G = US$ *and* $U \cap S = 1$.
2. $\mathrm{Soc}(G) = S$ *is a non-abelian minimal normal subgroup of* G, $G = US$. *In this case,* $\mathrm{C}_G(S) = 1$.
3. $\mathrm{Soc}(G) = A \times B$, *where* A *and* B *are the two unique minimal normal subgroups of* G, $G = AU = BU$ *and* $A \cap U = B \cap U = A \cap B = 1$. *In this case,* $A = \mathrm{C}_G(B)$, $B = \mathrm{C}_G(A)$, *and* $A \cong B \cong AB \cap U$ *are non-abelian.*

Large characteristically simple sections of a group
Primitive groups

Theorem (Baer, 1957)

Let G be a primitive group and let U be a core-free maximal subgroup of G. Exactly one of the following statements holds:

1. $\mathrm{Soc}(G) = S$ *is a self-centralising abelian minimal normal subgroup of* G, $G = US$ *and* $U \cap S = 1$ *(type 1).*
2. $\mathrm{Soc}(G) = S$ *is a non-abelian minimal normal subgroup of* G, $G = US$. *In this case,* $\mathrm{C}_G(S) = 1$ *(type 2).*
3. $\mathrm{Soc}(G) = A \times B$, *where* A *and* B *are the two unique minimal normal subgroups of* G, $G = AU = BU$ *and* $A \cap U = B \cap U = A \cap B = 1$. *In this case,* $A = \mathrm{C}_G(B)$, $B = \mathrm{C}_G(A)$, *and* $A \cong B \cong AB \cap U$ *are non-abelian (type 3).*

Large characteristically simple sections of a group

Primitive groups

Definition

The primitive group $[H/K] * G$ associated with a chief factor H/K of G is:

1. the semidirect product $[H/K](G/\mathrm{C}_G(H/K))$ if H/K is abelian, or
2. the quotient group $G/\mathrm{C}_G(H/K)$ if H/K is non-abelian.

Outline

Large characteristically simple sections of a group
New results

Theorem

Let G be a monolithic primitive group in which $B = \mathrm{Soc}(G)$ is non-abelian. Then G/B has no chief factors isomorphic to B.

Large characteristically simple sections of a group
New results

Theorem B

Let A be a non-abelian chief factor of a group G and suppose that in a given chief series of G there are k chief factors isomorphic to A. Then there exist two normal subgroups C and R of G such that $R \leq C$ and C/R is isomorphic to a direct product of k minimal normal subgroups of G/R isomorphic to A.

- This can be extended to non-Frattini abelian chief factors.
- In particular, $\mathrm{rk}_A(G)$ is the number of chief factors of G isomorphic to A in a given chief series of G.
- The proof depends on the precrown associated to a supplemented chief factor and a maximal subgroup supplementing it.

Outline

The upper bound
Our bounds

Definition

Let G be a group and let $n \in \mathbb{N}$, $n > 1$. We denote by $\mathrm{cr}_n^{\mathfrak{A}}(G)$ the number of crowns associated to complemented abelian chief factors of order n of G, that is, the number of G-isomorphism classes of complemented abelian chief factors of G.

- Clearly, $\mathrm{cr}_n^{\mathfrak{A}}(G) = 0$ unless n is a power of a prime.
- This invariant concerns type 1 maximal subgroups (G/M_G primitive of type 1).

The upper bound

Our bounds

Definition

Let $n \in \mathbb{N}$. The symbol $\mathrm{rks}_n(G)$ denotes the number of non-abelian chief factors A in a given chief series of G such that the associated primitive group $[A] * G$ has a core-free maximal subgroup of index n.

- This invariant concerns type 2 maximal subgroups.

The upper bound
Our bounds

Definition

Let $n \in \mathbb{N}$. The symbol $\mathrm{rko}_n(G)$ denotes the number of non-abelian chief factors A in a given chief series of G such that $|A| = n$.

Definition

Let $n \in \mathbb{N}$. The symbol $\mathrm{rkom}_n(G)$ denotes the maximum of the numbers $\mathrm{rk}_A(G)$ for A running over the isomorphism types of non-abelian chief factors of G with $|A| = n$.

- These invariants concern type 3 maximal subgroups.
- The non-abelian chief factors A of G of order n fall into at most two isomorphism classes.

The upper bound
Our bounds

Theorem A

Let G be a d-generated non-trivial group. Then

$$\max\{d, \max_A \frac{\log \mathrm{rk}_A(G)}{2\log \mathrm{l}(A)} - 2.63\} \leq \nu(G) \leq \eta(G),$$

where in the maximum on the left hand side, A runs over the isomorphism classes of non-abelian chief factors in a given chief series of G and $\eta(G)$ *is a function bounded by a linear combination of d and the maxima of* $\log_n \mathrm{cr}_n^{\mathfrak{A}}(G)$, $\log_n \mathrm{rks}_n(G)$, $\log_n \mathrm{rko}_n(G)$, *and* $\log_n \mathrm{rkom}_n(G)$.

The upper bound
Our bounds

Lemma (Borovik, Pyber, Shalev, 1996)

The number $g(n)$ of isomorphism classes of non-abelian simple subgroups of $\mathrm{Sym}(n)$ for $n \geq 5$ is $\mathrm{O}(n)$.

We precise the value $\mathrm{O}(n)$:

Lemma

The number $g(n)$ of isomorphism classes of non-abelian simple groups of $\mathrm{Sym}(n)$ for $n \geq 5$ is at most $4.89n + 1\,141.33$.

A. V. Borovik, L. Pyber, and A. Shalev.
Maximal subgroups in finite and profinite groups.
Trans. Amer. Math. Soc., 348(9):3745–3761, 1996.

The upper bound
Our bounds

Lemma

The number $s(n)$ of isomorphism classes of minimal normal subgroups of primitive groups of type 2 with a core-free maximal subgroup of index n satisfies the inequality $s(n) \leq n^{1.266}$.

Note that $\mathrm{rks}_n(G) \leq s(n)\mathrm{rk}_n(G)$.

The upper bound
Our bounds

Theorem

Let U be a maximal subgroup of type 1 of a d-generated group G and let $n = |G : U|$. Then the number of maximal subgroups M of G such that $\mathrm{Soc}(G/M_G)$ is G-isomorphic to $\mathrm{Soc}(G/U_G)$ is less than or equal to

$$\frac{n^d - n|\mathrm{H}^1(G/C, A)|}{q - 1},$$

where $A = C/U_G$ is the unique minimal normal subgroup of G/U_G and $q = |\mathrm{End}_{G/C}(A)|$. In particular, this number is less than n^d.

The upper bound
Our bounds

Corollary (number of type 1 maximal subgroups)

The number of type 1 *maximal subgroups* M *of index* $n = p^r$ *of a* d*-generated group* G *is less than or equal to* $(n^d - 1)\mathrm{cr}_n^{\mathfrak{A}}(G)$.

We use arguments of Dalla Volta and Lucchini (1998) and results of Gaschütz (1959).

F. Dalla Volta and A. Lucchini.
Finite groups that need more generators than any proper quotient.
J. Austral. Math. Soc. Ser. A, 64(1):82–91, 1998.

W. Gaschütz.
Die Eulersche Funktion endlicher auflösbarer Gruppen.
Illinois J. Math., 3(4):469–476, 1959.

The upper bound
Our bounds

Theorem (number of type 2 maximal subgroups)

Let G be a group and let $n \in \mathbb{N}$. The number of maximal subgroups of G of type 2 and index n is bounded by $\operatorname{rks}_n(G)n^2$.

The upper bound
Our bounds

Theorem (number of type 3 maximal subgroups)

Let G be a d-generated group and let $n \in \mathbb{N}$ which is a power of the order of a non-abelian simple group. The number of maximal subgroups of G of type 3 and index n is bounded by

$$n^2 \min\left\{n^d, \frac{\operatorname{rkom}_n(G) - 1}{2}\right\} \operatorname{rko}_n(G).$$

This result depends on the study of the crowns associated to non-abelian chief factors, since the minimal normal subgroups of G/M_G are G-connected.

The upper bound
Our bounds

Theorem

1. *If $n \in \mathbb{T}$ (power of a prime), then (types 1 and 2)*
$$\begin{aligned} \mathrm{m}_n(G) &\leq (n^d - 1)\mathrm{cr}_n^{\mathfrak{A}}(G) + n^2 \mathrm{rks}_n(G) \\ &\leq 2 \max\{n^d \mathrm{cr}_n^{\mathfrak{A}}(G), n^2 \mathrm{rks}_n(G)\}. \end{aligned}$$
2. *If $n \in \mathbb{S}$ (power of the order of a non-abelian simple group), then (types 2 and 3)*
$$\mathrm{m}_n(G) \leq n^2 \mathrm{rks}_n(G) + n^2 \min\left\{n^d, \frac{\mathrm{rkom}(G) - 1}{2}\right\} \mathrm{rko}_n(G).$$
$$\leq 2n^2 \max\left\{\mathrm{rks}_n(G), \min\left\{n^d, \frac{\mathrm{rkom}_n(G) - 1}{2}\right\} \mathrm{rko}_n(G)\right\}.$$
3. *If $n \notin \mathbb{S} \cup \mathbb{T}$, then $\mathrm{m}_n(G) \leq n^2 \mathrm{rks}_n(G)$ (type 2).*

The upper bound
Our bounds

Theorem A

Let G be a d-generated non-trivial group. Then, for

$$\begin{aligned}\eta(G) := \max\Big\{& d + 2.02 + \max\{\log_n 2 + \log_n \mathrm{cr}_n^{\mathfrak{A}}(G)\},\\ & 4.02 + \max\{\log_n 2 + \log_n \mathrm{rks}_n(G)\},\\ & 4.02 + \max\Big\{\min\{d + \log_n 2, \log_n \mathrm{rkom}_n(G)\}\\ & \qquad\qquad + \log_n \mathrm{rko}_n(G)\}\Big\},\end{aligned}$$

we have that

$$\nu(G) \leq \eta(G).$$

Outline

The upper bound
Consequences

The following result is Corollary 7.3 of Jaikin-Zapirain and Pyber, 2011, written in a stronger form.

Theorem (cf. Jaikin-Zapirain and Pyber, 2011, Corollary 7.3)

Let G be a d-generated group. There exists a constant c_6 such that the number of irreducible G-modules of size n is at most

$$n^{c_6 d} \max\{1, \mathrm{rk}_n(G)\}.$$

The upper bound
Consequences

This result can be used to obtain Theorem 9.5 of Jaikin-Zapirain and Pyber, 2011 from our results, because

$$\log_n \mathrm{cr}_n^{\mathfrak{A}}(G) \leq c_6 d + \log_n \max\{1, \mathrm{rk}_n(G)\},$$
$$\log_n \mathrm{rks}_n(G) \leq 1.266 + \log_n \max\{1, \mathrm{rk}_n(G)\},$$
$$\log_n \mathrm{rko}_n(G) \leq \log_2 2 + \log_n \max\{1, \mathrm{rk}_n(G)\}.$$

It follows that

$$\nu(G) \leq (c_6 + 1)d + 3.02 + \max \log_n \max\{1, \mathrm{rk}_n(G)\}.$$

The upper bound
Consequences

The bound of Jaikin-Zapirain and Pyber depends on a constant defined as a linear combination of constants that in many cases are known to exist, but no explicit values have been given for them. We precise the values in Theorem 9.5 of Jaikin-Zapirain and Pyber, 2011.

Theorem

Let G be a d-generated group. Then

$$\eta(G) \leq cd + \max_{n \geq 5} \frac{\log \max\{1, \mathrm{rk}_n(G)\}}{\log n} + 3,$$

where $c = 375.06$.

The upper bound
Consequences

This result depends on the previously mentioned result.

Corollary (cf. Jaikin-Zapirain, Pyber, 2011, Corollary 7.3)

Let G be a d-generated group. There exists a constant C_6 such that the number of irreducible G-modules of size n is at most

$$\max\{1, \mathrm{rk}_n(G)\} n^{C_6 d}.$$

This constant can be taken to be 374.06.

The upper bound

Consequences

A slightly different approach shows:

Theorem

The number of non-equivalent irreducible G-modules of size $n = p^r$, where p is a prime and $r \in \mathbb{N}$, is at most

$$n^{\min\{c_6 d + k_6 + \log_n \max\{1, \mathrm{rk}_n(G)\}, dr\}},$$

where $c_6 = 183.034$ and $k_6 = 74$.

Outline

The upper bound
Examples

Corollary

Let G be a d-generated group with no abelian chief factors. Then $\nu(G) \leq 4.289 + d + \max_{n\geq 5} \log_n \max\{1, \mathrm{rk}_n(G)\}$.

The upper bound
Examples

Construction

- G d-generated primitive group of type 1.
- $\Omega = \{\text{ordered generating } d\text{-tuples of } G\} = \Omega_1 \cup \cdots \cup \Omega_r$, with Ω_i orbits of the action of $\mathrm{Aut}(G)$ on Ω,
- $(g_{i1}, \ldots, g_{id}) \in \Omega_i$, $1 \leq i \leq r$,
- $g_j = \prod_{i=1}^{r} g_{ij} \in G^r$, $1 \leq j \leq d$.
- $\hat{G} = \langle g_1, \ldots, g_d \rangle$ is a subdirect product of G^r and $\hat{G}$ has as socle a direct product of all faithful and irreducible modules for G whose primitive group is isomorphic to G.
- This construction can be extended to many d-generated primitive groups with isomorphic socles.

The upper bound

Examples

- There are 3 isomorphism classes of 2-generated primitive groups of type 1 with socle of order 8: $G_1 = [C_2^3]C_7$, $G_2 = [C_2^3][C_7]C_3$, $G_3 = [C_2^3]\mathrm{GL}_3(2)$.
- We can construct a 2-generated group S with all possible crowns of abelian chief factors of order 8.

$$\mathrm{cr}_3^{\mathfrak{A}}(S) = 1, \quad \mathrm{cr}_7^{\mathfrak{A}}(S) = 9, \quad \mathrm{cr}_8^{\mathfrak{A}}(S) = 146, \quad \mathrm{rk}_{\mathrm{GL}_3(2)}(S) = 57.$$

- Bound of Jaikin-Zapirain and Pyber:
  $\nu(S) \leq 3 + 2c + \log_7 57$ with
  $3 + 2c + \log_7 57 \geq 5.07 + 2c \approx 755.198$.
- Bound of Theorem A: $\nu(S) \leq 6.75$.