Probabilistic Group Theory

Elisa Covato

MINGLE 2014

September, 2014

Introduction

A well known fact:

Groups are algebraic structures which arise naturally throughout mathematics, both pure and applied.

A not well known fact:

Probability has been successfully (and surprisingly!) applied to group theory in the solution of several important problems.

Probabilistic method

Suppose that we would like to prove that a class of groups has a member with a specified property.

- **Classic method**: Construct a member of the class with the desired property
- **Probabilistic method**: Show that a randomly chosen member of the class has the desired property (with positive probability)

In **probabilistic group theory** we are interested in:

- Alternative description of the structure of groups and their elements with probabilistic statements
- Application of probabilistic methods to prove deterministic theorems

How commutative a non-abelian group can be?

Let G be a finite **non-abelian** group.

Question

What is the probability that two randomly chosen elements commute?

Assuming that random elements are chosen independently and every pair of elements has the same probability $1/|G|^2$ of being chosen, the previous question can be interpreted as computing:

$$p = \frac{|\{(x, y) \in G \times G : xy = yx\}|}{|G|^2}$$

Answer

$p \leq \frac{5}{8}$

The unbearable ease of generating (some) groups

Let S_n be the set of all $n!$ permutations of $\{1, 2, \ldots, n\}$. This is the **symmetric group** of degree n.

Theorem (Jordan, 1870)

The symmetric group S_n can be generated by **two** *elements.*

Question

How many pairs of elements in S_n generate the whole group?

The unbearable ease of generating (some) groups

Netto's conjecture (1882) asserts that **almost** all pairs of elements of S_n generate the whole group.

Theorem (Dixon, 1969)

Let p_n the probability that two randomly chosen elements of S_n generate S_n. Then $p_n \to 1$ as $n \to \infty$.

In other words, it is very easy to find generating pairs in S_n: after a few random choices we are very likely to end up with one.

Question

Is this property shared by other important groups?

Generating simple finite groups

A finite group is said to be **simple** if its normal subgroups are only the trivial group and the group itself.

Finite simple groups are the building blocks of all finite groups.

Examples

- Any group of prime order is simple
- The set of even permutations of $\{1, \ldots, n\}$ forms a subgroup of S_n, denoted by A_n. Then A_n is simple if $n \geq 5$

It is well-known that every finite simple group is 2-generated.

Theorem (Dixon, 1969; Kantor-Lubotzky, 1990; Liebeck-Shalev,1995)

Let G be a finite simple group. Then the probability that two randomly chosen elements of G generate G tends to 1 as $|G| \to \infty$.

The (2,3)-generator problem

Problem

Which finite simple groups G can be generated by two elements x, y of orders 2 and 3, respectively?

The **(2,3)-generator problem** was open for nearly a century. It arose from the study of the modular group $PSL_2(\mathbb{Z})$.

It is known that $PSL_2(\mathbb{Z}) \cong \langle x \rangle * \langle y \rangle$, the free product of a group of order 2 and a group of order 3.Therefore the (2,3)-generator problem is equivalent to:

Which simple groups G are quotient of $PSL_2(\mathbb{Z})$?

Theorem (Liebeck-Sahlev, 1996; Lubeck-Malle, 1999)

All finite simple groups, **excepts for finitely many** *groups, can be obtained as quotient of the modular group* $PSL_2(Z)$.

Strategy for the proof

To show that a group G is (2,3)-generated (with some exceptions), we apply the **probabilistic method**.

(1) Define $P_{2,3}(G) = \frac{|\{(x,y)\in G\times G : x^2=y^3=1, G:\langle x,y\rangle\}|}{|G|^2}$

(2) Choose at random an element $x \in G$ and $y \in G$ s. t. $x^2 = y^3 = 1$

(3) If x, y do **not** generate G, then they both lie in some maximal subgroup M of G

(4) Compute $1 - P_{2,3}(G) \leq \sum_{M\subset G} \mathbb{P}(x \in M) \cdot \mathbb{P}(y \in M)$

(5) Show that, as $|G| \to \infty$, the quantity $1 - P_{2,3}(G)$ is bounded above by 0

Notice that $\mathbb{P}(x \in M)$ and $\mathbb{P}(y \in M)$ are functions of $|G : M|$.

Probability for infinite groups

For some infinite groups we can naturally define a **probability distribution**.

A **profinite group** is a compact and totally disconnected topological group (or, equivalently, it is an inverse limit of finite groups)

Examples

- The group of p-adic integers: $\mathbb{Z}_p = \varprojlim \mathbb{Z}/\mathbb{Z}_{p^n}$
- Matrix groups over $\mathbb{Z}_p$

As a compact group, each profinite group admits an invariant measure (**Haar measure**) of finite total measure. If we normalize the measure, then it turns the group into probability space.

We are allowed to describe profinite groups with probabilistic statements.

Some other related problems

The probabilistic method has been applied to solve other important problems

- The general (r, s)-generator problem
- Random generation by two conjugates
- Random generation by three elements of order two
- Generate random elements in a group
- Show that A_n is a homomorphic image of a Fuchsian group, for all sufficiently large n

Grazie!