Randomness, dimension, and profinite groups

André Nies

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

AMS/AustMS/NZMS joint meeting
Special session on computability theory and applications
December 2024

The plan

1. Profinite groups and their computable presentations
2. Algorithmic randomness in computable profinite groups
3. Fractal dimensions of closed subgroups

I. Profinite groups and their computable presentations

Profinite groups as inverse limits

An inverse system is a sequence $(G_n, p_n)_{n\in\mathbb{N}}$ where the G_n are finite groups, and the $p_n\colon G_{n+1} \to G_n$ are homomorphisms.

Its inverse limit is the topological group $G = \varprojlim_n (G_n, p_n)$, given up to isomorphism by a universal property from category theory.

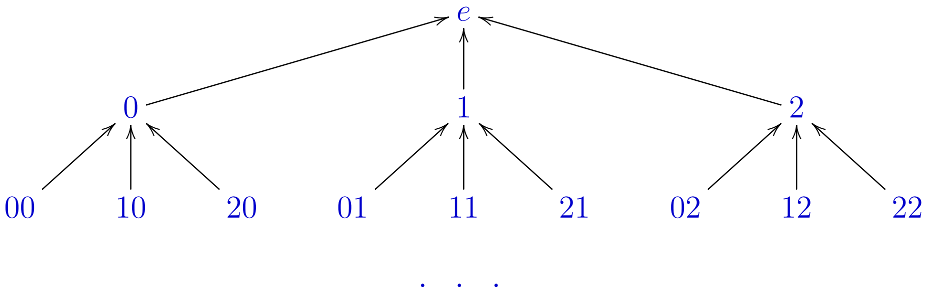
A separable topological group G is called profinite if

it is isomorphic to such an inverse limit.

G will always denote a profinite group, with a specified inverse system.

Inverse limit as group on a path space (1)

An inverse system $(G_n, p_n)_{n\in\mathbb{N}}$, with G_0 trivial, yields a finitely branching rooted tree T. The n-th level consists of G_n; the predecessor relation is given by the $p_n\colon G_{n+1} \to G_n$.



The first levels of the tree for $\mathbb{Z}_3$, the 3-adic integers.

$G_1 = C_3$, $G_2 = C_9$, etc.

Inverse limit as group on a path space (2)

Recall: an inverse system $(G_n, p_n)_{n\in\mathbb{N}}$, with G_0 trivial, yields a finitely branching rooted tree T. The n-th level consists of G_n; the predecessor relation is given by the $p_n \colon G_{n+1} \to G_n$.

- As the domain of the inverse limit one can concretely take the path space $[T]$.
- Its neutral element is the path consisting of the neutral elements in the G_n's.
- The group multiplication is given by

$$f \cdot g = \bigcup_n [f\restriction_n \cdot g\restriction_n] \text{ for } f, g \in [T].$$

- Similarly for inverse operation.
- These operations are continuous w.r.t. the topology on $[T]$.

Examples of profinite groups (1)

- Let $(\mathbb{Z}_p, +) = \varprojlim_n C_{p^n}$ where p is prime and C_{p^n} is the cyclic group of size p^n.
- Via the view as a tree, the elements of $\mathbb{Z}_p$ can be encoded by infinite sequences of digits in $\{0, \ldots, p-1\}$, with addition via the usual carry digits. Say $p = 3$:

$$\begin{array}{cccccc} & \ldots & 1 & 2 & 1 & 1 & 1 \\ + & \ldots & 0 & 2 & 1 & 2 & 0 \\ \hline = & \ldots & 2 & 2 & 0 & 0 & 1 \end{array}$$

- This is a pro-p group: all the G_n are p-groups.
- Let $k \geq 2$. Since $\mathbb{Z}_p$ is in fact a profinite ring, matrix groups such as upper unitriangular $\mathrm{UT}_k(\mathbb{Z}_p)$, and special linear $\mathrm{SL}_k(\mathbb{Z}_p)$ are profinite.
- For instance, $\mathrm{SL}_k(\mathbb{Z}_p) = \varprojlim_n \mathrm{SL}_k(C_{p^n})$.

Examples of profinite groups (2)

An extension of fields K/k is Galois if it is algebraic, normal, and separable.

Its Galois group $G = \mathrm{Gal}(K/k)$ consist of the automorphisms of K that fix k pointwise.

- $G = \mathrm{Gal}(K/k)$ is a profinite group with the Krull topology:
- If $K = \bigcup_{i\in\mathbb{N}} L_i$, where $L_{i+1} \geq L_i$ and each L_i is a normal finite extension of k, then $G \cong \varprojlim_i \mathrm{Gal}(L_i/k)$.

Galois correspondence

Fields L with $K \geq L \geq k$ correspond to closed subgroups of G. In the forward direction, send L to its pointwise stabiliser in G.

Residually finite groups, and profinite completions

A countable group L is called residually finite if for each $w \in L$, $w \neq e$, there is a finite quotient Q of L such that $w \neq e$ in Q.

For such L, there is a descending sequence of normal subgroups $(R_n)_{n\in\mathbb{N}}$ of L such that $\exists n R_n \subseteq R$ for each subgroup of finite index R. In particular, $\bigcap_n R_n = \{e\}$.

$\widehat{L} = \varprojlim_n L/R_n$ is the profinite completion of L.

Up to isomorphism, it is independent of the choice of such a sequence, by the universal property of inverse limits.

L embeds into $\widehat{L}$ via $w \mapsto (wR_n)_{n\in\mathbb{N}}$,

where wR_n is the image of w in the quotient L/R_n.

Example: $\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n!\mathbb{Z}$ is the profinite completion of $(\mathbb{Z}, +)$.

Co-c.e. and computable profinite groups

Recall: a profinite group is given by an inverse system $(G_n, p_n)_{n\in\mathbb{N}}$; the $p_n \colon G_{n+1} \to G_n$ are homomorphisms of finite groups.

Definition (Smith, 1981; LaRoche, 1981)

A co-c.e. profinite group G is given by a computable inverse system. The group is called computable if in addition, all the p_n's are onto.

Theorem (Smith, 1981)

(i) Some co-c.e. profinite group G is not isomorphic to a computable one. (ii) Each co-c.e. pro-p group is computable.

Proof. (i) let A be a properly Σ^0_2 set of primes, and let G be a co-c.e. presentation of $\prod_{p\in A} C_p$.
(ii) uses group theoretic methods such as Frattini subgroup.

Co-c.e., and computable in terms of the tree

Recall that an inverse system $(G_n, p_n)_{n\in\mathbb{N}}$ yields a finitely branching tree T with levels consisting of the G_n.

- To say that G is co-c.e. means that the tree T computable with computable branching, and
  the operations at each level are uniformly computable.
- To say G is computable means that also the tree has no leaves.

The neutral element of the group is given by a computable path.
Metakides and Nerode built an example of a computable profinite group where there are no others.
Smith 1981 proved preservation properties for computable G.
For instance, the derived group G' is computable, and G has a computable p-Sylow subgroup for each prime p.

Arbitrary effective tree $\Rightarrow$ nice effective tree

Fact: a separable topological group is profinite $\iff$ it is compact and 0-dimensional (the clopen sets form basis).

- If a topological structure for a finite functional signature σ is compact 0-dimensional, then it has a copy whose domain is $[T]$ for some finitely branching tree T.
- To define co-c.e. σ-structures, ask that T is computable with computable bound on branching, and operations computable.
- To define computable σ-structures, ask that also T has no leaves.

Theorem (Smith 1981/ Melnikov and N., 2022 in l.c. context)

Suppose a profinite group has a co-c.e. [computable] presentation in the general sense of topological algebra.

Then G has a co-c.e. [computable] presentation in the sense of effective inverse systems. The conversion is uniform.

Computably f.g. subgroups of profinite groups

- Recall that a discrete group L is called residually finite if each $w \in L - \{e\}$ we have $w \neq e$ in some finite quotient of L.
- The class of f.g. residually finite groups coincides with the f.g. abstract subgroups of profinite groups. Effectivise?

The effective version of "finitely generated subgroup" is computably f.g. subgroup:

an abstract subgroup of a computably profinite group generated by finitely many computable paths.

We will characterize the computably f.g. subgroups L of computable profinite groups by the following two conditions:

1: the word problem of L is Π^0_1

2: L is effectively residually finite.

Π-groups

Definition

A f.g. group L is called a Π-group if its word problem is Π^0_1. Thus, $L = F_k/N$ for some k and a Π^0_1 normal subgroup N of the free group F_k.

- Examples: all f.g. subgroups of the group S_{rec} of computable permutations of ω are Π-groups.
- Morozov (Higman's question revisited, 2000) constructed a Π-group that is NOT of this kind.
- Any computably f.g. subgroup of a computable profinite group G is embedded into S_{rec}, and hence a Π-group.
- To verify this, use its action on the tree for $(G_n, p_n)_{n\in\mathbb{N}}$.

Effectively residually finite Π-groups (1)

Definition

A Π-group $L = F_k/N$ is effectively residually finite (e.r.f.) if there is an algorithm that on $w \in F_k$, in case $w \notin N$ computes a finite quotient Q of L such that $w \neq e$ in the quotient. The quotient is given by a homomorphism $F_k \to Q$ whose kernel contains N.

Proposition

The computably f.g. subgroups of computably profinite groups are precisely the effectively residually finite Π-groups L.

The proof of right to left is by noting that there is a computable embedding of L into a computable profinite group H, with images of the generators of L computable.
(But this may not be the profinite completion $\overline{L}$. To get this, we'd need to be able to list all the finite index subgroups of L.)

Effectively residually finite Π-groups (2)

Proposition (Recall)

The computably f.g. subgroups of computably profinite groups are precisely the effectively residually finite (e.r.f.) Π-groups L.

- As a consequence, each e.r.f. Π-group L is isomorphic to a subgroup of the group of computable permutations.
- For, the computable profinite group $H \geq L$ acts faithfully on its computable tree T, and computable elements of H yield computable permutations of T.

Question

Is there a f.g., residually finite Π-group that is not effectively r.f.?

II. Algorithmic randomness in computable profinite groups

Joint with Willem Fouché and Matteo Vannacci

Haar measure

Any compact separable group has a unique translation invariant probability measure, called its Haar measure, we denote by μ.

If $G = \varprojlim_n G_n$ is profinite, this is the uniform measure on $[T]$, where T is the tree given by the inverse system.

If G is computable and infinite, the usual algorithmic test notions for Cantor space can be extended to the paths space $[T]$. So we can speak of Schnorr random elements of G etc.

“Almost everywhere” results for k-tuples (1)

An “almost everywhere” result for a profinite group G asserts that μ^k-almost every k-tuple $\overline{g} \in G^k$ satisfies some property of interest.

Recall $\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n!\mathbb{Z}$ is the profinite completion of $\mathbb{Z}$. For $\overline{g} \in G^k$, by $\langle \overline{g} \rangle$ one denotes the closure of the subgroup generated by $\overline{g}$.

Some “ almost everywhere” results for $\widehat{\mathbb{Z}}$ (Jarden, Lubotzky):

(1) $|\widehat{\mathbb{Z}} : \langle g \rangle| = \infty$ for a.e. $g \in \widehat{\mathbb{Z}}$.

(2) $|\widehat{\mathbb{Z}} : \langle \overline{g} \rangle| < \infty$ for a.e. $\overline{g} \in (\widehat{\mathbb{Z}})^k$, where $k \geq 2$.

"Almost everywhere" results for k-tuples (2)

Recall " almost everywhere" results for $\widehat{\mathbb{Z}}$ (Jarden, Lubotzky):

(1) $|\widehat{\mathbb{Z}} : \langle g \rangle| = \infty$ for a.e. $g \in \widehat{\mathbb{Z}}$.

(2) $|\widehat{\mathbb{Z}} : \langle \overline{g} \rangle| < \infty$ for a.e. $\overline{g} \in (\widehat{\mathbb{Z}})^k$, where $k \geq 2$.

Theorem (Algorithmic versions of these results)

(1) If $g \in \widehat{\mathbb{Z}}$ is Kurtz random then $|\widehat{\mathbb{Z}} : \langle g \rangle| = \infty$

(2) If $k \geq 2$ and $\overline{g} \in \widehat{\mathbb{Z}}^k$ is Schnorr random, then $|\widehat{\mathbb{Z}} : \langle \overline{g} \rangle| < \infty$; being Kurtz random is not sufficient.

When a k-tuple generates an open subgroup a.s.

We say a profinite G is a k-group if $|G\colon \langle \overline{g} \rangle| < \infty$, for a.e. $\overline{g} \in G^k$. This means $Q(G, k) = 1$ in the sense of Avinoam Mann (1996).

Each k-group is topologically finitely generated. So could as well require $\langle \overline{g} \rangle$ open. By the above, $\widehat{\mathbb{Z}}$ is a 2-group, but not a 1-group.

When a k-tuple generates an open subgroup a.s.

Recall a profinite G is a k-group if $|G\colon \langle \overline{g} \rangle| < \infty$, for a.e. $\overline{g} \in G^k$.

Proposition

Let the computable profinite group G be a k-group.
Then $|G : \langle \overline{g} \rangle| < \infty$ for each weakly 2-random $\overline{g} \in G^k$.

Proof:

- Let $V_m = \{\overline{g} \in G^k \colon |G : \langle \overline{g} \rangle| \geq m\}$.
- If $\overline{g} \in V_m$ this becomes apparent at some G_n in the inverse system. So V_m is uniformly Σ^0_1.
- Also $\mu^k(V_m) \to_m 0$ since G is a k-group.
- So $(V_m)_{m \in \mathbb{N}}$ is a weak 2-test. $\square$

How fast does $\mu^k(V_m)$ go to 0? Work in progress with Vannacci would show that if G is pro-p, then Schnorr randomness suffices.

Effective form of a.e. results for $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ (1)

We give algorithmic versions of “a.e.” theorems from “the bible”
Fried and Jarden, Field arithmetic (3d edition, 2005).

$G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) = Aut(\overline{\mathbb{Q}}, +, \times)$ is the absolute Galois group of $\mathbb{Q}$.
$\mathbb{Q}[X]$ has a splitting algorithm $\Rightarrow G$ is computable profinite.

Theorem (algorithmic form of Thm. 18.5.6 in Fried-Jarden)

Let $\overline{g} \in G^k$ be Kurtz random. Then $\langle \overline{g} \rangle$ is a free profinite group of rank k.

Effective form of a.e. results for $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ (2)

$G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is the absolute Galois group of $\mathbb{Q}$.

A field L is pseudo-algebraically closed (PAC) $\iff$ every absolutely irreducible polynomial $p \in L[X, Y]$ has a zero in L.

Theorem (algorithmic form of Thm. 27.4.8 in Fried-Jarden)

Let $g \in G$ be Kurtz random. Then the fixed field of the least closed normal subgroup containing g is PAC.

- Since Kurtz randomness is enough, the Fried-Jarden results prove more than what they say.
- Instead of $\mathbb{Q}$ can take computable "Hilbertian" field with splitting algorithm.

III. Fractal dimensions of closed subgroups

Joint with Elvira Mayordomo (see 2023-24 Logic Blog)

Closed subgroups of a profinite group

- Write $H \leq_c G$ to express that H is a closed subgroup of $G = \varprojlim_n (G_n, p_n)$.
- Let H_n be the natural projection of H into G_n. Let q_n be p_n restricted to H_{n+1}
- Then $H = \varprojlim_n (H_n, q_n)$ with onto maps.

Recall $G = [T]$ where T is the tree associated with the inverse system. Clearly the subgroup H is given as $[S]$ where S is the subtree associated with (H_n, q_n).

How to measure the size of H? Note that $\mu(H) = 0$ unless H has finite index (and hence is open in case that G is topologically f.g.)
Answer: Use fractal dimension!

Metrics on a profinite group

- For this we need a metric. The tree T for G gives us the usual ultrametric.
- Little problem: the inverse system for G the tree is based on can be somewhat arbitrary. Certainly it's not unique.
- Recall pro-p groups, where all the G_n have size a power of p.
- For G in such a class, there is a natural inverse system: Let R_n be the closed (normal) subgroup generated by the p^n-th powers. Clearly $\bigcap_n R_n = \{e\}$.
- Let $G_n = G/R_n$. Then $(G_n)_{n\in\mathbb{N}}$, with the canonical maps $G_{n+1} \to G_n$, forms an inverse system for G.
- If $G = \mathbb{Z}_p$, we get back $G_n = C_{p^n}$.
- For d-generated free pro-p groups the inverse system is quite complicated. G_n is the largest d-generated group of order p^n.

Lower and upper box (counting) dimension

Let M be a metric space, and $X \subseteq M$ be compact. For $\alpha > 0$, let $N_\alpha(X) =$ least size of a covering of X with sets of diameter $\leq \alpha$.

The lower box dimension is

$$\underline{\dim}_B(X) = \liminf_{\alpha \to 0^+} \frac{\log N_\alpha(X)}{\log(1/\alpha)}$$

The upper box dimension $\overline{\dim}_B(X)$ is defined as the limsup.

$\underline{\dim}_B(\text{Coastline}) = 1.25$

Source: wikipedia

Lower box dimension of $[S]$

Consider the metric space $[T]$ for a finitely branching tree $T \subseteq \mathbb{N}^*$.
Let $X = [S]$ where S is a subtree.

$\{[\sigma] \colon \sigma \in S_n\}$ is the "optimal covering" of $[S]$ for diameter $|T_n|^{-1}$.
Only α's of form $|T_n|^{-1}$ are relevant, so $\liminf_{\alpha \to 0^+} \frac{\log N_\alpha(X)}{\log(1/\alpha)}$ equals

$$\underline{\dim}_B([S]) = \liminf_{n \to \infty} \frac{\log |S_n|}{\log |T_n|}$$

Example (similar to the Cantor "no middle-third" set)

- Let $T = \{0, 1, 2\}^{<\omega}$ and S the subtree of strings without a 1.
- $\log |S_n| / \log |T_n| = \log 2 / \log 3$ for each n.
- So $\underline{\dim}_B[S] = \log_3(2)$

Apply to closed subgroups of G

Recall that

$$\underline{\dim}_B([S]) = \liminf_{n\to\infty} \frac{\log|S_n|}{\log|T_n|}$$

In the case of $H \leq_c G$ we have $|S_n| = |H_n|$, where H_n is the projection of H into G_n.

Example (Barnea-Shalev 1997, essentially)

Let G be the Cantor space with symmetric difference Δ. For each $0 \leq \alpha \leq \beta \leq 1$ there is $H \leq_c G$ with

$$\underline{\dim}_B(H) = \alpha \text{ and } \overline{\dim}_B(H) = \beta.$$

To see this, let $R \subseteq \mathbb{N}$ be a set with lower [upper] density α [β]. Let H be the subgroup $\mathcal{P}(R)$. We have $|S_n| = 2^{|X\cap n|}$, $|T_n| = 2^n$.

Hausdorff and packing dimension

- $\underline{\dim}_B(X)$ is easier to calculate, but less robust than Hausdorff dimension $\dim_H(X)$.

- Recall packing dimension $\dim_P$.

- We always have

$$\begin{aligned} \dim_H(X) &\leq \underline{\dim}_B(X) \\ \dim_P(X) &\leq \overline{\dim}_B(X) \end{aligned}$$

A simple point-to-set phenomenon

Recall that $dim(x)$ is the constructive dimension of a point x.
Here $x \in M$ for a computable metric space M with a designated dense sequence of points, encoded by binary strings.
Greenberg/ Miller 2011 study dim in path spaces h^ω, h computable.

Proposition (Mayordomo and N. (known?))

Let T be a computable tree. Let S be a computable subtree of T (all without leaves).

- For each $f \in [S]$,

$$dim(f) \leq \underline{\dim}_B(S)$$

- Suppose that S is uniformly branching.
  Then equality holds in the case that f is Martin-Löf random in $[S]$ with respect to the uniform measure μ_S.

Results for fractal dimensions

Theorem (Mayordomo and N.)

Suppose a subtree S of T is uniformly branching. Then

$$\begin{aligned} \text{Hausdorff dimension of } [S] &= \text{lower box dim. of } [S] \\ \text{Packing dimension of } [S] &= \text{upper box dim. of } [S] \end{aligned}$$

- This uses two versions of the point-to-set principle in general metric spaces (J. Lutz, N. Lutz and Mayordomo, 2023).
- For Hausdorff dimension we also have a 1-page direct proof.

Apply this to profinite groups: reprove a result that describes the Hausdorff dimension of closed subgroups of G.

Theorem (Barnea-Shalev, 1997)

Let $G = \varprojlim_n G_n$. Suppose that $H \leq_c G$. Let H_n be the projection of H into G_n. Then

$$\dim_H(H) = \underline{\dim}_B(H) = \liminf_{n\to\infty} \frac{\log|H_n|}{\log|G_n|}$$

They used Prop 2.6 in the topological algebra paper "Subgroups and subrings of profinite rings" by Abercrombie (1994). Our argument shows that this has nothing to do with groups- it only uses the tree structures. By our methods, we also obtain

$$\dim_P(H) = \overline{\dim}_B(H) = \limsup_{n\to\infty} \frac{\log|H_n|}{\log|G_n|}.$$

Dimension spectrum

- Main point of the Barnea-Shalev and sequel papers is the spectrum, namely, the set of possible dimensions of closed subgroups.
- For instance, the spectrum of $\mathbb{Z}_p^2$ is $\{0, 1/2, 1\}$.
- For especially nice pro-p-groups known as p-adic analytic, the Hausdorff dimension of a closed subgroup is k/n, where k is its dimension as a manifold over $\mathbb{Z}_p$, and the whole group as a manifold has dimension n.
- Open question from that area: among the pro-p groups, are the p-adic analytics the only ones with finite spectrum?