Profinite groups and computability theory

André Nies

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

Tian Yuan Mathematics Research Center
Computability theory and Descriptive set theory
June 2025

The plan

I. Profinite groups: definition and examples

II. Algorithmic presentations of profinite groups

III. Fractal dimensions of closed subgroups
(with Elvira Mayordomo, U Zaragoza)

IV. Algorithmic randomness in computable profinite groups
(with Willem Fouche, Pretoria and Matteo Vannacci, U Firenze)

I. Profinite groups

their definitions and examples

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 the universal property from category theory.

A separable topological group is called profinite if

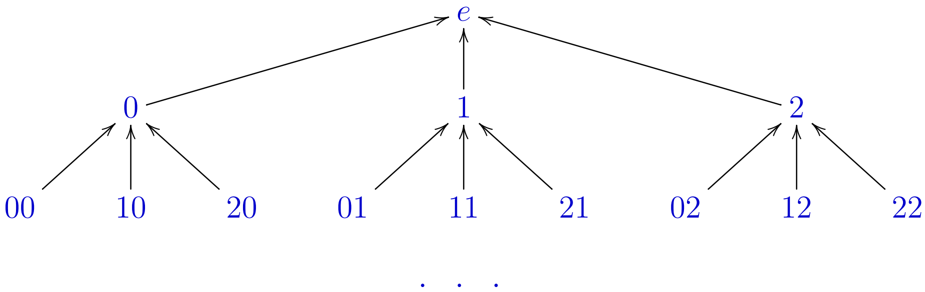
it is isomorphic to such an inverse limit.

Equivalently, the group is compact and 0-dimensional.

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

The inverse limit as a 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 the additive group of 3-adic integers.
$G_1 = C_3$, $G_2 = C_9$, etc.

The inverse limit as a group on a path space (2)

Recall: an inverse system of groups $(G_n, p_n)_{n\in\mathbb{N}}$, 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 maps $p_n\colon G_{n+1} \to G_n$.

- 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

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

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

Profinite groups given by p-adic integers

- Let p be a prime. Let $(\mathbb{Z}_p, +) = \varprojlim_n C_{p^n}$ where 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 $\{0, \dots, p-1\}$, with addition via the usual carry digits.

- This is a pro-p group: all the G_n have size a power of p.

- Let $k \geq 2$. Matrix groups such as
  - upper unitriangular $\mathrm{UT}_k(\mathbb{Z}_p)$
  - special linear $\mathrm{SL}_k(\mathbb{Z}_p)$

  are profinite. This uses that $(\mathbb{Z}_p, +, \times)$ is a profinite ring.

Profinite groups given by infinite Galois extensions

For a Galois extension K/k, 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:
- 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

$$G \cong \varprojlim_{i} \left(\mathrm{Gal}(L_i/k), p_i\right)$$

where $p_i(\sigma)$ is the restriction of σ to L_i.

Profinite groups from $\aleph_0$-categorical structures

Theorem (N. and Paolini, 2024, arxiv.org/pdf/2410.02248)

Let M be an $\aleph_0$-categorical structure with domain $\mathbb{N}$, and let $G = \mathrm{Aut}(M)$. Then N_G/G is profinite.

Here $N_G = \{\sigma \in \mathrm{Sym}(\mathbb{N})\colon G^\sigma = G\}$ is the normaliser of G; it coincides with $\mathrm{Aut}(\mathcal{E}_M)$ where $\mathcal{E}_M$ is the orbital structure of M. Any separable profinite group occurs (Evans and Hewitt, 1991).

Theorem (N. and Paolini, 2024)

(1) Let G as above. Then $\mathrm{Aut}(G)$ carries a natural Polish topology and $\mathrm{Inn}(G)$ is closed in it.
(2) $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ with the quotient topology is totally disconnected, locally compact (t.d.l.c.).

It is unknown whether $\mathrm{Out}(G)$ is in fact always profinite.

II. Algorithmic presentations of profinite groups

Co-c.e., and computable profinite groups

Recall: a profinite group is given by an inverse system $(G_n, p_n)_{n\in\mathbb{N}}$, where 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 that is topologically f.g. 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 the 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.

- G is co-c.e. if
  - the tree T is computable with a computable number of successors, and
  - the group operations at each level are uniformly computable.
- G is computable if, in addition, the tree has no leaves.

Preservation properties

Smith (1981) proved preservation properties for computable profinite groups. If G is computable then

- the derived group G' is computable
- for each prime p, the group G has a computable p-Sylow subgroup (that is, a maximal pro-p closed subgroup).

Arbitrary effective tree $\rightsquigarrow$ nice effective tree

- If a topological structure for a finite functional signature σ is compact and 0-dimensional, then it has a copy with domain $[T]$ for some finitely branching tree T.
- Co-c.e. σ-structures: T is computable, with computable bound on branching, and operations computable.
- Computable σ-structures: in addition, T has no leaves.

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

If a profinite group has a co-c.e. copy as a topological structure, then it has a co-c.e. presentation as defined above.
Same for computable. The transformations are uniform.

Computably f.g. subgroups of profinite groups

- A group L is called residually finite if each $w \in L - \{e\}$ remains $\neq e$ in some finite quotient of L.
- A f.g. group L is residually finite $\iff$ it is isomorphic to a subgroup of a profinite group.

  For "$\Rightarrow$", use the profinite completion.

Theorem

A f.g. group L is isomorphic to a subgroup of some computable profinite group that is generated by finitely many computable paths $\iff$ the following two conditions hold:

- L has a Π^0_1 word problem
- L is effectively residually finite.

III. Fractal dimensions of closed subgroups

Joint with Elvira Mayordomo (arXiv:2502.09995, 2025)

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 range of the natural projection of H into G_n.
- Let $q_n = p_n \restriction_{H_{n+1}}$. Then $H = \varprojlim_n (H_n, q_n)$, with onto maps.

Recall $G = [T]$ for the tree T associated with the inverse system. Then $H = [S]$ for its subtree S associated with (H_n, q_n).

H is a nullset for the uniform measure on $[T]$ (Haar measure), unless H has finite index (and hence is open in case that G is topologically f.g., by Nikolov and Segal 2008).

So, how can one measure the size of H? Using fractal dimensions!

Metrics on a profinite group

- Fractal dimensions are defined for bounded subsets of metric spaces. So we need a metric on G.

- The tree T for G provides us with an ultrametric:
  For distinct $g, h \in [T]$, let
  $$d(g,h) = \max\{|T_n|^{-1} \colon \; g(n) \neq h(n)\},$$
  where T_n is the n-th level of T (starting from 0).

- Problem: the tree is based on the inverse system for G, which in the general case is somewhat arbitrary.

- However, for some classes, there is a natural inverse system.

Natural metric on topologically f.g. pro-p group

A profinite group is called pro-p group if the size of every continuous finite quotient is a power of p.
If G is pro-p and (topologically) finitely generated, there is a natural inverse system:

- Let R_n be the subgroup of G generated by the p^n-th powers. Clearly $\bigcap_n R_n = \{e\}$.
- R_n is normal and open; let $G_n = G/R_n$.
- Then $(G_n, p_n)_{n\in\mathbb{N}}$, with the canonical maps $p_n\colon G_{n+1} \to G_n$, forms an inverse system for G.
- Inverse system is invariant under $\mathrm{Aut}(G)$.

Lower and upper box (or 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

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

$$\underline{\dim}_{\mathrm{Box}}(\text{Coastline}) = 1.25$$

Source: wikipedia

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

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. (Trees will have no leaves.)

$\{[\sigma] \colon \sigma \in S_n\}$ is the "optimal covering" of $[S]$ for diameter $|T_n|^{-1}$.
Only α's of form $|T_n|^{-1}$ matter, so

$$\underline{\dim}_{\text{Box}}([S]) = \liminf_{\alpha \to 0^+} \frac{\log N_\alpha(X)}{\log(1/\alpha)} = \liminf_{n \to \infty} \frac{\log |S_n|}{\log |T_n|}$$

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 $\underline{\dim}_{\text{Box}}[S] = \overline{\dim}_{\text{Box}}[S] = \log_3(2) \approx 0.631$

Box dimensions of closed subgroups of G

Recall that $G = [T]$. The subtree S describing $H \leq_c G$ satisfies $S_n = H_n$, where H_n is the projection of H into G_n. So

$$\underline{\dim}_{\mathrm{Box}}(H) = \liminf_{n\to\infty} \frac{\log |H_n|}{\log |G_n|}$$

Example (Barnea-Shalev 1997, essentially)

Let G be the Cantor space $\mathcal{P}(\mathbb{N})$ with symmetric difference Δ as the group multiplication. Let $G_n = \mathcal{P}(n)$.

For each $0 \leq \alpha \leq \beta \leq 1$ there is a closed subgroup H with

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

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 $|S_n| = 2^{|R\cap n|}$, $|T_n| = 2^n$.

Hausdorff and packing dimension

- $\dim_{\text{Hausdorff}}(X)$ is the sup of the r such that the r-dimensional Hausdorff measure $\mathcal{H}^r(X)$ is positive.

- Packing dimension $\dim_{\text{Packing}}(X)$ is defined in a similar way but "from the inside", via disjoint sets of balls with centre in X.

- We always have

$$\dim_{\text{Packing}}(X) \leq \overline{\dim}_{\text{Box}}(X)$$

$$\dim_{\text{Hausdorff}}(X) \leq \underline{\dim}_{\text{Box}}(X)$$

and also upward inequalities.

Coincidences of fractal dimensions for $[S]$

Theorem (Mayordomo and N., 2024)

Suppose a subtree S of T is levelwise uniformly branching. Then

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

- The proof uses two versions of the point-to-set principle in general metric spaces (J. Lutz, N. Lutz and Mayordomo, 2023). We will discuss this proof on the next two slides.

- For both equalities, we also have direct proofs of the inequalities $\geq$; the inequalities $\leq$ always hold.

- E.g., Tricot: $\dim_P[S] \geq \inf\{\overline{\dim}_B(V) : V \neq \emptyset \text{ open in } [S]\}$.

Proof of Theorem: constructive dimensions

Consider a computable metric space M with a dense sequence of designated points, encoded by binary strings.

The lower constructive dimension of a **point** $x \in M$ is defined by

$$cdim(x) := \liminf_{\alpha \to 0^+} C_\alpha(x) / \log(1/\alpha),$$

where $C_\alpha(x)$ is the least complexity of a designated point within radius α. The upper dimension $cDim(x)$ is defined using the sup.

Proposition (Mayordomo and N)

Let T be a computable tree. Let S be a computable subtree of T.

- $cdim(f) \le \underline{\dim}_{\text{Box}}(S)$ and $cDim(f) \le \overline{\dim}_{\text{Box}}(S)$ for each $f \in [S]$.
- If S is uniformly branching, then equalities hold when f is Martin-Löf random in $[S]$ w.r.t. the uniform measure on $[S]$.

Proof of Theorem: Point-to-set principles

Two point-to-set principles of Lutz, Lutz and Mayordomo (2023) determine the Hausdorff and packing dimension of a set $X \subseteq M$ in terms of the relativised algorithmic dimensions of the points in it:

$$\begin{aligned}
\dim_{\text{Hausdorff}}(X) &= \min_{A} \sup_{x \in X} \mathit{dim}^{A}(x), \\
\dim_{\text{Packing}}(X) &= \min_{A} \sup_{x \in X} \mathit{Dim}^{A}(x)
\end{aligned}$$

Using the previous proposition in relativised form, this shows

$$\dim_{\text{Hausdorff}}([S]) = \underline{\dim}_{\text{Box}}([S]) \text{ and } \dim_{\text{Packing}}([S]) = \overline{\dim}_{\text{Box}}([S]),$$

whenever S is a levelwise uniformly branching subtree of T.

Apply this to profinite groups G: purely geometric proof of 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

$$\dim_{\text{Hausdorff}}(H) = \underline{\dim}_{\text{Box}}(H) = \liminf_{n\to\infty} \frac{\log|H_n|}{\log|G_n|}$$

- They used Prop 2.6 in the topological algebra paper "Subgroups and subrings of profinite rings" by Abercrombie (1994).
- Our argument shows that this only needs to use the tree structures.

By our methods, we also obtain

$$\dim_{\text{Packing}}(H) = \overline{\dim}_{\text{Box}}(H) = \limsup_{n\to\infty} \frac{\log|H_n|}{\log|G_n|}.$$

Dimension spectrum of a f.g. pro-p group

- Important topic of the Barnea-Shalev 1997 paper and its sequels (such as B. Klopsch and co-authors) is the spectrum, namely, the set of possible dimensions of closed subgroups.
- For instance, the spectrum of $\mathbb{Z}_p^2$ is $\{0, \frac{1}{2}, 1\}$.
- 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.
- There is a f.g. pro-p group with "normal" spectrum $[0, 1]$ (de las Heras and Klopsch, 2022).
- Open question: among the f.g. pro-p groups, are the p-adic analytic ones the only ones with finite spectrum?

IV. 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 $G = \varprojlim_n (G_n, p_n)$ 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 space of paths $[T]$.

- Kurtz random: in *no* effectively closed null set.
- Schnorr random: in *no* null set of the form $\bigcap_m G_m$, where $(G_m)_{m\in\mathbb{N}}$ is a sequence of uniformly Σ^0_1 sets, and μG_m is a uniformly computable real.

“Almost everywhere” results for k-tuples

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

- For $\overline{g} \in G^k$, by $\langle \overline{g} \rangle$ one denotes the closure of the subgroup of G generated by $\overline{g}$.
- Let $G = \widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n!\mathbb{Z}$ be the free profinite group of rank 1.

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

(1) $\langle g \rangle$ has infinite index in $\widehat{\mathbb{Z}}$ for a.e. $g \in \widehat{\mathbb{Z}}$.

(2) $\langle \overline{g} \rangle$ has finite index in $\widehat{\mathbb{Z}}$ for for a.e. $\overline{g} \in (\widehat{\mathbb{Z}})^k$, where $k \geq 2$.

Algorithmic version

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 $|\widehat{\mathbb{Z}} : \langle \overline{g} \rangle| < \infty$; Kurtz randomness is not sufficient.

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

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

- Each k-group is topologically finitely generated.
- By the results above, $\widehat{\mathbb{Z}}$ is a 2-group, and not a 1-group.
- Nikolov and Segal (2008): each subgroup of finite index in a topologically f.g. profinite group is open.
- So in the definition above one could require as well that $\langle \overline{g} \rangle$ be open.

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

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

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. $\square$

Work in progress with Vannacci would show that if G is pro-p, then Schnorr randomness suffices.

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

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

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

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

Let $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. 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 $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$

$G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ 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, these Fried-Jarden results prove more than what they say.
- For instance, weakly 1-generic also suffices.

Summary

Algorithmic presentations of profinite groups

Reviwed co-c.e. and computable profinite groups. Characterized f.g. subgroups of computable profinite groups by Π^0_1 word problem and e.r.f.

Fractal dimensions of closed subgroups

Showed coincidence of Hausdorff and lower box dimension of $[S]$ when S is a uniformly branching subtree of T. Applied it for a geometric proof of Barnea-Shalev formula for Hausdorff dimension of closed subgroups. (arXiv: 2502.09995)

Algorithmic randomness in computable profinite groups

Algorithmic versions of a.e. theorems. Often the weak notion of Kurtz randomness suffices.