Profinite Groups and Algorithmic Randomness

Willem Fouché, André Nies, and Matteo Vannacci

CCC 2026
Kyoto

Some of Willem's interests that influenced me

- Algorithmic randomness, in particular related to Brownian motion (Advances paper, 2000)
- Structural Ramsey theory, non-Archimedean groups (Symmetry and the Ramsey degree of posets. Discrete Math, 1997; Algorithmic Randomness and Ramsey Properties of Countable Homogeneous Structures, Wollic 2012, arxiv.org/pdf/1308.5506.
- Foundations of quantum information theory (such as Gleason's theorem)

The plan for this talk

A. Profinite groups: definition, examples, algorithmic presentations

B. Algorithmic randomness in computable profinite groups

Profinite groups:

definition 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.

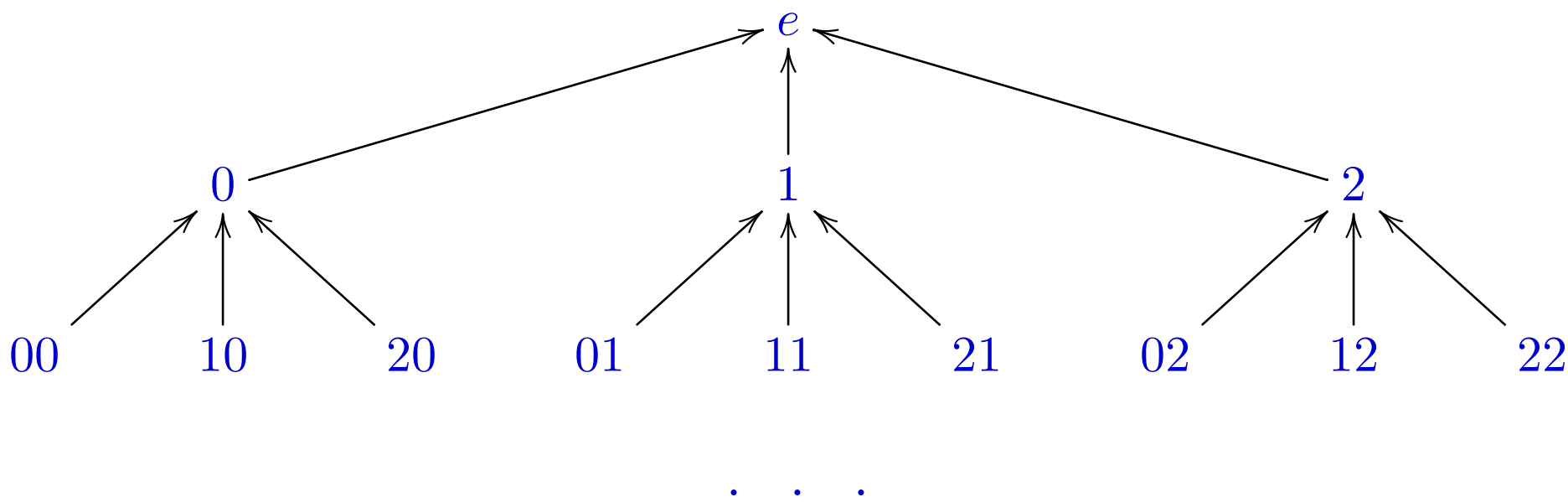
Its inverse limit is the topological group $G = \varprojlim_n (G_n, p_n)$, given up to isomorphism by the corresponding universal property from category theory.

A separable topological group is called profinite if it is isomorphic to such an inverse limit. Equivalently, the group is compact and 0-dimensional.

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

The inverse limit as a group on a path space

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 $p_n : G_{n+1} \to G_n$.



The first levels of the tree for the additive group of 3-adic integers.

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

Profinite groups given by infinite Galois extensions

For a Galois field extension L/k, its Galois group $G = \mathrm{Gal}(L/k)$ consist of the automorphisms of L that fix k pointwise.

$G = \mathrm{Gal}(L/k)$ is a profinite group:

- Let $L = \bigcup_{i \in \mathbb{N}} L_i$, where $L_{i+1} \geq L_i$ and each L_i is a normal finite field extension of k.
- Then

$$G \cong \varprojlim_i (\mathrm{Gal}(L_i/k), p_i)$$

$p_i(\sigma)$ is the restriction of σ to L_i, where $\sigma \in \mathrm{Gal}(L_{i+1}/k)$.

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).

Algorithmic presentations

of profinite groups

Co-r.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 $p_n : G_{n+1} \to G_n$ are homomorphisms of finite groups.

Definition (Smith, 1981; LaRoche, 1981)

A co-r.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-r.e. profinite group G is not isomorphic to a computable one.

(ii) Each co-r.e. pro-p group that is topologically f.g. is computable.

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) obtained 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.

Algorithmic randomness in computable profinite groups

Haar measure on profinite groups

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.

For $k \geq 2$, by μ^k denote the product Haar measure on G^k.

Algorithmic randomness notions for G

If G is computable and infinite, the usual algorithmic test notions for Cantor space can be extended to the space of paths $[T]$. The random notions below get stronger:

- 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 descending sequence of uniformly Σ^0_1 sets, and
  - μG_m is a computable real uniformly in m.
- Martin-Löf random: μG_m is a left-r.e. real uniformly in m.
- weakly 2-random: no restriction on the convergence μG_m to 0.

Algorithmic view of "almost everywhere" results

- Given a computable profinite group G, and property of tuples $(g_1, \ldots, g_k) \in G^k$ that holds with probability 1,
- how strong a randomness property on $(g_1, \ldots, g_k)$ is required for the property to hold?

Previous algorithmic analyses of "almost everywhere" results:

- A.e. differentiability of nondecreasing functions on $\mathbb{R}$ (Brattka, Miller, N., 2016)
- A.e. recurrence in symbolic dynamics (Downey, Nandakumar, N., 2019)

Closed subgroup generated by a k-tuple

An "almost everywhere" result for a profinite group G asserts that μ^k-almost every k-tuple $(g_1, \ldots, g_k)$ satisfies a given property.

Such a property is often given by the closed subgroup the elements generate.

Some notation.

- For $(g_1, \ldots, g_k) \in G^k$, by $\langle g_1, \ldots, g_k \rangle$ we denote the closure of the subgroup of G generated by $\{g_1, \ldots, g_k\}$.
- The index $|G : U|$ of a subgroup U of G is the number of its cosets.
- Let $\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n!\mathbb{Z}$ be the free profinite group of rank 1.

Algorithmic versions of a.e. results for $\widehat{\mathbb{Z}}$

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) $|\widehat{\mathbb{Z}} : \langle g_1, \ldots, g_k \rangle| < \infty$ for a.e. $(g_1, \ldots, g_k) \in (\widehat{\mathbb{Z}})^k$, when $k \geq 2$.

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 $(g_1, \ldots, g_k) \in \widehat{\mathbb{Z}}^k$ is Schnorr random, then $|\widehat{\mathbb{Z}} : \langle g_1, \ldots, g_k \rangle| < \infty$; Kurtz randomness is not sufficient.

(2) follows by exhibiting a Schnorr–Solovay test.

Let $R_n = (n\widehat{\mathbb{Z}})^k$. Then $\mu(R_n) = n^{-k}$. Since $\sum_n n^{-k} < \infty$ is computable for $k \geq 2$, Schnorr randomness ensures that $(g_1, \ldots, g_k) \notin R_n$ for all sufficiently large n, forcing $\overline{\langle g_1, \ldots, g_k \rangle}$ to have finite index in $\widehat{\mathbb{Z}}$.

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

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

- Each k-group is topologically finitely generated.
- $\widehat{\mathbb{Z}}$ is a 2-group, and not a 1-group.

Theorem

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

If G is the pro-p completion of a finitely presented group, then Kurtz randomness of $\overline{g}$ suffices.

Groups with polynomial sized covers

- Let $\mathcal{F}$ be a collection of open subgroups of a profinite group G.
- $\mathcal{F}$ is a cover if every closed subgroup of infinite index in G is contained in infinitely many subgroups from $\mathcal{F}$.

Theorem

- Suppose $\mathcal{F}$ is uniformly Σ^0_1.
- Suppose for some $c \in \mathbb{N}$, the number of index n subgroups $H \in \mathcal{F}$ is at most n^c for all n.

Then for any Martin-Löf random tuple $\overline{g} \in G^{\lfloor c+2 \rfloor}$, the closed subgroup $\langle \overline{g} \rangle$ is open in G.

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

Fried and Jarden, Field arithmetic (3d edition, 2005, 800 pp): understand a field L (in particular, Hilbertian field such as $\mathbb{Q}$) through its absolute Galois group $\mathrm{Gal}(\bar{L}/L)$ (a profinite group).

We give algorithmic versions of "a.e." theorems from FJ.

- Let $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) = \mathrm{Aut}(\overline{\mathbb{Q}}, +, \times)$.
- Since the polynomial ring $\mathbb{Q}[X]$ has a splitting algorithm, G is computable (Russell Miller).

Theorem (algorithmic form of Thm. 18.5.6 in Fried-Jarden 2005)

If $\overline{g} \in G^k$ be Kurtz random, $\langle \overline{g} \rangle$ 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 polynomial $p \in L[X, Y]$ that is irreducible in $\overline{L}$ has a zero in L.

Theorem (algorithmic form of Thm. 27.4.8 in Fried-Jarden 2005)

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

- Since Kurtz randomness suffices, the proofs of the Fried-Jarden results give more than what the theorems say.
- For instance, weakly 1-generic also suffices for the conclusion in both results.