The complexity of isomorphism between profinite groups

André Nies

Cabal Seminar, UCLA, March 9, 2016

Examples of profinite groups

Idea: a profinite group is fully determined by its finite quotients and how they interact.

- $(\mathbb{Z}_p, +)$, the additive group of p-adic integers for a prime p, is profinite. Say $p = 3$:

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

- $\mathbb{Z}_p$ is in fact a profinite ring: multiplication works as expected. This implies that matrix groups such as $\mathrm{UT}_n(\mathbb{Z}_p)$ and $\mathrm{SL}_n(\mathbb{Z}_p)$, $n \geq 2$ are profinite.
- The Galois group of a Galois extension of fields K/k (algebraic, normal, separable) is profinite.

Definition

A compact topological group G is called profinite if one of the following equivalent conditions holds.

(a) The clopen sets form a basis for the topology (i.e., G is totally disconnected).

(b) The open normal subgroups N form a base of neighbourhoods of the identity.

(c) G is the inverse limit of a surjective system of finite groups carrying the discrete topology.

E.g. (b)$\to$(c): open subgroups of a compact group have finite index, and $G = \varprojlim_{N \text{ open, normal}} G/N$. This is a closed subgroup of the cartesian product $\prod_N G/N$, consisting of those f such that $f(Ng) = Mg$ whenever $N \leq M$.

Examples in more detail

The p-adic integers $(\mathbb{Z}_p, +)$

- The topology is the same as the one of Cantor space (compact, perfect, totally disconnected).
- The subgroups are the $U_n = \{x \in \mathbb{Z}_p \colon x(0) = x(1) = \ldots = x(n-1) = 0\}$.
- We have $\mathbb{Z}_p / U_n = C_{p^n}$ (cyclic)
- $\mathbb{Z}_p = \varprojlim_n C_{p^n}$ with the natural maps $C_{p^{n+1}} \to C_{p^n}$.

Galois group of K/k

Suppose we have $K = \bigcup_{i \in \mathbb{N}} L_i$, $L_i \leq L_{i+1}$ and the $|L_i/k|$ are normal finite extensions. A basis of neighbourhoods of the identity in $\mathrm{Gal}(K/k)$ is given by the open normal subgroups $\mathrm{Gal}(K/L_i)$.

Leading question

Given profinite groups G, H, how hard is it to decide whether G and H are (topologically) isomorphic?

From now on all profinite groups will have a countable base.
Where should we look to calibrate the complexity of isomorphism?

- Descriptive set theory, which provides a way of comparing the complexity of equivalence relations on Polish spaces: Borel reducibility $\leq_B$.

  First we would need to represent profinite groups as points in Polish spaces (i.e. separable, complete metrizable).

- Computability theory might work for the profinite groups that are "computable" in the right sense. Lots of examples are computable. Considerable amount of research in the 1980s (Rick Smith, LaRoche, Feferman, Metakides and Nerode).

Representing a profinite group

as a point in a compact Polish space

The easy (but not very illuminating) way

Pick a universal (countably based) profinite group $\mathbb{P}$. For instance, the cartesian product of the finite alternating groups $\mathbb{P} = \prod_{n \geq 2} A_n$ works[1].

- Every profinite group is isomorphic to a closed subgroup of $\mathbb{P}$.
- $\mathcal{K}(\mathbb{P})$ is the Polish space of compact (i.e. closed) subsets of $\mathbb{P}$.
- It is metrised by the Hausdorff distance based on the canonical bi-invariant ultrametric on $\mathbb{P}$.
- Easy to check that to be a subgroup is a closed property in $\mathcal{K}(\mathbb{P})$.
- So the closed subgroups of $\mathbb{P}$ form a Polish space.

[1] See John Wilson's 1997 book, 4.1.4

Profinite free groups

Let $k \in \omega$. Recall F_k is the free group on generators $x_0, \ldots, x_{k-1}$. Let $\widehat{F}_k$ denote the profinite completion of F_k. That is,

$$\widehat{F}_k = \varprojlim_L F_k/L,$$

where L ranges over the closed normal subgroups of finite index in F_k. For instance, $\widehat{F}_1 = \prod_{p\,\text{prime}} (\mathbb{Z}_p, +)$.

Now let $k = \omega$. The profinite free group on ω generators is

$$\widehat{F}_\omega = \varprojlim_L F_\omega/L,$$

where L ranges over the closed normal subgroups of finite index in F_ω containing almost all the generators x_i.

Free group modulo a closed normal subgroup

(i) Every topologically finitely generated profinite group has the form $\widehat{F}_k/N$ (quotient topology) where N is a closed normal subgroup of $\widehat{F}_k$.

(ii) Every (countably based) profinite group G has the form $\widehat{F}_\omega/N$ where N is a closed normal subgroup of $\widehat{F}_\omega$.

(i) is easy. For (ii) use coset representatives to find a generating sequence of G converging to 1.

Let $\mathcal{N}(\widehat{F}_k)$ be the Polish space of closed normal subgroups of $\widehat{F}_k$.

- This is a closed subspace of the space of compact subsets $\mathcal{K}(\widehat{F}_k)$.
- The representation via $\mathcal{N}(\widehat{F}_\omega)$ is Borel equivalent to the representation via closed subgroups of $\mathbb{U} = \prod_n A_n$.

Borel reducibility $\leq_B$

- Let X, Y be Polish spaces. A function $g\colon X \to Y$ is Borel if the preimage of each open set in Y is Borel.
- Let E, F equivalence relations on X, Y respectively. We write $E \leq_B F$ if there is a Borel function $g\colon X \to Y$ such that

$$uEv \leftrightarrow g(u)Fg(v)$$

for each $u, v \in X$.

An equivalence relation is called smooth if it is Borel-below $\mathtt{id}_Y$, the identity relation on some Polish space Y (say, $\mathbb{R}$).

- Equivalence of Bernoulli shifts is smooth (Ornstein).
- E_0 (eventual equality of infinite bit sequences) is NOT smooth.
- E_0 is Borel equivalent to isomorphism of subgroups of $(\mathbb{Q}, +)$.

Isomorphism of f.g. profinite groups is smooth

Complexity classification of isomorphism between finitely generated profinite groups

- $\bigsqcup_{k<\omega} \mathcal{N}(\widehat{F}_k)$ is the space of finitely generated profinite groups.
- This is a Polish space: declare a set S open if $S \cap \mathcal{N}(\widehat{F}_k)$ is open for each $k < \omega$.

Theorem

The isomorphism relation $E_{f.g.}$ between finitely generated profinite groups is Borel equivalent to $\mathtt{id}_{\mathbb{R}}$.

$E_{f.g.}$ is smooth

We first show that $E_{f.g.} \leq_B \mathtt{id}_{\mathbb{R}}$. We may fix $k < \omega$.

- The automorphism group $Q = \mathtt{Aut}(\widehat{F}_k)$ is profinite. (For a characteristic open subgroup N of $\widehat{F}_k$, consider the automorphisms that induce the identity on $\widehat{F}_k/N$. In a f.g. profinite group, e has a base of nbhds of such N's)
- For $S, T \in \mathcal{N}(\widehat{F}_k)$, by a lemma of Gaschütz on generation in finite groups, we have[2]

$$\widehat{F}_k/S \cong \widehat{F}_k/T \leftrightarrow \text{some } \theta \in Q \text{ maps } S \text{ to } T$$

- The natural action of Q on $\mathcal{N}(\widehat{F}_k)$ is continuous.
- Then, since Q is compact, the orbit equivalence relation E of this action on $\mathcal{N}(\widehat{F}_k)$ is closed, and hence smooth. (Take as an invariant for S the leftmost path in the preimage of $[S]_E$ in Cantor space $\{0,1\}^{\mathbb{N}}$.)

[2] Lubotzky, 2001, Prop. 2.2, and thanks to him for pointing this out to me.

Identity on Cantor space is Borel below $E_{f.p.}$

- A profinite group H is called finitely presented if $H = \widehat{F}_k/R$, $k < \omega$, and R is finitely generated as a closed normal subgroup of $\widehat{F}_k$.
- There are continuum many non-isomorphic profinite groups that are f.p. as profinite groups[3].
- Claim follows by Silver's dichotomy theorem on Borel equivalence relations. We can also directly use the construction in the proof of Lubotzky. For any set P of primes, let

$$G_P = \prod_{p \in P} \mathrm{SL}_2(\mathbb{Z}_p) = \mathrm{SL}_2(\widehat{\mathbb{Z}}) / \prod_{q \notin P} \mathrm{SL}_2(\mathbb{Z}_q).$$

- G_P is finitely presented, and $P = Q \leftrightarrow G_P \cong G_Q$.
- $P \to G_P$ is a Borel map.

[3] Lubotzky (2005), Prop 6.1

Isomorphism of profinite groups is

classifiable by countable structures

Classifiability by countable structures

An equivalence relation E on a Polish space X is classifiable by countable structures if there is a countable signature $\mathcal{L}$ and a Borel function $g\colon\ X \to \mathtt{Mod}(\mathcal{L})$ such that

$$xEy \leftrightarrow g(x) \cong g(y).$$

($\mathtt{Mod}(\mathcal{L})$ is the Polish space of $\mathcal{L}$-structures with domain ω.)
By general facts in descriptive set theory, this is equivalent to:

there is a closed subgroup V of S_∞ with a continuous action on a Polish space $V \curvearrowright Y$ such that E is Borel below the orbit equivalence relation of the action.

Forward implication: let $Y = \mathtt{Mod}(\mathcal{L})$ and $V = S_\infty$ with its action by permuting the elements of the model.

- To obtain V and its action on a Polish space Y, we use that every infinite profinite group is homeomorphic to Cantor space $\{0,1\}^{\mathbb{N}}$, and the homeomorphism can be obtained "in a Borel way".
- So we can view the group operations as continuous functions on Cantor space.
- Y is the space of continuous binary functions on Cantor space that encode a "group difference operation" $\rho(a,b) = ab^{-1}$ where 0^ω is the identity.
- V is the group of homeomorphisms of Cantor space that fix 0^ω.
- V acts continuously on Y, and the orbit equivalence relation corresponds to isomorphism of the profinite groups.
- The group V can be seen naturally as a closed subgroup of $\mathtt{Aut}(D)$ via the usual Stone duality, where D is the countable dense Boolean algebra
- hence V can be viewed as a closed subgroup of S_∞.

Isomorphism of abelian profinite groups is

not smooth and not S_∞-complete

Pontryagin duality

The following was pointed out to me by A. Melnikov.

Pontryagin duality associates to each abelian locally compact group G the group G^* of continuous homomorphisms from G into the circle $\mathbb{T}$, with the compact-open topology.

For a morphism $\alpha\colon G \to H$, let $\alpha^*\colon H^* \to G^*$ be the morphism defined by $\alpha^*(\psi) = \alpha \circ \psi$.

The Pontryagin duality theorem says that $G \cong (G^*)^*$ via the application map $g \mapsto \lambda\phi.\, \phi(g)$, for each locally compact abelian group G.

Pontryagin duality: countable abelian torsion versus abelian profinite

A special case of this states that (discrete) countable abelian torsion groups A correspond to abelian profinite groups. We have $A \cong B$ iff $A^* \cong B^*$. The functor * and its inverse are Borel.

So isomorphism between abelian countable torsion groups is Borel equivalent to continuous isomorphism between abelian profinite groups.

This special case is not hard to prove: finite abelian groups are their own dual. Countable torsion abelian groups are direct limits of finite abelian groups. Isomorphism between abelian countable torsion groups is a familiar benchmark equivalence relation: neither smooth, nor S_∞ complete (Friedman and Stanley, 1989).

Isomorphism between profinite groups is

Borel complete for S_∞ orbit equivalence relations

Nil-2 groups of exponent p

- A group G is nilpotent of class 2 (nil-2 for short) if it satisfies the law $[[x, y], z] = 1$.
- Equivalently, the commutator subgroup is contained in the center.

For a prime p, the group of unitriangular matrices

$$\mathrm{UT}_3^3(\mathbb{Z}/p\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}$$

is in the variety $\mathcal{N}_2^p$ of nilpotent class 2 groups of exponent p.

S_∞-hardness

- We have proved earlier on that isomorphism between profinite groups is classifiable by countable structures.
- The following shows that isomorphism between profinite groups is complete within that class.

Theorem

Let $p \geq 3$ be prime. Any orbit equivalence relation of a continuous S_∞ action can be Borel reduced to isomorphism between profinite $\mathcal{N}_2^p$ groups.

The main result in Mekler (1981) implies a version of the theorem for countable abstract groups. We adapt his construction.

Turning a graph into a group

Mekler associates to each symmetric and irreflexive graph A a nil-2 exponent-p group $G(A)$ in such a way that isomorphic graphs yield isomorphic groups. In the countable case, the map G sends a countable graph A to a countable group $G(A)$ in a Borel way.

A symmetric and irreflexive graph is called nice if it has no triangles, no squares, and for each pair of distinct vertices x, y, there is a vertex z joined to x and not to y.

Mekler proves that a nice graph A can be interpreted in $G(A)$ using an interpretation Γ consisting of first-order formulas without parameters: $\Gamma(G(A)) \cong A$. In particular, for nice graphs A, B we have $A \cong B$ iff $G(A) \cong G(B)$.
Since isomorphism of nice graphs is S_∞-complete, so is isomorphism of countable $\mathcal{N}_2^p$ groups.

Mekler's construction

- Let F be the free $\mathcal{N}_2^p$ group on free generators $x_0, x_1, \ldots$.
- For $r \neq s$ we write $x_{r,s} = [x_r, x_s]$. The centre $Z(F)$ of F is an abelian group of exponent p that is freely generated by the x_{rs} for $r < s$.
- Given a graph A, let

$$G(A) = F/\langle x_{rs} \colon rAs \rangle_{\text{normal closure}}.$$

- The centre $Z = Z(G(A))$ is an abelian group of exponent p with a basis consisting of the $x_{r,s}$ such that $\neg rAs$.
- So every element in $G(A)$ has a unique normal form

$$\prod_{\langle r,s\rangle \in L} x_{r,s}^{\beta_{rs}} \prod_{i \in D} x_i^{\alpha_i},\ 0 < \alpha_\cdot, \beta_\cdot < p,$$

L a finite set of non-edges, D a finite set.

Profinite version of Mekler's construction

- Recall $G(A) = F/\langle x_{rs} \colon rAs \rangle$.
- Let R_n be the normal subgroup of $G(A)$ generated by the x_i, $i \geq n$.
- Let $\widehat{G}(A)$ be the completion of $G(A)$ w.r.t. the R_n, i.e.,

$$\widehat{G}(A) = \varprojlim_n G(A)/R_n.$$

- Each $G(A)/R_n$ is finite, so this is a profinite group. In the normal form $\prod_{\langle r,s \rangle \in L} x_{r,s}^{\beta_{rs}} \prod_{i \in D} x_i^{\alpha_i}$, the products are now allowed to be infinite.

Let A, B be a nice graphs. Then $A \cong B$ iff $\widehat{G}(A) \cong \widehat{G}(B)$.

Let A, B be a nice graphs. Then $A \cong B$ iff $\widehat{G}(A) \cong \widehat{G}(B)$.

Need to show that Mekler's interpretation still works:
$\Gamma(\widehat{G}(A)) \cong A$.
Summarize Mekler: Let H be a group with centre $Z(H)$. For $a \in H$ let $\bar{a}$ denote the coset $aZ(H)$.

- Write $\bar{a} \sim \bar{b}$ if a, b have the same centraliser. Let $[\bar{a}]$ be the $\sim$ equivalence class of $\bar{a}$.
- $[\bar{a}]R[\bar{b}] \leftrightarrow [\bar{a}], [\bar{b}], [\bar{1}]$ are all distinct and $[a, b] = 1$.

Let

$$\Gamma'(H) = \langle (\{[\bar{a}] \colon a \in H \setminus Z(H)\}, R\rangle.$$

$$\Gamma(H) = \{[\bar{a}] \colon \ |[\bar{a}]| = p - 1 \ \wedge \ \exists \bar{w}\, [\bar{a}]R[\bar{w}]\},$$

viewed as a subgraph of $\Gamma'(H)$.

Oligomorphic permutation groups

Profinite (countably based) groups coincide with the compact subgroups of S_∞. This means that each orbit w.r.t. the action on ω is finite.

- At the opposite end of the spectrum: $G \leq_c S_\infty$ is oligomorphic if for each n, there are only finitely many n-orbits.
- This is a Borel property of closed subgroups of S_∞ since it suffices to look at a dense subgroup, which can be obtained in a Borel way.

The isomorphism relation for oligomorphic groups is smooth. The real invariant associated with G is the first-order theory of the canonical omega-categorical Fraisse limit A with $\mathtt{Aut}(A) \cong G$.

Questions

- How complex is isomorphism of closed subgroups of S_∞? (These are also known as nonarchimedean groups.)
- How complex is isomorphism of compact Polish groups?

References:

These slides from my web site;

Complexity of isomorphism between profinite groups, on arXiv shortly.