# Elementarity of Subgroups and Complexity of Theories of Profinite Subgroups of $S_\omega$ via Tree Presentations

Jason Block

Computable Structure Theory and Interactions

# Profinite Groups

A topological group is called profinite if it is isomorphic to the inverse limit of an inverse system of discrete finite groups. Equivalently a topological group is profinite if it is compact, Hausdorff, and totally disconnected.

Examples:

- Finite groups
- Direct products of finite groups
- The $p$-adic integers $\mathbb{Z}_p$ under addition
- Galois groups

# Profinite Groups

A topological group is called profinite if it is isomorphic to the inverse limit of an inverse system of discrete finite groups. Equivalently a topological group is profinite if it is compact, Hausdorff, and totally disconnected.

Examples:

- Finite groups
- Direct products of finite groups
- The $p$-adic integers $\mathbb{Z}_p$ under addition
- Galois groups

In [5], R. Miller investigated the absolute Galois group of $\mathbb{Q}$ (that is, $(\overline{\mathbb{Q}})$) viewed as a subgroup of $S_\omega$ (the group of permutations of $\mathbb{N}$).

# Approach

- Although $S_\omega$ is size continuum, both it and its closed subgroups can be presented as the set of paths through a countable tree.
- The subgroups of $S_\omega$ that can be presented this way with finite branching trees are exactly the profinite ones.
- We use these presentations to find the complexities of the theories of profinite subgroups $G$ of $S_\omega$, as well as to find to what degree certain nicely defined countable subgroups of $G$ are elementary subgroups.

# Tree Presentations

## Definition

Let $G$ be a subgroup of $S_\omega$. We define the tree $T_G$ to be the subtree of $\mathbb{N}^{<\omega}$ containing all initial segments of elements of $G$. That is,

$$T_G := \{\tau \in \mathbb{N}^{<\omega} : (\exists g \in G, n \in \mathbb{N})[\tau = g(0)g(1)\cdots g(n)]\}$$

where $m \in \mathbb{N}$ is mapped to $g(m)$ under $g$. We define the ordering of $T_G$ via initial segments and write $\tau \sqsubset \sigma$ if $\tau$ is an initial segment of $\sigma$.

# Tree Presentations

## Definition

Let $G$ be a subgroup of $S_\omega$. We define the tree $T_G$ to be the subtree of $\mathbb{N}^{<\omega}$ containing all initial segments of elements of $G$. That is,

$$T_G := \{\tau \in \mathbb{N}^{<\omega} : (\exists g \in G, n \in \mathbb{N})[\tau = g(0)g(1)\cdots g(n)]\}$$

where $m \in \mathbb{N}$ is mapped to $g(m)$ under $g$. We define the ordering of $T_G$ via initial segments and write $\tau \sqsubset \sigma$ if $\tau$ is an initial segment of $\sigma$.

Let $G$ be a subgroup of $S_\omega$. We define the degree of $T_G$ ($\deg(T_G)$) to be the join of the Turing degrees of

- The domain of $T_G$ under some computable coding of $\mathbb{N}^{<\omega}$ in which $\sqsubset$ is decidable; and
- A branching function $Br : T_G \to \mathbb{N} \cup \{\infty\}$ such that $Br(\tau)$ is equal to the number of direct successors of $\tau$ in $T_G$.

# Topology

Given a tree $T \subset \mathbb{N}^{<\omega}$, we define $[T]$ to be the set of all paths through $T$. We endow $[T]$ with the standard product topology in which the basic clopen sets are those of the form $\{f \in \mathbb{N}^{\omega} : \tau \sqsubset f\}$ for some $\tau \in T$.

# Topology

Given a tree $T \subset \mathbb{N}^{<\omega}$, we define $[T]$ to be the set of all paths through $T$. We endow $[T]$ with the standard product topology in which the basic clopen sets are those of the form $\{f \in \mathbb{N}^\omega : \tau \sqsubset f\}$ for some $\tau \in T$.

In order for every path in $[T_G]$ to represent an element of $G$, we must have that $G$ is a closed subgroup of $S_\omega$.

# Profinite Groups and Orbits

Given a subgroup $G$ of $S_\omega$ and $n \in \mathbb{N}$, we define the orbit of $n$ under $G$ as

$$\mathrm{orb}_G(n) := \{g(n) \in \mathbb{N} : g \in G\}.$$

**Proposition**

*Let $G$ be a subgroup of $S_\omega$. The following are equivalent:*

**(1)** *$G$ is compact,*

**(2)** *$G$ is closed and all orbits under $G$ are finite,*

**(3)** *$G$ is profinite.* □

# Orbit Independence

Let $G$ be a profinite subgroup of $S_\omega$. Let $\{O_{G,n}\}_{n\in\mathbb{N}}$ be an enumeration of the orbits under $G$ (all of which are finite). Define

$$H_n := \{g \restriction O_{G,n} : g \in G\}.$$

**Definition**

We say that $G$ has orbit independence if it is isomorphic to the Cartesian product of all $H_n$. That is,

$$G \cong \prod_{n\in\mathbb{N}} H_n.$$

# Orbit Independence

Let $G$ be a profinite subgroup of $S_\omega$. Let $\{O_{G,n}\}_{n\in\mathbb{N}}$ be an enumeration of the orbits under $G$ (all of which are finite). Define

$$H_n := \{g \restriction O_{G,n} : g \in G\}.$$

**Definition**

We say that $G$ has orbit independence if it is isomorphic to the Cartesian product of all $H_n$. That is,

$$G \cong \prod_{n\in\mathbb{N}} H_n.$$

A non-example: $G = \{1_G, (0\,1)(2\,3)\}$ does not have orbit independence. Note that $G \cong C_2$, $H_0 = \{1, (0\,1)\} \cong C_2$, $H_1 = \{1, (2\,3)\} \cong C_2$, and $H_n$ is trivial for all $n > 1$. Thus $G \ncong \prod_n H_n \cong C_2 \times C_2$.

# Finite Approximations

Let $G$ be a profinite subgroup of $S_\omega$. Given $g \in G$, define $g_k = g \restriction \bigcup_{n \le k} O_{G,n}$. Define

$$G_k := \{g_k : g \in G\}.$$

# Finite Approximations

Let $G$ be a profinite subgroup of $S_\omega$. Given $g \in G$, define $g_k = g \upharpoonright \bigcup_{n \leq k} O_{G,n}$. Define

$$G_k := \{g_k : g \in G\}.$$

Note, by defining $\pi_k : G_{k+1} \to G_k$ by $\pi_k(g_{k+1}) = g_k$, we get that $G$ is isomorphic to the inverse limit of $\{G_k, \pi_k\}_{k \in \mathbb{N}}$.

# Existential Theory and Entire First Order Theory

Let $G$ be a profinite subgroup of $S_\omega$. The only obvious upper bound for the complexity of the existential theory is $\Sigma^1_1$. The only obvious upper bound for the complexity of $Th(G)$ is $\Sigma^1_\omega$.

# Existential Theory and Entire First Order Theory

Let $G$ be a profinite subgroup of $S_\omega$. The only obvious upper bound for the complexity of the existential theory is $\Sigma^1_1$. The only obvious upper bound for the complexity of $Th(G)$ is $\Sigma^1_\omega$.

However, we show that:

- The existential theory is $\Sigma^0_2$ relative to $\deg(T_G)$. Additionally, if $G$ has orbit independence then the existential theory is $\Sigma^0_1$ relative to $\deg(T_G)$.
- If $G$ has orbit independence, $Th(G)$ is $\Delta^0_2$ relative $\deg(T_G)$.

# Sentences

**Lemma**

*Every atomic sentence in the language of groups is true in every group.*

Proof: Every such sentence has the form $1^n = 1^m$ with $n, m \in \mathbb{Z}$. $\square$

# Sentences

**Lemma**

*Every atomic sentence in the language of groups is true in every group.*

Proof: Every such sentence has the form $1^n = 1^m$ with $n, m \in \mathbb{Z}$. $\square$

**Lemma**

*Let $G$ be a profinite subgroup of $S_\omega$ with orbit independence. Let $\alpha$ be an existential sentence in the language of groups. We have that $G \models \alpha$ if and only if $G_k \models \alpha$ for some $k \in \mathbb{N}$.*

Proof Sketch: Let $\alpha = \exists(\bar{x})\beta(\bar{x})$ with $\beta$ quantifier free. If $G_k \models \beta(\bar{\gamma})$, then by extending $\bar{\gamma}$ by the identity at all "levels" above $k$ we get a witness to $\beta$ in $G^{<\omega}$.

# Existential Theory With Orbit Independence

**Theorem**

*Let $G$ be a profinite subgroup of $S_\omega$ with orbit independence. The existential theory of $G$ is $\Sigma^0_1$ relative to $\deg(T_G)$.*

Proof: Let $\alpha$ be an existential sentence. By the previous lemma, $G \models \alpha$ if and only if

$$(\exists k)[G_k \models \alpha]$$

which is $\Sigma^0_1$ relative to $\deg(T_G)$. □

# Existential Theory With Orbit Independence

**Theorem**

*Let $G$ be a profinite subgroup of $S_\omega$ with orbit independence. The existential theory of $G$ is $\Sigma^0_1$ relative to $\deg(T_G)$.*

Proof: Let $\alpha$ be an existential sentence. By the previous lemma, $G \models \alpha$ if and only if

$$(\exists k)[G_k \models \alpha]$$

which is $\Sigma^0_1$ relative to $\deg(T_G)$. $\square$

This theorem is sharp.

# Proof of Sharpness

**Proposition**

*There exists a profinite subgroup $G$ of $S_\omega$ with orbit independence such that $T_G$ is computable and the existential theory of $G$ is $\Sigma^0_1$ complete.*

Proof Sketch: For all $n \in \mathbb{N}$, define the formula

$$\alpha_n := (\exists x)[x \neq 1 \,\&\, x^{p_n} = 1]$$

where $\{p_n\}_{n\in\mathbb{N}}$ is an enumeration of the primes. We build $G$ such that $T_G$ is computable but $G \models \alpha_n$ if and only if $n \in \emptyset'$.

# Existential Theory Without Orbit Independence

**Theorem**

*Let $G$ be any profinite subgroup of $S_\omega$ (not necessarily with orbit independence). The existential theory of $G$ is $\Sigma^0_2$ relative to $\deg(T_G)$.*

Proof Sketch: Suppose $\alpha = \exists \bar{x} \beta$ with $\beta$ quantifier free. It turns out that given any $\bar{g} \in G^{<\omega}$, $G \models \beta(\bar{g})$ if and only if $G_k \models \beta(\bar{g}_k)$ for all but finitely many $k \in \mathbb{N}$.

This theorem is sharp.

# Proof of Sharpness

**Proposition**

*There exists a profinite subgroup $G$ of $S_\omega$ (without orbit independence) with $T_G$ computable such that the existential theory of $G$ is $\Sigma^0_2$ complete.*

Proof Sketch: We build $G$ so that it will contain an element of order $p_n$ if and only if $n \in \mathrm{Fin}$ (that is, if $\Phi_n$ has finite domain).

# Strategy for $p_0 = 2$

We essentially start to build a copy of the 2-adic integers within $G$. Every time the domain of $\Phi_0$ gets a new element we add another "layer" of the 2-adics to $G$. When a new layer is added at stage $s$, any element that had order 2 when restricted to $G_s$ will not be order 2 in $G_{s+1}$. However, a new order 2 element is added to $G_{s+1}$.

# Feferman-Vaught Corollary

**Lemma**

*If $G$ has orbit independence, then given any first order sentence $\alpha$ in the language of groups, $G \models \alpha$ if and only if $G_k \models \alpha$ for all but finitely many $k$.*

This follows from the Feferman-Vaught Theorem.

# Feferman-Vaught Corollary

**Lemma**

*If $G$ has orbit independence, then given any first order sentence $\alpha$ in the language of groups, $G \models \alpha$ if and only if $G_k \models \alpha$ for all but finitely many $k$.*

This follows from the Feferman-Vaught Theorem.

Note, this does NOT always hold if $G$ does not have orbit independence. Counter example: $\mathbb{Z}_2$.

# Entire First Order Theory W/ Orbit Independence

**Theorem**

*Let $G$ be a profinite subgroup of $S_\omega$ with orbit independence. The first order theory of $G$ is $\Delta_2^0$ relative to $\deg(T_G)$.*

Proof: $G \models \alpha$ iff $(\exists n)(\forall k > n)[G_k \models \alpha]$. Additionally, $G \not\models \alpha$ iff $(\exists n)(\forall k > n)[G_k \models \neg\alpha]$. Thus, both $Th(G)$ and its complement are $\Sigma_2^0$ relative to $\deg(T_G)$.

# Entire First Order Theory W/ Orbit Independence

**Theorem**

*Let $G$ be a profinite subgroup of $S_\omega$ with orbit independence. The first order theory of $G$ is $\Delta^0_2$ relative to $\deg(T_G)$.*

Proof: $G \models \alpha$ iff $(\exists n)(\forall k > n)[G_k \models \alpha]$. Additionally, $G \not\models \alpha$ iff $(\exists n)(\forall k > n)[G_k \models \neg\alpha]$. Thus, both $Th(G)$ and its complement are $\Sigma^0_2$ relative to $\deg(T_G)$.

Open Question: How complicated can $Th(G)$ be when $G$ does not have orbit independence?

# A countable subgroup of $G$

Let $G$ be a profinite subgroup of $S_\omega$. Define $G_{\{\mathbf{0}\}}$ to be the set of all computable elements of $G$.

# A countable subgroup of $G$

Let $G$ be a profinite subgroup of $S_\omega$. Define $G_{\{\mathbf{0}\}}$ to be the set of all computable elements of $G$.

To what extent is $G_{\{\mathbf{0}\}}$ an elementary subgroup of $G$?

What happens if take the elements of $G$ of some higher Turing degree?

# Turing Ideals and $G_I$

A collection $I$ of Turing degrees is called a *Turing ideal* if

- $I$ is downwards closed (under $\leq_T$); and
- Given $\boldsymbol{c}, \boldsymbol{d} \in I$, we have $\boldsymbol{c} \oplus \boldsymbol{d} \in I$.

We call $I$ a *Scott ideal* if for every $\boldsymbol{c} \in I$ there exists $\boldsymbol{d} \in I$ that is PA relative to $\boldsymbol{c}$.

# Turing Ideals and $G_I$

A collection $I$ of Turing degrees is called a *Turing ideal* if

- $I$ is downwards closed (under $\leq_T$); and
- Given $\boldsymbol{c}, \boldsymbol{d} \in I$, we have $\boldsymbol{c} \oplus \boldsymbol{d} \in I$.

We call $I$ a *Scott ideal* if for every $\boldsymbol{c} \in I$ there exists $\boldsymbol{d} \in I$ that is PA relative to $\boldsymbol{c}$.

Given a subgroup $G$ of $S_\omega$ and a Turing ideal $I$ with $\deg(T_G) \in I$, we define $G_I$ to be the subgroup of $G$ all of whose elements are of degree in $I$. That is,

$$G_I = \{g \in G : \deg(g) \in I\}.$$

# Turing Ideals and $G_I$

A collection $I$ of Turing degrees is called a *Turing ideal* if

- $I$ is downwards closed (under $\leq_T$); and
- Given $\boldsymbol{c}, \boldsymbol{d} \in I$, we have $\boldsymbol{c} \oplus \boldsymbol{d} \in I$.

We call $I$ a *Scott ideal* if for every $\boldsymbol{c} \in I$ there exists $\boldsymbol{d} \in I$ that is PA relative to $\boldsymbol{c}$.

Given a subgroup $G$ of $S_\omega$ and a Turing ideal $I$ with $\deg(T_G) \in I$, we define $G_I$ to be the subgroup of $G$ all of whose elements are of degree in $I$. That is,

$$G_I = \{g \in G : \deg(g) \in I\}.$$

Question: To what degree is $G_I$ an elementary substructure of $G$?

# Elementarity

Let $\mathcal{A}$ be a substructure of $\mathcal{B}$ and let $\Gamma$ be a class of formulas. We say that $\mathcal{A}$ is a $\Gamma$-elementary substructure if for all formulas $\gamma \in \Gamma$ and tuples $\bar{a} \in \mathcal{A}$,

$$\mathcal{A} \models \gamma(\bar{a}) \iff \mathcal{B} \models \gamma(\bar{a}).$$

We express this as

$$\mathcal{A} \preceq_{\Gamma} \mathcal{B}.$$

If this holds for all first order formulas $\gamma$, then we simply say that $\mathcal{A}$ is an elementary substructure of $\mathcal{B}$ and write

$$\mathcal{A} \preceq \mathcal{B}.$$

# Definitely Not Always Elementary

**Proposition**

*There exists a profinite subgroup $G$ of $S_\omega$ such that $G_{\{\mathbf{0}\}}$ is not an $\exists$-elementary subgroup of $G$.*

To prove this, we build a $G$ along with a computable $g \in G$ such that $g$ has a square root in $G$ but no computable square root. Defining $\alpha(x) = (\exists y)[y^2 = x]$, we have $G \models \alpha(g)$ but $G_{\{\mathbf{0}\}} \not\models \alpha(g)$.

# Definitely Not Always Elementary

**Proposition**

*There exists a profinite subgroup $G$ of $S_\omega$ such that $G_{\{\mathbf{0}\}}$ is not an $\exists$-elementary subgroup of $G$.*

To prove this, we build a $G$ along with a computable $g \in G$ such that $g$ has a square root in $G$ but no computable square root. Defining $\alpha(x) = (\exists y)[y^2 = x]$, we have $G \models \alpha(g)$ but $G_{\{\mathbf{0}\}} \not\models \alpha(g)$.

Note, the $G$ that we build will NOT have orbit independence and $\{\mathbf{0}\}$ is NOT a Scott ideal.

# With Orbit Independence

**Theorem**

*Given a profinite subgroup of G with orbit independence and any Turing ideal I,*

$$G_I \preceq_\exists G.$$

If $G$ has orbit independence, then by previous Lemma given any quantifier free $\alpha(x)$, $G \models \alpha(g)$ iff $G_k \models \alpha(g_k)$ for some $k \in \mathbb{N}$. If $G$ has orbit independence, then there is some computable $g' \in G$ extending $g_k$ and we must have $G \models \alpha(g')$. Thus,

$$G \models \exists x \alpha(x) \iff G_I \models \exists x \alpha(x).$$

# With a Scott Ideal

**Theorem**

*Given any profinite subgroup $G$ of $S_\omega$ and a Scott ideal $I$,*

$$G_I \preceq_\exists G.$$

*Furthermore if $G$ has orbit independence, then*

$$G_I \preceq G.$$

# The Key Lemmas

**Lemma**

*Let $G$ be any profinite subgroup of $S_\omega$. If $\alpha$ is quantifier free, then $G \models \alpha(g)$ if and only if $G_k \models \alpha(g_k)$ for all but finitely many $k \in \mathbb{N}$.*

**Lemma**

*Let $G$ be a profinite subgroup of $S_\omega$ with orbit independence. If $\beta$ is ANY first order formula, then $G \models \beta(g)$ if and only if $G_k \models \beta(g_k)$ for all but finitely many $k \in \mathbb{N}$.*

# Using the Scott Ideals

Suppose $G$ has orbit independence, $\beta$ is any first order formula, and $G \models \exists x \beta(x)$. Fix a witness $g$. Must have that for some $L$

$$k \geq L \implies G_k \models \beta(g_k).$$

# Using the Scott Ideals

Suppose $G$ has orbit independence, $\beta$ is any first order formula, and $G \models \exists x \beta(x)$. Fix a witness $g$. Must have that for some $L$

$$k \geq L \implies G_k \models \beta(g_k).$$

We can define a tree $T_\beta$ with root $g_L$ all of whose elements are finite extensions of $g_L$ that still satisfy $\beta$. If $I$ is a Scott ideal, there will be an $I$ computable path $g'$ through $T_\beta$. We will have $G_I \models \beta(g'_k)$. Thus,

$$G \models \exists x \beta(x) \implies G_I \models \exists x \beta(x).$$

# Using the Scott Ideals

Suppose $G$ has orbit independence, $\beta$ is any first order formula, and $G \models \exists x \beta(x)$. Fix a witness $g$. Must have that for some $L$

$$k \geq L \implies G_k \models \beta(g_k).$$

We can define a tree $T_\beta$ with root $g_L$ all of whose elements are finite extensions of $g_L$ that still satisfy $\beta$. If $I$ is a Scott ideal, there will be an $I$ computable path $g'$ through $T_\beta$. We will have $G_I \models \beta(g'_k)$. Thus,

$$G \models \exists x \beta(x) \implies G_I \models \exists x \beta(x).$$

Applying induction, we get

$$G_I \preceq G.$$

# Summary

Thus, to get that $G_I$ is an elementary subgroup of $G$ it is sufficient to have that $I$ is a Scott ideal and that $G$ has orbit independence.

# Summary

Thus, to get that $G_I$ is an elementary subgroup of $G$ it is sufficient to have that $I$ is a Scott ideal and that $G$ has orbit independence.

If $G$ does not have orbit independence and $I$ is not a Scott ideal, then we need not even have $G \preceq_{\exists} G$.

# Summary

Thus, to get that $G_I$ is an elementary subgroup of $G$ it is sufficient to have that $I$ is a Scott ideal and that $G$ has orbit independence.

If $G$ does not have orbit independence and $I$ is not a Scott ideal, then we need not even have $G \preceq_\exists G$.

If $G$ has orbit independence but $I$ is not a Scott ideal, or if $G$ does not have orbit independence but $I$ is a Scott ideal, then $G_I \preceq_\exists G$. However, must we have $G_I \preceq G$? (Open question)

# References


- Feferman, S., Vaught R.: The first order properties of products of algebraic systems. Fundamenta Mathematicae **47**(1), 57â103 1959.
- Greenberg, N., Melnikov A., Nies A., Turetsky D.: Effectively Closed Subgroups of the Infinite Symmetric Group. Proceedings of the American Mathematical Society **146**(12), 5421-5435 (2018)
- La Roche, P.: Effective Galois Theory. The Jounal of Symbolic Logic **46**(2), 385-392 (1981)
- Metakides, G., Nerode, A.: Effective Content of Field Theory. Annals of Mathematical Logic **17** 289-320, (1979)
- Miller, R.: Computability for the absolute Galois group of $\mathbb{Q}$. To appear, available at arXiv:2307.08935
- Smith, R.: Effective aspects of profinite groups. The Journal of Symbolic Logic **46**(4), 851-863 (1981)