Profinite groups: algebra and topology

Dan Segal

april 2010

Outline

Profinite groups arise in nature as Galois groups of infinite algebraic extensions.
But they have an interesting theory in their own right.

A profinite group is a compact topological group that is built out of finite groups. Properties of the topological group reflect group-theoretic properties of all the finite groups.

If we forget the topology we wouldn't expect this to remain true: it doesn't in general. However: in the special case where the profinite group is *topologically finitely generated*,

$$\{ \text{ open subgroups } \} = \{ \text{ subgroups of finite index } \}$$

Hence: algebraic structure determines the topology.
Proposed by Serre in the 1970s, not proved until 2003.
Related to *algebraic properties of finite groups*: specifically the behaviour of word-values.

Outline

Profinite groups arise in nature as Galois groups of infinite algebraic extensions.
But they have an interesting theory in their own right.

A profinite group is a compact topological group that is built out of finite groups. Properties of the topological group reflect group-theoretic properties of all the finite groups.

If we forget the topology we wouldn't expect this to remain true: it doesn't in general. However: in the special case where the profinite group is *topologically finitely generated*,

{ open subgroups } = { subgroups of finite index }

Hence: algebraic structure determines the topology.
Proposed by Serre in the 1970s, not proved until 2003.
Related to *algebraic properties of finite groups*: specifically the behaviour of word-values.

Outline

Profinite groups arise in nature as Galois groups of infinite algebraic extensions.
But they have an interesting theory in their own right.

A profinite group is a compact topological group that is built out of finite groups. Properties of the topological group reflect group-theoretic properties of all the finite groups.

If we forget the topology we wouldn't expect this to remain true: it doesn't in general. However: in the special case where the profinite group is *topologically finitely generated*,

$$\{ \text{ open subgroups } \} = \{ \text{ subgroups of finite index } \}$$

Hence: algebraic structure determines the topology.
Proposed by Serre in the 1970s, not proved until 2003.
Related to *algebraic properties of finite groups*: specifically the behaviour of word-values.

Outline

Profinite groups arise in nature as Galois groups of infinite algebraic extensions.
But they have an interesting theory in their own right.

A profinite group is a compact topological group that is built out of finite groups. Properties of the topological group reflect group-theoretic properties of all the finite groups.

If we forget the topology we wouldn't expect this to remain true: it doesn't in general. However: in the special case where the profinite group is *topologically finitely generated*,

{ open subgroups } = { subgroups of finite index }

Hence: algebraic structure determines the topology.
Proposed by Serre in the 1970s, not proved until 2003.
Related to *algebraic properties of finite groups*: specifically the behaviour of word-values.

Outline

Profinite groups arise in nature as Galois groups of infinite algebraic extensions.
But they have an interesting theory in their own right.

A profinite group is a compact topological group that is built out of finite groups. Properties of the topological group reflect group-theoretic properties of all the finite groups.

If we forget the topology we wouldn't expect this to remain true: it doesn't in general. However: in the special case where the profinite group is *topologically finitely generated*,

$$\{ \text{ open subgroups } \} = \{ \text{ subgroups of finite index } \}$$

Hence: algebraic structure determines the topology.
Proposed by Serre in the 1970s, not proved until 2003.
Related to *algebraic properties of finite groups*: specifically the behaviour of word-values.

Examples of profinite groups

1. E/k an algebraic Galois extension of fields. Then

$$\mathrm{Gal}(E/k) = \varprojlim_{\Lambda} \mathrm{Gal}(K/k)$$

where $\Lambda = \{$ finite Galois extensions K of k with $K \subseteq E$ $\}$, with the restriction maps

$$\mathrm{Gal}(K_2/k) \to \mathrm{Gal}(K_1/k) \quad (K_2 \supseteq K_1)$$

2. T a locally finite rooted tree. Then

$$\mathrm{Aut}(T) = \varprojlim_{m \in \mathbb{N}} \mathrm{Aut}(T[m])$$

where $T[m]$ is the ball of radius m in T centred at the root.

Examples of profinite groups

1. E/k an algebraic Galois extension of fields. Then

$$\mathrm{Gal}(E/k) = \varprojlim_{\Lambda} \mathrm{Gal}(K/k)$$

where $\Lambda = \{$ finite Galois extensions K of k with $K \subseteq E$ $\}$, with the restriction maps

$$\mathrm{Gal}(K_2/k) \to \mathrm{Gal}(K_1/k) \quad (K_2 \supseteq K_1)$$

2. T a locally finite rooted tree. Then

$$\mathrm{Aut}(T) = \varprojlim_{m \in \mathbb{N}} \mathrm{Aut}(T[m])$$

where $T[m]$ is the ball of radius m in T centred at the root.

Definition of profinite groups

In general, suppose we have a directed set Λ, finite groups G_λ $(\lambda \in \Lambda)$ and epimorphisms $\theta_{\lambda\mu} : G_\lambda \to G_\mu$ $(\lambda \geq \mu)$, all compatible in the obvious way. The *inverse limit* of the system (G_λ) is

$$G = \varprojlim_{\Lambda} G_\lambda = \{\mathbf{g} = (g_\lambda) \mid g_\lambda \theta_{\lambda\mu} = g_\mu \ \forall \lambda > \mu\} \leq \prod_{\Lambda} G_\lambda$$

Give each finite group G_λ its discrete topology and $\prod G_\lambda$ the product topology. This becomes a compact Hausdorff group by Tychonoff's Theorem. Also G is a *closed* subgroup. So G satisfies

Definition A *profinite group* is a compact Hausdorff totally disconnected topological group.

More useful definition:

a compact Hausdorff group whose open subgroups form a base for the neighbourhoods of 1.

Definition of profinite groups

In general, suppose we have a directed set Λ, finite groups G_λ ($\lambda \in \Lambda$) and epimorphisms $\theta_{\lambda\mu} : G_\lambda \to G_\mu$ ($\lambda \geq \mu$), all compatible in the obvious way. The *inverse limit* of the system (G_λ) is

$$G = \varprojlim_{\Lambda} G_\lambda = \{\mathbf{g} = (g_\lambda) \mid g_\lambda \theta_{\lambda\mu} = g_\mu \ \forall \lambda > \mu\} \leq \prod_{\Lambda} G_\lambda$$

Give each finite group G_λ its discrete topology and $\prod G_\lambda$ the product topology. This becomes a compact Hausdorff group by Tychonoff's Theorem. Also G is a *closed* subgroup. So G satisfies

Definition A *profinite group* is a compact Hausdorff totally disconnected topological group.

More useful definition:

a compact Hausdorff group whose open subgroups form a base for the neighbourhoods of 1.

Definition of profinite groups

In general, suppose we have a directed set Λ, finite groups G_λ ($\lambda \in \Lambda$) and epimorphisms $\theta_{\lambda\mu} : G_\lambda \to G_\mu$ ($\lambda \geq \mu$), all compatible in the obvious way. The *inverse limit* of the system (G_λ) is

$$G = \lim_{\longleftarrow \Lambda} G_\lambda = \{\mathbf{g} = (g_\lambda) \mid g_\lambda \theta_{\lambda\mu} = g_\mu \ \forall \lambda > \mu\} \leq \prod_\Lambda G_\lambda$$

Give each finite group G_λ its discrete topology and $\prod G_\lambda$ the product topology. This becomes a compact Hausdorff group by Tychonoff's Theorem. Also G is a *closed* subgroup. So G satisfies

Definition A *profinite group* is a compact Hausdorff totally disconnected topological group.

More useful definition:

a compact Hausdorff group whose open subgroups form a base for the neighbourhoods of 1.

Writing $\mathcal{N}(G) = \{\text{open normal subgroups of } G\}$ we have

$$G = \varprojlim (G/N \mid N \in \mathcal{N}(G))$$

Fundamental observation: in any compact group, open subgroups have *finite index*.

Is the converse true?
No! Let C_n be a group of order 2 for each n and take

$$G_n = C_1 \times \cdots \times C_n$$

projecting onto C_{n-1} in the obvious way. Then

$$G = \varprojlim G_n = \prod_{j \in \mathbb{N}} C_j$$

has countably many open subgroups but $2^{2^{\aleph_0}}$ subgroups of index 2.
More interesting example: there is a profinite group G such that G/N is perfect for each $N \in \mathcal{N}(G)$, but having (non-open) normal subgroups of index 2.

Writing $\mathcal{N}(G) = \{\text{open normal subgroups of } G\}$ we have

$$G = \varprojlim (G/N \mid N \in \mathcal{N}(G))$$

Fundamental observation: in any compact group, open subgroups have *finite index*.

Is the converse true?

No! Let C_n be a group of order 2 for each n and take

$$G_n = C_1 \times \cdots \times C_n$$

projecting onto C_{n-1} in the obvious way. Then

$$G = \varprojlim G_n = \prod_{j \in \mathbb{N}} C_j$$

has countably many open subgroups but $2^{2^{\aleph_0}}$ subgroups of index 2.

More interesting example: there is a profinite group G such that G/N is perfect for each $N \in \mathcal{N}(G)$, but having (non-open) normal subgroups of index 2.

Writing $\mathcal{N}(G) = \{\text{open normal subgroups of } G\}$ we have

$$G = \varprojlim (G/N \mid N \in \mathcal{N}(G))$$

Fundamental observation: in any compact group, open subgroups have *finite index*.

Is the converse true?

No! Let C_n be a group of order 2 for each n and take

$$G_n = C_1 \times \cdots \times C_n$$

projecting onto C_{n-1} in the obvious way. Then

$$G = \varprojlim G_n = \prod_{j \in \mathbb{N}} C_j$$

has countably many open subgroups but $2^{2^{\aleph_0}}$ subgroups of index 2.

More interesting example: there is a profinite group G such that G/N is perfect for each $N \in \mathcal{N}(G)$, but having (non-open) normal subgroups of index 2.

Writing $\mathcal{N}(G) = \{\text{open normal subgroups of } G\}$ we have

$$G = \varprojlim (G/N \mid N \in \mathcal{N}(G))$$

Fundamental observation: in any compact group, open subgroups have *finite index*.

Is the converse true?

No! Let C_n be a group of order 2 for each n and take

$$G_n = C_1 \times \cdots \times C_n$$

projecting onto C_{n-1} in the obvious way. Then

$$G = \varprojlim G_n = \prod_{j \in \mathbb{N}} C_j$$

has countably many open subgroups but $2^{2^{\aleph_0}}$ subgroups of index 2.

More interesting example: there is a profinite group G such that G/N is perfect for each $N \in \mathcal{N}(G)$, but having (non-open) normal subgroups of index 2.

Writing $\mathcal{N}(G) = \{\text{open normal subgroups of } G\}$ we have

$$G = \varprojlim (G/N \mid N \in \mathcal{N}(G))$$

Fundamental observation: in any compact group, open subgroups have *finite index*.

Is the converse true?
No! Let C_n be a group of order 2 for each n and take

$$G_n = C_1 \times \cdots \times C_n$$

projecting onto C_{n-1} in the obvious way. Then

$$G = \varprojlim G_n = \prod_{j \in \mathbb{N}} C_j$$

has countably many open subgroups but $2^{2^{\aleph_0}}$ subgroups of index 2.
More interesting example: there is a profinite group G such that G/N is perfect for each $N \in \mathcal{N}(G)$, but having (non-open) normal subgroups of index 2.

Serre's theorem (1975) In a finitely generated pro-p group, every subgroup of finite index is open.

Finitely generated is meant in the topological sense. In fact, for G profinite

$$\mathrm{d}(G) = \sup\{\mathrm{d}(G/N) \mid N \in \mathcal{N}(G)\}$$

where $\mathrm{d}(G)$ is the minimal size of a topological (ordinary in finite case) generating set .

Philosophy: qualitative properties of topological (profinite) group G reflect *uniform* algebraic properties of (continuous) finite quotients G/N ($N \in \mathcal{N}(G)$).

Serre's question Is ST true for *all* f.g. profinite groups?

Need to understand what 'finite-index subgroups of G are open' means *algebraically* for the finite quotients G/N ($N \in \mathcal{N}(G)$)!

Serre's theorem (1975) In a finitely generated pro-p group, every subgroup of finite index is open.

Finitely generated is meant in the topological sense. In fact, for G profinite

$$\mathrm{d}(G) = \sup\{\mathrm{d}(G/N) \mid N \in \mathcal{N}(G)\}$$

where $\mathrm{d}(G)$ is the minimal size of a topological (ordinary in finite case) generating set .

Philosophy: qualitative properties of topological (profinite) group G reflect *uniform* algebraic properties of (continuous) finite quotients G/N $(N \in \mathcal{N}(G))$.

Serre's question Is ST true for *all* f.g. profinite groups?

Need to understand what 'finite-index subgroups of G are open' means *algebraically* for the finite quotients G/N $(N \in \mathcal{N}(G))$!

Serre's theorem (1975) In a finitely generated pro-p group, every subgroup of finite index is open.

Finitely generated is meant in the topological sense. In fact, for G profinite

$$\mathrm{d}(G) = \sup\{\mathrm{d}(G/N) \mid N \in \mathcal{N}(G)\}$$

where $\mathrm{d}(G)$ is the minimal size of a topological (ordinary in finite case) generating set .

Philosophy: qualitative properties of topological (profinite) group G reflect *uniform* algebraic properties of (continuous) finite quotients G/N $(N \in \mathcal{N}(G))$.

Serre's question Is ST true for *all* f.g. profinite groups?

Need to understand what 'finite-index subgroups of G are open' means *algebraically* for the finite quotients G/N $(N \in \mathcal{N}(G))$!

Serre's theorem (1975) In a finitely generated pro-p group, every subgroup of finite index is open.

Finitely generated is meant in the topological sense. In fact, for G profinite

$$\mathrm{d}(G) = \sup\{\mathrm{d}(G/N) \mid N \in \mathcal{N}(G)\}$$

where $\mathrm{d}(G)$ is the minimal size of a topological (ordinary in finite case) generating set .

Philosophy: qualitative properties of topological (profinite) group G reflect *uniform* algebraic properties of (continuous) finite quotients G/N ($N \in \mathcal{N}(G)$).

Serre's question Is ST true for *all* f.g. profinite groups?

Need to understand what 'finite-index subgroups of G are open' means *algebraically* for the finite quotients G/N ($N \in \mathcal{N}(G)$)!

Consider

$$G'G^p = \langle [x,y]z^p \mid x,y,z \in G \rangle.$$

Since $G/G'G^p$ is elementary abelian, its subgroups of index p have trivial intersection, i.e.

$$G'G^p = \bigcap \{N \mid N \lhd G,\ |G/N| = p\}\ .$$

Open subgroups are closed. So if each index-p subgroup is open then $G'G^p$ is *closed*. If G is a **finitely generated pro-p group**, the converse is also true (easy); and an easy induction shows:

all subgroups of index p open $\iff$ *all subgroups of finite index open.*

What does it mean for $G'G^p$ to be closed?

Consider

$$G'G^p = \langle [x,y]z^p \mid x,y,z \in G \rangle.$$

Since $G/G'G^p$ is elementary abelian, its subgroups of index p have trivial intersection, i.e.

$$G'G^p = \bigcap \{N \mid N \lhd G,\ |G/N| = p\}\ .$$

Open subgroups are closed. So if each index-p subgroup is open then $G'G^p$ is *closed*. If G is a **finitely generated pro-p group**, the converse is also true (easy); and an easy induction shows:

all subgroups of index p open $\iff$ all subgroups of finite index open.

What does it mean for $G'G^p$ to be closed?

Consider

$$G'G^p = \langle [x,y]z^p \mid x,y,z \in G \rangle.$$

Since $G/G'G^p$ is elementary abelian, its subgroups of index p have trivial intersection, i.e.

$$G'G^p = \bigcap \{N \mid N \lhd G,\ |G/N| = p\}\ .$$

Open subgroups are closed. So if each index-p subgroup is open then $G'G^p$ is *closed*. If G is a **finitely generated pro-p group**, the converse is also true (easy); and an easy induction shows:

all subgroups of index p open $\iff$ *all subgroups of finite index open.*

What does it mean for $G'G^p$ to be closed?

Consider

$$G'G^p = \langle [x,y]z^p \mid x,y,z \in G \rangle.$$

Since $G/G'G^p$ is elementary abelian, its subgroups of index p have trivial intersection, i.e.

$$G'G^p = \bigcap \{N \mid N \lhd G,\ |G/N| = p\}\ .$$

Open subgroups are closed. So if each index-p subgroup is open then $G'G^p$ is *closed*. If G is a **finitely generated pro-p group**, the converse is also true (easy); and an easy induction shows:

all subgroups of index p open $\iff$ *all subgroups of finite index open.*

What does it mean for $G'G^p$ to be closed?

Write $w(x, y, z) = [x, y]z^p$ and set

$$G_w = \left\{ w(\mathbf{g})^{\pm 1} \mid \mathbf{g} \in G \times G \times G \right\}.$$

Then

$$G'G^p = w(G) = \bigcup_{n=1}^{\infty} G_w^{*n}$$

where $G_w^{*n} = G_w \cdot G_w \cdot \ldots \cdot G_w$ (n times).

Now the map $w : G^{(3)} \to G$ is continuous and G is compact, so G_w^{*n} is compact, hence closed in G, for each n.
Baire category Theorem implies that the following are equivalent:

(a) *$w(G)$ is closed*
(b) *$w(G)$ is closed and for some n, G_w^{*n} contains a non-empty open subset of $w(G)$*
(c) *for some n, $G_w^{*n} = w(G)$.*

Write $w(x,y,z) = [x,y]z^p$ and set

$$G_w = \left\{ w(\mathbf{g})^{\pm 1} \mid \mathbf{g} \in G \times G \times G \right\}.$$

Then

$$G'G^p = w(G) = \bigcup_{n=1}^{\infty} G_w^{*n}$$

where $G_w^{*n} = G_w \cdot G_w \cdot \ldots \cdot G_w$ (n times).

Now the map $w : G^{(3)} \to G$ is continuous and G is compact, so G_w^{*n} is compact, hence closed in G, for each n.

Baire category Theorem implies that the following are equivalent:

(a) *$w(G)$ is closed*

(b) *$w(G)$ is closed and for some n, G_w^{*n} contains a non-empty open subset of $w(G)$*

(c) *for some n, $G_w^{*n} = w(G)$.*

Write $w(x,y,z) = [x,y]z^p$ and set

$$G_w = \left\{ w(\mathbf{g})^{\pm 1} \mid \mathbf{g} \in G \times G \times G \right\}.$$

Then

$$G' G^p = w(G) = \bigcup_{n=1}^{\infty} G_w^{*n}$$

where $G_w^{*n} = G_w \cdot G_w \cdot \ldots \cdot G_w$ (n times).

Now the map $w : G^{(3)} \to G$ is continuous and G is compact, so G_w^{*n} is compact, hence closed in G, for each n.
Baire category Theorem implies that the following are equivalent:

(a) *$w(G)$ is closed*
(b) *$w(G)$ is closed and for some n, G_w^{*n} contains a non-empty open subset of $w(G)$*
(c) *for some n, $G_w^{*n} = w(G)$.*

Moreover:

$$w(G) = G_w^{*n} \iff w(G/N) = (G/N)_w^{*n} \quad \forall N \in \mathcal{N}(G).$$

So: $w(G)$ is closed iff w has *bounded width* in all finite continuous quotients of G.

In general, a f.g. profinite group may not have any subroups of prime index. However, each subgroup H of finite index in G contains a normal subgroup H_0 of finite index, and taking $q = |G/H_0|$ we have

$$G^q \leq H_0 \leq H$$

where $G^q = \langle x^q \mid x \in G \rangle$. If G^q is open then H is open.

Theorem (N. Nikolov & DS) If G is a f.g. profinite group and $q \in \mathbb{N}$ then G^q is open in G.

Moreover:

$$w(G) = G_w^{*n} \iff w(G/N) = (G/N)_w^{*n} \quad \forall N \in \mathcal{N}(G).$$

So: $w(G)$ is closed iff w has *bounded width* in all finite continuous quotients of G.

In general, a f.g. profinite group may not have any subroups of prime index. However, each subgroup H of finite index in G contains a normal subgroup H_0 of finite index, and taking $q = |G/H_0|$ we have

$$G^q \leq H_0 \leq H$$

where $G^q = \langle x^q \mid x \in G \rangle$. If G^q is open then H is open.

Theorem (N. Nikolov & DS) If G is a f.g. profinite group and $q \in \mathbb{N}$ then G^q is open in G.

Moreover:

$$w(G) = G_w^{*n} \iff w(G/N) = (G/N)_w^{*n} \quad \forall N \in \mathcal{N}(G).$$

So: $w(G)$ is closed iff w has *bounded width* in all finite continuous quotients of G.

In general, a f.g. profinite group may not have any subroups of prime index. However, each subgroup H of finite index in G contains a normal subgroup H_0 of finite index, and taking $q = |G/H_0|$ we have

$$G^q \leq H_0 \leq H$$

where $G^q = \langle x^q \mid x \in G \rangle$. If G^q is open then H is open.

Theorem (N. Nikolov & DS) If G is a f.g. profinite group and $q \in \mathbb{N}$ then G^q is open in G.

Corollary 1 *If G is a f.g. profinite group then every subgroup of finite index in G is open.*

Corollary 2 *Every group homomorphism from a f.g. profinite group to any profinite group is continuous. The topology on a f.g. profinite group is uniquely determined by the group structure.*

Taking $w(x) = x^q$, we see as before that NS is equivalent to

Theorem *Given d, $q \in \mathbb{N}$ there exists $f \in \mathbb{N}$ such that: in any d-generator* finite *group, every product of q^{th} powers is equal to a product of f q^{th} powers.*

(Slight cheat: this also depends on positive solution to *Restricted Burnside Problem* (Zelmanov *et al*), which implies
G^q open $\iff$ G^q closed,
and a long roundabout argument that we only found in 2009; Corollary 1 was proved in 2003 using other words.)

Corollary 1 *If G is a f.g. profinite group then every subgroup of finite index in G is open.*

Corollary 2 *Every group homomorphism from a f.g. profinite group to any profinite group is continuous. The topology on a f.g. profinite group is uniquely determined by the group structure.*

Taking $w(x) = x^q$, we see as before that NS is equivalent to

Theorem *Given d, $q \in \mathbb{N}$ there exists $f \in \mathbb{N}$ such that: in any d-generator* finite *group, every product of q^{th} powers is equal to a product of f q^{th} powers.*

(Slight cheat: this also depends on positive solution to *Restricted Burnside Problem* (Zelmanov *et al*), which implies

G^q open $\iff$ G^q closed,

and a long roundabout argument that we only found in 2009; Corollary 1 was proved in 2003 using other words.)

Corollary 1 *If G is a f.g. profinite group then every subgroup of finite index in G is open.*

Corollary 2 *Every group homomorphism from a f.g. profinite group to any profinite group is continuous. The topology on a f.g. profinite group is uniquely determined by the group structure.*

Taking $w(x) = x^q$, we see as before that NS is equivalent to

Theorem *Given d, $q \in \mathbb{N}$ there exists $f \in \mathbb{N}$ such that: in any d-generator* finite *group, every product of q^{th} powers is equal to a product of f q^{th} powers.*

(Slight cheat: this also depends on positive solution to *Restricted Burnside Problem* (Zelmanov *et al*), which implies
G^q open $\iff$ G^q closed,
and a long roundabout argument that we only found in 2009; Corollary 1 was proved in 2003 using other words.)

Corollary 1 *If G is a f.g. profinite group then every subgroup of finite index in G is open.*

Corollary 2 *Every group homomorphism from a f.g. profinite group to any profinite group is continuous. The topology on a f.g. profinite group is uniquely determined by the group structure.*

Taking $w(x) = x^q$, we see as before that NS is equivalent to

Theorem *Given $d, q \in \mathbb{N}$ there exists $f \in \mathbb{N}$ such that: in any d-generator* finite *group, every product of q^{th} powers is equal to a product of f q^{th} powers.*

(Slight cheat: this also depends on positive solution to *Restricted Burnside Problem* (Zelmanov *et al*), which implies
G^q open $\iff$ G^q closed,
and a long roundabout argument that we only found in 2009; Corollary 1 was proved in 2003 using other words.)

Uniformly elliptic words

Definition A group word w is uniformly elliptic if for each $d \in \mathbb{N}$ there exists $f \in \mathbb{N}$ such that $w(H) = H_w^{*f}$ for every d-generator finite group H.

Each uniformly elliptic word carries topological information about profinite groups: *w is uniformly elliptic if and only if $w(G)$ is closed in G for every f. g. profinite group G.*

Suppose we want to prove that w is uniformly elliptic.
H a d-generator finite group. We need to *Assume* :

♡ $w(H) = \langle g_1, \ldots, g_m \rangle$ where $g_1, \ldots, g_m \in H_w$ and m depends only on w and d.

Uniformly elliptic words

Definition A group word w is uniformly elliptic if for each $d \in \mathbb{N}$ there exists $f \in \mathbb{N}$ such that $w(H) = H_w^{*f}$ for every d-generator finite group H.

Each uniformly elliptic word carries topological information about profinite groups: *w is uniformly elliptic if and only if $w(G)$ is closed in G for every f. g. profinite group G.*

Suppose we want to prove that w is uniformly elliptic.
H a d-generator finite group. We need to *Assume* :

♡ $w(H) = \langle g_1, \ldots, g_m \rangle$ where $g_1, \ldots, g_m \in H_w$ and m depends only on w and d.

Uniformly elliptic words

Definition A group word w is uniformly elliptic if for each $d \in \mathbb{N}$ there exists $f \in \mathbb{N}$ such that $w(H) = H_w^{*f}$ for every d-generator finite group H.

Each uniformly elliptic word carries topological information about profinite groups: *w is uniformly elliptic if and only if $w(G)$ is closed in G for every f. g. profinite group G.*

Suppose we want to prove that w is uniformly elliptic.
H a d-generator finite group. We need to *Assume* :

♡ $w(H) = \langle g_1, \ldots, g_m \rangle$ where $g_1, \ldots, g_m \in H_w$ and m depends only on w and d.

Uniformly elliptic words

Definition A group word w is uniformly elliptic if for each $d \in \mathbb{N}$ there exists $f \in \mathbb{N}$ such that $w(H) = H_w^{*f}$ for every d-generator finite group H.

Each uniformly elliptic word carries topological information about profinite groups: *w is uniformly elliptic if and only if $w(G)$ is closed in G for every f. g. profinite group G.*

Suppose we want to prove that w is uniformly elliptic.
H a d-generator finite group. We need to *Assume* :

$\heartsuit$ $w(H) = \langle g_1, \ldots, g_m \rangle$ where $g_1, \ldots, g_m \in H_w$ and m depends only on w and d.

Set $\mathcal{X} = H_w$ and $G = \langle \mathcal{X} \rangle = w(H)$. Choose $K \lhd G$ such that

$G = K \cdot \mathcal{X}^{*t}$
$K = [K, G]$ plus a technical condition ♣

(here t depends on w and d only).

Key Theorem *Let $G = \langle g_1, \ldots, g_m \rangle$ be a finite group and K a normal subgroup satisfying ♣. Then*

$$K = ([K, g_1] \cdot \ldots \cdot [K, g_m])^{*f}$$

where f depends only on m.

Since $g \in \mathcal{X} \implies [K, g] \subseteq \mathcal{X}^{*2}$ we can then deduce that

$$\begin{aligned} w(H) = G &= ([K, g_1] \cdot \ldots \cdot [K, g_m])^{*f} \cdot \mathcal{X}^{*t} \\ &= \mathcal{X}^{*(2f+t)} = H_w^{*(2f+t)}. \end{aligned}$$

Actually we couldn't quite prove this; and ♡ doesn't (a priori) hold for $w = x^q$. The fact that is does is a *consequence* of our theorem!

Set $\mathcal{X} = H_w$ and $G = \langle \mathcal{X} \rangle = w(H)$. Choose $K \lhd G$ such that

$G = K \cdot \mathcal{X}^{*t}$
$K = [K, G]$ plus a technical condition ♣

(here t depends on w and d only).

Key Theorem *Let $G = \langle g_1, \ldots, g_m \rangle$ be a finite group and K a normal subgroup satisfying ♣. Then*

$$K = ([K, g_1] \cdot \ldots \cdot [K, g_m])^{*f}$$

where f depends only on m.

Since $g \in \mathcal{X} \implies [K, g] \subseteq \mathcal{X}^{*2}$ we can then deduce that

$$w(H) = G = ([K, g_1] \cdot \ldots \cdot [K, g_m])^{*f} \cdot \mathcal{X}^{*t} = \mathcal{X}^{*(2f+t)} = H_w^{*(2f+t)}.$$

Actually we couldn't quite prove this; and ♡ doesn't (a priori) hold for $w = x^q$. The fact that is does is a *consequence* of our theorem!

Set $\mathcal{X} = H_w$ and $G = \langle \mathcal{X} \rangle = w(H)$. Choose $K \lhd G$ such that

$G = K \cdot \mathcal{X}^{*t}$
$K = [K, G]$ plus a technical condition ♣

(here t depends on w and d only).

Key Theorem *Let $G = \langle g_1, \ldots, g_m \rangle$ be a finite group and K a normal subgroup satisfying ♣. Then*

$$K = ([K, g_1] \cdot \ldots \cdot [K, g_m])^{*f}$$

where f depends only on m.

Since $g \in \mathcal{X} \implies [K, g] \subseteq \mathcal{X}^{*2}$ we can then deduce that

$$w(H) = G = ([K, g_1] \cdot \ldots \cdot [K, g_m])^{*f} \cdot \mathcal{X}^{*t}$$
$$= \mathcal{X}^{*(2f+t)} = H_w^{*(2f+t)}.$$

Actually we couldn't quite prove this; and ♡ doesn't (a priori) hold for $w = x^q$. The fact that is does is a *consequence* of our theorem!

Set $\mathcal{X} = H_w$ and $G = \langle \mathcal{X} \rangle = w(H)$. Choose $K \lhd G$ such that

$G = K \cdot \mathcal{X}^{*t}$
$K = [K, G]$ plus a technical condition ♣

(here t depends on w and d only).

Key Theorem *Let $G = \langle g_1, \dots, g_m \rangle$ be a finite group and K a normal subgroup satisfying ♣. Then*

$$K = ([K, g_1] \cdot \ldots \cdot [K, g_m])^{*f}$$

where f depends only on m.

Since $g \in \mathcal{X} \implies [K, g] \subseteq \mathcal{X}^{*2}$ we can then deduce that

$$w(H) = G = ([K, g_1] \cdot \ldots \cdot [K, g_m])^{*f} \cdot \mathcal{X}^{*t}$$
$$= \mathcal{X}^{*(2f+t)} = H_w^{*(2f+t)}.$$

Actually we couldn't quite prove this; and ♡ doesn't (a priori) hold for $w = x^q$. The fact that is does is a *consequence* of our theorem!

Proof of the Key Theorem - rough idea

Solve an equation by successive approximations (à la *Hensel's Lemma*):

$$h = \prod_{i=1}^{f} [x_{i1}, g_1] \dots [x_{im}, g_m] := \Phi(\mathbf{x}) \qquad (*)$$

Constant: $h \in K$
Parameters: $g_1, \dots, g_m$
Unknowns: $x_{ij} \in K$
Pick $N \lhd G$ minimal subject to

$$K \geq N = [N, G] > 1.$$

Assume inductively that we've found $u_{ij} \in K$ such that

$$h = \Phi(\mathbf{u}) \cdot \varepsilon$$

with 'error term' $\varepsilon \in N$. Seek $y_{ij} \in N$ such that $(*)$ holds with $x_{ij} = y_{ij} u_{ij}$.

Proof of the Key Theorem - rough idea

Solve an equation by successive approximations (à la *Hensel's Lemma*):

$$h = \prod_{i=1}^{f} [x_{i1}, g_1] \dots [x_{im}, g_m] := \Phi(\mathbf{x}) \qquad (*)$$

Constant: $h \in K$
Parameters: $g_1, \dots, g_m$
Unknowns: $x_{ij} \in K$
Pick $N \lhd G$ minimal subject to

$$K \geq N = [N, G] > 1.$$

Assume inductively that we've found $u_{ij} \in K$ such that

$$h = \Phi(\mathbf{u}) \cdot \varepsilon$$

with 'error term' $\varepsilon \in N$. Seek $y_{ij} \in N$ such that $(*)$ holds with $x_{ij} = y_{ij} u_{ij}$.

Proof of the Key Theorem - rough idea

Solve an equation by successive approximations (à la *Hensel's Lemma*):

$$h = \prod_{i=1}^{f} [x_{i1}, g_1] \ldots [x_{im}, g_m] := \Phi(\mathbf{x}) \qquad (*)$$

Constant: $h \in K$
Parameters: $g_1, \ldots, g_m$
Unknowns: $x_{ij} \in K$
Pick $N \lhd G$ minimal subject to

$$K \geq N = [N, G] > 1.$$

Assume inductively that we've found $u_{ij} \in K$ such that

$$h = \Phi(\mathbf{u}) \cdot \varepsilon$$

with 'error term' $\varepsilon \in N$. Seek $y_{ij} \in N$ such that $(*)$ holds with $x_{ij} = y_{ij} u_{ij}$.

Equivalently: solve

$$\varepsilon = \Phi'_{\mathbf{u}}(\mathbf{y}),$$

an equation in N with operators from G.

Case 1: N is a small nilpotent group. Uses linear and 'quadratic' algebra over finite fields.

Case 2: N is a direct product of isomorphic simple groups. Reduces to solving many equations in *one finite simple group* (with operators).

In fact to make induction work we need to show that the equations have *many* solutions. Ultimately it comes down to arithmetic in finite fields – in case 2, **CFSG** tells us that (nearly always) we're dealing with a matrix group over some $\mathbb{F}_q$.

Equivalently: solve

$$\varepsilon = \Phi'_{\mathbf{u}}(\mathbf{y}),$$

an equation in N with operators from G.

Case 1: N is a small nilpotent group. Uses linear and 'quadratic' algebra over finite fields.

Case 2: N is a direct product of isomorphic simple groups. Reduces to solving many equations in *one finite simple group* (with operators).

In fact to make induction work we need to show that the equations have *many* solutions. Ultimately it comes down to arithmetic in finite fields – in case 2, **CFSG** tells us that (nearly always) we're dealing with a matrix group over some $\mathbb{F}_q$.

Equivalently: solve

$$\varepsilon = \Phi'_{\mathbf{u}}(\mathbf{y}),$$

an equation in N with operators from G.

Case 1: N is a small nilpotent group. Uses linear and 'quadratic' algebra over finite fields.

Case 2: N is a direct product of isomorphic simple groups. Reduces to solving many equations in *one finite simple group* (with operators).

In fact to make induction work we need to show that the equations have *many* solutions. Ultimately it comes down to arithmetic in finite fields – in case 2, **CFSG** tells us that (nearly always) we're dealing with a matrix group over some $\mathbb{F}_q$.

Equivalently: solve

$$\varepsilon = \Phi'_{\mathbf{u}}(\mathbf{y}),$$

an equation in N with operators from G.

Case 1: N is a small nilpotent group. Uses linear and 'quadratic' algebra over finite fields.

Case 2: N is a direct product of isomorphic simple groups. Reduces to solving many equations in *one finite simple group* (with operators).

In fact to make induction work we need to show that the equations have *many* solutions. Ultimately it comes down to arithmetic in finite fields – in case 2, **CFSG** tells us that (nearly always) we're dealing with a matrix group over some $\mathbb{F}_q$.

Which words are uniformly elliptic?

1) 'Simple commutators'

$[x, y],\ [x_1, x_2, \ldots, x_c] = [[x_1, x_2, \ldots, x_{c-1}], x_c]\ (c > 2)$

2)'Non-commutator words': thinking of $w = w(x_1, \ldots, x_k)$ as an element of the free group F on $x_1, \ldots, x_k$, say w is a *non-commutator word* if $w \notin F' = [F, F]$.

(1) can be deduced from the Key Theorem. (2) follows from Theorem NS: if w is a non-commutator word then

$$w = x_1^{e_1} \ldots x_k^{e_k} v$$

where $v \in F'$ and $e_j \neq 0$ for some j. Now let G be a f.g. profinite group, and put $q = e_j$. Then

$$w(G) \geq G^q;$$

as G^q is open in G, so is $w(G)$.

Which words are uniformly elliptic?

1) 'Simple commutators'

$[x, y], \; [x_1, x_2, \ldots, x_c] = [[x_1, x_2, \ldots, x_{c-1}], x_c] \; (c > 2)$

2)'Non-commutator words': thinking of $w = w(x_1, \ldots, x_k)$ as an element of the free group F on $x_1, \ldots, x_k$, say w is a *non-commutator word* if $w \notin F' = [F, F]$.

(1) can be deduced from the Key Theorem. (2) follows from Theorem NS: if w is a non-commutator word then

$$w = x_1^{e_1} \ldots x_k^{e_k} v$$

where $v \in F'$ and $e_j \neq 0$ for some j. Now let G be a f.g. profinite group, and put $q = e_j$. Then

$$w(G) \geq G^q;$$

as G^q is open in G, so is $w(G)$.

Which words are uniformly elliptic?

1) ‘Simple commutators’

$$[x, y], \ [x_1, x_2, \ldots, x_c] = [[x_1, x_2, \ldots, x_{c-1}], x_c] \ (c > 2)$$

2)‘Non-commutator words’: thinking of $w = w(x_1, \ldots, x_k)$ as an element of the free group F on $x_1, \ldots, x_k$, say w is a *non-commutator word* if $w \notin F' = [F, F]$.

(1) can be deduced from the Key Theorem. (2) follows from Theorem NS: if w is a non-commutator word then

$$w = x_1^{e_1} \ldots x_k^{e_k} v$$

where $v \in F'$ and $e_j \neq 0$ for some j. Now let G be a f.g. profinite group, and put $q = e_j$. Then

$$w(G) \geq G^q;$$

as G^q is open in G, so is $w(G)$.

Maybe *all* words are uniformly elliptic? No!

Exercise Let V be a d-dimensional vector space and let $m < d/2$. Show that $V \wedge V$ contains elements that can't be expressed as

$$\sum_{i=1}^{m} u_i \wedge v_i.$$

This implies that the word $[x, y]$ has width at least $d/2$ in the finite group $G = F/\gamma_3(F)F^p$ where F is free of rank d.
Let $H = G \rtimes \langle t \rangle$ where t (of order d) permutes the d generators of G cyclically.
Then $\mathrm{d}(H) = 2$, but

the word $\delta_2 = [[x, y], [z, t]]$ has width at least $d/2$ in H.

Maybe *all* words are uniformly elliptic? No!

Exercise Let V be a d-dimensional vector space and let $m < d/2$. Show that $V \wedge V$ contains elements that can't be expressed as

$$\sum_{i=1}^{m} u_i \wedge v_i.$$

This implies that the word $[x, y]$ has width at least $d/2$ in the finite group $G = F/\gamma_3(F)F^p$ where F is free of rank d.
Let $H = G \rtimes \langle t \rangle$ where t (of order d) permutes the d generators of G cyclically.
Then $\mathrm{d}(H) = 2$, but

the word $\delta_2 = [[x, y], [z, t]]$ has width at least $d/2$ in H.

Maybe *all* words are uniformly elliptic? No!

Exercise Let V be a d-dimensional vector space and let $m < d/2$. Show that $V \wedge V$ contains elements that can't be expressed as

$$\sum_{i=1}^{m} u_i \wedge v_i.$$

This implies that the word $[x, y]$ has width at least $d/2$ in the finite group $G = F/\gamma_3(F)F^p$ where F is free of rank d.

Let $H = G \rtimes \langle t \rangle$ where t (of order d) permutes the d generators of G cyclically.

Then $\mathrm{d}(H) = 2$, but

the word $\delta_2 = [[x, y], [z, t]]$ has width at least $d/2$ in H.

Maybe *all* words are uniformly elliptic? No!

Exercise Let V be a d-dimensional vector space and let $m < d/2$. Show that $V \wedge V$ contains elements that can't be expressed as

$$\sum_{i=1}^{m} u_i \wedge v_i .$$

This implies that the word $[x, y]$ has width at least $d/2$ in the finite group $G = F/\gamma_3(F)F^p$ where F is free of rank d.
Let $H = G \rtimes \langle t \rangle$ where t (of order d) permutes the d generators of G cyclically.
Then $\mathrm{d}(H) = 2$, but

the word $\delta_2 = [[x, y], [z, t]]$ has width at least $d/2$ in H.

Maybe *all* words are uniformly elliptic? No!

Exercise Let V be a d-dimensional vector space and let $m < d/2$. Show that $V \wedge V$ contains elements that can't be expressed as

$$\sum_{i=1}^{m} u_i \wedge v_i.$$

This implies that the word $[x, y]$ has width at least $d/2$ in the finite group $G = F/\gamma_3(F)F^p$ where F is free of rank d.
Let $H = G \rtimes \langle t \rangle$ where t (of order d) permutes the d generators of G cyclically.
Then $\mathrm{d}(H) = 2$, but

the word $\delta_2 = [[x, y], [z, t]]$ has width at least $d/2$ in H.

As d is arbitrary it follows that δ_2 is *not* uniformly elliptic (even in finite p-groups, if we choose d to range over powers of p).

Jaikin's Theorem Let p be a prime and w a non-trivial word. Then $w(G)$ is closed in G for every finitely generated pro-p group G if and only if

$$w \notin F''(F')^p. \qquad (\mathrm{J}(p))$$

In general, $\mathrm{J}(p)$ for every prime p is a *necessary* condition for w to be u.e.

Main problem *Is it sufficient?*

As d is arbitrary it follows that δ_2 is *not* uniformly elliptic (even in finite p-groups, if we choose d to range over powers of p).

Jaikin's Theorem Let p be a prime and w a non-trivial word. Then $w(G)$ is closed in G for every finitely generated pro-p group G if and only if

$$w \notin F''(F')^p. \qquad (\mathrm{J}(p))$$

In general, J(p) for every prime p is a *necessary* condition for w to be u.e.

Main problem *Is it sufficient?*

As d is arbitrary it follows that δ_2 is *not* uniformly elliptic (even in finite p-groups, if we choose d to range over powers of p).

Jaikin's Theorem Let p be a prime and w a non-trivial word. Then $w(G)$ is closed in G for every finitely generated pro-p group G if and only if

$$w \notin F''(F')^p. \quad (\mathrm{J}(p))$$

In general, $\mathrm{J}(p)$ for every prime p is a *necessary* condition for w to be u.e.

Main problem *Is it sufficient?*

some references

D. Segal, *Words: notes on verbal width in groups.*
LMS Lect. notes **361**, CUP, Cambridge, 2009.

N. Nikolov and D. Segal, Finite index subgroups in profinite groups,
C. R. Acad, Sci. Paris, Ser. I **337** (2003), 303-308.

N. Nikolov and D. Segal, On finitely generated profinite groups,
I: strong completeness and uniform bounds;
II: products in quasisimple groups,
Annals of Math. **165** (2007), 171-238, 239-273.

N. Nikolov and D. Segal, Powers in finite groups,
arXiv.math.GR: 0909.4639.

A. Jaikin-Zapirain, On the verbal width of finitely generated pro-p groups,
Revista Mat. Iberoamericana **24** (2008), 617-630.

D. Segal, On verbal subgroups of adelic groups,
J. Algebra, in press [**doi:**10.1016/j.jalgebra.2009.03.024]

N. Nikolov, Strange images of profinite groups,
arXiv:0901.0244

D. Segal, Words,
to appear in *Proceedings of Groups St Andrews/Bath 2009*.