On the lattice of subgroups of free groups[1]

Pascal Weil

LaBRI, Université de Bordeaux and CNRS

Algebraic Cryptography Center
Stevens Institute of Technology, October 2008

[1] joint work with A. Miasnikov (McGill), E. Ventura (Barcelona), P. Silva (Porto)

Subgroups in free groups

- We consider a free group $F = F(A)$ – where A is a finite alphabet ($|A| \geq 2$)

Subgroups in free groups

- We consider a free group $F = F(A)$ – where A is a finite alphabet ($|A| \geq 2$)
- and the lattice of its finitely generated subgroups, $H \leq_{\text{fg}} F$

Subgroups in free groups

- We consider a free group $F = F(A)$ – where A is a finite alphabet ($|A| \geq 2$)
- and the lattice of its finitely generated subgroups, $H \leq_{\text{fg}} F$
- Every subgroup of F is free

Subgroups in free groups

- We consider a free group $F = F(A)$ – where A is a finite alphabet ($|A| \geq 2$)
- and the lattice of its finitely generated subgroups, $H \leq_{\text{fg}} F$
- Every subgroup of F is free
- but a free group may sit in many different ways in another

Subgroups in free groups

- We consider a free group $F = F(A)$ – where A is a finite alphabet ($|A| \geq 2$)
- and the lattice of its finitely generated subgroups, $H \leq_{\text{fg}} F$
- Every subgroup of F is free
- but a free group may sit in many different ways in another
- e.g. as a finite index subgroup, $H \leq_{\text{fi}} F$, $F = Hg_1 \cup \cdots \cup Hg_n$ – relates to finite group theory

Subgroups in free groups

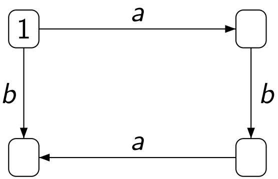
- We consider a free group $F = F(A)$ – where A is a finite alphabet ($|A| \geq 2$)
- and the lattice of its finitely generated subgroups, $H \leq_{\mathrm{fg}} F$
- Every subgroup of F is free
- but a free group may sit in many different ways in another
- e.g. as a finite index subgroup, $H \leq_{\mathrm{fi}} F$, $F = Hg_1 \cup \cdots \cup Hg_n$ – relates to finite group theory
- or as a free factor, $H \leq_{\mathrm{ff}} F$, every basis of H can be extended to a basis of F – looks closer to vector spaces

Representation of subgroups: Stallings graph

- $H = \langle abab^{-1}, aba^{-1}b^{-1}, aba^3b^{-1} \rangle$

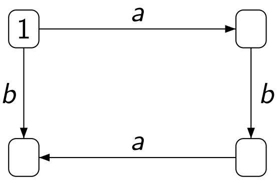
Representation of subgroups: Stallings graph

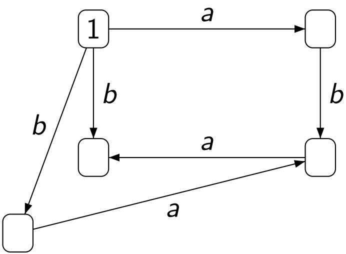
- $H = \langle abab^{-1}, aba^{-1}b^{-1}, aba^3b^{-1} \rangle$



Representation of subgroups: Stallings graph

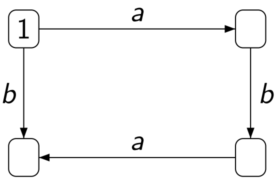
- $H = \langle abab^{-1}, aba^{-1}b^{-1}, aba^3b^{-1} \rangle$

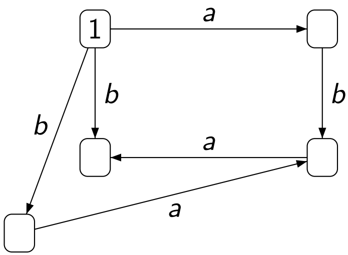


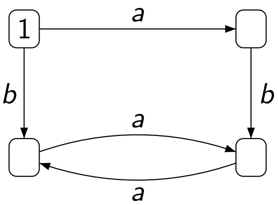


Representation of subgroups: Stallings graph

- $H = \langle abab^{-1}, aba^{-1}b^{-1}, aba^3b^{-1}\rangle$

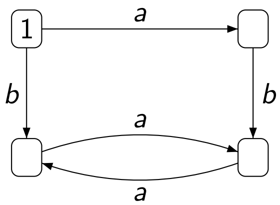






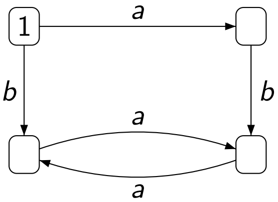
Representation of subgroups: Stallings graph

- $H = \langle abab^{-1}, aba^{-1}b^{-1}, aba^3b^{-1}\rangle$
- Stallings graph: finite, connected, deterministic and co-deterministic, with a distinguished vertex 1; every vertex $v \neq 1$ has valency at least 2 (Stallings 1983)



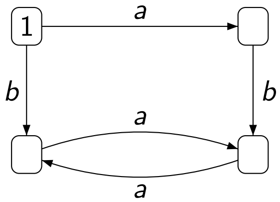
Representation of subgroups: Stallings graph

- $H = \langle abab^{-1}, aba^{-1}b^{-1}, aba^3b^{-1}\rangle$
- Stallings graph: finite, connected, deterministic and co-deterministic, with a distinguished vertex 1; every vertex $v \neq 1$ has valency at least 2 (Stallings 1983)
- $H =$ all reduced words that read from 1 to 1



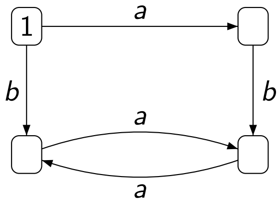
Representation of subgroups: Stallings graph

- $H = \langle abab^{-1}, aba^{-1}b^{-1}, aba^3b^{-1} \rangle$
- this graph (automaton) is denoted by $\Gamma(H)$, or $\Gamma_A(H)$. It characterizes H, not the generating set



Representation of subgroups: Stallings graph

- $H = \langle abab^{-1}, aba^{-1}b^{-1}, aba^3b^{-1} \rangle$
- this graph (automaton) is denoted by $\Gamma(H)$, or $\Gamma_A(H)$. It characterizes H, not the generating set
- $\Gamma(H)$ is computable in $O(n \log^* n)$ (Touikan 2006)



Subgroups of subgroups

- $H \leq_{\text{fg}} K \leq_{\text{fg}} F$ if and only if there exists $\Gamma(H) \longrightarrow \Gamma(K)$, a labeled graph morphism mapping 1 to 1

Subgroups of subgroups

- $H \leq_{\text{fg}} K \leq_{\text{fg}} F$ if and only if there exists $\Gamma(H) \longrightarrow \Gamma(K)$, a labeled graph morphism mapping 1 to 1
- Why? because a reduced word is in H iff it labels a loop at 1 in $\Gamma(H)$

Subgroups of subgroups

- $H \leq_{\text{fg}} K \leq_{\text{fg}} F$ if and only if there exists $\Gamma(H) \longrightarrow \Gamma(K)$, a labeled graph morphism mapping 1 to 1
- Why? because a reduced word is in H iff it labels a loop at 1 in $\Gamma(H)$
- If $H \leq_{\text{fg}} K$, then this graph morphism is unique, written φ_H^K

Subgroups of subgroups

- $H \leq_{\mathrm{fg}} K \leq_{\mathrm{fg}} F$ if and only if there exists $\Gamma(H) \longrightarrow \Gamma(K)$, a labeled graph morphism mapping 1 to 1
- Why? because a reduced word is in H iff it labels a loop at 1 in $\Gamma(H)$
- If $H \leq_{\mathrm{fg}} K$, then this graph morphism is unique, written φ_H^K
- If φ_H^K is one-to-one (on vertices), i.e. $\Gamma(H)$ is a subgraph of $\Gamma(K)$, then $H \leq_{\mathrm{ff}} K$

Subgroups of subgroups

- $H \leq_{\text{fg}} K \leq_{\text{fg}} F$ if and only if there exists $\Gamma(H) \longrightarrow \Gamma(K)$, a labeled graph morphism mapping 1 to 1
- Why? because a reduced word is in H iff it labels a loop at 1 in $\Gamma(H)$
- If $H \leq_{\text{fg}} K$, then this graph morphism is unique, written φ_H^K
- If φ_H^K is one-to-one (on vertices), i.e. $\Gamma(H)$ is a subgraph of $\Gamma(K)$, then $H \leq_{\text{ff}} K$
- If φ_H^K is onto (on vertices and edges), we say that K is an *overgroup* of H (or *principal quotient*)

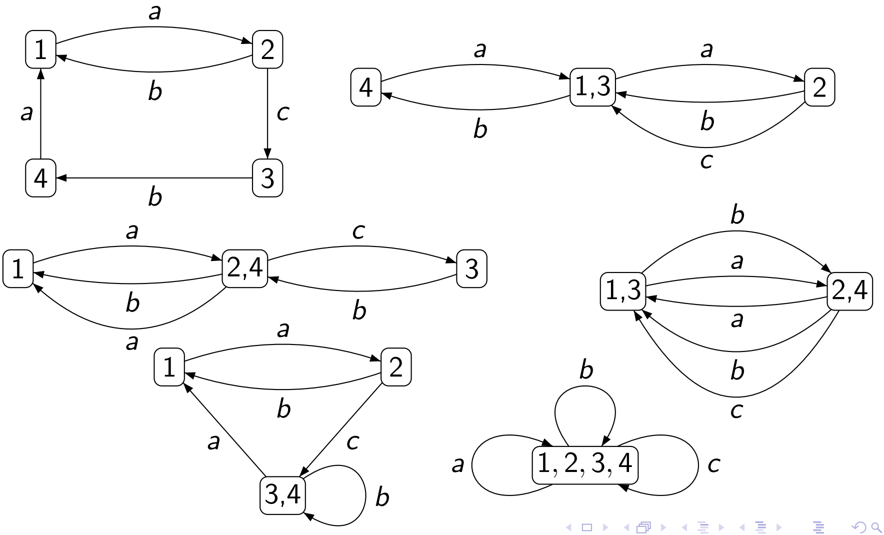
Subgroups of subgroups

- $H \leq_{\text{fg}} K \leq_{\text{fg}} F$ if and only if there exists $\Gamma(H) \longrightarrow \Gamma(K)$, a labeled graph morphism mapping 1 to 1
- Why? because a reduced word is in H iff it labels a loop at 1 in $\Gamma(H)$
- If $H \leq_{\text{fg}} K$, then this graph morphism is unique, written φ_H^K
- If φ_H^K is one-to-one (on vertices), i.e. $\Gamma(H)$ is a subgraph of $\Gamma(K)$, then $H \leq_{\text{ff}} K$
- If φ_H^K is onto (on vertices and edges), we say that K is an *overgroup* of H (or *principal quotient*)
- $\mathcal{O}_A(H)$, the set of overgroups of H, is a finite lattice. Depends on A

Subgroups of subgroups

- $H \leq_{\rm fg} K \leq_{\rm fg} F$ if and only if there exists $\Gamma(H) \longrightarrow \Gamma(K)$, a labeled graph morphism mapping 1 to 1
- Why? because a reduced word is in H iff it labels a loop at 1 in $\Gamma(H)$
- If $H \leq_{\rm fg} K$, then this graph morphism is unique, written φ_H^K
- If φ_H^K is one-to-one (on vertices), i.e. $\Gamma(H)$ is a subgraph of $\Gamma(K)$, then $H \leq_{\rm ff} K$
- If φ_H^K is onto (on vertices and edges), we say that K is an *overgroup* of H (or *principal quotient*)
- $\mathcal{O}_A(H)$, the set of overgroups of H, is a finite lattice. Depends on A
- Computable. May have exponential size.

Example: the six quotients of $\Gamma_A(\langle ab, acba \rangle)$



Takahasi's theorem

Theorem (Takahasi 1951)

Given $H \leq_{\text{fg}} F$, there exists a finite and computable collection $K_1, \ldots, K_n$ of extensions of H, such that whenever $H \leq K \leq F$, then $H \leq K_i \leq_{\text{ff}} K$ for some i.

Takahasi's theorem

Theorem (Takahasi 1951)

Given $H \leq_{\text{fg}} F$, there exists a finite and computable collection $K_1, \ldots, K_n$ of extensions of H, such that whenever $H \leq K \leq F$, then $H \leq K_i \leq_{\text{ff}} K$ for some i.

- Since $H \leq K$, consider $\varphi_H^K \colon \Gamma(H) \longrightarrow \Gamma(K)$

Takahasi's theorem

Theorem (Takahasi 1951)

Given $H \leq_{\text{fg}} F$, there exists a finite and computable collection $K_1, \ldots, K_n$ of extensions of H, such that whenever $H \leq K \leq F$, then $H \leq K_i \leq_{\text{ff}} K$ for some i.

- Since $H \leq K$, consider $\varphi_H^K \colon \Gamma(H) \longrightarrow \Gamma(K)$
- The range of φ_H^K is a subgraph of $\Gamma(K)$:

Takahasi's theorem

Theorem (Takahasi 1951)

Given $H \leq_{\text{fg}} F$, there exists a finite and computable collection $K_1, \ldots, K_n$ of extensions of H, such that whenever $H \leq K \leq F$, then $H \leq K_i \leq_{\text{ff}} K$ for some i.

- Since $H \leq K$, consider $\varphi_H^K \colon \Gamma(H) \longrightarrow \Gamma(K)$
- The range of φ_H^K is a subgraph of $\Gamma(K)$:
- let L such that $\Gamma(L) = \varphi_H^K(\Gamma(H))$: then $L \in \mathcal{O}_A(H)$ and $L \leq_{\text{ff}} K$.

Takahasi's theorem

Theorem (Takahasi 1951)

Given $H \leq_{\text{fg}} F$, there exists a finite and computable collection $K_1, \ldots, K_n$ of extensions of H, such that whenever $H \leq K \leq F$, then $H \leq K_i \leq_{\text{ff}} K$ for some i.

- Since $H \leq K$, consider $\varphi_H^K\colon \Gamma(H) \longrightarrow \Gamma(K)$
- The range of φ_H^K is a subgraph of $\Gamma(K)$:
- let L such that $\Gamma(L) = \varphi_H^K(\Gamma(H))$: then $L \in \mathcal{O}_A(H)$ and $L \leq_{\text{ff}} K$.
- End of proof! $\mathcal{O}_A(H)$ will do as a Takahasi family for H

Takahasi's theorem

Theorem (Takahasi 1951)

Given $H \leq_{\mathrm{fg}} F$, there exists a finite and computable collection $K_1, \ldots, K_n$ of extensions of H, such that whenever $H \leq K \leq F$, then $H \leq K_i \leq_{\mathrm{ff}} K$ for some i.

- Since $H \leq K$, consider $\varphi_H^K \colon \Gamma(H) \longrightarrow \Gamma(K)$
- The range of φ_H^K is a subgraph of $\Gamma(K)$:
- let L such that $\Gamma(L) = \varphi_H^K(\Gamma(H))$: then $L \in \mathcal{O}_A(H)$ and $L \leq_{\mathrm{ff}} K$.
- End of proof! $\mathcal{O}_A(H)$ will do as a Takahasi family for H
- See Ventura 1997, Margolis, Sapir, Weil 2001, Kapovich, Miasnikov 2002

Algebraic extensions

- Say that K is an *algebraic* extension of H, $H \leq_{\text{alg}} K$, if H does not sit in a proper free factor of K: $H \leq L \leq_{\text{ff}} K$ implies $L = K$ (Kapovich, Miasnikov)

Algebraic extensions

- Say that K is an *algebraic* extension of H, $H \leq_{\text{alg}} K$, if H does not sit in a proper free factor of K: $H \leq L \leq_{\text{ff}} K$ implies $L = K$ (Kapovich, Miasnikov)
- If $H \leq_{\text{alg}} K$, then $H \leq K_i \leq_{\text{ff}} K$ for some overgroup K_i: $\text{AE}(H) \subseteq \mathcal{O}_A(H)$

Algebraic extensions

- Say that K is an *algebraic* extension of H, $H \leq_{\text{alg}} K$, if H does not sit in a proper free factor of K: $H \leq L \leq_{\text{ff}} K$ implies $L = K$ (Kapovich, Miasnikov)
- If $H \leq_{\text{alg}} K$, then $H \leq K_i \leq_{\text{ff}} K$ for some overgroup K_i: $\text{AE}(H) \subseteq \mathcal{O}_A(H)$
- $\text{AE}(H)$ is finite; it is the minimum Takahasi family for H; it is independent of the choice of A

Algebraic extensions

- Say that K is an *algebraic* extension of H, $H \leq_{\text{alg}} K$, if H does not sit in a proper free factor of K: $H \leq L \leq_{\text{ff}} K$ implies $L = K$ (Kapovich, Miasnikov)
- If $H \leq_{\text{alg}} K$, then $H \leq K_i \leq_{\text{ff}} K$ for some overgroup K_i: $\text{AE}(H) \subseteq \mathcal{O}_A(H)$
- $\text{AE}(H)$ is finite; it is the minimum Takahasi family for H; it is independent of the choice of A
- Question: Is $\text{AE}(H) = \bigcap_A \mathcal{O}_A(H)$?

AE(H) is computable

- *Recall:* $H \leq_{\text{alg}} K$ *if* H *does not sit in a proper free factor of* K*:* $H \leq L \leq_{\text{ff}} K$ *implies* $L = K$

AE(H) is computable

- *Recall: $H \leq_{\text{alg}} K$ if H does not sit in a proper free factor of K: $H \leq L \leq_{\text{ff}} K$ implies $L = K$*
- AE(H) is computable: compute $\mathcal{O}_A(H)$; if $K, K' \in \mathcal{O}_A(H)$ and $K \leq_{\text{ff}} K'$, delete K'

AE(H) is computable

- *Recall:* $H \leq_{\text{alg}} K$ *if* H *does not sit in a proper free factor of* K*:* $H \leq L \leq_{\text{ff}} K$ *implies* $L = K$
- AE(H) is computable: compute $\mathcal{O}_A(H)$; if $K, K' \in \mathcal{O}_A(H)$ and $K \leq_{\text{ff}} K'$, delete K'
- If $H \leq_{\text{fi}} F$, $\text{AE}(H) = \mathcal{O}_A(H)$ is the lattice of all extensions of H

AE(H) is computable

- *Recall: $H \leq_{\text{alg}} K$ if H does not sit in a proper free factor of K: $H \leq L \leq_{\text{ff}} K$ implies $L = K$*
- AE(H) is computable: compute $\mathcal{O}_A(H)$; if $K, K' \in \mathcal{O}_A(H)$ and $K \leq_{\text{ff}} K'$, delete K'
- If $H \leq_{\text{fi}} F$, AE(H) $= \mathcal{O}_A(H)$ is the lattice of all extensions of H
- In our example, $H = \langle ab, acba \rangle$, $|\mathcal{O}_A(H)| = 6$ but AE(H) $= \{H\}$.

AE(H) is computable

- *Recall:* $H \leq_{\text{alg}} K$ *if* H *does not sit in a proper free factor of* K*:* $H \leq L \leq_{\text{ff}} K$ *implies* $L = K$
- AE(H) is computable: compute $\mathcal{O}_A(H)$; if $K, K' \in \mathcal{O}_A(H)$ and $K \leq_{\text{ff}} K'$, delete K'
- If $H \leq_{\text{fi}} F$, $\text{AE}(H) = \mathcal{O}_A(H)$ is the lattice of all extensions of H
- In our example, $H = \langle ab, acba \rangle$, $|\mathcal{O}_A(H)| = 6$ but $\text{AE}(H) = \{H\}$.
- $H \leq_{\text{ff}} F$ if and only if $\text{AE}(H) = \{H\}$

algebraic extensions vs. free multiples: dual notions

Let $H \leq K \leq L$

- If $H \leq_{\text{ff}} K \leq_{\text{ff}} L$, then $H \leq_{\text{ff}} L$; $H \leq_{\text{alg}} K \leq_{\text{alg}} L$, then $H \leq_{\text{alg}} L$
- If $H \leq_{\text{ff}} L$, then $H \leq_{\text{ff}} K$; if $H \leq_{\text{alg}} L$, then $K \leq_{\text{alg}} L$
- If $H \leq_{\text{ff}} K$ and $H \leq_{\text{ff}} K'$, then $H \leq_{\text{ff}} K \cap K'$; if $H \leq_{\text{alg}} K$ and $H \leq_{\text{alg}} K'$, then $H \leq_{\text{alg}} \langle K, K' \rangle$

algebraic extensions vs. free multiples: dual notions

Let $H \leq K \leq L$

- If $H \leq_{\text{ff}} K \leq_{\text{ff}} L$, then $H \leq_{\text{ff}} L$; $H \leq_{\text{alg}} K \leq_{\text{alg}} L$, then $H \leq_{\text{alg}} L$
- If $H \leq_{\text{ff}} L$, then $H \leq_{\text{ff}} K$; if $H \leq_{\text{alg}} L$, then $K \leq_{\text{alg}} L$
- If $H \leq_{\text{ff}} K$ and $H \leq_{\text{ff}} K'$, then $H \leq_{\text{ff}} K \cap K'$; if $H \leq_{\text{alg}} K$ and $H \leq_{\text{alg}} K'$, then $H \leq_{\text{alg}} \langle K, K' \rangle$
- $\text{AE}(H)$ admits a greatest element: the *algebraic closure* of H, the least free factor $\text{cl}(H)$ of F containing H

algebraic extensions vs. free multiples: dual notions

Let $H \leq K \leq L$

- If $H \leq_{\rm ff} K \leq_{\rm ff} L$, then $H \leq_{\rm ff} L$; $H \leq_{\rm alg} K \leq_{\rm alg} L$, then $H \leq_{\rm alg} L$
- If $H \leq_{\rm ff} L$, then $H \leq_{\rm ff} K$; if $H \leq_{\rm alg} L$, then $K \leq_{\rm alg} L$
- If $H \leq_{\rm ff} K$ and $H \leq_{\rm ff} K'$, then $H \leq_{\rm ff} K \cap K'$; if $H \leq_{\rm alg} K$ and $H \leq_{\rm alg} K'$, then $H \leq_{\rm alg} \langle K, K' \rangle$
- $\mathrm{AE}(H)$ admits a greatest element: the *algebraic closure* of H, the least free factor $\mathrm{cl}(H)$ of F containing H
- If $H \leq_{\rm fg} K$, there is also an algebraic closure of H in K, $\mathrm{cl}_K(H)$

algebraic extensions vs. free multiples: dual notions

Let $H \leq K \leq L$

- If $H \leq_{\text{ff}} K \leq_{\text{ff}} L$, then $H \leq_{\text{ff}} L$; $H \leq_{\text{alg}} K \leq_{\text{alg}} L$, then $H \leq_{\text{alg}} L$
- If $H \leq_{\text{ff}} L$, then $H \leq_{\text{ff}} K$; if $H \leq_{\text{alg}} L$, then $K \leq_{\text{alg}} L$
- If $H \leq_{\text{ff}} K$ and $H \leq_{\text{ff}} K'$, then $H \leq_{\text{ff}} K \cap K'$; if $H \leq_{\text{alg}} K$ and $H \leq_{\text{alg}} K'$, then $H \leq_{\text{alg}} \langle K, K' \rangle$
- $\text{AE}(H)$ admits a greatest element: the *algebraic closure* of H, the least free factor $\text{cl}(H)$ of F containing H
- If $H \leq_{\text{fg}} K$, there is also an algebraic closure of H in K, $\text{cl}_K(H)$
- A characterization: let $\varphi \in \text{Aut}(F)$ such that $\varphi(H)$ has minimum size, and let $B \subseteq A$ be the set of letters in $\varphi(H)$: then $\text{cl}(H) = \varphi^{-1}\langle B \rangle$ (Ventura 2009)

Malnormal and pure closures

- If a class of subgroups $\mathcal{P}$ is closed under finite intersection and free factors, then every $H \leq_{\text{fg}} F$ admits a $\mathcal{P}$-closure, which is an algebraic extension

Malnormal and pure closures

- If a class of subgroups $\mathcal{P}$ is closed under finite intersection and free factors, then every $H \leq_{\text{fg}} F$ admits a $\mathcal{P}$-closure, which is an algebraic extension
- This closure is computable if $\mathcal{P}$ is decidable

Malnormal and pure closures

- If a class of subgroups $\mathcal{P}$ is closed under finite intersection and free factors, then every $H \leq_{\mathrm{fg}} F$ admits a $\mathcal{P}$-closure, which is an algebraic extension
- This closure is computable if $\mathcal{P}$ is decidable
- H is *malnormal* if $x \notin H$ implies $H \cap H^x = 1$: the malnormal closure of H exists, it is an algebraic extension (in particular: it has finite rank) and it is computable

Malnormal and pure closures

- If a class of subgroups $\mathcal{P}$ is closed under finite intersection and free factors, then every $H \leq_{\text{fg}} F$ admits a $\mathcal{P}$-closure, which is an algebraic extension
- This closure is computable if $\mathcal{P}$ is decidable
- H is *malnormal* if $x \notin H$ implies $H \cap H^x = 1$: the malnormal closure of H exists, it is an algebraic extension (in particular: it has finite rank) and it is computable
- H is *pure* if $n \neq 0$ and $x^n \in H$ implies $x \in H$: same result as for malnormality

Pro-$\mathcal{V}$ closures

- Let $\mathcal{V}$ be a class of finite groups closed under sub, direct products and extensions: e.g. p-groups, solvable groups. Consider the pro-$\mathcal{V}$ topology on F

Pro-$\mathcal{V}$ closures

- Let $\mathcal{V}$ be a class of finite groups closed under sub, direct products and extensions: e.g. p-groups, solvable groups. Consider the pro-$\mathcal{V}$ topology on F
- H is closed in the pro-$\mathcal{V}$ topology if for all $x \notin H$, there exists $H \leq K \leq_{\text{fi}} F$ such that $x \notin K$ and $F/\bigcap H^x \in \mathcal{V}$

Pro-$\mathcal{V}$ closures

- Let $\mathcal{V}$ be a class of finite groups closed under sub, direct products and extensions: e.g. p-groups, solvable groups. Consider the pro-$\mathcal{V}$ topology on F
- H is closed in the pro-$\mathcal{V}$ topology if for all $x \notin H$, there exists $H \leq K \leq_{\text{fi}} F$ such that $x \notin K$ and $F/\bigcap H^x \in \mathcal{V}$
- The pro-$\mathcal{V}$ closure of H exists, is an algebraic extension, has finite rank. The pro-p closure is computable.

Pro-$\mathcal{V}$ closures

- Let $\mathcal{V}$ be a class of finite groups closed under sub, direct products and extensions: e.g. p-groups, solvable groups. Consider the pro-$\mathcal{V}$ topology on F
- H is closed in the pro-$\mathcal{V}$ topology if for all $x \notin H$, there exists $H \leq K \leq_{\text{fi}} F$ such that $x \notin K$ and $F/\bigcap H^x \in \mathcal{V}$
- The pro-$\mathcal{V}$ closure of H exists, is an algebraic extension, has finite rank. The pro-p closure is computable.
- The question is open for the pro-solvable closure...

e-algebraic extensions

- If $H \leq K$ is *elementary* (i.e. $K = \langle H, x\rangle$), then $H \leq_{\mathrm{alg}} K$ if $\mathrm{rank}(K) \leq \mathrm{rank}(H)$ and $H \leq_{\mathrm{ff}} K$ if $\mathrm{rank}(K) = \mathrm{rank}(H) + 1$

e-algebraic extensions

- If $H \leq K$ is *elementary* (i.e. $K = \langle H, x \rangle$), then $H \leq_{\mathrm{alg}} K$ if $\mathrm{rank}(K) \leq \mathrm{rank}(H)$ and $H \leq_{\mathrm{ff}} K$ if $\mathrm{rank}(K) = \mathrm{rank}(H) + 1$
- Say that $H \leq_{\mathrm{ealg}} K$ if $H \leq_{\mathrm{alg}} K_1 \leq_{\mathrm{alg}} \cdots \leq_{\mathrm{alg}} K_n \leq_{\mathrm{alg}} K$ and each extension is elementary; if $H \leq_{\mathrm{ealg}} K$, then $\mathrm{rank}(K) \leq \mathrm{rank}(H)$

e-algebraic extensions

- If $H \leq K$ is *elementary* (i.e. $K = \langle H, x\rangle$), then $H \leq_{\text{alg}} K$ if $\text{rank}(K) \leq \text{rank}(H)$ and $H \leq_{\text{ff}} K$ if $\text{rank}(K) = \text{rank}(H) + 1$
- Say that $H \leq_{\text{ealg}} K$ if $H \leq_{\text{alg}} K_1 \leq_{\text{alg}} \cdots \leq_{\text{alg}} K_n \leq_{\text{alg}} K$ and each extension is elementary; if $H \leq_{\text{ealg}} K$, then $\text{rank}(K) \leq \text{rank}(H)$
- If $H \leq_{\text{ealg}} K$ and $H \leq_{\text{ealg}} K'$, then $H \leq_{\text{ealg}} \langle K, K'\rangle$: H admits an elementary-algebraic closure, which may be smaller than its algebraic closure; it is computable

e-algebraic extensions

- If $H \leq K$ is *elementary* (i.e. $K = \langle H, x \rangle$), then $H \leq_{\text{alg}} K$ if $\text{rank}(K) \leq \text{rank}(H)$ and $H \leq_{\text{ff}} K$ if $\text{rank}(K) = \text{rank}(H) + 1$
- Say that $H \leq_{\text{ealg}} K$ if $H \leq_{\text{alg}} K_1 \leq_{\text{alg}} \cdots \leq_{\text{alg}} K_n \leq_{\text{alg}} K$ and each extension is elementary; if $H \leq_{\text{ealg}} K$, then $\text{rank}(K) \leq \text{rank}(H)$
- If $H \leq_{\text{ealg}} K$ and $H \leq_{\text{ealg}} K'$, then $H \leq_{\text{ealg}} \langle K, K' \rangle$: H admits an elementary-algebraic closure, which may be smaller than its algebraic closure; it is computable
- The malnormal and the pure closure of H are e-algebraic extensions: their rank is at most $\text{rank}(H)$

e-algebraic extensions

- If $H \leq K$ is *elementary* (i.e. $K = \langle H, x\rangle$), then $H \leq_{\text{alg}} K$ if $\text{rank}(K) \leq \text{rank}(H)$ and $H \leq_{\text{ff}} K$ if $\text{rank}(K) = \text{rank}(H) + 1$
- Say that $H \leq_{\text{ealg}} K$ if $H \leq_{\text{alg}} K_1 \leq_{\text{alg}} \cdots \leq_{\text{alg}} K_n \leq_{\text{alg}} K$ and each extension is elementary; if $H \leq_{\text{ealg}} K$, then $\text{rank}(K) \leq \text{rank}(H)$
- If $H \leq_{\text{ealg}} K$ and $H \leq_{\text{ealg}} K'$, then $H \leq_{\text{ealg}} \langle K, K'\rangle$: H admits an elementary-algebraic closure, which may be smaller than its algebraic closure; it is computable
- The malnormal and the pure closure of H are e-algebraic extensions: their rank is at most $\text{rank}(H)$
- The same inequality holds for the pro-$\mathcal{V}$ closure of H: is it an e-algebraic extension?

Finite index and covers

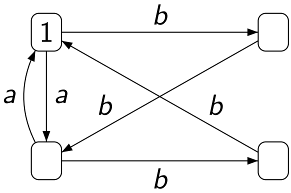
- Let $H \leq_{\text{fg}} K \leq_{\text{fg}} F$. Wlog, they are cyclically reduced (no vertex of degree 1)

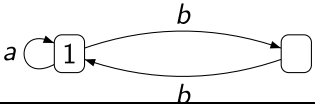
Finite index and covers

- Let $H \leq_{\text{fg}} K \leq_{\text{fg}} F$. Wlog, they are cyclically reduced (no vertex of degree 1)
- $H \leq_{\text{fi}} K$ if and only if $\Gamma(H) \longrightarrow \Gamma(K)$ is a cover: an onto morphism such that, for every edge $k \xrightarrow{a} k'$ in $\Gamma(K)$ and every pre-image h of k, there is an edge $h \xrightarrow{a} h'$ for some h' in $\Gamma(H)$

Finite index and covers

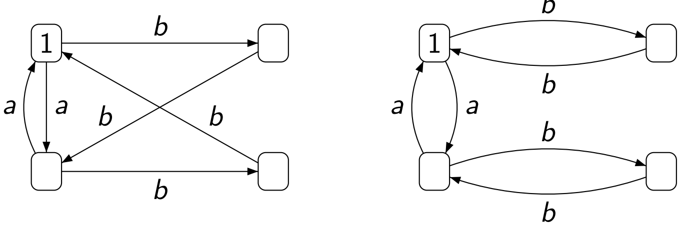
- Let $H \leq_{\rm fg} K \leq_{\rm fg} F$. Wlog, they are cyclically reduced (no vertex of degree 1)
- $H \leq_{\rm fi} K$ if and only if $\Gamma(H) \longrightarrow \Gamma(K)$ is a cover: an onto morphism such that, for every edge $k \xrightarrow{a} k'$ in $\Gamma(K)$ and every pre-image h of k, there is an edge $h \xrightarrow{a} h'$ for some h' in $\Gamma(H)$

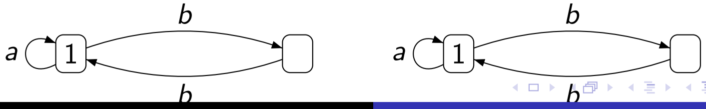




Finite index and covers

- Let $H \leq_{\text{fg}} K \leq_{\text{fg}} F$. Wlog, they are cyclically reduced (no vertex of degree 1)
- $H \leq_{\text{fi}} K$ if and only if $\Gamma(H) \longrightarrow \Gamma(K)$ is a cover: an onto morphism such that, for every edge $k \xrightarrow{a} k'$ in $\Gamma(K)$ and every pre-image h of k, there is an edge $h \xrightarrow{a} h'$ for some h' in $\Gamma(H)$





Simple remarks

- If $H \leq_{\text{fi}} L$ then $H \leq_{\text{fi}} K \leq_{\text{fi}} L$

Simple remarks

- If $H \leq_{\text{fi}} L$ then $H \leq_{\text{fi}} K \leq_{\text{fi}} L$
- If $H, K \leq_{\text{fi}} L$, then $H \cap K \leq_{\text{fi}} L$ (the pull-back of covers is a cover)

Simple remarks

- If $H \leq_{\text{fi}} L$ then $H \leq_{\text{fi}} K \leq_{\text{fi}} L$
- If $H, K \leq_{\text{fi}} L$, then $H \cap K \leq_{\text{fi}} L$ (the pull-back of covers is a cover)
- If $H \leq_{\text{fi}} K, L$, then $H \leq_{\text{fi}} \langle K, L\rangle$ (Greenberg, the push-out of covers is a cover)

Simple remarks

- If $H \leq_{\text{fi}} L$ then $H \leq_{\text{fi}} K \leq_{\text{fi}} L$
- If $H, K \leq_{\text{fi}} L$, then $H \cap K \leq_{\text{fi}} L$ (the pull-back of covers is a cover)
- If $H \leq_{\text{fi}} K, L$, then $H \leq_{\text{fi}} \langle K, L \rangle$ (Greenberg, the push-out of covers is a cover)
- If $H \leq L$, then $H \not\leq_{\text{fi}} L * L'$: every finite-index extension is algebraic

Simple remarks

- If $H \leq_{\text{fi}} L$ then $H \leq_{\text{fi}} K \leq_{\text{fi}} L$
- If $H, K \leq_{\text{fi}} L$, then $H \cap K \leq_{\text{fi}} L$ (the pull-back of covers is a cover)
- If $H \leq_{\text{fi}} K, L$, then $H \leq_{\text{fi}} \langle K, L \rangle$ (Greenberg, the push-out of covers is a cover)
- If $H \leq L$, then $H \not\leq_{\text{fi}} L * L'$: every finite-index extension is algebraic
- the lattice of finite-index extensions of H is finite and computable

Simple remarks

- If $H \leq_{\text{fi}} L$ then $H \leq_{\text{fi}} K \leq_{\text{fi}} L$
- If $H, K \leq_{\text{fi}} L$, then $H \cap K \leq_{\text{fi}} L$ (the pull-back of covers is a cover)
- If $H \leq_{\text{fi}} K, L$, then $H \leq_{\text{fi}} \langle K, L\rangle$ (Greenberg, the push-out of covers is a cover)
- If $H \leq L$, then $H \not\leq_{\text{fi}} L * L'$: every finite-index extension is algebraic
- the lattice of finite-index extensions of H is finite and computable
- Let H_{fi} be the maximal finite-index extension: then $H \leq_{\text{ealg}} H_{\text{fi}}$, so $\text{rank}(H_{\text{fi}}) \leq \text{rank}(H)$

Simple remarks

- If $H \leq_{\text{fi}} L$ then $H \leq_{\text{fi}} K \leq_{\text{fi}} L$
- If $H, K \leq_{\text{fi}} L$, then $H \cap K \leq_{\text{fi}} L$ (the pull-back of covers is a cover)
- If $H \leq_{\text{fi}} K, L$, then $H \leq_{\text{fi}} \langle K, L\rangle$ (Greenberg, the push-out of covers is a cover)
- If $H \leq L$, then $H \not\leq_{\text{fi}} L * L'$: every finite-index extension is algebraic
- the lattice of finite-index extensions of H is finite and computable
- Let H_{fi} be the maximal finite-index extension: then $H \leq_{\text{ealg}} H_{\text{fi}}$, so $\text{rank}(H_{\text{fi}}) \leq \text{rank}(H)$
- H_{fi} is the commensurator of H (all x such that $H \cap H^x \leq_{\text{fi}} H, H^x$)

Computing the finite-index extensions of H (cycl. reduced)

- If p is a vertex of $\Gamma(H)$, let $\tilde{L}_p(H) =$ the language accepted by $\Gamma(H)$ with initial state p, all states final
- $L_p(H) =$ set of reduced words in $\tilde{L}_p(H)$

Computing the finite-index extensions of H (cycl. reduced)

- If p is a vertex of $\Gamma(H)$, let $\tilde{L}_p(H)$ = the language accepted by $\Gamma(H)$ with initial state p, all states final
- $L_p(H)$ = set of reduced words in $\tilde{L}_p(H)$

Theorem

$\Gamma(H)/(p = q)$ is a finite index extension if and only if $L_p(H) = L_q(H)$ (or $\tilde{L}_p(H) = \tilde{L}_q(H)$)

Counting the finite index extensions of H

- Say $p \sim q$ is $p, q \in \Gamma(H)$ and $L_p(H) = L_q(H)$

Counting the finite index extensions of H

- Say $p \sim q$ is $p, q \in \Gamma(H)$ and $L_p(H) = L_q(H)$
- $\sim$ is a union of connected components of $\Gamma(H) \times_A \Gamma(H)$

Counting the finite index extensions of H

- Say $p \sim q$ is $p, q \in \Gamma(H)$ and $L_p(H) = L_q(H)$
- $\sim$ is a union of connected components of $\Gamma(H) \times_A \Gamma(H)$

if $p \xrightarrow{u} r$, then $L_r(H) = \{\mathrm{red}(\bar{u}x) \mid x \in L_p(H)\}$
if $p \sim q$ and $(p, q) \xrightarrow{u} (p', q')$, then $p' \sim q'$

Counting the finite index extensions of H

- Say $p \sim q$ is $p, q \in \Gamma(H)$ and $L_p(H) = L_q(H)$
- $\sim$ is a union of connected components of $\Gamma(H) \times_A \Gamma(H)$
- and $p \sim q$ if and only if the component projections from to connected component of (p, q) are covers of $\Gamma(H)$ and $\Gamma(K)$

Counting the finite index extensions of H

- Say $p \sim q$ is $p, q \in \Gamma(H)$ and $L_p(H) = L_q(H)$
- $\sim$ is a union of connected components of $\Gamma(H) \times_A \Gamma(H)$
- and $p \sim q$ if and only if the component projections from to connected component of (p, q) are covers of $\Gamma(H)$ and $\Gamma(K)$
- Every $\sim$-class contains some $(1, r)$, so if $\Gamma(H)$ has n vertices, there are at most n classes, and each is non trivial (so the corresponding quotient has at most $n/2$ elements)

Counting the finite index extensions of H

- Say $p \sim q$ is $p, q \in \Gamma(H)$ and $L_p(H) = L_q(H)$
- $\sim$ is a union of connected components of $\Gamma(H) \times_A \Gamma(H)$
- and $p \sim q$ if and only if the component projections from to connected component of (p, q) are covers of $\Gamma(H)$ and $\Gamma(K)$
- Every $\sim$-class contains some $(1, r)$, so if $\Gamma(H)$ has n vertices, there are at most n classes, and each is non trivial (so the corresponding quotient has at most $n/2$ elements)
- So if there are at most $f(n)$ finite index extensions, then $f(n) \leq nf(n/2)$, $f(n) \leq n^{\frac{1}{2}(1+\log_2 n)} = \sqrt{n\ 2^{\log_2^2 n}}$

Computing all finite extensions of H

- Let $H \leq_{\text{fi}} K \leq F$ and $\varphi\colon \Gamma(H) \longrightarrow \Gamma(K)$ (cover). Then $L_p(H) = L_{\varphi(p)}(K)$

Computing all finite extensions of H

- Let $H \leq_{\text{fi}} K \leq F$ and $\varphi\colon \Gamma(H) \longrightarrow \Gamma(K)$ (cover). Then $L_p(H) = L_{\varphi(p)}(K)$
- So $H \leq_{\text{fi}} K$ iff $\Gamma(K)$ is obtained by performing some identifications $p = q$ such that $L_p(H) = L_q(H)$, and then reducing the graph

Computing all finite extensions of H

- Let $H \leq_{\text{fi}} K \leq F$ and $\varphi\colon \Gamma(H) \longrightarrow \Gamma(K)$ (cover). Then $L_p(H) = L_{\varphi(p)}(K)$
- So $H \leq_{\text{fi}} K$ iff $\Gamma(K)$ is obtained by performing some identifications $p = q$ such that $L_p(H) = L_q(H)$, and then reducing the graph
- $\Gamma(H_{\text{fi}})$ is obtained by performing all identifications $p = q$ such that $L_p(H) = L_q(H)$. No reduction is necessary

Computing all finite extensions of H

- Let $H \leq_{\text{fi}} K \leq F$ and $\varphi\colon \Gamma(H) \longrightarrow \Gamma(K)$ (cover). Then $L_p(H) = L_{\varphi(p)}(K)$
- So $H \leq_{\text{fi}} K$ iff $\Gamma(K)$ is obtained by performing some identifications $p = q$ such that $L_p(H) = L_q(H)$, and then reducing the graph
- $\Gamma(H_{\text{fi}})$ is obtained by performing all identifications $p = q$ such that $L_p(H) = L_q(H)$. No reduction is necessary
- To find all these pairs (p, q): minimize the automaton $\Gamma(H)$ with all states final! This can be done in $\mathcal{O}(n \log n)$

Malnormal subgroups (H cyclically reduced)

- We saw that the malnormal closure of H exists and is computable; it is an e-algebraic extension

Malnormal subgroups (H cyclically reduced)

- We saw that the malnormal closure of H exists and is computable; it is an e-algebraic extension
- H is malnormal iff every non-diagonal connected component of $\Gamma(H) \times_A \Gamma(H)$ is a tree... (Kapovich, Miasnikov)

Malnormal subgroups (H cyclically reduced)

- We saw that the malnormal closure of H exists and is computable; it is an e-algebraic extension
- H is malnormal iff every non-diagonal connected component of $\Gamma(H) \times_A \Gamma(H)$ is a tree... (Kapovich, Miasnikov)
- ... iff $L_p(H) \cap L_q(H)$ is finite for each $p \neq q$

Malnormal subgroups (H cyclically reduced)

- We saw that the malnormal closure of H exists and is computable; it is an e-algebraic extension
- H is malnormal iff every non-diagonal connected component of $\Gamma(H) \times_A \Gamma(H)$ is a tree... (Kapovich, Miasnikov)
- ... iff $L_p(H) \cap L_q(H)$ is finite for each $p \neq q$
- Malnormality is decidable in time $\mathcal{O}(n^2 \log n)$

Malnormal subgroups (H cyclically reduced)

- We saw that the malnormal closure of H exists and is computable; it is an e-algebraic extension
- H is malnormal iff every non-diagonal connected component of $\Gamma(H) \times_A \Gamma(H)$ is a tree. . . (Kapovich, Miasnikov)
- . . . iff $L_p(H) \cap L_q(H)$ is finite for each $p \neq q$
- Malnormality is decidable in time $\mathcal{O}(n^2 \log n)$
- A malnormal subgroup has no proper finite index extensions

Malnormal subgroups (H cyclically reduced)

- We saw that the malnormal closure of H exists and is computable; it is an e-algebraic extension
- H is malnormal iff every non-diagonal connected component of $\Gamma(H) \times_A \Gamma(H)$ is a tree... (Kapovich, Miasnikov)
- ... iff $L_p(H) \cap L_q(H)$ is finite for each $p \neq q$
- Malnormality is decidable in time $\mathcal{O}(n^2 \log n)$
- A malnormal subgroup has no proper finite index extensions
- $\Gamma(H_{\mathrm{mal}})$ is computed by repeatedly applying the following procedure: *identify all pairs $p, q \in \Gamma(H)$ such that $L_p(H) \cap L_q(H)$ is infinite, and reduce.*

Malnormal subgroups (H cyclically reduced)

- We saw that the malnormal closure of H exists and is computable; it is an e-algebraic extension
- H is malnormal iff every non-diagonal connected component of $\Gamma(H) \times_A \Gamma(H)$ is a tree… (Kapovich, Miasnikov)
- … iff $L_p(H) \cap L_q(H)$ is finite for each $p \neq q$
- Malnormality is decidable in time $\mathcal{O}(n^2 \log n)$
- A malnormal subgroup has no proper finite index extensions
- $\Gamma(H_{\text{mal}})$ is computed by repeatedly applying the following procedure: *identify all pairs $p, q \in \Gamma(H)$ such that $L_p(H) \cap L_q(H)$ is infinite, and reduce.*
- H_{mal} is computable in time $\mathcal{O}(n^3 \log n)$

Thank you for your attention!