Using graphs to understand the lattice of subgroups of a free group

Enric Ventura

Departament de Matemàtica Aplicada III
Universitat Politècnica de Catalunya

Algebra Seminar, Aalto University

Sept. 4th, 2013.

Outline

Outline

Free group: the construction

Definition

- *Let $A = \{a_1, \ldots, a_r\}$ be a finite alphabet, and consider (formally) $\tilde{A} = \{a_1, \ldots, a_r, a_1^{-1}, \ldots, a_r^{-1}\}$.*
- *A word on A is a finite sequence of symbols $w = a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}$, where $a_{i_j} \in A$ and $\epsilon_j = \pm 1$. The length of w is $\ell(w) = n$.*
- *The empty word is the only one with zero letters, denoted 1; $\ell(1) = 0$.*
- *The collection of all words on A is denoted $\tilde{A}^*$.*
- *Operation of concatenation in $\tilde{A}^*$: $u \cdot v = uv$; $\ell(uv) = \ell(u) + \ell(v)$.*

Definition

- *Two consecutive letters in $w \in \tilde{A}^*$ of the form $a_i a_i^{-1}$ or $a_i^{-1} a_i$ are called a cancellation. A word w is called reduced if it has no cancellations. Denote $R(A) \subseteq \tilde{A}^*$ the set of reduced words.*
- *The reduction is the equivalence relation $\sim$ generated by*

$$u a_i^{\epsilon} a_i^{-\epsilon} v \sim uv.$$

Free group: the construction

Definition

- *Let* $A = \{a_1, \ldots, a_r\}$ *be a finite* *alphabet*, *and consider (formally)* $\tilde{A} = \{a_1, \ldots, a_r, a_1^{-1}, \ldots, a_r^{-1}\}$.
- *A* *word* *on A is a finite sequence of symbols* $w = a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}$, *where* $a_{i_j} \in A$ *and* $\epsilon_j = \pm 1$. *The* *length* *of w is* $\ell(w) = n$.
- *The* *empty* *word is the only one with zero letters, denoted* 1; $\ell(1) = 0$.
- *The collection of all words on A is denoted* $\tilde{A}^*$.
- *Operation of* *concatenation* *in* $\tilde{A}^*$: $u \cdot v = uv$; $\ell(uv) = \ell(u) + \ell(v)$.

Definition

- *Two consecutive letters in* $w \in \tilde{A}^*$ *of the form* $a_i a_i^{-1}$ *or* $a_i^{-1} a_i$ *are called a* *cancellation*. *A word w is called* *reduced* *if it has no cancellations. Denote* $R(A) \subseteq \tilde{A}^*$ *the set of reduced words.*
- *The* *reduction* *is the equivalence relation* $\sim$ *generated by*

$$ua_i^{\epsilon} a_i^{-\epsilon} v \sim uv.$$

Free group: the construction

Definition

- *Let $A = \{a_1, \ldots, a_r\}$ be a finite alphabet, and consider (formally) $\tilde{A} = \{a_1, \ldots, a_r, a_1^{-1}, \ldots, a_r^{-1}\}$.*
- *A word on A is a finite sequence of symbols $w = a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}$, where $a_{i_j} \in A$ and $\epsilon_j = \pm 1$. The length of w is $\ell(w) = n$.*
- *The empty word is the only one with zero letters, denoted 1; $\ell(1) = 0$.*
- *The collection of all words on A is denoted $\tilde{A}^*$.*
- *Operation of concatenation in $\tilde{A}^*$: $u \cdot v = uv$; $\ell(uv) = \ell(u) + \ell(v)$.*

Definition

- *Two consecutive letters in $w \in \tilde{A}^*$ of the form $a_i a_i^{-1}$ or $a_i^{-1} a_i$ are called a cancellation. A word w is called reduced if it has no cancellations. Denote $R(A) \subseteq \tilde{A}^*$ the set of reduced words.*
- *The reduction is the equivalence relation $\sim$ generated by*

$$ua_i^{\epsilon} a_i^{-\epsilon} v \sim uv.$$

Free group: the construction

Definition

- Let $A = \{a_1, \ldots, a_r\}$ be a finite alphabet, and consider (formally) $\tilde{A} = \{a_1, \ldots, a_r, a_1^{-1}, \ldots, a_r^{-1}\}$.
- A word on A is a finite sequence of symbols $w = a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}$, where $a_{i_j} \in A$ and $\epsilon_j = \pm 1$. The length of w is $\ell(w) = n$.
- The empty word is the only one with zero letters, denoted 1; $\ell(1) = 0$.
- The collection of all words on A is denoted $\tilde{A}^*$.
- Operation of concatenation in $\tilde{A}^*$: $u \cdot v = uv$; $\ell(uv) = \ell(u) + \ell(v)$.

Definition

- Two consecutive letters in $w \in \tilde{A}^*$ of the form $a_i a_i^{-1}$ or $a_i^{-1} a_i$ are called a cancellation. A word w is called reduced if it has no cancellations. Denote $R(A) \subseteq \tilde{A}^*$ the set of reduced words.
- The reduction is the equivalence relation $\sim$ generated by

$$u a_i^{\epsilon} a_i^{-\epsilon} v \sim uv.$$

Free group: the construction

Definition

- Let $A = \{a_1, \ldots, a_r\}$ be a finite alphabet, and consider (formally) $\tilde{A} = \{a_1, \ldots, a_r, a_1^{-1}, \ldots, a_r^{-1}\}$.
- A word on A is a finite sequence of symbols $w = a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}$, where $a_{i_j} \in A$ and $\epsilon_j = \pm 1$. The length of w is $\ell(w) = n$.
- The empty word is the only one with zero letters, denoted 1; $\ell(1) = 0$.
- The collection of all words on A is denoted $\tilde{A}^*$.
- Operation of concatenation in $\tilde{A}^*$: $u \cdot v = uv$; $\ell(uv) = \ell(u) + \ell(v)$.

Definition

- Two consecutive letters in $w \in \tilde{A}^*$ of the form $a_i a_i^{-1}$ or $a_i^{-1} a_i$ are called a cancellation. A word w is called reduced if it has no cancellations. Denote $R(A) \subseteq \tilde{A}^*$ the set of reduced words.
- The reduction is the equivalence relation $\sim$ generated by

$$ua_i^{\epsilon} a_i^{-\epsilon} v \sim uv.$$

Free group: the construction

Definition

- Let $A = \{a_1, \ldots, a_r\}$ be a finite alphabet, and consider (formally) $\tilde{A} = \{a_1, \ldots, a_r, a_1^{-1}, \ldots, a_r^{-1}\}$.
- A word on A is a finite sequence of symbols $w = a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}$, where $a_{i_j} \in A$ and $\epsilon_j = \pm 1$. The length of w is $\ell(w) = n$.
- The empty word is the only one with zero letters, denoted 1; $\ell(1) = 0$.
- The collection of all words on A is denoted $\tilde{A}^*$.
- Operation of concatenation in $\tilde{A}^*$: $u \cdot v = uv$; $\ell(uv) = \ell(u) + \ell(v)$.

Definition

- Two consecutive letters in $w \in \tilde{A}^*$ of the form $a_i a_i^{-1}$ or $a_i^{-1} a_i$ are called a cancellation. A word w is called reduced if it has no cancellations. Denote $R(A) \subseteq \tilde{A}^*$ the set of reduced words.
- The reduction is the equivalence relation $\sim$ generated by

$$u a_i^{\epsilon} a_i^{-\epsilon} v \sim uv.$$

Free group: the construction

Definition

- Let $A = \{a_1, \ldots, a_r\}$ be a finite alphabet, and consider (formally) $\tilde{A} = \{a_1, \ldots, a_r, a_1^{-1}, \ldots, a_r^{-1}\}$.
- A word on A is a finite sequence of symbols $w = a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}$, where $a_{i_j} \in A$ and $\epsilon_j = \pm 1$. The length of w is $\ell(w) = n$.
- The empty word is the only one with zero letters, denoted 1; $\ell(1) = 0$.
- The collection of all words on A is denoted $\tilde{A}^*$.
- Operation of concatenation in $\tilde{A}^*$: $u \cdot v = uv$; $\ell(uv) = \ell(u) + \ell(v)$.

Definition

- Two consecutive letters in $w \in \tilde{A}^*$ of the form $a_i a_i^{-1}$ or $a_i^{-1} a_i$ are called a cancellation. A word w is called reduced if it has no cancellations. Denote $R(A) \subseteq \tilde{A}^*$ the set of reduced words.
- The reduction is the equivalence relation $\sim$ generated by

$$u a_i^{\epsilon} a_i^{-\epsilon} v \sim uv.$$

Free group: the construction

Definition

- *The free group on A is* $F(A) = \tilde{A}^* / \sim$ *with the operation of concatenation (i.e. concatenation + reduction).*
- *The neutral element is 1, and the inverse of* $w = a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}$ *is* $w^{-1} = (a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n})^{-1} = a_{i_n}^{-\epsilon_n} \cdots a_{i_1}^{-\epsilon_1}$.
- *Of course,* $(a_i^{-1})^{-1} = a_i$.

Lemma

For every $w \in \tilde{A}^*$*, there is a unique* $\overline{w} \in R(A)$*, s.t.* $w = \overline{w}$ *in* $F(A)$.

This allows us "forget" the $\sim$*, and work in* $F(A)$ *by just manipulating words (and reducing every time it is possible).*

Definition

The length of an element $w \in F(A)$ *is* $|w| = \ell(\overline{w})$.

Free group: the construction

Definition

- *The free group on A is $F(A) = \tilde{A}^* / \sim$ with the operation of concatenation (i.e. concatenation + reduction).*
- *The neutral element is 1, and the inverse of $w = a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}$ is $w^{-1} = (a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n})^{-1} = a_{i_n}^{-\epsilon_n} \cdots a_{i_1}^{-\epsilon_1}$.*
- *Of course, $(a_i^{-1})^{-1} = a_i$.*

Lemma

For every $w \in \tilde{A}^*$, there is a unique $\overline{w} \in R(A)$, s.t. $w = \overline{w}$ in $F(A)$.

This allows us "forget" the $\sim$, and work in $F(A)$ by just manipulating words (and reducing every time it is possible).

Definition

The length of an element $w \in F(A)$ is $|w| = \ell(\overline{w})$.

Free group: the construction

Definition

- *The free group on A is $F(A) = \tilde{A}^* / \sim$ with the operation of concatenation (i.e. concatenation + reduction).*
- *The neutral element is 1, and the inverse of $w = a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}$ is $w^{-1} = (a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n})^{-1} = a_{i_n}^{-\epsilon_n} \cdots a_{i_1}^{-\epsilon_1}$.*
- *Of course, $(a_i^{-1})^{-1} = a_i$.*

Lemma

For every $w \in \tilde{A}^*$, there is a unique $\overline{w} \in R(A)$, s.t. $w = \overline{w}$ in $F(A)$.

This allows us "forget" the $\sim$, and work in $F(A)$ by just manipulating words (and reducing every time it is possible).

Definition

The length of an element $w \in F(A)$ is $|w| = \ell(\overline{w})$.

Free group: the construction

Definition

- *The* free group *on* A *is* $F(A) = \tilde{A}^* / \sim$ *with the operation of concatenation (i.e.* concatenation + reduction*).*
- *The* neutral *element is* 1*, and the* inverse *of* $w = a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}$ *is* $w^{-1} = (a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n})^{-1} = a_{i_n}^{-\epsilon_n} \cdots a_{i_1}^{-\epsilon_1}$.
- *Of course,* $(a_i^{-1})^{-1} = a_i$.

Lemma

For every $w \in \tilde{A}^*$*, there is a unique* $\overline{w} \in R(A)$*, s.t.* $w = \overline{w}$ *in* $F(A)$*.*

This allows us "forget" the $\sim$*, and work in* $F(A)$ *by just manipulating words (and reducing every time it is possible).*

Definition

The length *of an element* $w \in F(A)$ *is* $|w| = \ell(\overline{w})$*.*

Free group: the construction

Definition

- *The free group on A is $F(A) = \tilde{A}^* / \sim$ with the operation of concatenation (i.e. concatenation + reduction).*
- *The neutral element is 1, and the inverse of $w = a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}$ is $w^{-1} = (a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n})^{-1} = a_{i_n}^{-\epsilon_n} \cdots a_{i_1}^{-\epsilon_1}$.*
- *Of course, $(a_i^{-1})^{-1} = a_i$.*

Lemma

For every $w \in \tilde{A}^*$, there is a unique $\overline{w} \in R(A)$, s.t. $w = \overline{w}$ in $F(A)$.

This allows us "forget" the $\sim$, and work in $F(A)$ by just manipulating words (and reducing every time it is possible).

Definition

The length of an element $w \in F(A)$ is $|w| = \ell(\overline{w})$.

Free group: the construction

Definition

- *The free group on A is $F(A) = \tilde{A}^* / \sim$ with the operation of concatenation (i.e. concatenation + reduction).*
- *The neutral element is 1, and the inverse of $w = a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n}$ is $w^{-1} = (a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n})^{-1} = a_{i_n}^{-\epsilon_n} \cdots a_{i_1}^{-\epsilon_1}$.*
- *Of course, $(a_i^{-1})^{-1} = a_i$.*

Lemma

For every $w \in \tilde{A}^*$, there is a unique $\overline{w} \in R(A)$, s.t. $w = \overline{w}$ in $F(A)$.

This allows us "forget" the $\sim$, and work in $F(A)$ by just manipulating words (and reducing every time it is possible).

Definition

The length of an element $w \in F(A)$ is $|w| = \ell(\overline{w})$.

The rank of a free group

Clearly, r is the only relevant information about $A = \{a_1, \ldots, a_r\}$. That is,

$$\#A = \#B \quad \Rightarrow \quad F(A) \simeq F(B).$$

Proposition

Let A and B be two finite sets. Then,

$$\#A = \#B \quad \Leftrightarrow \quad F(A) \simeq F(B).$$

Definition

The rank of $F(A)$ is the cardinal of A, $r(F(A)) = \#A = r$. $F(A)$ is usually denoted just F_r.

Example

What is F_1 ? ... And F_2 ?

The rank of a free group

Clearly, r is the only relevant information about $A = \{a_1, \ldots, a_r\}$. That is,

$$\#A = \#B \quad \Rightarrow \quad F(A) \simeq F(B).$$

Proposition

Let A and B be two finite sets. Then,

$$\#A = \#B \quad \Leftrightarrow \quad F(A) \simeq F(B).$$

Definition

The rank of $F(A)$ is the cardinal of A, $r(F(A)) = \#A = r$. $F(A)$ is usually denoted just F_r.

Example

What is F_1 ? ... And F_2 ?

The rank of a free group

Clearly, r is the only relevant information about $A = \{a_1, \ldots, a_r\}$. That is,

$$\#A = \#B \quad \Rightarrow \quad F(A) \simeq F(B).$$

Proposition

Let A and B be two finite sets. Then,

$$\#A = \#B \quad \Leftrightarrow \quad F(A) \simeq F(B).$$

Definition

The rank of $F(A)$ is the cardinal of A, $r(F(A)) = \#A = r$. $F(A)$ is usually denoted just F_r.

Example

What is F_1 ? ... And F_2 ?

The rank of a free group

Clearly, r is the only relevant information about $A = \{a_1, \ldots, a_r\}$. That is,

$$\#A = \#B \quad \Rightarrow \quad F(A) \simeq F(B).$$

Proposition

Let A and B be two finite sets. Then,

$$\#A = \#B \quad \Leftrightarrow \quad F(A) \simeq F(B).$$

Definition

The rank of $F(A)$ is the cardinal of A, $r(F(A)) = \#A = r$. $F(A)$ is usually denoted just F_r.

Example

What is F_1 ? ... And F_2 ?

The rank of a free group

Clearly, r is the only relevant information about $A = \{a_1, \ldots, a_r\}$. That is,

$$\#A = \#B \quad \Rightarrow \quad F(A) \simeq F(B).$$

Proposition

Let A and B be two finite sets. Then,

$$\#A = \#B \quad \Leftrightarrow \quad F(A) \simeq F(B).$$

Definition

The rank of $F(A)$ is the cardinal of A, $r(F(A)) = \#A = r$. $F(A)$ is usually denoted just F_r.

Example

What is F_1 ? ... And F_2 ?

Main property of free groups

Proposition

For every group G and elements $g_1, \ldots, g_r \in G$ there exists a unique morphism $\varphi \colon F(A) \to G$ mapping a_i to g_i.

Corollary

Every group G is a quotient of a free group.

So, philosophically ...

- *ALL GROUP THEORY is somehow reflected inside free groups,*
- *plus: ... great! let's concentrate on free groups ...*
- *minus: ... free groups must be VERY complicated ...*

Main property of free groups

Proposition

For every group G and elements $g_1, \ldots, g_r \in G$ there exists a unique morphism $\varphi\colon F(A) \to G$ mapping a_i to g_i.

Corollary

Every group G is a quotient of a free group.

So, philosophically ...

- *ALL GROUP THEORY is somehow reflected inside free groups,*
- *plus: ... great! let's concentrate on free groups ...*
- *minus: ... free groups must be VERY complicated ...*

Main property of free groups

Proposition

For every group G and elements $g_1, \ldots, g_r \in G$ there exists a unique morphism $\varphi\colon F(A) \to G$ mapping a_i to g_i.

Corollary

Every group G is a quotient of a free group.

So, philosophically ...

- *ALL GROUP THEORY is somehow reflected inside free groups,*
- *plus: ... great! let's concentrate on free groups ...*
- *minus: ... free groups must be VERY complicated ...*

Main property of free groups

Proposition

For every group G and elements $g_1, \ldots, g_r \in G$ there exists a unique morphism $\varphi\colon F(A) \to G$ mapping a_i to g_i.

Corollary

Every group G is a quotient of a free group.

So, philosophically ...

- *ALL GROUP THEORY is somehow reflected inside free groups,*
- *plus: ... great! let's concentrate on free groups ...*
- *minus: ... free groups must be VERY complicated ...*

Main property of free groups

Proposition

For every group G and elements $g_1, \ldots, g_r \in G$ there exists a unique morphism $\varphi \colon F(A) \to G$ mapping a_i to g_i.

Corollary

Every group G is a quotient of a free group.

So, philosophically ...

- *ALL GROUP THEORY is somehow reflected inside free groups,*
- *plus: ... great! let's concentrate on free groups ...*
- *minus: ... free groups must be VERY complicated ...*

Membership problem

Definition

Let G be a group. The membership problem in G consists on finding an algorithm to do the following:

input: $g_0, g_1, \ldots, g_n \in G$;

output: YES if $g_0 \in \langle g_1, \ldots, g_n \rangle \leqslant G$,
NO if $g_0 \notin \langle g_1, \ldots, g_n \rangle \leqslant G$.

Theorem

There are groups G with UNSOLVABLE membership problem.

Proposition

- *Finite groups have solvable membership problem.*
- *$\mathbb{Z}^n$ and $\mathbb{Q}^n$ have solvable membership problem.*
- *What about F_r ?*

Membership problem

Definition

Let G be a group. The ***membership problem*** *in G consists on finding an algorithm to do the following:*

input: $g_0, g_1, \ldots, g_n \in G$;

output: YES if $g_0 \in \langle g_1, \ldots, g_n \rangle \leqslant G$,
NO if $g_0 \notin \langle g_1, \ldots, g_n \rangle \leqslant G$.

Theorem

There are groups G with UNSOLVABLE membership problem.

Proposition

- *Finite groups have solvable membership problem.*
- $\mathbb{Z}^n$ *and* $\mathbb{Q}^n$ *have solvable membership problem.*
- *What about* F_r *?*

Membership problem

Definition

Let G be a group. The membership problem in G consists on finding an algorithm to do the following:

input: $g_0, g_1, \ldots, g_n \in G$;

output: YES if $g_0 \in \langle g_1, \ldots, g_n \rangle \leqslant G$,
NO if $g_0 \notin \langle g_1, \ldots, g_n \rangle \leqslant G$.

Theorem

There are groups G with UNSOLVABLE membership problem.

Proposition

- *Finite groups have solvable membership problem.*
- $\mathbb{Z}^n$ *and* $\mathbb{Q}^n$ *have solvable membership problem.*
- *What about* F_r *?*

Membership problem

Definition

Let G be a group. The membership problem in G consists on finding an algorithm to do the following:

input: $g_0, g_1, \ldots, g_n \in G$;

output: YES if $g_0 \in \langle g_1, \ldots, g_n \rangle \leqslant G$,
NO if $g_0 \notin \langle g_1, \ldots, g_n \rangle \leqslant G$.

Theorem

There are groups G with UNSOLVABLE membership problem.

Proposition

- *Finite groups have solvable membership problem.*
- $\mathbb{Z}^n$ *and* $\mathbb{Q}^n$ *have solvable membership problem.*
- *What about* F_r *?*

Membership problem

Definition

Let G be a group. The membership problem in G consists on finding an algorithm to do the following:

input: $g_0, g_1, \ldots, g_n \in G$;

output: YES if $g_0 \in \langle g_1, \ldots, g_n \rangle \leqslant G$,
NO if $g_0 \notin \langle g_1, \ldots, g_n \rangle \leqslant G$.

Theorem

There are groups G with UNSOLVABLE membership problem.

Proposition

- *Finite groups have solvable membership problem.*
- $\mathbb{Z}^n$ *and* $\mathbb{Q}^n$ *have solvable membership problem.*
- *What about* F_r *?*

Membership problem

Definition

Let G be a group. The membership problem in G consists on finding an algorithm to do the following:

input: $g_0, g_1, \ldots, g_n \in G$;

output: YES if $g_0 \in \langle g_1, \ldots, g_n \rangle \leqslant G$,
NO if $g_0 \notin \langle g_1, \ldots, g_n \rangle \leqslant G$.

Theorem

There are groups G with UNSOLVABLE membership problem.

Proposition

- *Finite groups have solvable membership problem.*
- $\mathbb{Z}^n$ *and* $\mathbb{Q}^n$ *have solvable membership problem.*
- *What about* F_r *?*

Membership problem

Definition

Let G be a group. The membership problem in G consists on finding an algorithm to do the following:

input: $g_0, g_1, \ldots, g_n \in G$;

output: YES if $g_0 \in \langle g_1, \ldots, g_n \rangle \leqslant G$,
NO if $g_0 \notin \langle g_1, \ldots, g_n \rangle \leqslant G$.

Theorem

There are groups G with UNSOLVABLE membership problem.

Proposition

- *Finite groups have solvable membership problem.*
- *$\mathbb{Z}^n$ and $\mathbb{Q}^n$ have solvable membership problem.*
- *What about F_r ?*

Membership problem

Definition

Let G be a group. The membership problem in G consists on finding an algorithm to do the following:

input: $g_0, g_1, \ldots, g_n \in G;$

output: *YES if* $g_0 \in \langle g_1, \ldots, g_n \rangle \leqslant G,$
NO if $g_0 \notin \langle g_1, \ldots, g_n \rangle \leqslant G.$

Theorem

There are groups G with UNSOLVABLE membership problem.

Proposition

- *Finite groups have solvable membership problem.*
- $\mathbb{Z}^n$ *and* $\mathbb{Q}^n$ *have solvable membership problem.*
- *What about* F_r *?*

A first example

Example

Consider the subgroup of $F_2 = F(\{a, b\})$ *given by*

$$H = \langle \underbrace{baba^{-1}}_{w_1}, \underbrace{aba^{-1}}_{w_2}, \underbrace{aba^2}_{w_3} \rangle.$$

Is $bab^2a^{-1} \in H$? YES, $bab^2a^{-1} = w_1 w_2$.

Is $b \in H$? YES, $b = w_1 w_2^{-1}$.

Is $a \in H$? ... ummm ... I see $a^3 = w_2^{-1} w_3$.

A first example

Example

Consider the subgroup of $F_2 = F(\{a, b\})$ *given by*

$$H = \langle \underbrace{baba^{-1}}_{w_1}, \underbrace{aba^{-1}}_{w_2}, \underbrace{aba^2}_{w_3} \rangle.$$

Is $bab^2a^{-1} \in H$ *?* *YES,* $bab^2a^{-1} = w_1 w_2$.

Is $b \in H$ *?* *YES,* $b = w_1 w_2^{-1}$.

Is $a \in H$ *?* *... ummm ...* *I see* $a^3 = w_2^{-1} w_3$.

A first example

Example

Consider the subgroup of $F_2 = F(\{a, b\})$ given by

$$H = \langle \underbrace{baba^{-1}}_{w_1}, \underbrace{aba^{-1}}_{w_2}, \underbrace{aba^2}_{w_3} \rangle .$$

Is $bab^2a^{-1} \in H$? YES, $bab^2a^{-1} = w_1 w_2$.

Is $b \in H$? YES, $b = w_1 w_2^{-1}$.

Is $a \in H$? ... ummm ... I see $a^3 = w_2^{-1} w_3$.

A first example

Example

Consider the subgroup of $F_2 = F(\{a, b\})$ *given by*

$$H = \langle \underbrace{baba^{-1}}_{w_1}, \underbrace{aba^{-1}}_{w_2}, \underbrace{aba^2}_{w_3} \rangle.$$

Is $bab^2a^{-1} \in H$ *?* *YES,* $bab^2a^{-1} = w_1 w_2$.

Is $b \in H$ *?* *YES,* $b = w_1 w_2^{-1}$.

Is $a \in H$ *?* *... ummm ...* *I see* $a^3 = w_2^{-1} w_3$.

A first example

Example

Consider the subgroup of $F_2 = F(\{a, b\})$ *given by*

$$H = \langle \underbrace{baba^{-1}}_{w_1}, \underbrace{aba^{-1}}_{w_2}, \underbrace{aba^2}_{w_3} \rangle.$$

Is $bab^2a^{-1} \in H$? *YES,* $bab^2a^{-1} = w_1 w_2$.

Is $b \in H$? *YES,* $b = w_1 w_2^{-1}$.

Is $a \in H$? *... ummm ... I see* $a^3 = w_2^{-1} w_3$.

A first example

Example

Consider the subgroup of $F_2 = F(\{a, b\})$ given by

$$H = \langle \underbrace{baba^{-1}}_{w_1}, \underbrace{aba^{-1}}_{w_2}, \underbrace{aba^2}_{w_3} \rangle.$$

Is $bab^2a^{-1} \in H$? YES, $bab^2a^{-1} = w_1w_2$.

Is $b \in H$? YES, $b = w_1w_2^{-1}$.

Is $a \in H$? ... ummm ... I see $a^3 = w_2^{-1}w_3$.

A first example

Example

Consider the subgroup of $F_2 = F(\{a, b\})$ given by

$$H = \langle \underbrace{baba^{-1}}_{w_1}, \underbrace{aba^{-1}}_{w_2}, \underbrace{aba^2}_{w_3} \rangle.$$

Is $bab^2a^{-1} \in H$? YES, $bab^2a^{-1} = w_1w_2$.

Is $b \in H$? YES, $b = w_1w_2^{-1}$.

Is $a \in H$? ... ummm ... I see $a^3 = w_2^{-1}w_3$.

A first example

In fact, $a \notin H$ because the total number of a's must be multiple of 3 !!!

$aba^2 \in H$ *but* $a^2ba \notin H$ *... why?*

Is $bab^2a^3b^{-1}a^{-1}b^4aba^{-4} \in H$ *? ... exercise*

A first example

In fact, $a \notin H$ *because the total number of a's must be multiple of 3 !!!*

$aba^2 \in H$ *but* $a^2ba \notin H$ *... why?*

Is $bab^2a^3b^{-1}a^{-1}b^4aba^{-4} \in H$ *? ... exercise*

A first example

In fact, $a \notin H$ because the total number of a's must be multiple of 3 !!!

$aba^2 \in H$ *but* $a^2ba \notin H$ *... why?*

Is $bab^2a^3b^{-1}a^{-1}b^4aba^{-4} \in H$ *? ... exercise*

A first example

In fact, $a \notin H$ *because the total number of a's must be multiple of 3 !!!*

$aba^2 \in H$ *but* $a^2ba \notin H$ *... why?*

Is $bab^2a^3b^{-1}a^{-1}b^4aba^{-4} \in H$ *?* ... exercise

A first example

In fact, $a \notin H$ *because the total number of a's must be multiple of 3 !!!*

$aba^2 \in H$ *but* $a^2ba \notin H$ *... why?*

Is $bab^2a^3b^{-1}a^{-1}b^4aba^{-4} \in H$ *? ... exercise*

Intersection problem

Definition

Let G be a group. The intersection problem in G consists on finding an algorithm to do the following:

input: $u_1, \ldots, u_n, v_1, \ldots, v_m \in G$;

output: $w_1, \ldots, w_p \in G$ *such that* $\langle u_1, \ldots, u_n \rangle \cap \langle v_1, \ldots, v_m \rangle = \langle w_1, \ldots, w_p \rangle$

Proposition

- *Finite groups have solvable intersection problem.*
- $\mathbb{Z}^n$ *and* $\mathbb{Q}^n$ *have solvable intersection problem.*
- *What about* F_r *?*

Intersection problem

Definition

Let G be a group. The intersection problem in G consists on finding an algorithm to do the following:

input: $u_1, \ldots, u_n, v_1, \ldots, v_m \in G$;

output: $w_1, \ldots, w_p \in G$ *such that*
$\langle u_1, \ldots, u_n \rangle \cap \langle v_1, \ldots, v_m \rangle = \langle w_1, \ldots, w_p \rangle$

Proposition

- *Finite groups have solvable intersection problem.*
- $\mathbb{Z}^n$ *and* $\mathbb{Q}^n$ *have solvable intersection problem.*
- *What about* F_r *?*

Intersection problem

Definition

Let G be a group. The intersection problem in G consists on finding an algorithm to do the following:

input: $u_1, \ldots, u_n, v_1, \ldots, v_m \in G$;

output: $w_1, \ldots, w_p \in G$ *such that* $\langle u_1, \ldots, u_n \rangle \cap \langle v_1, \ldots, v_m \rangle = \langle w_1, \ldots, w_p \rangle$

Proposition

- *Finite groups have solvable intersection problem.*
- $\mathbb{Z}^n$ *and* $\mathbb{Q}^n$ *have solvable intersection problem.*
- *What about* F_r *?*

Intersection problem

Definition

Let G be a group. The intersection problem in G consists on finding an algorithm to do the following:

input: $u_1, \ldots, u_n, v_1, \ldots, v_m \in G$;

output: $w_1, \ldots, w_p \in G$ *such that* $\langle u_1, \ldots, u_n \rangle \cap \langle v_1, \ldots, v_m \rangle = \langle w_1, \ldots, w_p \rangle$

Proposition

- *Finite groups have solvable intersection problem.*
- $\mathbb{Z}^n$ *and* $\mathbb{Q}^n$ *have solvable intersection problem.*
- *What about* F_r *?*

A first example

Example

Consider F_2 and the subgroups $H = \langle a, b^2, bab\rangle$ and $K = \langle b^2, ba^2\rangle$. Can you find generators for $H \cap K$?

- *Clearly, $b^2 \in H \cap K$ ...*
- *Less obvious but still easy, $a^{-2}b^2a^2 \in H \cap K$ because*

$$a^{-2}b^2a^2 = (a)^{-2}(b^2)(a)^2 \in H,$$

$$a^{-2}b^2a^2 = (ba^2)^{-1}(b^2)(ba^2) \in K.$$

- *Something else?* $H \cap K = \langle b^2, a^{-2}b^2a^2, \ldots (?) \ldots \rangle$
- *How to be sure you found everything ?*

A first example

Example

Consider F_2 and the subgroups $H = \langle a, b^2, bab \rangle$ and $K = \langle b^2, ba^2 \rangle$. Can you find generators for $H \cap K$?

- *Clearly, $b^2 \in H \cap K$ ...*
- *Less obvious but still easy, $a^{-2}b^2a^2 \in H \cap K$ because*

$$a^{-2}b^2a^2 = (a)^{-2}(b^2)(a)^2 \in H,$$

$$a^{-2}b^2a^2 = (ba^2)^{-1}(b^2)(ba^2) \in K.$$

- *Something else? $H \cap K = \langle b^2, a^{-2}b^2a^2, \ldots (?) \ldots \rangle$*
- *How to be sure you found everything ?*

A first example

Example

Consider F_2 and the subgroups $H = \langle a, b^2, bab \rangle$ and $K = \langle b^2, ba^2 \rangle$. Can you find generators for $H \cap K$?

- *Clearly, $b^2 \in H \cap K$ ...*
- *Less obvious but still easy, $a^{-2}b^2a^2 \in H \cap K$ because*

$$a^{-2}b^2a^2 = (a)^{-2}(b^2)(a)^2 \in H,$$

$$a^{-2}b^2a^2 = (ba^2)^{-1}(b^2)(ba^2) \in K.$$

- *Something else? $H \cap K = \langle b^2, a^{-2}b^2a^2, \ldots (?) \ldots \rangle$*
- *How to be sure you found everything ?*

A first example

Example

Consider F_2 and the subgroups $H = \langle a, b^2, bab \rangle$ and $K = \langle b^2, ba^2 \rangle$. Can you find generators for $H \cap K$?

- *Clearly, $b^2 \in H \cap K$ ...*
- *Less obvious but still easy, $a^{-2}b^2a^2 \in H \cap K$ because*

$$a^{-2}b^2a^2 = (a)^{-2}(b^2)(a)^2 \in H,$$

$$a^{-2}b^2a^2 = (ba^2)^{-1}(b^2)(ba^2) \in K.$$

- *Something else?* $H \cap K = \langle b^2, a^{-2}b^2a^2, \ldots (?) \ldots \rangle$
- *How to be sure you found everything ?*

A first example

Example

Consider F_2 and the subgroups $H = \langle a, b^2, bab \rangle$ and $K = \langle b^2, ba^2 \rangle$. Can you find generators for $H \cap K$?

- *Clearly, $b^2 \in H \cap K$ ...*
- *Less obvious but still easy, $a^{-2}b^2a^2 \in H \cap K$ because*

$$a^{-2}b^2a^2 = (a)^{-2}(b^2)(a)^2 \in H,$$

$$a^{-2}b^2a^2 = (ba^2)^{-1}(b^2)(ba^2) \in K.$$

- *Something else?* $H \cap K = \langle b^2, a^{-2}b^2a^2, \ldots (?) \ldots \rangle$
- *How to be sure you found everything ?*

Outline

Automata

Definition

Let A be an alphabet. An A-automaton $\mathcal{A}$ is an oriented graph with labels from A at the edges, and with a basepoint, $\mathcal{A} = (V, E, q_0)$, where

- *V is a finite set (of vertices),*
- *$E \subseteq V \times A \times V$ is the set of edges,*
- *$q_0 \in V$ is the basepoint.*

Note that $\mathcal{A}$ admits loops, and parallel edges with different labels.

Definition

An A-automaton $\mathcal{A}$ is connected if its underlying graph is connected (as undirected graph).

Definition

An A-automaton $\mathcal{A}$ is trim if it has no vertices of degree 1 except maybe the basepoint.

Automata

Definition

Let A be an alphabet. An A-automaton $\mathcal{A}$ is an oriented graph with labels from A at the edges, and with a basepoint, $\mathcal{A} = (V, E, q_0)$, where

- *V is a finite set (of vertices),*
- *$E \subseteq V \times A \times V$ is the set of edges,*
- *$q_0 \in V$ is the basepoint.*

Note that $\mathcal{A}$ admits loops, and parallel edges with different labels.

Definition

An A-automaton $\mathcal{A}$ is connected if its underlying graph is connected (as undirected graph).

Definition

An A-automaton $\mathcal{A}$ is trim if it has no vertices of degree 1 except maybe the basepoint.

Automata

Definition

Let A be an alphabet. An A-automaton $\mathcal{A}$ is an oriented graph with labels from A at the edges, and with a basepoint, $\mathcal{A} = (V, E, q_0)$, where

- *V is a finite set (of vertices),*
- *$E \subseteq V \times A \times V$ is the set of edges,*
- *$q_0 \in V$ is the basepoint.*

Note that $\mathcal{A}$ admits loops, and parallel edges with different labels.

Definition

An A-automaton $\mathcal{A}$ is connected if its underlying graph is connected (as undirected graph).

Definition

An A-automaton $\mathcal{A}$ is trim if it has no vertices of degree 1 except maybe the basepoint.

Automata

Definition

Let A be an alphabet. An A-automaton $\mathcal{A}$ is an oriented graph with labels from A at the edges, and with a basepoint, $\mathcal{A} = (V, E, q_0)$, where

- *V is a finite set (of vertices),*
- *$E \subseteq V \times A \times V$ is the set of edges,*
- *$q_0 \in V$ is the basepoint.*

Note that $\mathcal{A}$ admits loops, and parallel edges with different labels.

Definition

An A-automaton $\mathcal{A}$ is connected if its underlying graph is connected (as undirected graph).

Definition

An A-automaton $\mathcal{A}$ is trim if it has no vertices of degree 1 except maybe the basepoint.

Automata

Definition

Let A be an alphabet. An A-automaton $\mathcal{A}$ is an oriented graph with labels from A at the edges, and with a basepoint, $\mathcal{A} = (V, E, q_0)$, where

- *V is a finite set (of vertices),*
- *$E \subseteq V \times A \times V$ is the set of edges,*
- *$q_0 \in V$ is the basepoint.*

Note that $\mathcal{A}$ admits loops, and parallel edges with different labels.

Definition

An A-automaton $\mathcal{A}$ is connected if its underlying graph is connected (as undirected graph).

Definition

An A-automaton $\mathcal{A}$ is trim if it has no vertices of degree 1 except maybe the basepoint.

Automata

Definition

Let A be an alphabet. An A-automaton $\mathcal{A}$ is an oriented graph with labels from A at the edges, and with a basepoint, $\mathcal{A} = (V, E, q_0)$, where

- *V is a finite set (of vertices),*
- *$E \subseteq V \times A \times V$ is the set of edges,*
- *$q_0 \in V$ is the basepoint.*

Note that $\mathcal{A}$ admits loops, and parallel edges with different labels.

Definition

An A-automaton $\mathcal{A}$ is connected if its underlying graph is connected (as undirected graph).

Definition

An A-automaton $\mathcal{A}$ is trim if it has no vertices of degree 1 except maybe the basepoint.

Automata

Definition

Let A be an alphabet. An A-automaton $\mathcal{A}$ is an oriented graph with labels from A at the edges, and with a basepoint, $\mathcal{A} = (V, E, q_0)$, where

- *V is a finite set (of vertices),*
- *$E \subseteq V \times A \times V$ is the set of edges,*
- *$q_0 \in V$ is the basepoint.*

Note that $\mathcal{A}$ admits loops, and parallel edges with different labels.

Definition

An A-automaton $\mathcal{A}$ is connected if its underlying graph is connected (as undirected graph).

Definition

An A-automaton $\mathcal{A}$ is trim if it has no vertices of degree 1 except maybe the basepoint.

Paths

Definition

Let $\mathcal{A}$ be an A-automaton.

- *A path of length n in $\mathcal{A}$:*

$$\gamma = p_0 \xrightarrow{a_{i_1}^{\epsilon_1}} p_1 \xrightarrow{a_{i_2}^{\epsilon_2}} p_2 \cdots p_{n-1} \xrightarrow{a_{i_n}^{\epsilon_n}} p_n$$

- *the label of γ is label$(\gamma) = a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n} \in \tilde{A}^*$,*
- *notation: $\gamma = p \xrightarrow{w} q$ means a path from p to q with label w.*
- *The notion of reduced path.*

Lemma

Let $p \xrightarrow{w} q$ be a path in $\mathcal{A}$. If w is reduced then $p \xrightarrow{w} q$ is reduced. The convers is not true.

Paths

Definition

Let $\mathcal{A}$ be an A-automaton.

- *A path of length n in $\mathcal{A}$:*

$$\gamma = p_0 \xrightarrow{a_{i_1}^{\epsilon_1}} p_1 \xrightarrow{a_{i_2}^{\epsilon_2}} p_2 \cdots p_{n-1} \xrightarrow{a_{i_n}^{\epsilon_n}} p_n$$

- *the label of γ is $label(\gamma) = a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n} \in \tilde{A}^*$,*
- *notation: $\gamma = p \xrightarrow{w} q$ means a path from p to q with label w.*
- *The notion of reduced path.*

Lemma

Let $p \xrightarrow{w} q$ be a path in $\mathcal{A}$. If w is reduced then $p \xrightarrow{w} q$ is reduced. The convers is not true.

Paths

Definition

Let $\mathcal{A}$ be an A-automaton.

- *A path of length n in $\mathcal{A}$:*

$$\gamma = p_0 \xrightarrow{a_{i_1}^{\epsilon 1}} p_1 \xrightarrow{a_{i_2}^{\epsilon 2}} p_2 \cdots p_{n-1} \xrightarrow{a_{i_n}^{\epsilon n}} p_n$$

- *the label of γ is $label(\gamma) = a_{i_1}^{\epsilon 1} \cdots a_{i_n}^{\epsilon n} \in \tilde{A}^*$,*
- *notation: $\gamma = p \xrightarrow{w} q$ means a path from p to q with label w.*
- *The notion of reduced path.*

Lemma

Let $p \xrightarrow{w} q$ be a path in $\mathcal{A}$. If w is reduced then $p \xrightarrow{w} q$ is reduced. The convers is not true.

Paths

Definition

Let $\mathcal{A}$ be an A-automaton.

- *A path of length n in $\mathcal{A}$:*

$$\gamma = p_0 \xrightarrow{a_{i_1}^{\epsilon_1}} p_1 \xrightarrow{a_{i_2}^{\epsilon_2}} p_2 \cdots p_{n-1} \xrightarrow{a_{i_n}^{\epsilon_n}} p_n$$

- *the label of γ is $label(\gamma) = a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n} \in \tilde{A}^*$,*
- *notation: $\gamma = p \xrightarrow{w} q$ means a path from p to q with label w.*
- *The notion of reduced path.*

Lemma

Let $p \xrightarrow{w} q$ be a path in $\mathcal{A}$. If w is reduced then $p \xrightarrow{w} q$ is reduced. The convers is not true.

Paths

Definition

Let $\mathcal{A}$ be an A-automaton.

- *A path of length n in $\mathcal{A}$:*

$$\gamma = p_0 \xrightarrow{a_{i_1}^{\epsilon_1}} p_1 \xrightarrow{a_{i_2}^{\epsilon_2}} p_2 \cdots p_{n-1} \xrightarrow{a_{i_n}^{\epsilon_n}} p_n$$

- *the label of γ is $label(\gamma) = a_{i_1}^{\epsilon_1} \cdots a_{i_n}^{\epsilon_n} \in \tilde{A}^*$,*
- *notation: $\gamma = p \xrightarrow{w} q$ means a path from p to q with label w.*
- *The notion of reduced path.*

Lemma

Let $p \xrightarrow{w} q$ be a path in $\mathcal{A}$. If w is reduced then $p \xrightarrow{w} q$ is reduced. The convers is not true.

Determinism

Definition

An A-automaton $\mathcal{A}$ is deterministic if

- $e = (p, a, q) \in E$, $e' = (p, a, q') \in E$ imply $q = q'$ (so, $e = e'$),
- $e = (p, a, q) \in E$, $e' = (p', a, q) \in E$ imply $p = p'$ (so, $e = e'$).

Lemma

Let $\mathcal{A}$ be a deterministic A-automaton. Then we have,

i) $p \xrightarrow{w} q$ is reduced $\Leftrightarrow$ w is reduced,

ii) $\exists\, p \xrightarrow{w} q$, $\exists\, p \xrightarrow{w} q'$ then $q = q'$ (so, they are the same path),

iii) $\exists\, p \xrightarrow{w} q$, $\exists\, p' \xrightarrow{w} q$ then $p = p'$ (so, they are the same path),

iv) A reduced w can ONLY be spelled by a unique possible path (if any) from $\mathcal{A}$ with a given origin or end,

v) if $\exists\, p \xrightarrow{w} q$ then $\exists\, p \xrightarrow{\overline{w}} q'$.

Determinism

Definition

An A-automaton $\mathcal{A}$ is deterministic if

- $e = (p, a, q) \in E$, $e' = (p, a, q') \in E$ imply $q = q'$ (so, $e = e'$),
- $e = (p, a, q) \in E$, $e' = (p', a, q) \in E$ imply $p = p'$ (so, $e = e'$).

Lemma

Let $\mathcal{A}$ be a deterministic A-automaton. Then we have,

i) $p \xrightarrow{w} q$ is reduced $\Leftrightarrow$ w is reduced,

ii) $\exists\, p \xrightarrow{w} q, \exists\, p \xrightarrow{w} q'$ then $q = q'$ (so, they are the same path),

iii) $\exists\, p \xrightarrow{w} q, \exists\, p' \xrightarrow{w} q$ then $p = p'$ (so, they are the same path),

iv) A reduced w can ONLY be spelled by a unique possible path (if any) from $\mathcal{A}$ with a given origin or end,

v) if $\exists\, p \xrightarrow{w} q$ then $\exists\, p \xrightarrow{\overline{w}} q'$.

Determinism

Definition

An A-automaton $\mathcal{A}$ is deterministic if

- $e = (p, a, q) \in E$, $e' = (p, a, q') \in E$ *imply* $q = q'$ *(so,* $e = e'$*),*
- $e = (p, a, q) \in E$, $e' = (p', a, q) \in E$ *imply* $p = p'$ *(so,* $e = e'$*).*

Lemma

Let $\mathcal{A}$ be a deterministic A-automaton. Then we have,

i) $p \xrightarrow{w} q$ *is reduced* $\Leftrightarrow$ w *is reduced,*

ii) $\exists\, p \xrightarrow{w} q$, $\exists\, p \xrightarrow{w} q'$ *then* $q = q'$ *(so, they are the same path),*

iii) $\exists\, p \xrightarrow{w} q$, $\exists\, p' \xrightarrow{w} q$ *then* $p = p'$ *(so, they are the same path),*

iv) *A reduced w can ONLY be spelled by a unique possible path (if any) from $\mathcal{A}$ with a given origin or end,*

v) *if* $\exists\, p \xrightarrow{w} q$ *then* $\exists\, p \xrightarrow{\overline{w}} q'$.

Determinism

Definition

An A-automaton $\mathcal{A}$ is deterministic if

- $e = (p, a, q) \in E$, $e' = (p, a, q') \in E$ *imply* $q = q'$ *(so,* $e = e'$*),*
- $e = (p, a, q) \in E$, $e' = (p', a, q) \in E$ *imply* $p = p'$ *(so,* $e = e'$*).*

Lemma

Let $\mathcal{A}$ be a deterministic A-automaton. Then we have,

i) $p \xrightarrow{w} q$ *is reduced* $\Leftrightarrow$ w *is reduced,*

ii) $\exists\ p \xrightarrow{w} q$, $\exists\ p \xrightarrow{w} q'$ *then* $q = q'$ *(so, they are the same path),*

iii) $\exists\ p \xrightarrow{w} q$, $\exists\ p' \xrightarrow{w} q$ *then* $p = p'$ *(so, they are the same path),*

iv) *A reduced w can ONLY be spelled by a unique possible path (if any) from $\mathcal{A}$ with a given origin or end,*

v) *if* $\exists\ p \xrightarrow{w} q$ *then* $\exists\ p \xrightarrow{\overline{w}} q'$.

Determinism

Definition

An A-automaton $\mathcal{A}$ is deterministic if

- $e = (p, a, q) \in E$, $e' = (p, a, q') \in E$ *imply* $q = q'$ *(so,* $e = e'$*),*
- $e = (p, a, q) \in E$, $e' = (p', a, q) \in E$ *imply* $p = p'$ *(so,* $e = e'$*).*

Lemma

Let $\mathcal{A}$ be a deterministic A-automaton. Then we have,

i) $p \xrightarrow{w} q$ *is reduced* $\Leftrightarrow$ w *is reduced,*

ii) $\exists\ p \xrightarrow{w} q$, $\exists\ p \xrightarrow{w} q'$ *then* $q = q'$ *(so, they are the same path),*

iii) $\exists\ p \xrightarrow{w} q$, $\exists\ p' \xrightarrow{w} q$ *then* $p = p'$ *(so, they are the same path),*

iv) *A reduced w can ONLY be spelled by a unique possible path (if any) from $\mathcal{A}$ with a given origin or end,*

v) *if* $\exists\ p \xrightarrow{w} q$ *then* $\exists\ p \xrightarrow{\overline{w}} q'$.

Determinism

Definition

An A-automaton $\mathcal{A}$ is deterministic if

- $e = (p, a, q) \in E$, $e' = (p, a, q') \in E$ *imply* $q = q'$ *(so,* $e = e'$*),*
- $e = (p, a, q) \in E$, $e' = (p', a, q) \in E$ *imply* $p = p'$ *(so,* $e = e'$*).*

Lemma

Let $\mathcal{A}$ be a deterministic A-automaton. Then we have,

i) $p \xrightarrow{w} q$ *is reduced* $\Leftrightarrow$ w *is reduced,*

ii) $\exists\ p \xrightarrow{w} q$, $\exists\ p \xrightarrow{w} q'$ *then* $q = q'$ *(so, they are the same path),*

iii) $\exists\ p \xrightarrow{w} q$, $\exists\ p' \xrightarrow{w} q$ *then* $p = p'$ *(so, they are the same path),*

iv) *A reduced w can ONLY be spelled by a unique possible path (if any) from $\mathcal{A}$ with a given origin or end,*

v) *if* $\exists\ p \xrightarrow{w} q$ *then* $\exists\ p \xrightarrow{\overline{w}} q'$.

The language of an automaton

Definition

The language of an A-automaton $\mathcal{A}$, is

$$L(\mathcal{A}) = \{w \in \tilde{A}^* \mid \exists\, q_0 \xrightarrow{w} q_0\} \subseteq F(A).$$

Also called the fundamental group of $\mathcal{A}$ at q_0.

Observation

$L(\mathcal{A})$ is a subgroup of $F(A)$.

Example

$L\Big($

$\Big) = \langle a, b \rangle$ *and* $L\Big($

$\Big) = \langle a, b^2 \rangle$*, both inside the free group* $F(\{a, b\})$.

The language of an automaton

Definition

The language of an A-automaton $\mathcal{A}$, is

$$L(\mathcal{A}) = \{ w \in \tilde{A}^* \mid \exists\, q_0 \xrightarrow{w} q_0 \} \subseteq F(A).$$

Also called the fundamental group of $\mathcal{A}$ at q_0.

Observation

$L(\mathcal{A})$ is a subgroup of $F(A)$.

Example

$L\Big($

$\Big) = \langle a, b \rangle$ *and* $L\Big($

$\Big) = \langle a, b^2 \rangle$*, both inside the free group* $F(\{a, b\})$.

The language of an automaton

Definition

The language of an A-automaton $\mathcal{A}$, is

$$L(\mathcal{A}) = \{w \in \tilde{A}^* \mid \exists\, q_0 \xrightarrow{w} q_0\} \subseteq F(A).$$

Also called the fundamental group of $\mathcal{A}$ at q_0.

Observation

$L(\mathcal{A})$ is a subgroup of $F(A)$.

Example

$L\Big($

$\Big) = \langle a, b \rangle$ *and* $L\Big($

$\Big) = \langle a, b^2 \rangle$, *both inside the free group* $F(\{a, b\})$.

The language of an automaton

Definition

The *language* *of an A-automaton* $\mathcal{A}$*, is*

$$L(\mathcal{A}) = \{w \in \tilde{A}^* \mid \exists\, q_0 \xrightarrow{w} q_0\} \subseteq F(A).$$

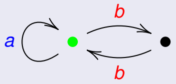
Also called the *fundamental group of* $\mathcal{A}$ *at* q_0.

Observation

$L(\mathcal{A})$ *is a subgroup of* $F(A)$.

Example

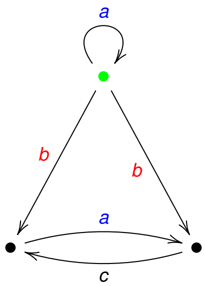
$L($ 

$) = \langle a, b\rangle$ *and* $L\Bigg($ 

$\Bigg) = \langle a, b^2\rangle$, *both inside the free group* $F(\{a, b\})$.

Back to the membership problem

$\mathcal{A} =$



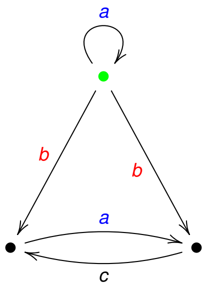
$a \in L(\mathcal{A})$

$bab^{-1} \in L(\mathcal{A})$

But $ba^2cb^{-1} \in L(\mathcal{A})$, because $ba^2cb^{-1} = bab^{-1}bacb^{-1} \in L(\mathcal{A})$.

Back to the membership problem

$\mathcal{A} =$



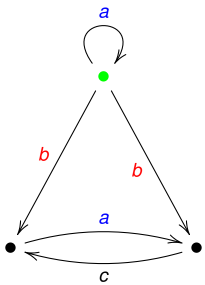
$a \in L(\mathcal{A})$

$bab^{-1} \in L(\mathcal{A})$

But $ba^2cb^{-1} \in L(\mathcal{A})$, because $ba^2cb^{-1} = bab^{-1}bacb^{-1} \in L(\mathcal{A})$.

Back to the membership problem

$\mathcal{A} =$



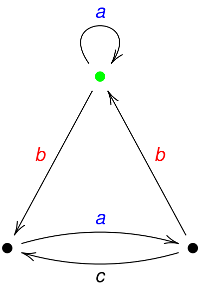
$a \in L(\mathcal{A})$

$bab^{-1} \in L(\mathcal{A})$

But $ba^2cb^{-1} \in L(\mathcal{A})$, because $ba^2cb^{-1} = bab^{-1}bacb^{-1} \in L(\mathcal{A})$.

Back to the membership problem

$\mathcal{B} =$



$a \in L(\mathcal{B})$

$bab \in L(\mathcal{B})$

$bab^{-1} \notin L(\mathcal{B})$

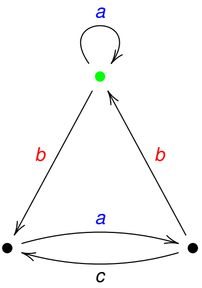
$ba^2cb^{-1} \notin L(\mathcal{B})$

Observation

Membership in F_r is solvable for language subgroups of (given) deterministic automata.

Back to the membership problem

$\mathcal{B} =$



$a \in L(\mathcal{B})$

$bab \in L(\mathcal{B})$

$bab^{-1} \notin L(\mathcal{B})$

$ba^2cb^{-1} \notin L(\mathcal{B})$

Observation

Membership in F_r is solvable for language subgroups of (given) deterministic automata.

Outline

Stallings automata

Definition

A ***Stallings automaton over A*** *is a finite A-automaton (V, E, q_0), such that:*

1- *it is* ***connected****,*

2- *it is* ***trim****, (****no*** *vertex of degree 1 except possibly q_0),*

3- *it is* ***deterministic*** *(****no*** *two edges with the same label go out of (or in to) the same vertex).*

NO :

YES :

Stallings automata

Definition

A Stallings automaton over A is a finite A-automaton (V, E, q_0), such that:

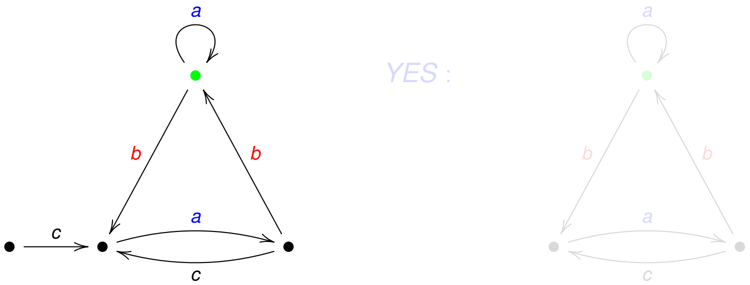
1- *it is connected,*

2- *it is trim, (no vertex of degree 1 except possibly q_0),*

3- *it is deterministic (no two edges with the same label go out of (or in to) the same vertex).*

NO :

YES :



Stallings automata

Definition

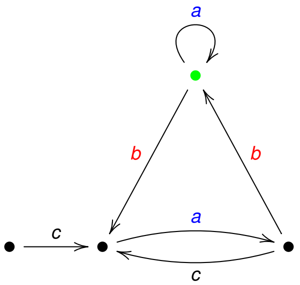
A Stallings automaton over A is a finite A-automaton (V, E, q_0), such that:

1- *it is connected,*

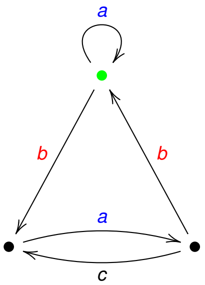
2- *it is trim, (no vertex of degree 1 except possibly q_0),*

3- *it is deterministic (no two edges with the same label go out of (or in to) the same vertex).*

NO :



YES :



Stallings automata

In the influent paper

J. R. Stallings, Topology of finite graphs, Inventiones Math. 71 (1983), 551-565,

Stallings (building on previous works) gave a bijection between finitely generated subgroups of $F(A)$ and Stallings automata:

$$\{\text{f.g. subgroups of } F(A)\} \quad \longleftrightarrow \quad \{\text{Stallings automata over } A\},$$

which is crucial for the modern understanding of the lattice of subgroups of $F(A)$.

Stallings automata

In the influent paper

J. R. Stallings, Topology of finite graphs, Inventiones Math. 71 (1983), 551-565,

Stallings (building on previous works) gave a bijection between finitely generated subgroups of $F(A)$ and Stallings automata:

$$\{\text{f.g. subgroups of } F(A)\} \longleftrightarrow \{\text{Stallings automata over } A\},$$

which is crucial for the modern understanding of the lattice of subgroups of $F(A)$.

Stallings automata

In the influent paper

J. R. Stallings, Topology of finite graphs, Inventiones Math. 71 (1983), 551-565,

Stallings (building on previous works) gave a bijection between finitely generated subgroups of $F(A)$ and Stallings automata:

$$\{\text{f.g. subgroups of } F(A)\} \quad \longleftrightarrow \quad \{\text{Stallings automata over } A\},$$

which is crucial for the modern understanding of the lattice of subgroups of $F(A)$.

Reading the subgroup from the automata

Definition

To any given Stallings automaton $\mathcal{A} = (V, E, q_0)$, we associate its ***language****:*

$$L(\mathcal{A}) = \{ \text{ labels of closed paths at } q_0 \} \leqslant F(A).$$

$$L(\mathcal{A}) = \{1, a, a^{-1}, bab, bc^{-1}b, babab^{-1}cb^{-1}, \ldots\}$$

$$L(\mathcal{A}) \not\ni bc^{-1}bcaa$$

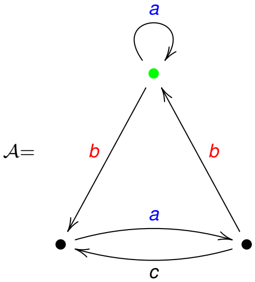
Membership problem in $L(\mathcal{A})$ is solvable.

Reading the subgroup from the automata

Definition

To any given Stallings automaton $\mathcal{A} = (V, E, q_0)$, we associate its language:

$$L(\mathcal{A}) = \{ \text{ labels of closed paths at } q_0 \} \leqslant F(A).$$



$L(\mathcal{A}) = \{1, a, a^{-1}, bab, bc^{-1}b, babab^{-1}cb^{-1}, \ldots\}$

$L(\mathcal{A}) \not\ni bc^{-1}bcaa$

Membership problem in $L(\mathcal{A})$ is solvable.

A basis for $\mathcal{A}$

Proposition

For every Stallings automaton $\mathcal{A} = (V, E, q_0)$, the group $L(\mathcal{A})$ is free of rank $rk(L(\mathcal{A})) = 1 - |V| + |E|$.

Proof:

- Take a maximal tree T in $\mathcal{A}$.
- Write $T[p, q]$ for the geodesic (i.e. the unique reduced path) in T from p to q.
- For every $e \in EX - ET$, $x_e = label(T[q_0, \iota e] \cdot e \cdot T[\tau e, q_0]) \in L(\mathcal{A})$.
- Not difficult to see that $\{x_e \mid e \in E - ET\}$ is a basis for $L(\mathcal{A})$.
- And, $|E - ET| = |E| - |ET| = |E| - (|VT| - 1) = 1 - |V| + |E|$. □

A basis for $\mathcal{A}$

Proposition

For every Stallings automaton $\mathcal{A} = (V, E, q_0)$, the group $L(\mathcal{A})$ is free of rank $rk(L(\mathcal{A})) = 1 - |V| + |E|$.

Proof:

- Take a maximal tree T in $\mathcal{A}$.
- Write $T[p, q]$ for the geodesic (i.e. the unique reduced path) in T from p to q.
- For every $e \in EX - ET$, $x_e = label(T[q_0, \iota e] \cdot e \cdot T[\tau e, q_0]) \in L(\mathcal{A})$.
- Not difficult to see that $\{x_e \mid e \in E - ET\}$ is a basis for $L(\mathcal{A})$.
- And, $$\begin{aligned} |E - ET| &= |E| - |ET| \\ &= |E| - (|VT| - 1) = 1 - |V| + |E|. \ \square \end{aligned}$$

A basis for $\mathcal{A}$

Proposition

For every Stallings automaton $\mathcal{A} = (V, E, q_0)$, the group $L(\mathcal{A})$ is free of rank $rk(L(\mathcal{A})) = 1 - |V| + |E|$.

Proof:

- Take a maximal tree T in $\mathcal{A}$.
- Write $T[p, q]$ for the geodesic (i.e. the unique reduced path) in T from p to q.
- For every $e \in EX - ET$, $x_e = label(T[q_0, \iota e] \cdot e \cdot T[\tau e, q_0]) \in L(\mathcal{A})$.
- Not difficult to see that $\{x_e \mid e \in E - ET\}$ is a basis for $L(\mathcal{A})$.
- And, $|E - ET| = |E| - |ET| = |E| - (|VT| - 1) = 1 - |V| + |E|$. $\square$

A basis for $\mathcal{A}$

Proposition

For every Stallings automaton $\mathcal{A} = (V, E, q_0)$, the group $L(\mathcal{A})$ is free of rank $rk(L(\mathcal{A})) = 1 - |V| + |E|$.

Proof:

- Take a maximal tree T in $\mathcal{A}$.
- Write $T[p, q]$ for the geodesic (i.e. the unique reduced path) in T from p to q.
- For every $e \in EX - ET$, $x_e = label(T[q_0, \iota e] \cdot e \cdot T[\tau e, q_0]) \in L(\mathcal{A})$.
- Not difficult to see that $\{x_e \mid e \in E - ET\}$ is a basis for $L(\mathcal{A})$.
- And, $|E - ET| = |E| - |ET| = |E| - (|VT| - 1) = 1 - |V| + |E|$. $\square$

A basis for $\mathcal{A}$

Proposition

For every Stallings automaton $\mathcal{A} = (V, E, q_0)$, the group $L(\mathcal{A})$ is free of rank $rk(L(\mathcal{A})) = 1 - |V| + |E|$.

Proof:

- Take a maximal tree T in $\mathcal{A}$.
- Write $T[p, q]$ for the geodesic (i.e. the unique reduced path) in T from p to q.
- For every $e \in EX - ET$,
  $x_e = label(T[q_0, \iota e] \cdot e \cdot T[\tau e, q_0]) \in L(\mathcal{A})$.
- Not difficult to see that $\{x_e \mid e \in E - ET\}$ is a basis for $L(\mathcal{A})$.
- And, $|E - ET| = |E| - |ET| = |E| - (|VT| - 1) = 1 - |V| + |E|$. □

A basis for $\mathcal{A}$

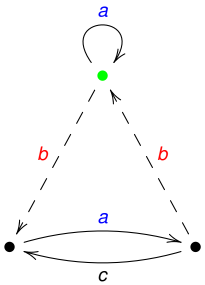
Proposition

For every Stallings automaton $\mathcal{A} = (V, E, q_0)$, the group $L(\mathcal{A})$ is free of rank $rk(L(\mathcal{A})) = 1 - |V| + |E|$.

Proof:

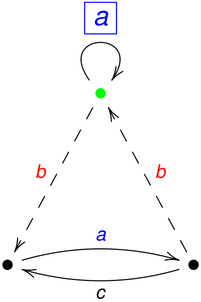
- Take a maximal tree T in $\mathcal{A}$.
- Write $T[p, q]$ for the geodesic (i.e. the unique reduced path) in T from p to q.
- For every $e \in EX - ET$, $x_e = label(T[q_0, \iota e] \cdot e \cdot T[\tau e, q_0]) \in L(\mathcal{A})$.
- Not difficult to see that $\{x_e \mid e \in E - ET\}$ is a basis for $L(\mathcal{A})$.
- And, $$\begin{aligned} |E - ET| &= |E| - |ET| \\ &= |E| - (|VT| - 1) = 1 - |V| + |E|. \ \square \end{aligned}$$

Example



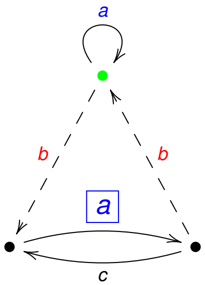
$H = \langle \quad \rangle$

Example



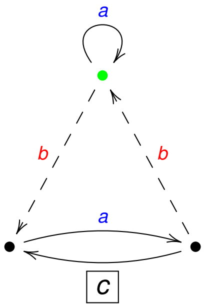
$H = \langle a, \quad \rangle$

Example



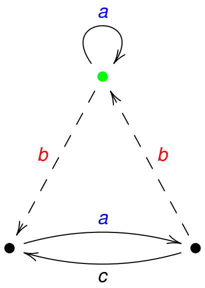
$H = \langle a, \ bab, \quad \rangle$

Example



$H = \langle a, \; bab, \; b^{-1}cb^{-1} \rangle$

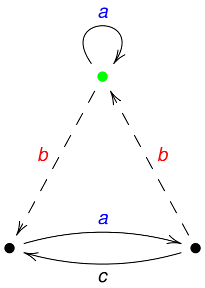
Example



$H = \langle a,\ bab,\ b^{-1}cb^{-1} \rangle \leqslant F(\{a, b, c\})$

$rk(H) = 1 - 3 + 5 = 3.$

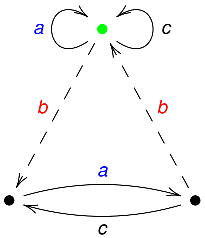
Example



$H = \langle a,\ bab,\ b^{-1}cb^{-1} \rangle \leqslant F(\{a, b, c\})$

$rk(H) = 1 - 3 + 5 = 3.$

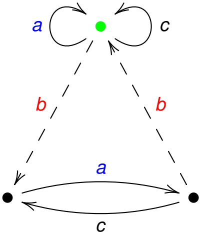
Example-2



$H = \langle a,\ c,\ bab,\ b^{-1}cb^{-1} \rangle \leqslant F(\{a, b, c\})$.

$rk(H) = 1 - 3 + 6 = 4$ and it is a subgroup of F_3 !!!

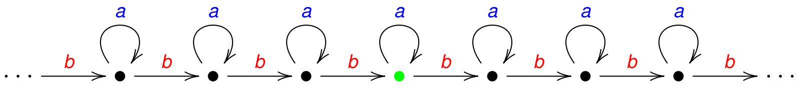
Example-2



$H = \langle a,\ c,\ bab,\ b^{-1}cb^{-1} \rangle \leqslant F(\{a, b, c\})$.

$rk(H) = 1 - 3 + 6 = 4$ and it is a subgroup of F_3 !!!

Example-3



$$F_{\aleph_0} \simeq H = \langle \ldots, b^{-2}ab^2, b^{-1}ab, a, bab^{-1}, b^2ab^{-2}, \ldots \rangle \leqslant F_2.$$

Constructing the automaton from the subgroup

Given $H = \langle w_1, \ldots, w_n \rangle \in F(A)$*, construct the* ***flower automaton****, denoted* $\mathcal{F}(H)$.

Clearly, $L(\mathcal{F}(H)) = H$.

... But $\mathcal{F}(H)$ *is not in general deterministic...*

Constructing the automaton from the subgroup

Given $H = \langle w_1, \ldots, w_n \rangle \in F(A)$, construct the flower automaton, denoted $\mathcal{F}(H)$.

Clearly, $L(\mathcal{F}(H)) = H$.

... But $\mathcal{F}(H)$ is not in general deterministic...

Constructing the automaton from the subgroup

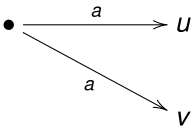
Given $H = \langle w_1, \ldots, w_n \rangle \in F(A)$, construct the flower automaton, denoted $\mathcal{F}(H)$.

Clearly, $L(\mathcal{F}(H)) = H$.

... But $\mathcal{F}(H)$ is not in general deterministic...

Constructing the automaton from the subgroup

In any automaton $\mathcal{A}$ containing the following situation, for $a \in A^{\pm 1}$,

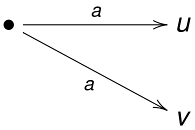


we can fold and identify vertices u and v to obtain

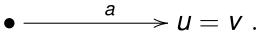
This operation, $\mathcal{A} \rightsquigarrow \mathcal{A}'$, is called a Stallings folding.

Constructing the automaton from the subgroup

In any automaton $\mathcal{A}$ containing the following situation, for $a \in A^{\pm 1}$,



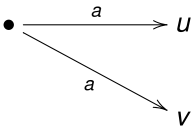
we can fold and identify vertices u and v to obtain



This operation, $\mathcal{A} \rightsquigarrow \mathcal{A}'$, is called a Stallings folding.

Constructing the automaton from the subgroup

In any automaton $\mathcal{A}$ containing the following situation, for $a \in A^{\pm 1}$,



we can fold and identify vertices u and v to obtain

$$\bullet \xrightarrow{\;a\;} u = v\ .$$

This operation, $\mathcal{A} \rightsquigarrow \mathcal{A}'$, is called a Stallings folding.

Constructing the automata from the subgroup

Lemma (Stallings)

If $\mathcal{A} \rightsquigarrow \mathcal{A}'$ is a Stallings folding then $L(\mathcal{A}) = L(\mathcal{A}')$.

Given a f.g. subgroup $H = \langle w_1, \ldots, w_n \rangle \leqslant F_A$ (we assume w_i are reduced words), do the following:

1- *Draw the flower automaton,*

2- *Perform successive foldings until obtaining a Stallings automaton, denoted $\Gamma(H)$.*

Constructing the automata from the subgroup

Lemma (Stallings)

If $\mathcal{A} \rightsquigarrow \mathcal{A}'$ is a Stallings folding then $L(\mathcal{A}) = L(\mathcal{A}')$.

Given a f.g. subgroup $H = \langle w_1, \ldots, w_n \rangle \leqslant F_A$ (we assume w_i are reduced words), do the following:

1- *Draw the flower automaton,*

2- *Perform successive foldings until obtaining a Stallings automaton, denoted $\Gamma(H)$.*

Constructing the automata from the subgroup

Lemma (Stallings)

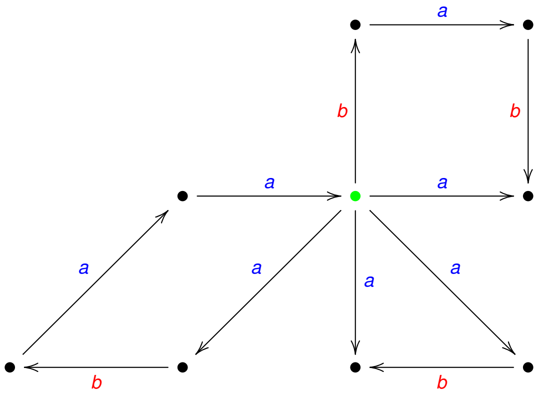
If $\mathcal{A} \rightsquigarrow \mathcal{A}'$ is a Stallings folding then $L(\mathcal{A}) = L(\mathcal{A}')$.

Given a f.g. subgroup $H = \langle w_1, \ldots, w_n \rangle \leqslant F_A$ (we assume w_i are reduced words), do the following:

1- *Draw the flower automaton,*

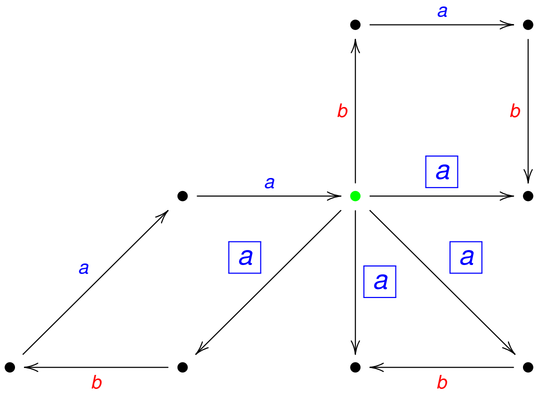
2- *Perform successive foldings until obtaining a Stallings automaton, denoted $\Gamma(H)$.*

Example: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



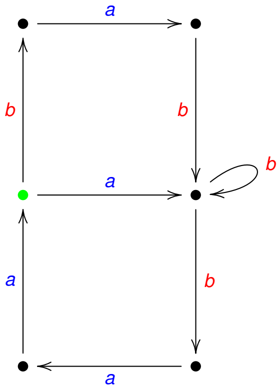
Flower(H)

Example: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



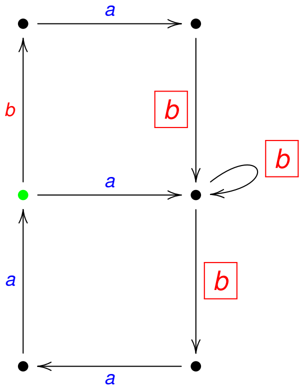
Flower(H)

Example: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



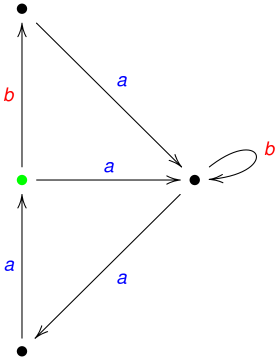
Folding #1

Example: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



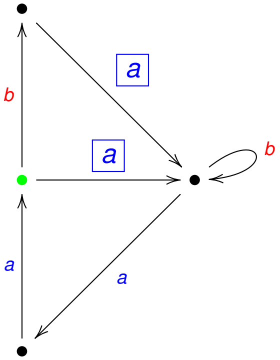
Folding $\#1$.

Example: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



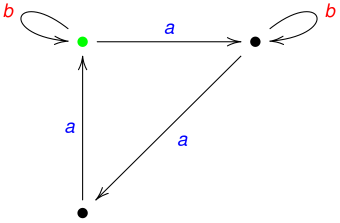
Folding #2.

Example: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



Folding #2.

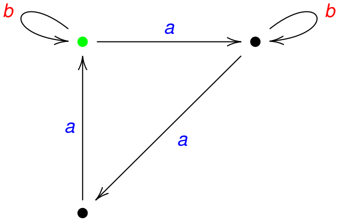
Example: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



Folding #3. $\Gamma(H)$

By Stallings Lemma, $L(\Gamma(H)) = H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$

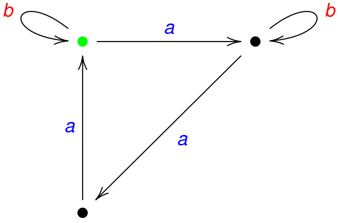
Example: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



Folding #3. $\Gamma(H)$

By Stallings Lemma, $L(\Gamma(H)) = H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$

Example: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



Folding $\#3$. $\Gamma(H)$

By Stallings Lemma, $L(\Gamma(H)) = H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$
$= \langle b, aba^{-1}, a^3 \rangle$

Local confluence

It can be shown that

Proposition

The automaton $\Gamma(H)$ does not depend on the sequence of foldings.

Proposition

The automaton $\Gamma(H)$ does not depend on the generators of H.

Theorem

The following is a well defined bijection:

$$\begin{array}{ccc} \{\text{f.g. subgroups of } F_A\} & \longleftrightarrow & \{\text{Stallings automata}\} \\ H & \rightarrow & \Gamma(H) \\ L(\mathcal{A}) & \leftarrow & \mathcal{A} \end{array}$$

Local confluence

It can be shown that

Proposition

The automaton $\Gamma(H)$ does not depend on the sequence of foldings.

Proposition

The automaton $\Gamma(H)$ does not depend on the generators of H.

Theorem

The following is a well defined bijection:

$$\begin{array}{rcl} \{\text{f.g. subgroups of } F_A\} & \longleftrightarrow & \{\text{Stallings automata}\} \\ H & \to & \Gamma(H) \\ L(\mathcal{A}) & \leftarrow & \mathcal{A} \end{array}$$

Local confluence

It can be shown that

Proposition

The automaton $\Gamma(H)$ does not depend on the sequence of foldings.

Proposition

The automaton $\Gamma(H)$ does not depend on the generators of H.

Theorem

The following is a well defined bijection:

$$\begin{array}{rcl} \{\text{f.g. subgroups of } F_A\} & \longleftrightarrow & \{\text{Stallings automata}\} \\ H & \to & \Gamma(H) \\ L(\mathcal{A}) & \leftarrow & \mathcal{A} \end{array}$$

Outline

Nielsen-Schreier Theorem

Corollary (Nielsen-Schreier)

Every subgroup of F_A is free.

- Finite automata work for the finitely generated case, but everything extends easily to the general case (using infinite graphs).
- The original proof (1920's) is combinatorial and much more technical.

Nielsen-Schreier Theorem

Corollary (Nielsen-Schreier)

Every subgroup of F_A is free.

- Finite automata work for the finitely generated case, but everything extends easily to the general case (using infinite graphs).
- The original proof (1920's) is combinatorial and much more technical.

Nielsen-Schreier Theorem

Corollary (Nielsen-Schreier)

Every subgroup of F_A is free.

- Finite automata work for the finitely generated case, but everything extends easily to the general case (using infinite graphs).
- The original proof (1920's) is combinatorial and much more technical.

Membership problem

Theorem

Free groups have solvable membership problem.

Proof:

- Given w_0 and $H = \langle w_1, \ldots, w_n \rangle$ in F_m,
- Construct the flower automaton $\mathcal{F}(H)$,
- Fold to obtain $\Gamma(H)$,
- Check whether $\overline{w_0}$ is readable as a loop in $\Gamma(H)$ at the basepoint.

Membership problem

Theorem

Free groups have solvable membership problem.

Proof:

- Given w_0 and $H = \langle w_1, \ldots, w_n \rangle$ in F_m,
- Construct the flower automaton $\mathcal{F}(H)$,
- Fold to obtain $\Gamma(H)$,
- Check whether $\overline{w_0}$ is readable as a loop in $\Gamma(H)$ at the basepoint.

Membership problem

Theorem

Free groups have solvable membership problem.

Proof:

- Given w_0 and $H = \langle w_1, \ldots, w_n \rangle$ in F_m,
- Construct the flower automaton $\mathcal{F}(H)$,
- Fold to obtain $\Gamma(H)$,
- Check whether $\overline{w_0}$ is readable as a loop in $\Gamma(H)$ at the basepoint.

Membership problem

Theorem

Free groups have solvable membership problem.

Proof:

- Given w_0 and $H = \langle w_1, \ldots, w_n \rangle$ in F_m,
- Construct the flower automaton $\mathcal{F}(H)$,
- Fold to obtain $\Gamma(H)$,
- Check whether $\overline{w_0}$ is readable as a loop in $\Gamma(H)$ at the basepoint.

Membership problem

Theorem

Free groups have solvable membership problem.

Proof:

- Given w_0 and $H = \langle w_1, \ldots, w_n \rangle$ in F_m,
- Construct the flower automaton $\mathcal{F}(H)$,
- Fold to obtain $\Gamma(H)$,
- Check whether $\overline{w_0}$ is readable as a loop in $\Gamma(H)$ at the basepoint.

Intersection problem

Theorem

Free groups have solvable intersection problem.

Proof:

- Given $H = \langle u_1, \ldots, u_n \rangle$ and $K = \langle v_1, \ldots, v_m \rangle$,
- Construct the Stallings graphs $\Gamma(H)$ and $\Gamma(K)$,
- Construct the pull-back graph $\Gamma(H) \times_A \Gamma(K)$,
- Take the connected component of the basepoint and trim it,
- This is, precisely, $\Gamma(H \cap K)$,
- Choose a maximal tree and compute a basis for $H \cap K$. □

Intersection problem

Theorem

Free groups have solvable intersection problem.

Proof:

- Given $H = \langle u_1, \ldots, u_n \rangle$ and $K = \langle v_1, \ldots, v_m \rangle$,
- Construct the Stallings graphs $\Gamma(H)$ and $\Gamma(K)$,
- Construct the pull-back graph $\Gamma(H) \times_A \Gamma(K)$,
- Take the connected component of the basepoint and trim it,
- This is, precisely, $\Gamma(H \cap K)$,
- Choose a maximal tree and compute a basis for $H \cap K$. $\square$

Intersection problem

Theorem

Free groups have solvable intersection problem.

Proof:

- Given $H = \langle u_1, \ldots, u_n \rangle$ and $K = \langle v_1, \ldots, v_m \rangle$,
- Construct the Stallings graphs $\Gamma(H)$ and $\Gamma(K)$,
- Construct the pull-back graph $\Gamma(H) \times_A \Gamma(K)$,
- Take the connected component of the basepoint and trim it,
- This is, precisely, $\Gamma(H \cap K)$,
- Choose a maximal tree and compute a basis for $H \cap K$. $\square$

Intersection problem

Theorem

Free groups have solvable intersection problem.

Proof:

- Given $H = \langle u_1, \ldots, u_n \rangle$ and $K = \langle v_1, \ldots, v_m \rangle$,
- Construct the Stallings graphs $\Gamma(H)$ and $\Gamma(K)$,
- Construct the pull-back graph $\Gamma(H) \times_A \Gamma(K)$,
- Take the connected component of the basepoint and trim it,
- This is, precisely, $\Gamma(H \cap K)$,
- Choose a maximal tree and compute a basis for $H \cap K$. □

Intersection problem

Theorem

Free groups have solvable intersection problem.

Proof:

- Given $H = \langle u_1, \ldots, u_n \rangle$ and $K = \langle v_1, \ldots, v_m \rangle$,
- Construct the Stallings graphs $\Gamma(H)$ and $\Gamma(K)$,
- Construct the pull-back graph $\Gamma(H) \times_A \Gamma(K)$,
- Take the connected component of the basepoint and trim it,
- This is, precisely, $\Gamma(H \cap K)$,
- Choose a maximal tree and compute a basis for $H \cap K$. $\square$

Intersection problem

Theorem

Free groups have solvable intersection problem.

Proof:

- Given $H = \langle u_1, \ldots, u_n \rangle$ and $K = \langle v_1, \ldots, v_m \rangle$,
- Construct the Stallings graphs $\Gamma(H)$ and $\Gamma(K)$,
- Construct the pull-back graph $\Gamma(H) \times_A \Gamma(K)$,
- Take the connected component of the basepoint and trim it,
- This is, precisely, $\Gamma(H \cap K)$,
- Choose a maximal tree and compute a basis for $H \cap K$. $\square$

Intersection problem

Theorem

Free groups have solvable intersection problem.

Proof:

- Given $H = \langle u_1, \ldots, u_n \rangle$ and $K = \langle v_1, \ldots, v_m \rangle$,
- Construct the Stallings graphs $\Gamma(H)$ and $\Gamma(K)$,
- Construct the pull-back graph $\Gamma(H) \times_A \Gamma(K)$,
- Take the connected component of the basepoint and trim it,
- This is, precisely, $\Gamma(H \cap K)$,
- Choose a maximal tree and compute a basis for $H \cap K$. $\square$

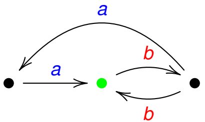
Computing intersections: an example

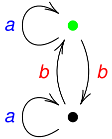
Let $H = \langle a, b^2, bab \rangle$ and $K = \langle b^2, ba^2 \rangle$ be subgroups of F_2.
To compute a basis for $H \cap K$:

$H \cap K = ?$ Clear that $b^2 \in H \cap K$, but.... something else?

Computing intersections: an example

Let $H = \langle a, b^2, bab \rangle$ and $K = \langle b^2, ba^2 \rangle$ be subgroups of F_2.
To compute a basis for $H \cap K$:

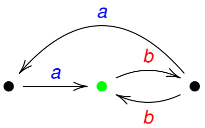


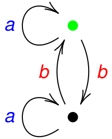


$H \cap K = ?$ Clear that $b^2 \in H \cap K$, but.... something else?

Computing intersections: an example

Let $H = \langle a, b^2, bab \rangle$ and $K = \langle b^2, ba^2 \rangle$ be subgroups of F_2.
To compute a basis for $H \cap K$:

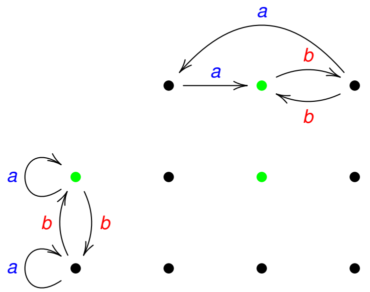




$H \cap K = ?$ Clear that $b^2 \in H \cap K$, but.... something else?

Computing intersections: an example

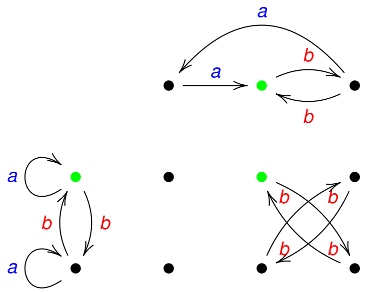
Let $H = \langle a, b^2, bab \rangle$ and $K = \langle b^2, ba^2 \rangle$ be subgroups of F_2.
To compute a basis for $H \cap K$:



$H \cap K = \langle b^2, \ldots (?) \ldots \rangle$

Computing intersections: an example

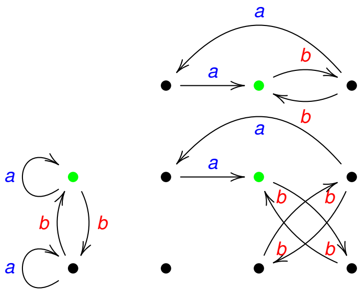
Let $H = \langle a, b^2, bab \rangle$ and $K = \langle b^2, ba^2 \rangle$ be subgroups of F_2.
To compute a basis for $H \cap K$:



$H \cap K = \langle b^2, \quad \rangle$

Computing intersections: an example

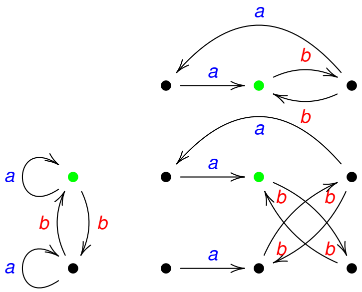
Let $H = \langle a, b^2, bab \rangle$ and $K = \langle b^2, ba^2 \rangle$ be subgroups of F_2.
To compute a basis for $H \cap K$:



$H \cap K = \langle b^2, a^{-2}b^2a^2, \quad \rangle$

Computing intersections: an example

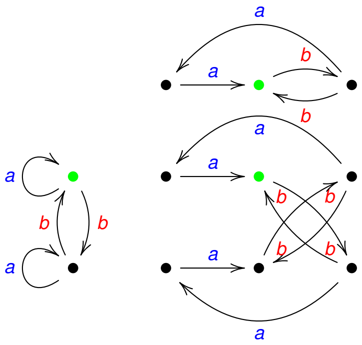
Let $H = \langle a, b^2, bab \rangle$ and $K = \langle b^2, ba^2 \rangle$ be subgroups of F_2.
To compute a basis for $H \cap K$:



$H \cap K = \langle b^2, a^{-2}b^2a^2, \quad \rangle$

Computing intersections: an example

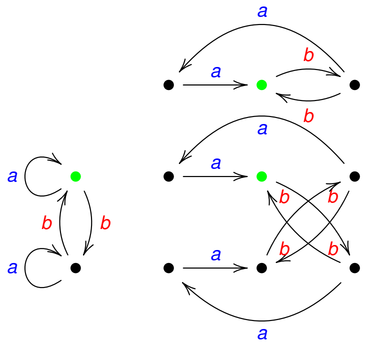
Let $H = \langle a, b^2, bab \rangle$ and $K = \langle b^2, ba^2 \rangle$ be subgroups of F_2.
To compute a basis for $H \cap K$:



$H \cap K = \langle b^2, a^{-2}b^2a^2, ba^2ba^2 \rangle$ ... and nothing else.

Computing intersections: an example

Let $H = \langle a, b^2, bab \rangle$ and $K = \langle b^2, ba^2 \rangle$ be subgroups of F_2.
To compute a basis for $H \cap K$:



$H \cap K = \langle b^2, a^{-2}b^2a^2, ba^2ba^2 \rangle$ ... and nothing else.

Rank of the intersection

Theorem (Howson)

The intersection of finitely generated subgroups of $F(A)$ is again finitely generated.

But the intersection can have bigger rank: "$3 = 3 \cap 2 \leqslant 2$"

Theorem (H. Neumann)

$\tilde{r}(H \cap K) \leqslant 2\tilde{r}(H)\tilde{r}(K)$, *where* $\tilde{r}(H) = \max\{0, r(H) - 1\}$.

Theorem (Friedman, Mineyev 2012 (with simpl. by W. Dicks))

$\tilde{r}(H \cap K) \leqslant \tilde{r}(H)\tilde{r}(K)$.

In the example, $3 - 1 \leqslant (3 - 1)(2 - 1)$.

Rank of the intersection

Theorem (Howson)

The intersection of finitely generated subgroups of $F(A)$ is again finitely generated.

But the intersection can have bigger rank: "$3 = 3 \cap 2 \leqslant 2$"

Theorem (H. Neumann)

$\tilde{r}(H \cap K) \leqslant 2\tilde{r}(H)\tilde{r}(K)$, *where* $\tilde{r}(H) = \max\{0, r(H) - 1\}$.

Theorem (Friedman, Mineyev 2012 (with simpl. by W. Dicks))

$\tilde{r}(H \cap K) \leqslant \tilde{r}(H)\tilde{r}(K)$.

In the example, $3 - 1 \leqslant (3 - 1)(2 - 1)$.

Rank of the intersection

Theorem (Howson)

The intersection of finitely generated subgroups of $F(A)$ is again finitely generated.

But the intersection can have bigger rank: "$3 = 3 \cap 2 \leqslant 2$"

Theorem (H. Neumann)

$\tilde{r}(H \cap K) \leqslant 2\tilde{r}(H)\tilde{r}(K)$, *where* $\tilde{r}(H) = \max\{0, r(H) - 1\}$.

Theorem (Friedman, Mineyev 2012 (with simpl. by W. Dicks))

$\tilde{r}(H \cap K) \leqslant \tilde{r}(H)\tilde{r}(K)$.

In the example, $3 - 1 \leqslant (3 - 1)(2 - 1)$.

Rank of the intersection

Theorem (Howson)

The intersection of finitely generated subgroups of $F(A)$ is again finitely generated.

But the intersection can have bigger rank: "$3 = 3 \cap 2 \leqslant 2$"

Theorem (H. Neumann)

$\tilde{r}(H \cap K) \leqslant 2\tilde{r}(H)\tilde{r}(K)$, *where* $\tilde{r}(H) = \max\{0, r(H) - 1\}$.

Theorem (Friedman, Mineyev 2012 (with simpl. by W. Dicks))

$\tilde{r}(H \cap K) \leqslant \tilde{r}(H)\tilde{r}(K)$.

In the example, $3 - 1 \leqslant (3 - 1)(2 - 1)$.

Rank of the intersection

Theorem (Howson)

The intersection of finitely generated subgroups of $F(A)$ is again finitely generated.

But the intersection can have bigger rank: "$3 = 3 \cap 2 \leqslant 2$"

Theorem (H. Neumann)

$\tilde{r}(H \cap K) \leqslant 2\tilde{r}(H)\tilde{r}(K)$, *where* $\tilde{r}(H) = \max\{0, r(H) - 1\}$.

Theorem (Friedman, Mineyev 2012 (with simpl. by W. Dicks))

$\tilde{r}(H \cap K) \leqslant \tilde{r}(H)\tilde{r}(K)$.

In the example, $3 - 1 \leqslant (3 - 1)(2 - 1)$.

THANKS

KIITOS