Algorithmic Problems in Free Groups

April 5, 2024

Pascal WEIL, CNRS

Freely reduced words

A a finite alphabet / set $\neq \emptyset$

$\bar{A} = \{ \bar{a} \mid a \in A \}$

$\bar{A} \cap A = \emptyset$

$\tilde{A} = A \cup \bar{A}$

$\tilde{A}^* =$ all words on alph $\tilde{A}$

1 is the empty word

Notation $\bar{\bar{a}} = a$ for each $a \in A$

$$x \longmapsto \bar{x}$$
$$\tilde{A} \longrightarrow \tilde{A} \quad \text{bij}$$

Want to see $\bar{a}$ as an (group) <u>inverse</u> of a

Let $\sim$ be the congruence on $\tilde{A}^*$ generated by $a\bar{a} \sim \bar{a}a \sim 1$ for every $a \in \tilde{A}$

$u, v \in \tilde{A}^*$

$u \sim v$ iff $\exists\, u_0 = u, u_1, \dots, u_{n-1}, u_n = v$

s.t. $u_i = pa\bar{a}q$ and $u_{i+1} = pq$

or $u_i = pq$ $u_{i+1} = pa\bar{a}q$

Exple $a b \bar{a} a b \bar{b} a$

$\sim a b b \bar{b} a$

$\sim \boxed{aba}$ reduced

$\sim a \bar{a} a b a$

A word is reduced (freely) if it contains no $a\bar{a}$ or $\bar{a}a$ $(a \in \tilde{A})$

Prop $\boxed{\text{Every word } u \in \tilde{A}^* \text{ is } \sim\text{-equivalent to a unique reduced word}}$ written $\mathrm{red}(u)$

$u = p a \bar{a} a q$

$\downarrow$

$p a q$

B an alphabet, elements are called letters

words are finite sequences of letters

sequences of length 1 = B

sequence of length 0 = the empty word

B^* = all words

$1 \in B^*$, $1 \notin B$

Free group

$F(A)$ = the set of all reduced words in $\tilde{A}^*$

$u, v \in F(A)$

$u \cdot v = \text{red}(uv)$

This operation is associative

- $\sim$ is a congruence
  that is: if $u_1 \sim u_1'$
  $u_2 \sim u_2'$
  then $u_1 u_2 \sim u_1' u_2'$
- $\text{red}(u)$ is unique

1 is an identity element
$(1 \cdot u = u \cdot 1 = u)$

$a \cdot \bar{a} = \bar{a} \cdot a = 1$ for $a \in \tilde{A}$

$\bar{a} = a^{-1}$

$u = a_1 \ldots a_n$ $\quad u^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_1^{-1}$
$a_i \in \tilde{A}$ $\quad = \bar{a}_n \, \bar{a}_{n-1} \ldots \bar{a}_1$

$F(A)$ is a group called the free group on A

$F(A) = \tilde{A}^* / \sim$ quotient monoid, which turns out to be a gp.

- Let G be any group and $\varphi : A \to G$ be any map. Then φ ~~extends~~ extends uniquely to a group homomorphism $\hat{\varphi} : F(A) \to G$

$abac \xmapsto{\hat{\varphi}} \varphi(a)\varphi(b)\varphi(a)\varphi(c)$

$a\bar{a} \mapsto \varphi(a)\underbrace{\varphi(\bar{a})}$ make that $\varphi(\bar{a}) = \varphi(a)^{-1}$

$\hat{\varphi}(\bar{a}) = \varphi(a)^{-1}$

$a.\bar{a}$ in $F(A)$ is 1 so $\hat{\varphi}(a.\bar{a}) = \underbrace{\hat{\varphi}(a)}_{\varphi(a)}\hat{\varphi}(\bar{a}) = 1$

What if I change alphabet

$F(A)$ isomorphic $F(B)$?

Theorem $F(A) \cong F(B)$ iff $|A| = |B|$

card(A) = card(B)

Sketch of proof of $\boxed{\Longrightarrow}$

$$F(A) \xrightarrow{\pi_A} (\mathbb{Z}/2\mathbb{Z})^A = \underbrace{\bigoplus_{a \in A} \mathbb{Z}/2\mathbb{Z}\, a}_{\text{vector space over the field } \mathbb{Z}/2\mathbb{Z} \text{ with basis } A}$$

$$a \longmapsto 1 \cdot a$$

$a \in A$

$|A|$ = rank of $F(A)$

π_A is a surjective group homomorphism

if $F(A) \xrightarrow{\varphi} F(B)$ is an isomorphism

$$\begin{tikzcd} F(A) \arrow[r, "\varphi"] \arrow[d, "\pi_A"'] & F(B) \arrow[d, "\pi_B"] \\ V_A \; (\mathbb{Z}/2\mathbb{Z})^A \arrow[r, "\varphi_2"] & (\mathbb{Z}/2\mathbb{Z})^B \; V_B \end{tikzcd}$$

φ_2 isom

$|A| = \dim V_A$

$|B| = \dim V_B$

$F(A)$ has rank $|A|$

A is a basis of $F(A)$

by def^n: every el^t of $F(A)$ can be written in a unique way as a reduced word on $\tilde{A}$ (in $\tilde{A}^*$)

$A = \{a, b\}$

$\{a, b^{-1}\}$ is also a basis

$\{ab, b\}$ ————

$\{b^{-1}ab, b\}$ ————

$\{\underline{b^{-1}ab^2}, \underline{b^{-1}ab}\}$ ————

if $\{u, v\}$ is a basis, then

$\{u, v^{-1}\}$ is a basis

$\{uv, v\}$ is a basis

All basis have cardinality $\text{rank}(F(A))$

if $u_1, \ldots, u_n$ is a basis of F $= |A|$

If $\{u_1, \dots, u_n\}$ is a basis of $F(A)$

and $B = \{b_1, \dots, b_n\}$ is a set with n elts

then $F(B) \longrightarrow F(A)$ is an isomorphism

$b_i \longmapsto u_i$

Problem given $u_1, \dots, u_r$ in $F(A)$ (where $|A| = r$)

decide whether $\{u_1, \dots, u_r\}$ is a basis of $F(A)$.

$A = \{a, b\}$

$\{aba, ba^{-1}b\}$ basis ?

Subgroups of free groups

Theorem (Nielsen, early 20^{th} century)

$\boxed{\text{Every (finitely generated) subgroup of } F(A) \text{ is free}}$

Contrary to vector spaces
if H is a subgroup of $F(A)$
rank (H) may be greater than $|A|$
may even be ∞

Example in $F(a,b)$

any subset of $\{ b^i a b^{-i} \mid i \in \mathbb{Z} \}$ is a basis
of the subgroup it generates

Problems given $g, g_1, \dots, g_n$ in $F(A)$
let $H = \langle g_1, \dots, g_n \rangle$

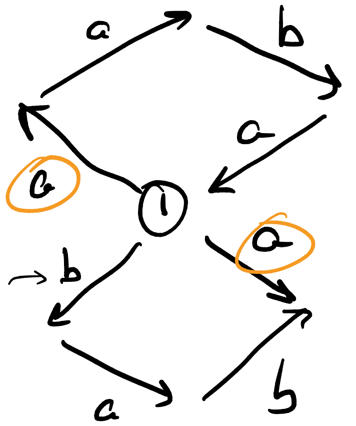
1) is $\{g_1, \dots, g_n\}$ a basis of H?
2) $rk(H)$?
3) is $g \in H$?

Stallings graph of a subgroup

$H \longmapsto \Gamma(H)$ a finite connected graph

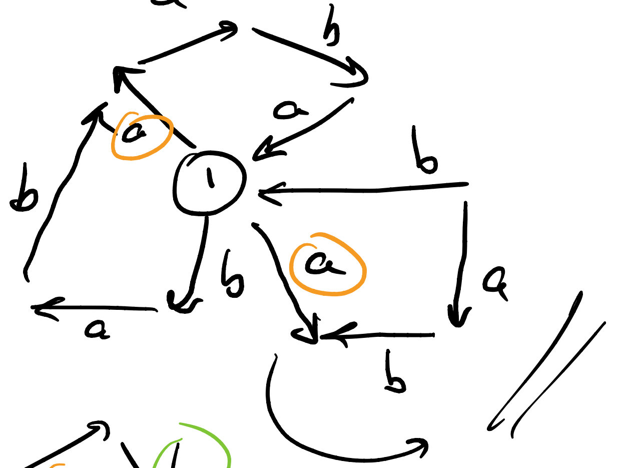
subgp

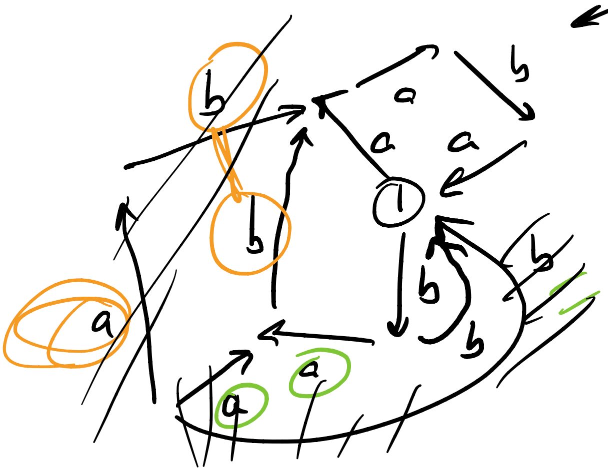
$H = \langle a^2ba,\ baba^{-1},\ \underline{b^{-1}aba^{-1}},\ a^3,\ b^2 \rangle$

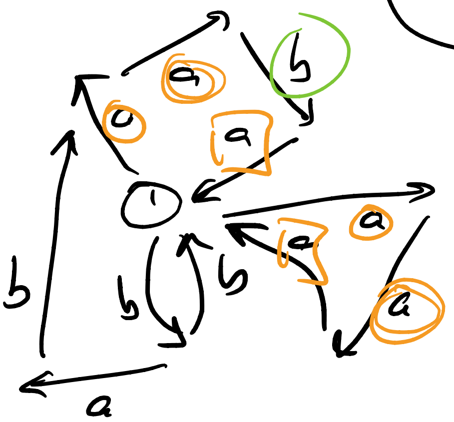


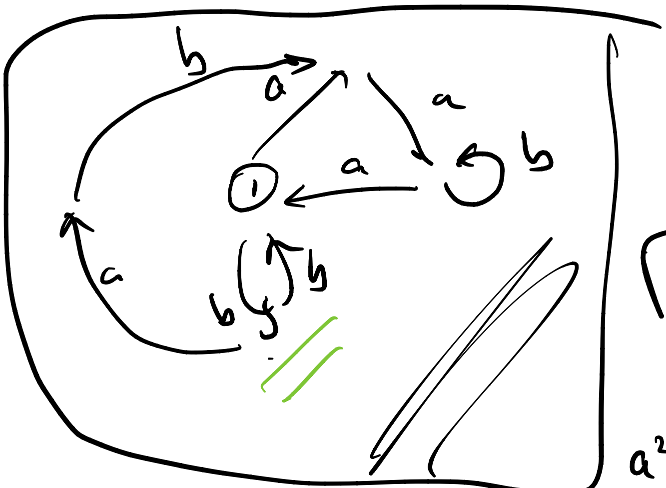
determinism

codeterminism









$\Gamma(H)$

$\Gamma(H)$ does not depend on the set of generators of H

It depends on H only

$a^2b \notin H$

$bababa \in H$.

Γ_0 = bouquet of circles

$\downarrow$ folding $\qquad$ $L(\Gamma_i)$ = language in $\tilde{A}^*$

Γ_1

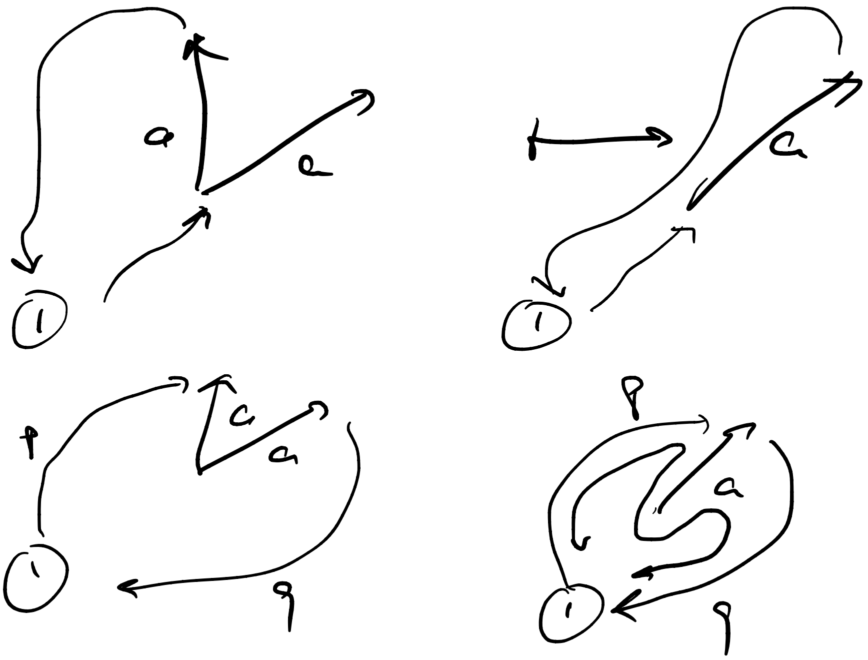
$\downarrow$ folding $\qquad$ $\forall u \in H\ \exists v \in L(\Gamma_0)$ such that $u = \mathrm{red}(v)$

Γ_2

$\vdots$

$\downarrow$

$\Gamma(H)$



$p\,\bar{a}\,t\,a\,q$

<u>Thm</u> A reduced word is in H iff it is accepted by $\Gamma(H)$ (seen as an automaton)

You start with generators of H

$(h_1, \dots, h_n)$

construct $\Gamma(H)$

given $g, h_1, \dots, h_n$, $H = \langle h_1, \dots, h_n \rangle$

is g in H?

<u>Prop</u> $g \in H$ iff g can be read in $\Gamma(H)$ as a circuit at the base vertex

Is $g_1, g_2, \dots g_r$ a basis of $F(A)$ (where $|A| = r$)

Let $H = \langle g_1, \dots, g_r \rangle$

$\Gamma(H)$

H is $F(A) \iff \Gamma(H) = \Gamma(F(A))$

$\{g_1, \dots, g_r\}$ is a basis of $F(A)$

$\iff \Gamma(H) =$

Computation of $\cap$-sections

H, K 2 subgrps of $F(A)$

Compute $H \cap K$

The St. graph for $H \cap K$ is obtained from $\Gamma(H)$ and $\Gamma(K)$ by the same product construction used to recognize $L_1 \cap L_2$ when L_1, L_2 are regular languages

Stallings 1983

Corollary: if $rk(H), rk(K) < \infty$ then $rk(H \cap K) < \infty$ (Howson's thm 1954)

Surveys

Enric Ventura

Jordi Delgado

(Barcelona)

see also my webpage