# Logspace computations in graph products

Volker Diekert[1]

Universität Stuttgart

Webinar 2013, April 11

[1] Joint work with Jonathan Kausch and Armin Weiß

# Preliminaries

Groups: finitely generated $\bar{g} = g^{-1}$ in all groups.

**Word problem: $\mathrm{WP}(G)$**

- Input: Word $w$ written in generators.
- Question: Do we have $w = 1$ in $G$ ?

"Natural groups" seem to have an "easy" word problem.

$$\mathrm{TC}^0 \subseteq \mathrm{NC}^1 \subseteq \mathrm{LOG} \subseteq \mathsf{NLOG} \subseteq \mathsf{LOGCFL} \subseteq \mathrm{NC}^2 \subseteq \mathrm{NC} \subseteq \mathbf{P}$$

- $\mathrm{WP}(BS(1,2)) \in \mathrm{TC}^0$, actually $\mathrm{TC}^0$ complete.
- $\mathrm{WP}$(finite nonsolvable) is $\mathrm{NC}^1$ complete (Barrington 1989)
- $\mathrm{WP}(F_2)$ is $\mathrm{NC}^1$ hard, and $\mathrm{WP}(F_2) \in \mathrm{LOG}$
- Linear groups have a WP in $\mathrm{LOG}$.
- Hyperbolic groups have a WP in $\mathrm{NC}^2$ (Cai 1992) (and in LOGCFL by Lohrey 2004)

In this talk "easy" means "$\mathrm{LOG}=$ Dlogspace"

# Graph groups, RAAGs (Right angled Artin groups)

A RAAG is given by a finite undirected graph $(V, I)$ with generating set $V$ and defining relations $\alpha\beta = \beta\alpha$ for all $(\alpha, \beta) \in I$.

$$G(V, I) = F(V) / \{ \alpha\beta = \beta\alpha \mid (\alpha, \beta) \in I \}$$

- RAAGs are subgroups of right angled Coxeter groups (RACGs) and Coxeter groups are linear: Hence WP is in logspace (classical).
- Shortlex normal forms are $\mathrm{LOG}$ computable in RAAGs and RACGs.
  (D., Lohrey, Kausch: AMS Meeting Las Vegas 2011.
  & Contemporary Mathematics, **582** 77-94, 2012.)
  Hence: Conjugacy in RAAGs and RACGs is in $\mathrm{LOG}$).
- Geodesic lengths are $\mathrm{LOG}$ computable in Coxeter groups, but open whether we can compute geodesics in $\mathrm{LOG}$.

# Related algorithmic problems

**$G$ a fixed group**

- Word problem.
- Compute geodesic lengths.
- Compute Parikh-image of geodesic.
- Compute geodesics.
- Conjugacy problem.

# Generalize from RAAGs and RACGs to graph products

Setting: Given a finite undirected graph $(V, I)$ and for each node $\alpha \in V$ a finitely generated node-group $G_\alpha$.

The graph product $G = G(V, I; (G_\alpha)_{\alpha \in V})$ is defined as the quotient group of the free product $\star_{\alpha \in V} G_\alpha$ with defining relations

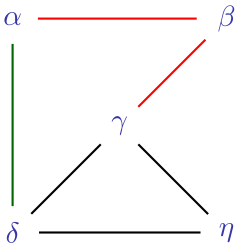
$$g_\alpha h_\beta = h_\beta g_\alpha \text{ for all } g_\alpha \in G_\alpha,\ h_\beta \in G_\beta,\ (\alpha, \beta) \in I.$$

**Baby cases:** Direct products or $G = \mathbb{Z}/2\mathbb{Z} \star \mathbb{Z}/2\mathbb{Z} = \mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$

- Proofs for RAAGs and RACGs used $\mathrm{WP} \in \mathrm{LOG}$ via linear representations.
- Here: "Explicit" Bass-Serre Theory.
  = First part of my talk.

# A picture of a graph product

$G =$ graph product of




Let $A = G_\alpha \star G_\gamma$. Then

$$G = (G_\beta \times A) \star_A ((G_\alpha \times G_\delta) \star_{G_\delta} (G_\gamma \times G_\delta \times G_\eta))$$

# Word problem, shortest normal forms for graph products

Let $\mathcal{C}$ be some "usual" complexity class which is closed under complementation and with $\mathsf{WP}(F_2) \in \mathcal{C}$

For example $\mathcal{C} = \mathrm{LOG}, \mathrm{NLOG}, \mathrm{NC}, \mathbf{P}, \mathbf{PSPACE}, \ldots$

**Theorem 1.**

Let WP of all $G_\alpha$ be in $\mathcal{C}$. Then:

- The WP of the graph product is in $\mathcal{C}$.
- Geodesics can be computed in $\mathcal{C}$.
  (Here $|g| = 1$ for all $1 \neq g \in G_\alpha$.)

**Corollary**

If shortlex-nfs of all $G_\alpha$ are computable in $\mathcal{C}$, then the same is true for the graph product.

# Conjugacy for graph products

**Theorem 2**

If the Conjugacy Problem of all $G_\alpha$ is in $\mathcal{C}$, then the Conjugacy Problem of the graph product is in $\mathcal{C}$.

**Special Case**

The Conjugacy Problem of RAAGs and RACGs is in $\mathrm{LOG}$.

# Ingredients for proofs

- Complexity: logspace transducers (with oracles).
- Rewriting: dependence graphs.
- Combinatorial group theory.

# Proof for Theorem 1: Outline for $\mathcal{C} = \mathrm{LOG}$

1.) Induction on $|V|$.
2.) Solve WP for semi-direct extensions, e.g., using Bass-Serre.
3.) Back to graph products: "semi-direct" products are direct products.
4.) Compute geodesics. (This is the core of the result.)

1.) Start induction: Choose node $\beta$ and group $B = G_\beta$ as "base group", $A = G(\mathsf{link}(\beta))$ and $C = B \times A$.

$$G = P \star_A C.$$

Projection $C = A \times B \to A$ and inclusion $A \subseteq P$ induce

$$1 \to H \to P \star_A C \xrightarrow{\pi} P \to 1.$$

# Word problem in semi-direct extensions

2.) We are in a special situation of a semi-direct extension.

- There is $P$. Here $P$ is a "smaller" graph product.
- $A \leq P$ subgroup of $P$. Here $A$ is the link of some node $\alpha$.
- $B$ "base" group. Here $G_\alpha$.
- $C = B \rtimes A$ a semi-direct product. Here $C = B \times A$.

$G$ is the semi-direct extension of $P$ by $B \rtimes A$:

$$G = P \star_A (B \rtimes A).$$

We have $1 \to H \to G \xrightarrow{\pi} P \to 1$ and $G = H \rtimes P$.
Kernel $H$ acts on the Bass-Serre tree $\mathsf{BST}(P \overset{A}{\text{———}} C)$.

# Action of $H$ on the Bass-Serre tree of $P \overset{A}{\text{———}} C$

Vertex set: $\{\, gP \ \mid g \in G \,\} \amalg \{\, gC \ \mid g \in G \,\}$. Let $h \in H$.

Action: $hgP = gP \iff g^{-1}hg \in H \cap P = \{1\} \iff h = 1.$

$$H \backslash \{\, gP \ \mid g \in G = H \cdot P \,\} = \{*\} \quad \& \quad \mathrm{Stab}(gP) = \{1\}$$

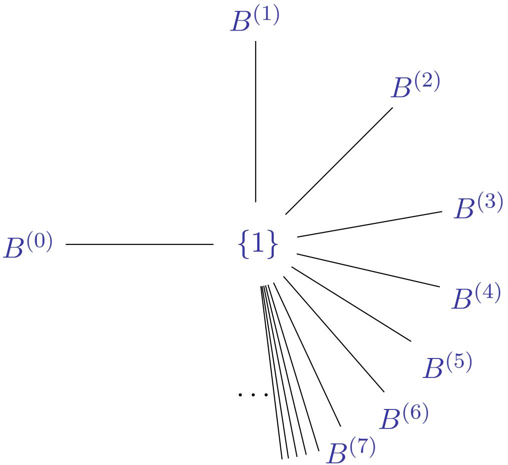
$$hgC = gC \iff g^{-1}hg \in H \cap C = B \iff h \in B^g.$$

$$H \backslash \{\, gC \ \mid g \in G \,\} = H \backslash G / C \quad \& \quad \mathrm{Stab}(gC) \cong B$$

- Bass-Serre: $H$ is a free product of groups $B^g = gBg^{-1}$.
- Number of free factors is $|H \backslash G/C| = |P/A|$.

# Kernel $H$ as a free product

$H$ is the fundamental group of a "star" with trivial center and $[P : A]$ rays, because $P \subseteq G$ induces bijection $P/A = H \backslash G/C$.



# Solving the Word Problem. Input: Word $w$

Compute $\pi(w) \in P$. For example, if $w = g_0 b_1 g_1 b_2 g_2$, then $\pi(w) = g_0 g_1 g_2$.

If $\pi(w) \neq 1$ we are done.

Hence $\pi(w) = 1$ and $w \in H$, and in the example $g_0 g_1 g_2 = 1$.

$$w = g_0 b_1 g_1 b_2 g_2 = g_0 b_1 \overline{g_0} g_0 g_1 b_2 \overline{g_0 g_1} g_0 g_1 g_2 = (g_0 b_1 \overline{g_0})(g_0 g_1 b_2 \overline{g_0 g_1}).$$

More general, let $w = g_0 b_1 g_1 \cdots b_m g_m \in H = \star_\nu B^{(\nu)}$.

**Claim:** Under some "natural assumption" there are "easy to compute" $a_i \in A$ and indices $\nu(i)$ such that we obtain a factorization in free factors:

$$w = b_1^{a_1} \cdots b_m^{a_m} \quad \text{with } b_i^{a_i} \in B^{(\nu(i))}.$$

# Computation of $a_i$ and indices $\nu(i)$

For $w = g_0 b_1 g_1 \cdots b_m g_m \in H$ let $p_i = g_0 \cdots g_i$ for $0 \leq i < m$.

For each $i$ let $\nu(i) \in \{0, \ldots, m-1\}$ be minimal such that there is $a_{i+1} \in A$ with

$$\overline{p_{\nu(i)}}\, p_i = a_{i+1}.$$

Define a new index set $N = \{ \nu(i) \mid 0 \leq i < m \}$.

We obtain

$$w = b_1^{a_1} \cdots b_m^{a_m} \in \star_{\nu \in N} B^{(\nu)} \quad \text{with } b_i^{a_i} \in B^{(\nu(i))}$$

**Assumption**

"Extended" membership problem for $A$ can be solved in $\mathrm{LOG}$:

- Input: $p, p' \in P, b \in B$.
- Output: If $\overline{p}p' = a \in A$ then $b^a \in B$ else $\overline{p}p' \notin A$.

# Reduction to the Word Problem in free groups.

Notation: We write $b^{(\nu)}$ for elements in $B^{(\nu)}$. Hence, $w = b_1^{(\nu_1)} \cdots b_m^{(\nu_m)}$ where for simplicity of notation $b_i = b_i^{a_i}$.

Consider $\psi : \star_{\nu \in N} B^{(\nu)} \to B$ where $\psi(b^{(\nu)}) = b$.

Compute $\psi(w) = b_1 \cdots b_m \in B$. If $\psi(w) \neq 1$ we are done. Hence $\psi(w) = 1$ and $b_1 \cdots b_m \in K = \ker(\psi)$.

Its kernel $K$ acts freely on the Bass-Serre tree; and hence $\left\langle b_1^{(\nu_1)}, \ldots, b_m^{(\nu_m)} \right\rangle$ is a f.g. free subgroup, but we need to find and rewrite $w$ in some basis $X$ such that

$$F(X) = \left\langle b_1^{(\nu_1)}, \ldots, b_m^{(\nu_m)} \right\rangle.$$

How to find $X$: "omitted in the talk".

# Final steps for semi-direct extensions

For $\mathrm{LOG}$:

- Rewrite $w \in K$ in the basis $X$.
- By a logspace reduction embed $F(X)$ into $F(a, b)$.
- Embed $F(a, b)$ into $\mathrm{SL}(2, \mathbb{Z})$.
- Solve the WP of $\mathrm{SL}(2, \mathbb{Z})$ in $\mathrm{LOG}$ by "Chinese remaindering".

# Back to graph products

$C = B \times A$ is a direct product.

Recall, $(V, I)$ is a finite undirected graph and for each node $\alpha \in V$ a finitely generated node-group $G_\alpha$.

The graph product $G = G(V, I; (G_\alpha)_{\alpha \in V})$ is defined as the quotient group of the free product $\star_{\alpha \in V} G_\alpha$ with defining relations

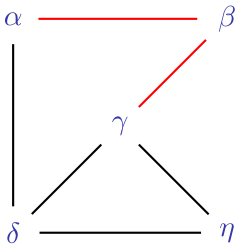
$$g_\alpha h_\beta = h_\beta g_\alpha \text{ for all } g_\alpha \in G_\alpha,\ h_\beta \in G_\beta,\ (\alpha, \beta) \in I.$$

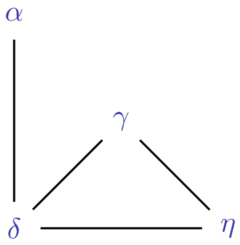
**Simplifications:**

- $b^a = b$ for all $a \in A$ and $b \in B$.
- $A \leq P$ is a retract, i.e., $w \in A \iff w = \pi_A(w)$.
  Hence, membership in $A$ reduces to WP in $P$.

**Consequence:** $\mathrm{WP}(G) \in \mathcal{C}$.

# $G$, $P$, $A$, and $B$ in the example again

$G =$ 


$P =$ 


$$A = G_\alpha \star G_\gamma \quad B = G_\beta \quad C = B \times A.$$

# Dependence graph representation of group elements

Let $\Gamma$ be the disjoint union over all $\Gamma_\alpha = G_\alpha \setminus \{1\}$, where $\alpha \in V$.

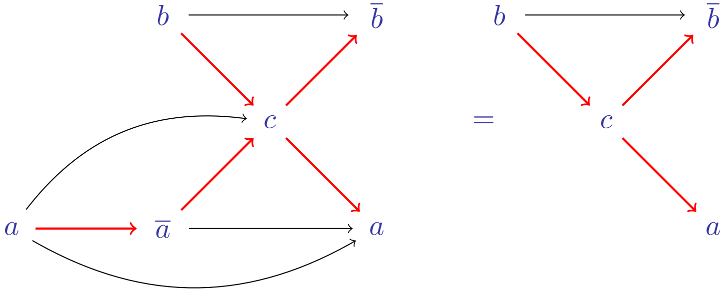
For a word $w = a_1 \cdots a_n \in \Gamma^*$ define a node-labeled acyclic graph $D(w)$ as follows:

- The vertex set is $\{1, \ldots, n\}$.
- Label of vertex $i$ is the letter $a_i \in G_{\alpha_i}$.
- Arcs are from $i$ to $j$ if both, $i < j$ and $(\alpha_i, \alpha_j) \notin I$.

# Graphical representation of group elements

Let $G(V, I)$ with $V = \{a, b, c\}$ and $I = \{(a, b), (b, a)\}$.

Dependence graph (Hasse diagram): $ab\overline{a}ca\overline{b} =$



# Confluent trace rewriting

**Rewriting**: Whenever there is an arc in the Hasse-diagram from $i$ to $j$ with labels $f$ and $g$ with $f, g \in \Gamma_\alpha$ multiply $fg = h$ in $G_\alpha$.

- If $h = 1$, remove nodes $i$ and $j$.
- If $h \neq 1$, remove node $j$ and relabel node $i$ by $h$.

**Lemma (D., Lohrey)**

This procedure is confluent and yields normal forms for group elements in the graph product.

If the procedure terminates in a graph with $m$ vertices, we call the graph normal form of $w$, and $m$ the geodesic length of $w$. A word $w$ is called geodesic, if its length is the geodesic length.

The normal form of $1$ is the empty graph with $m = 0$.

# Computing geodesics

For the proof of Theorem 1 we have to compute geodesics in logspace.

To show this for the graph product $G$, but we may use already that we can solve its WP in $\mathrm{LOG}$ (resp. $\mathcal{C}$).

The input is a word $w = g_1 \cdots g_n$ where $g_i$ are generators of some group $G_\alpha$. We want to rewrite $w$ as a geodesic, i.e., $w = a_1 \cdots a_{n'}$ with $a_i \in \bigcup_{\alpha \in V} G_\alpha \setminus \{1\}$ such that $n'$ is minimal.

We do this in $|V|$ rounds of logspace reductions. In round $\alpha$ we minimize the number of $a_i \in \Gamma_\alpha$.

# Algorithm for round $\alpha$

Start round $\alpha$ with $w = u_0 a_1 u_1 \cdots a_n u_n$ where the $a_i$ correspond to "letters" in $\Gamma_\alpha$.

- From left-to-right: Stop at $a_i$. Compute the maximal $m \geq i$ such that

$$a_i u_i \cdots a_m u_m = a_i \cdots a_m u_i \cdots u_m \in G$$

- Replace $a_i u_i \cdots a_m u_m$ by $a' u_i \cdots u_m$ with $a' = a_i \cdots a_m \in G_\alpha$.
- If $m = n$ then the round is finished, otherwise move to $a_{m+1}$.

The proof that each round terminates in a word with a minimal number of letters from $\Gamma_\alpha$ is on "confluent trace rewriting" on dependence graphs.

# Conjugacy

Input: $u, v \in \Gamma^*$. Question $u \sim v$ in $G$?

Solution:

1.) Wlog. $u, v$ are geodesics.
2.) Wlog. $u, v$ have connected dependence graphs with more than one vertex.
3.) Compute cyclically reduced dependence graphs.
4.) Check that $|u|_\alpha = |v|_\alpha$ for all $\alpha \in V$.
5.) Check that $u$ appears as a factor in $v^{|V|}$.

# Concluding remarks

- Theorem 2 relies on Theorem 1 (Computation of geodesics).
- The proofs use rather different technical concepts.
  1.) Graph products as semi-direct extensions.
  2.) Bass-Serre-theory.
  3.) Dependence graph representation and confluent trace rewriting.

Thank you

# Technical Annex

Some missing details on proofs.

# Number of free factors (talk: skip slide)

Compute the vertex set $H \backslash \{ gC \mid g \in G \} = H \backslash G/C$.

**Claim:** The inclusion $P \subseteq G$ induces a bijection:

$$P/A \to H \backslash G/C, \ fA \mapsto HfC$$

**Proof of Claim:** Since $G = H \cdot P$, it is surjective.

For $g \in G$ let $f_g \in Hg \cap P$. Note that $f_g$ is unique.

Define $HgC \mapsto f_g A$. It is enough to show that $f_g A$ is well-defined.

Let $h \in H$, $a \in A$, and $b \in B$ and $g' = hgab \in HgC$. We have to show that $f_{g'} \in f_g A$.

Since $H$ is normal and $B \subseteq H$, we have $g' \in gabH \subseteq gaH = Hga = Hf_g a$. Hence $f_{g'} = f_g a \in f_g A$.

# Computing a basis

Let $w = b_1^{(\nu_1)} \cdots b_m^{(\nu_m)} \in K$ with $m \geq 1$ and $1 \neq b_i \in B^{(\nu(i))}$. Since $w \in K$, we have $m \geq 2$.

Let $g_i^{(\ell)} = (b_1 \cdots b_i)^{(\ell)}$. In particular, $b_1^{(\ell)} = g_1^{(\ell)}$ and $g_m^{(\ell)} = 1$.

For each $1 \leq i < m$, consider the factor $b_i^{(k)} b_{i+1}^{(\ell)}$. Replace $b_i^{(k)} b_{i+1}^{(\ell)}$ by

$$b_i^{(k)} \, (\overline{b_i}^{(\ell)} \cdots \overline{b_1}^{(\ell)})({b_1}^{(\ell)} \cdots {b_i}^{(\ell)}) \, b_{i+1}^{(\ell)} = b_i^{(k)} \, \overline{g_i}^{(\ell)} g_{i+1}^{(\ell)}.$$

The input word becomes (after this logspace-procedure) a word

$$w = g_1^{(\nu_1)} \overline{g_1}^{(\nu_2)} \, g_2^{(\nu_2)} \overline{g_2}^{(\nu_3)} \cdots g_{n-1}^{(\nu_{n-1})} \overline{g_{n-1}}^{(\nu_n)} \in K$$

Notation: $(i, g, j) = g^{(i)} \overline{g}^{(j)} \in K$. We have $(i, g, j)^{-1} = (j, g, i)$. But the set of $(i, g, j)$ is not a basis since e.g.,

$$(i, g, k)(k, g, j) = (i, g, j).$$

## Computing a basis

Since $w \in K$, rewrite $w$ as a product in $(i, g, j) = g^{(i)}\overline{g}^{(j)}$.

- $1 \neq g \in B$ and $i \neq j$
- $g^{(i)} \in B^{(i)}$ and $\overline{g}^{(j)} \in B^{(j)}$
- $\psi(g^{(i)}) = g$ and $\psi(\overline{g}^{(j)}) = g^{-1}$
- Rewrite $(i, g, j) = (i, g, 0)(0, g, j)$ whenever $i \neq 0 \neq j$.

Thus, we can rewrite $w$ as a product in $(i, g, 0)^{\pm 1}$ with $1 \neq g \in B$.
More precisely, let $X = \{ (i, g, 0) \mid i \neq 0, g \neq 1 \}$, then

$$w \in (X \cup \overline{X})^*.$$

**Lemma**

$X = \{ (i,g,0) \mid i \neq 0, g \neq 1 \} \subseteq K$ *forms a basis of a free subgroup.*

**Proof.** Consider a non-empty freely reduced word $u$ in $(X \cup \overline{X})^*$ and let $\pi(u)$ its image in $K \subseteq \star_{\nu \in N} B^{(\nu)}$.

Let $u = v\,(i,g,j)$, where $v \in (X \cup \overline{X})^*$ and $(i,g,j) \in (X \cup \overline{X})$. We show:

- $\pi(u) \neq 1 \in K$.
- The last factor of $\pi(u)$ in the free product $\star_{\nu \in N} B^{(\nu)}$ is $\overline{g}^{(j)}$.
- If $j = 0$, then the last two factors of $\pi(u)$ are $h^{(i)}\overline{g}^{(0)}$ for some $h$.

For $|u| = 1$ we have $\pi(u) = g^{(i)}\overline{g}^{(j)}$ as desired. Hence let $u = v'(k,f,\ell)(i,g,j)$. By induction the last factor of $\pi(v)$ is $\overline{f}^{(\ell)}$.

For $\ell \neq i$ we conclude that the last three factors of $\pi(u)$ are $\overline{f}^{(\ell)}g^{(i)}\overline{g}^{(j)}$. Hence, we may assume that $\ell = i$.

# Proof of lemma

We have $u = v'(k, f, i)(i, g, j)$. For $i \neq 0$ we must have $k = 0$. Hence $f \neq g$ since $u$ is freely reduced.

For $f \neq g$ the last two factors of $\pi(u)$ are $(\overline{f}g)^{(i)}\overline{g}^{(j)}$.

Now, assume $f = g$, then we must have $k \neq j$.

Hence we may assume that we have $u = v'(k, g, 0)(0, g, j)$ with $k \neq j$.

By induction, the last two factors of $\pi(v)$ are $h^{(k)}\overline{g}^{(0)}$. Hence, the last two factors of $\pi(u)$ are $h^{(k)}\overline{g}^{(j)}$. □

# Proof that the Algorithm is correct I (talk: skip slide)

We use the lemma on trace rewriting in order to conclude that $w$ is **not** geodesic if and only if there is a node $\beta \in V$ and a factor $bub'$ with $b, b' \in \Gamma_\beta$ such that $u \in I(\beta)$. Here and in the following

$$I(\beta) = \left(\bigcup \{\, G_\alpha \mid (\alpha, \beta) \in I \,\}\right)^* .$$

Let $\alpha \in V$ be a node. We say that a word $w \in \Gamma^*$ is $\alpha$-geodesic, if

the number of letters from $\Gamma_\alpha$ is minimal w.r.t. all words which represent the same element in $G$.

**Lemma**

*Let $w = u_0 a_1 u_1 \cdots a_n u_n \in \Gamma^*$ such that the $a_i$ correspond to the letters from $\Gamma_\alpha$. Then $w$ is $\alpha$-geodesic if and only if $a_i u_i a_{i+1} \neq a_i a_{i+1} u_i \in G$ for all $1 \leq i < n$.*

# Proof, 1. slide

If $a_i u_i a_{i+1} = a_i a_{i+1} u_i \in G$ for some $1 \leq i < n$, then $w$ is not $\alpha$-geodesic. Hence, let $a_i u_i a_{i+1} \neq a_i a_{i+1} u_i \in G$ for all $1 \leq i < n$. We have to show that $w$ is $\alpha$-geodesic. This is true, if $w$ is geodesic. Hence we may assume that $w$ is not geodesic. Then there is a factor $bub'$ with $b, b' \in G_\beta$ and $u \in I(\beta)$. Since $a_i u_i a_{i+1} \neq a_i a_{i+1} u_i$ we must have $\alpha \neq \beta$. If the factor $bub'$ is a factor inside some $u_i$, then we can rewrite it by $bb'u$ and we obtain a word $w'$ which satisfies the same property, but which $\Gamma$ length is shorter. Hence $w'$ is $\alpha$-geodesic. This implies that $w$ is $\alpha$-geodesic, too.

# Proof, 2. slide

Thus we may assume that for some $i < j$ we have $u_i = p_i b q_i$ and $u_j = p_j b' q_j$ with $q_i, p_j \in I(\beta)$. Moreover, $(\alpha, \beta) \in I$. Now, inside the group $G$ we have:

$$\begin{aligned} a_i p_i b q_i a_{i+1} = a_i a_{i+1} p_i b q_i &\iff a_i p_i b q_i a_{i+1} b' = a_i a_{i+1} p_i b q_i b' \\ &\iff a_i p_i b b' q_i a_{i+1} = a_i a_{i+1} p_i b b' q_i, \\ a_j p_j b' q_j a_{j+1} = a_j a_{j+1} p_j b' q_j &\iff b' a_j p_j q_j a_{j+1} = b' a_j a_{j+1} p_j q_j \\ &\iff a_j p_j q_j a_{j+1} = a_j a_{j+1} p_j q_j. \end{aligned}$$

Thus, $u_0 a_1 u_1 \cdots a_n u_n$ is $\alpha$-geodesic if and only if $u_0 a_1 u_1 \cdots a_i p_i b b' q_i a_{i+1} \cdots a_j p_j q_j a_{j+1} \cdots a_n u_n$ is $\alpha$-geodesic. Again we may rewrite the factor $bub'$ by $bb'u$ and we may conclude as above that $w$ is $\alpha$-geodesic. $\square$

# $\alpha$-prefixes

Let $w = u_0 a_1 u_1 \cdots a_n u_n \in \Gamma^*$ such that the $a_k$ correspond to the letters from $\Gamma_\alpha$. We say that $u_0 a_1 u_1 \cdots a_i u_i$ is an $\alpha$-prefix, if there is no factor $a_\ell u_\ell \cdots a_m u_m = a_\ell \cdots a_m u_\ell \cdots u_m \in G$ with $\ell \leq i$ and $\ell < m$. Note that $u_0$ is an $\alpha$-prefix.

**Lemma**

*Let $w = u_0 a_1 u_1 \cdots a_n u_n \in \Gamma^*$ such that the $a_i$ correspond to the letters from $\Gamma_\alpha$. Let $0 \leq i < n$ such that $u_0 a_1 u_1 \cdots a_i u_i$ is $\alpha$-prefix and let $m$ be maximal such that*
$a_{i+1} u_{i+1} \cdots a_m u_m = a_{i+1} \cdots a_m u_{i+1} \cdots u_m \in G$.
*Then $u_0 a_1 u_1 \cdots a_i u_i [a_{i+1} \cdots a_m] u_{i+1} \cdots u_m$ is an $\alpha$-prefix of*
$u_0 a_1 u_1 \cdots a_i u_i [a_{i+1} \cdots a_m] u_{i+1} \cdots u_m a_{m+1} u_{m+1} \cdots a_n u_n$.

Proof. This follows because $m$ was chosen to be maximal.

# Correctness of the algorithm to compute geodesics

The invariant of an $\alpha$ round is that from left to right $\alpha$-prefixes are computed. This follows from the last lemma. At the end of the round the word $w$ becomes an $\alpha$-prefix. But then we can apply the first lemma in order to see that $w$ is $\alpha$-geodesic. Hence the result.