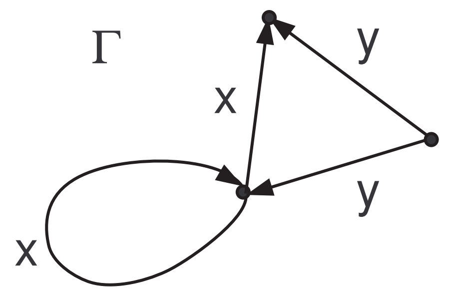
Membership problem in $\mathbb{Z}^n$-free groups

Andrey Nikolaev
Stevens Institute of Technology
(joint with Denis Serbin)

Stallings' foldings in free groups

Consider oriented graphs Γ whose edges are labeled by elements of a finite alphabet $X \cup X^{-1}$.

Example. $X = \{x, y\}$



Label of an edge e is denoted $\mu(e)$. Define $\mu(e^{-1}) = \mu(e)^{-1}$.

A path p in Γ has a label $\mu(p) = \mu(e_1) \cdots \mu(e_k)$ which is a word in the alphabet $X \cup X^{-1}$.

Let $v \in V(\Gamma)$. Define the language of Γ with respect to v to be

$$L(\Gamma, v) = \{\mu(p) \mid p \text{ is a reduced loop in } \Gamma \text{ at } v\},$$

where "reduced" stands for "without back-tracking".

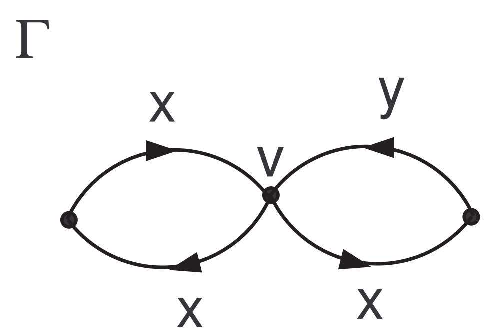
The set

$$\overline{L(\Gamma, v)} = \{\overline{w} \mid w \in L(\Gamma, v)\},$$

where "$^{-}$" denotes free reduction, is a subgroup of $F(X)$.

On the other hand, if H is a finitely generated subgroup of $F(X)$ then it is easy to construct a graph Γ such that $H = \overline{L(\Gamma, v)}$ for some $v \in V(\Gamma)$.

Example. Let $H = \langle x^2, xy \rangle < F(x, y)$ and take Γ to be a bouquet of loops at a vertex v, labeled by the generators of H.



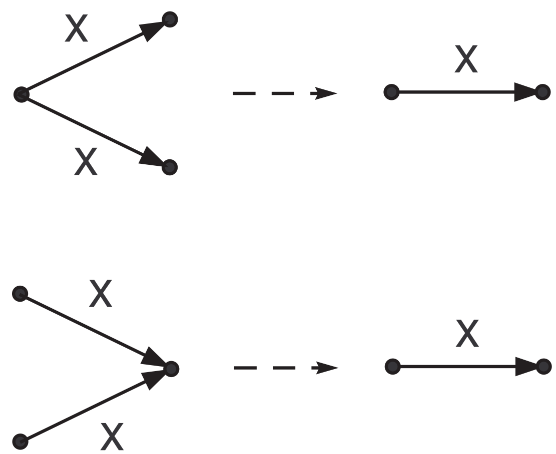
Obviously, $H = \overline{L(\Gamma, v)}$.

The idea to work with X-labeled graphs rather than subgroups of $F(X)$ was introduced by J. Stallings (1983).

Many problems for subgroups of a free group now can be restated in terms of graphs and easily solved. But graphs representing subgroups have to be folded.

An X-labeled graph Γ is folded if it does not have subgraphs of the form

Consider the following operations called foldings

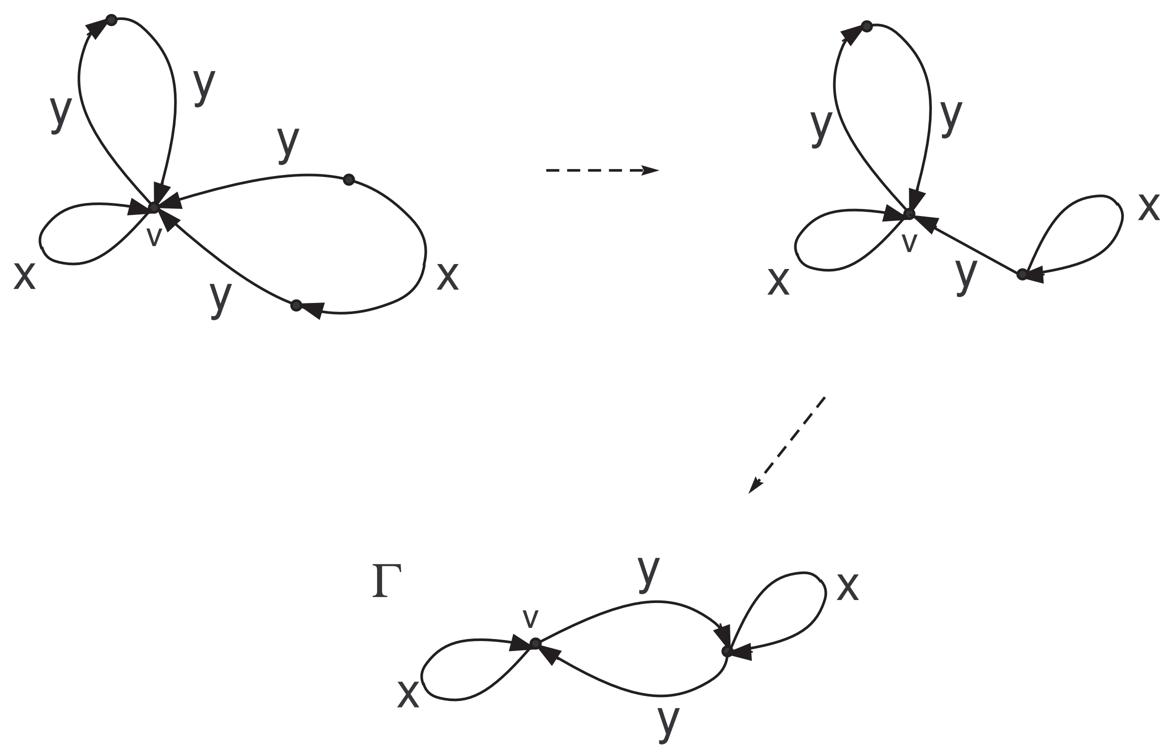


Fact. If Δ is obtained from Γ by a folding, so that $w \in V(\Delta)$ corresponds to $v \in V(\Gamma)$. Then $\overline{L(\Gamma, v)} = \overline{L(\Delta, w)}$.

Fact. For every finitely generated $H \leq F(X)$ there exists a folded X-labeled graph Γ such that $H = \overline{L(\Gamma, v)}$ for some $v \in V(\Gamma)$.

We start with a bouquet of loops labeled by generators of H and perform all possible foldings.

Example: $H = \langle x, y^2, y^{-1}xy \rangle < F(x, y)$.



Fact. If Γ is folded then $\overline{L(\Gamma, v)} = L(\Gamma, v)$

Let $H \leq F(X)$ and let Γ be a folded X-digraph such that $H = L(\Gamma, v)$ for some $v \in V(\Gamma)$. If $g \in F(X)$ then

$$g \in H \Longleftrightarrow g \in L(\Gamma, v).$$

It is easy to check the last inclusion which gives a solution of the Subgroup Membership Problem.

A way to look at Stalling graphs:

1. $F(X)$ represented by reduced words in alphabet $X \cup X^{-1}$.
$F(X) \hookrightarrow R(\mathbb{Z}, X)$.

2. Graphs labeled by words in $X \cup X^{-1}$.

3. Stallings foldings, Stallings graph. In a folded graph element of a group is readable iff corresponding reduced word is readable.

4. Solution to Membership problem and numerous other problems.

Fully residually free groups and U-foldings

If G is a f.g. fully residually free group, then $G \hookrightarrow F^{\mathbb{Z}[t]}$, where $F^{\mathbb{Z}[t]}$ is Lyndon's free group.

$F^{\mathbb{Z}[t]}$ can be defined as a union of chain of groups

$$F(X) = F_0 < F_1 < \ldots < F_n < \cdots$$

where $F = F(X)$ is a free group on an alphabet X, and F_k is generated by F_{k-1} and formal expressions of the type

$$\{w^\alpha \mid w \in F_{k-1},\ \alpha \in \mathbb{Z}[t]\}.$$

That is, every element of F_k can be viewed as a parametric word of the type

$$w_1^{\alpha_1} w_2^{\alpha_2} \cdots w_m^{\alpha_m},$$

where $m \in \mathbb{N},\ w_i \in F_{k-1}$, and $\alpha_i \in \mathbb{Z}[t]$.

Moreover, for a specific f.g. G we can take part of this chain "that matters": $G \hookrightarrow F_n$,

$$F(X) = F_0 < F_1 < \ldots < F_n,$$

where $F_k = \langle F_{k-1}, u_k^\alpha | \alpha \in \mathbb{Z}[t] \rangle$ (Miasnikov, Kharlampovich).

Idea: Treat u^α as an infinite word $uuu \cdots uuu$.

Ordered abelian groups

Let Λ be an ordered abelian group (any $a, b \in A$ are comparable and for any $c \in \Lambda :\quad a \leq b \;\Rightarrow\; a + c \leq b + c$).

Examples.

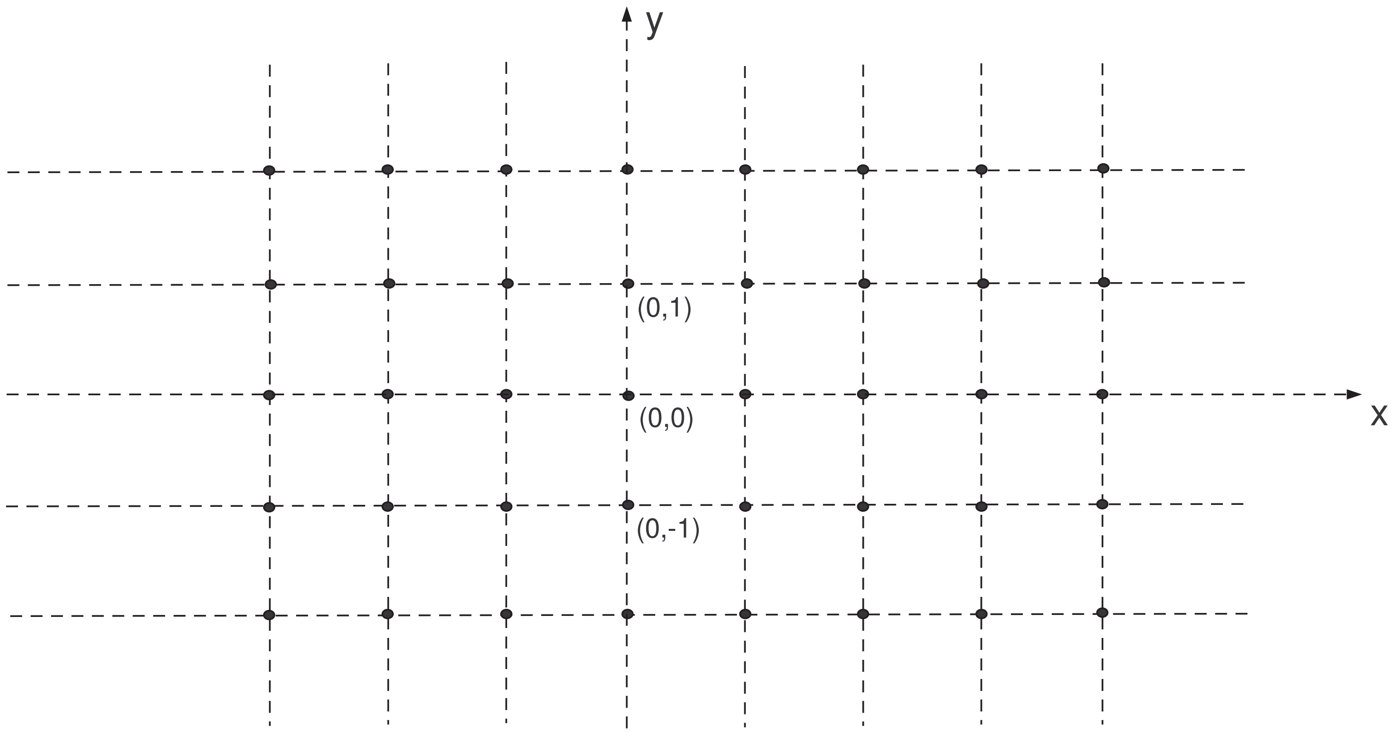
1. archimedean case: $\Lambda = \mathbb{R},\ \Lambda = \mathbb{Z}$ with usual order.
2. non-archimedean case: $\Lambda = \mathbb{Z}^2$ with the right lexicographic order

$$(a, b) < (c, d) \iff b < d \text{ or } b = d \text{ and } a < c.$$

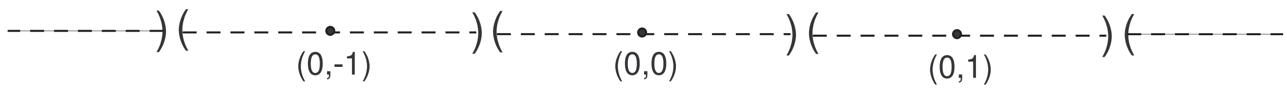
In particular,

$$(0, 1) > (n, 0) \text{ for every } n \in \mathbb{Z}.$$

$\mathbb{Z}^2$



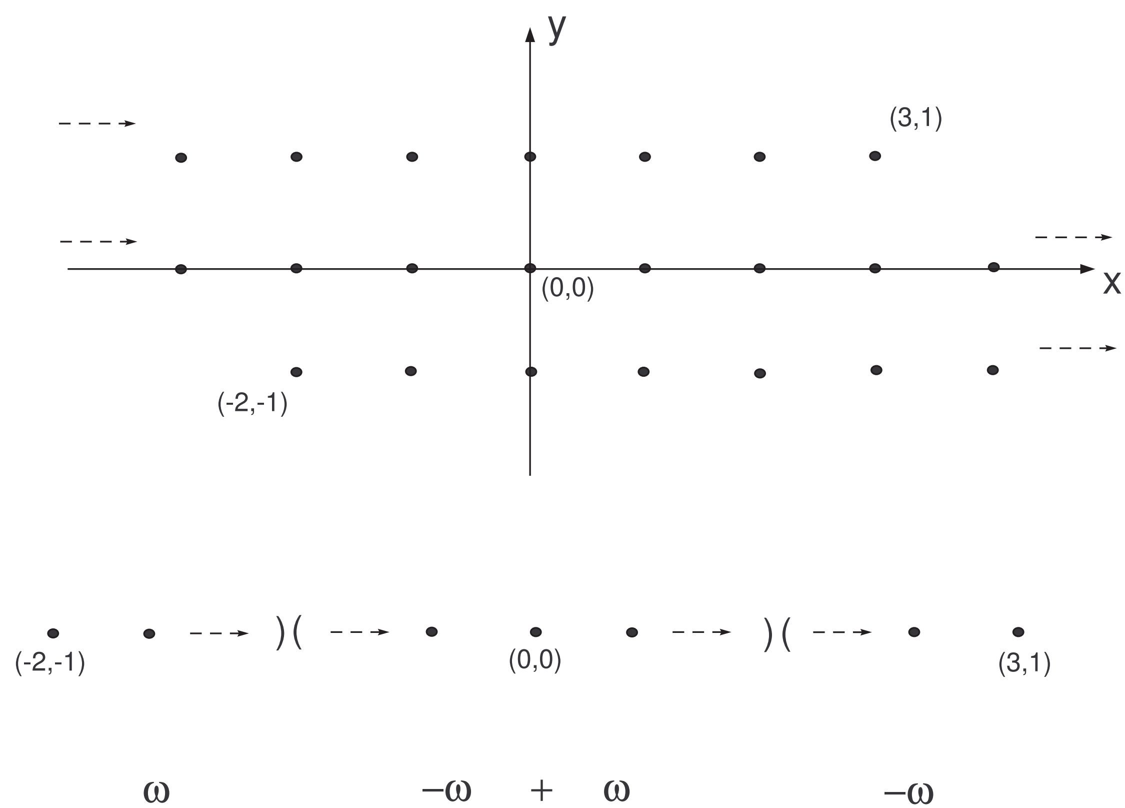
$\mathbb{Z}^2$ with the right lexicographic order



For $\alpha, \beta \in \Lambda$ the closed segment $[\alpha, \beta]$ is defined by

$$[\alpha, \beta] = \{\gamma \in \Lambda \mid \alpha \leq \gamma \leq \beta \ \}.$$

Example. $\Lambda = \mathbb{Z}^2,\ [(-2,-1),(3,1)]$



Infinite words

Let Λ be a discretely ordered abelian group (contains a minimal positive element 1_Λ) and $X = \{x_i \mid i \in I\}$ be a set.

A Λ-word is a function of the type

$$w : [1_\Lambda, \alpha] \to X^{\pm},$$

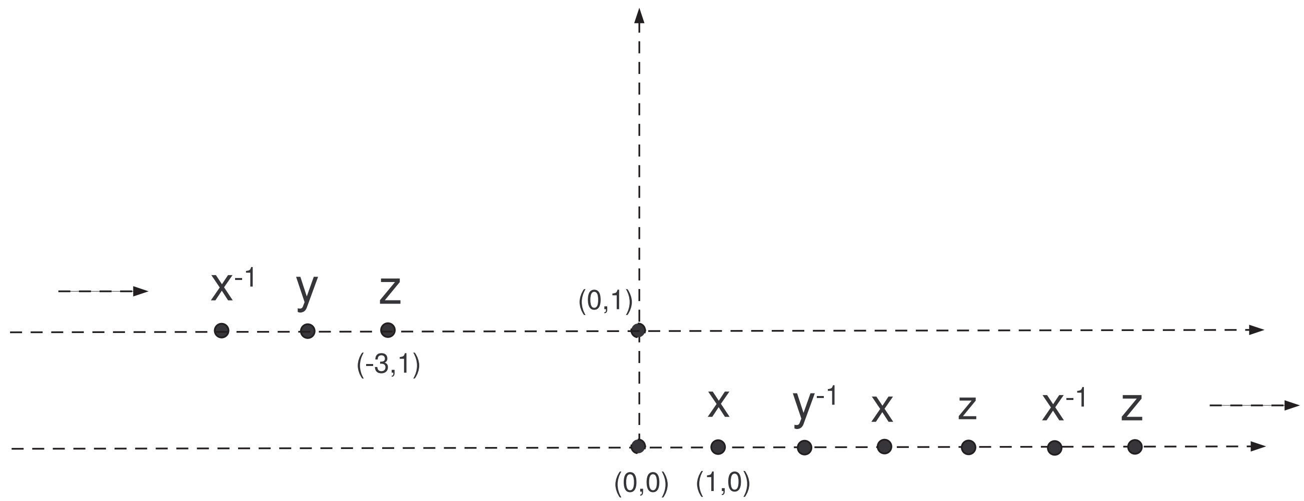
where $\alpha \geq 0$. The element α is called the length $|w|$ of w.

By ε we denote the empty Λ-word (when $\alpha = 0$).

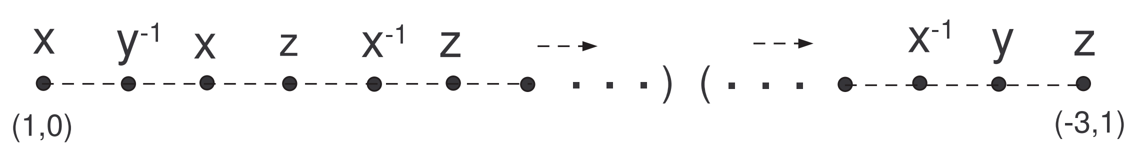
w is reduced $\Longleftrightarrow$ no subwords xx^{-1}, $x^{-1}x$ $(x \in X)$.

$R(\Lambda, X) =$ the set of all reduced Λ-words.

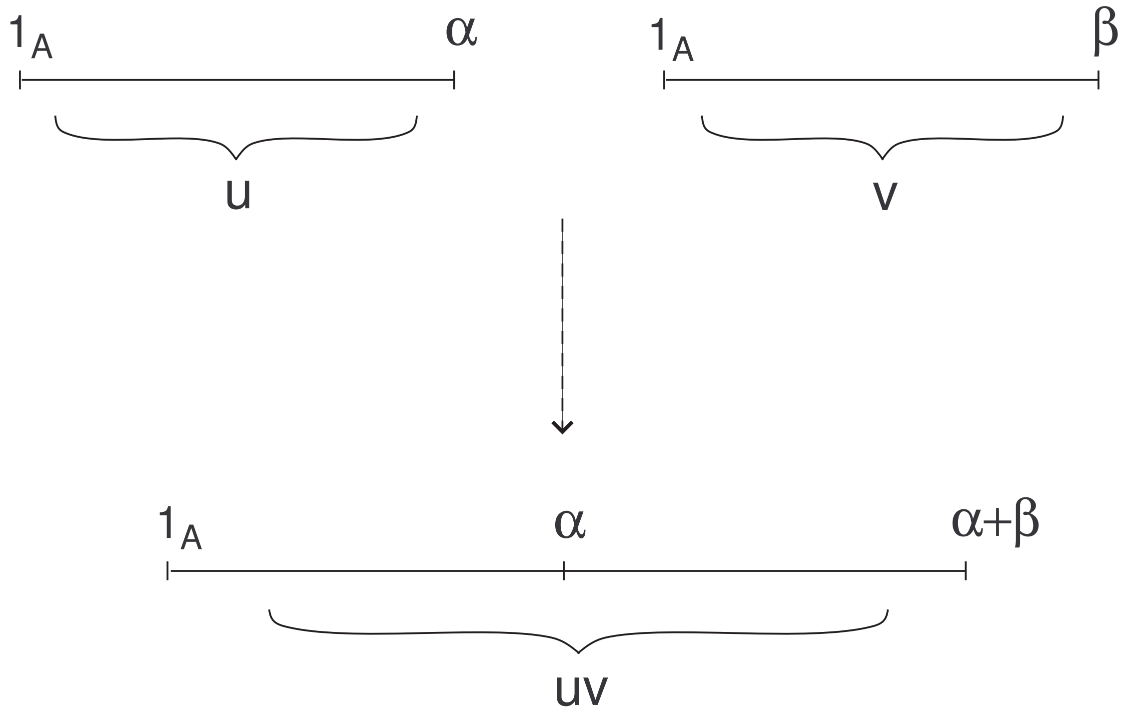
Example. $X = \{x, y, z\},\ \Lambda = \mathbb{Z}^2$



In "linear" notation

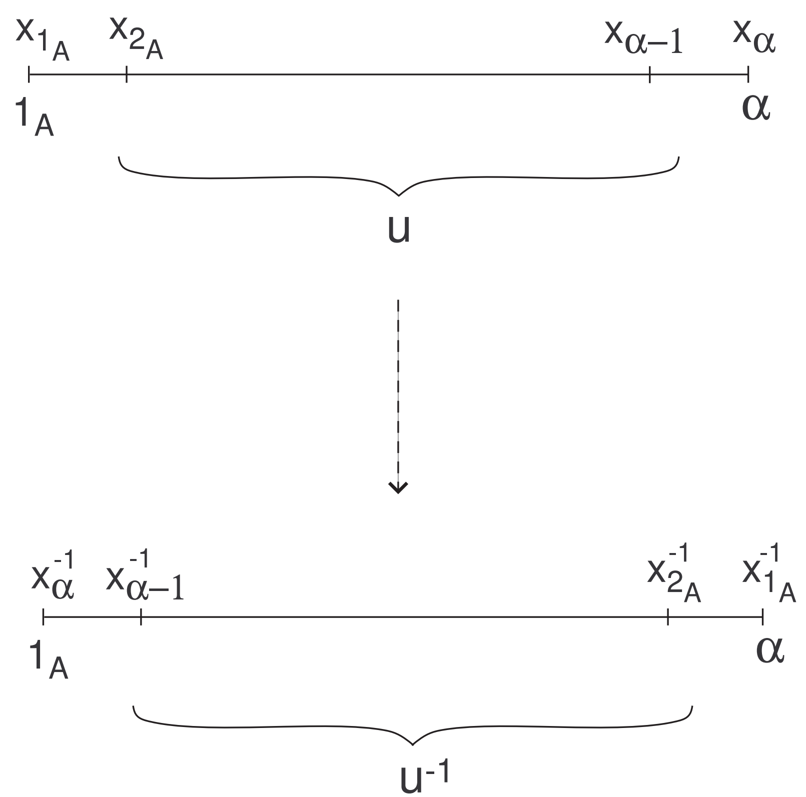


Concatenation of Λ-words

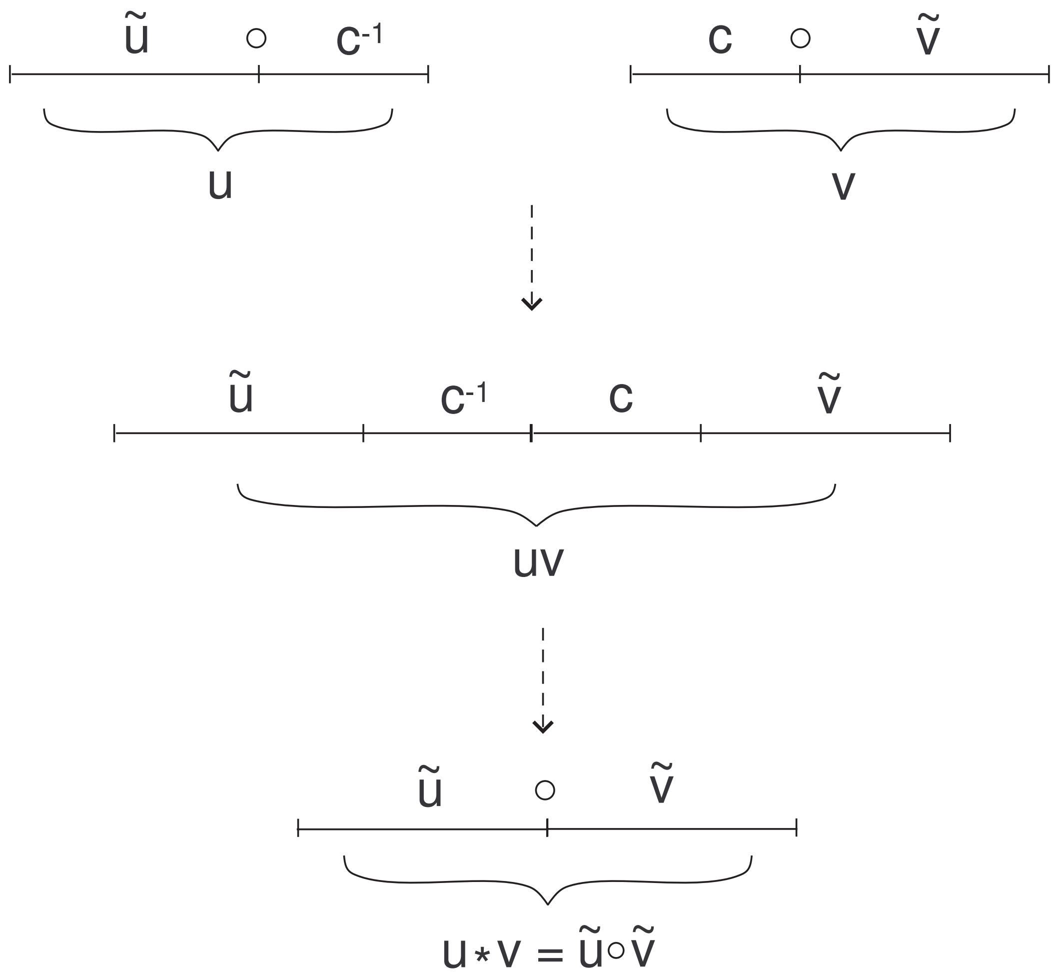


We write $u \circ v$ instead of uv in the case when uv is reduced.

Inversion of Λ-words



Multiplication of Λ-words



Multiplication of Λ-words

Let $u, v \in R(\Lambda, X)$.

Suppose u and v can be represented in the form

$$u = \tilde{u} \circ c^{-1}, v = c \circ \tilde{v},$$

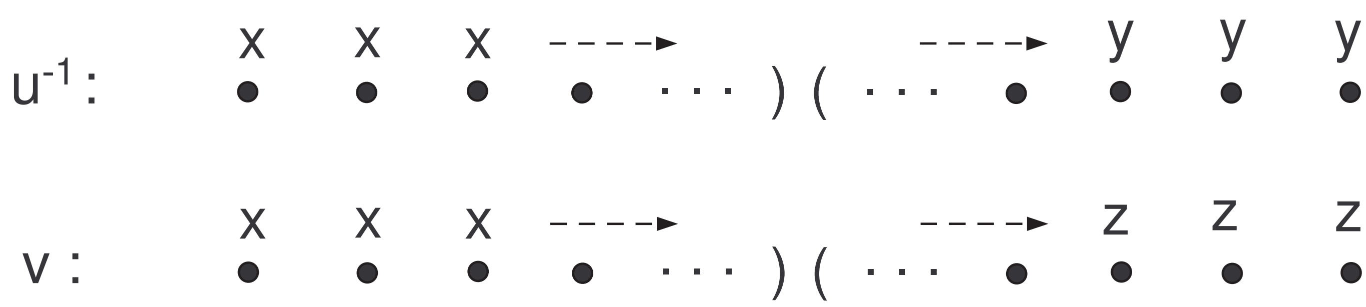
where $c \in R(\Lambda, X)$ is of maximal possible length.

Then define

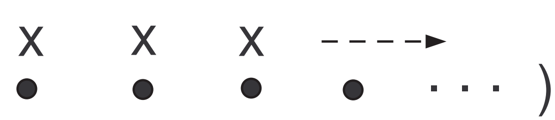
$$u * v = \tilde{u} \circ \tilde{v}.$$

The decomposition of u and v above exists only if u^{-1} and v have the maximal common initial part defined on a closed segment.

Example. $u, v \in R(\mathbb{Z}^2, X)$



The common initial part of u^{-1} and v is



which is not defined on a closed segment. Hence, $u * v$ is not defined.

Cyclic decomposition

$v \in R(\Lambda, X)$ is cyclically reduced if $v(1_\Lambda)^{-1} \neq v(|v|)$.

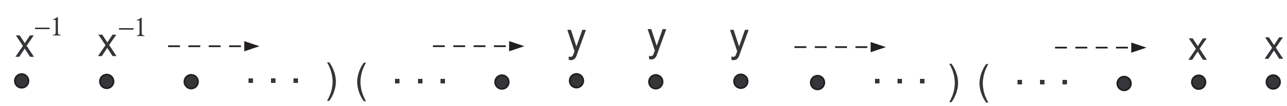
$v \in R(\Lambda, X)$ admits a cyclic decomposition if

$$v = c^{-1} \circ u \circ c,$$

where $c, u \in R(A, X)$ and u is cyclically reduced.

Example. $u \in R(\mathbb{Z}^2, X)$ does not admit a cyclic decomposition

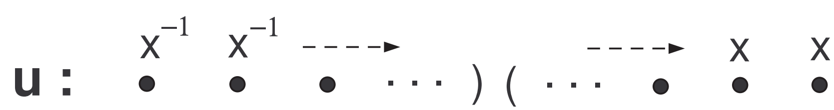
u :



Torsion

$R(\Lambda, X)$ has elements of order 2.

Example. $u \in R(\mathbb{Z}^2, X)$



has order 2.

Fact. Let $u \in R(\Lambda, X)$. If $u * u$ is defined then either u admits a cyclic decomposition (thus, has infinite order), or has order 2.

$F^{\mathbb{Z}[t]}$ as a group of infinite words

Recall that a f.g. fully residually free G embeds into F_n,

$$F(X) = F_0 < F_1 < \ldots < F_n,$$

where $F_k = \langle F_{k-1}, u_k^\alpha | \alpha \in \mathbb{Z}[t] \rangle$.

Theorem. (Miasnikov, Remeslennikov, Serbin) There exists an embedding

$$\phi : F_n \hookrightarrow R(\mathbb{Z}^N, X).$$

Moreover, this embedding is effective and representation of elements of $F^{\mathbb{Z}[t]}$ by infinite words introduces "nice" normal forms on $F^{\mathbb{Z}[t]}$.

(in fact, $\phi : F^{\mathbb{Z}[t]} \hookrightarrow R^*(\mathbb{Z}[t], X)$.)

Example. Let $X = \{x, y\}, F = F(X)$. If $u \in F$ is cyclically reduced then

$$G = \langle F, s \mid s^{-1}us = u \rangle$$

is embeddable into $R(\mathbb{Z}^2, X)$.

Indeed, $F \subset R^*(\mathbb{Z}^2, X)$ and we define s as an "infinite power" of u

$$s = [uuuu\cdots)(\cdots uuuu] = u^t$$

It is easy to see that

$$u \circ s = s \circ u.$$

Elements of $G = \langle F, s \mid s^{-1}us = u\rangle$ viewed as infinite words have normal forms.

If $g \in G$ then its normal form

$$\pi(g) = g_1 \circ u^{\alpha_1} \circ g_2 \circ \cdots \circ u^{\alpha_n} \circ g_{n+1},$$

where $g_i \in F,\ \alpha_i \in \mathbb{Z}^2 - \mathbb{Z}$.

Normal forms can be computed easily.

Example. Let $u = xy \in F$ and $g = (y^{-1}x^{-1})\ s\ x^{-1}\ s^{-1} \in G$. Then, a representation of g as an infinite word is

$$g = (y^{-1}x^{-1}) * u^t * x^{-1} * u^{-t} = (y^{-1}x^{-1}) * (u \circ u^{t-1}) * x^{-1} * u^{-t} =$$

$$= (y^{-1}x^{-1}) * ((xy) \circ u^{t-1}) * x^{-1} * u^{-t} = u^{t-1} \circ x^{-1} \circ u^{-t}.$$

Generalization of Stallings' foldings to $F^{\mathbb{Z}[t]}$

Theorem. (Miasnikov, Remeslennikov, Serbin) Let G be a f.g. subgroup of $F^{\mathbb{Z}[t]}$. Then there exists a finite labeled directed graph Γ_G such that

$$g \in G \text{ if and only if } \Gamma_G \text{ "accepts" } \pi(g).$$

In other words Γ_G solves the Subgroup Membership Problem in $F^{\mathbb{Z}[t]}$. Moreover, Γ_G can be constructed effectively, given generators of G.

Edges of Γ_G are labeled by letters from the alphabet

$$\{X \cup X^{-1}\} \cup \{u^{\alpha} \mid u \in U, \alpha \in \mathbb{Z}[t]\},$$

where U is a special subset of $F^{\mathbb{Z}[t]}$.

Graphs labeled by X and u_i^α. U-foldings.

1. A $g \in G$ represented by its reduced form $\pi(g)$. $G \hookrightarrow R(\mathbb{Z}^N, X)$.

2. Graphs labeled by special infinite words.

3. U-foldings, U-folded graphs. In U-folded graph an element is readable iff its normal form is readable.

4. Solution to Membership problem and numerous other problems (2004-2008):

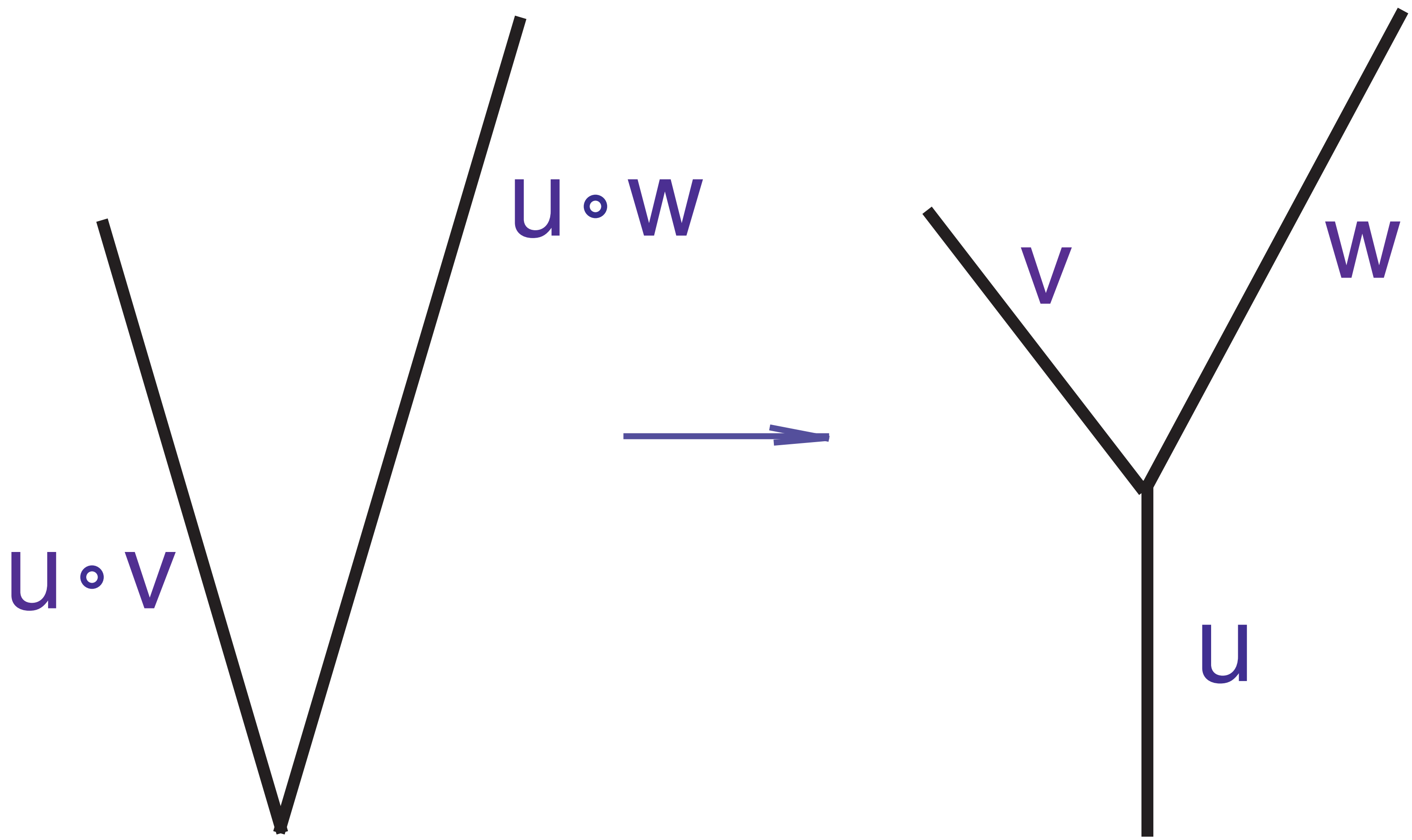
Miasnikov, Remeslennikov, Serbin. Membership problem.

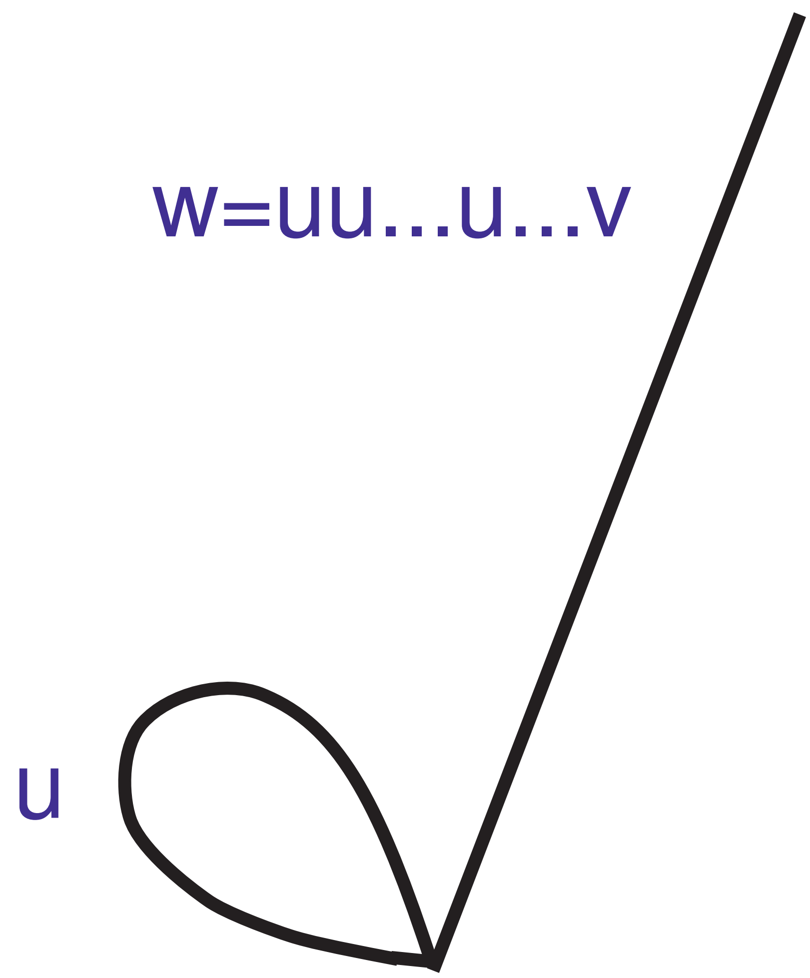
Kharlampovich, Miasnikov, Remeslennikov, Serbin. Intersection, Houson property, conjugacy, normality, malnormality.

Serbin, N. Finite index, Greenberg-Stallings, commensurator.

Proof of Subgroup Separability in terms of U-graphs is not known.

Can we organize Stallings-like graph technique for arbitrary f.g. subgroups of $R^*(\mathbb{Z}^n, X)$?


u ∘ w
u ∘ v
v
w
u


w=uu...u...v
u

Λ-trees

Let Λ be an ordered abelian group, for example $\mathbb{Z}^n$ with right lexicographic order.

The following definition is due to Morgan and Shalen (1984).

A Λ-tree is a geodesic Λ-metric space (X, d) such that for all $x, y, z \in X$
$[x, y] \cap [x, z] = [x, w]$ for some $w \in X$,
$[x, y] \cap [y, z] = \{y\} \Rightarrow [x, z] = [x, y] \cup [y, z]$.

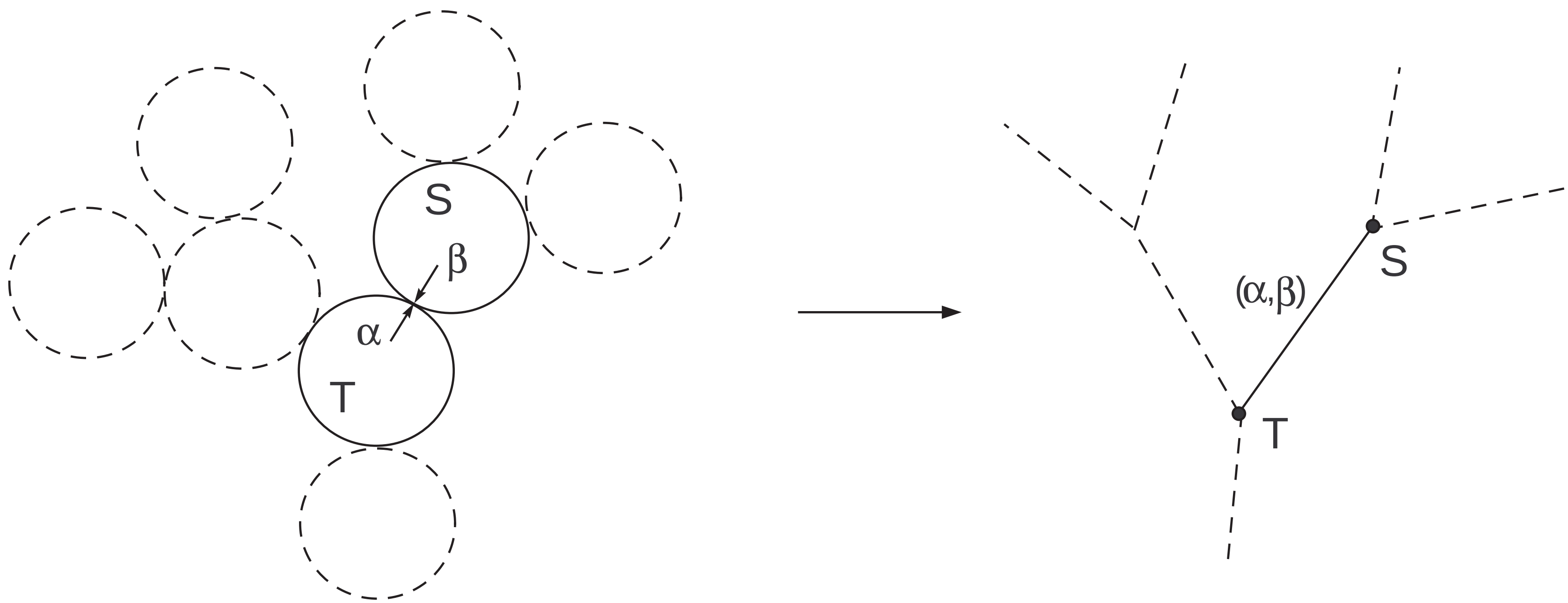
Examples.

$n = 1.$

$\mathbb{Z}$-tree is a “usual” simplicial tree.

$n = 2$.

$\mathbb{Z}^2$-tree can be viewed as a "tree of $\mathbb{Z}$-trees".



An isometric action of a group on a Λ-tree X is free if there are no inversions and the stabilizer of each point of X is trivial. We say that a group G is Λ-free if G admits such an action on some Λ-tree.

Alperin–Bass Program. Find the group theoretic information carried by free action on a Λ-tree.

Problem. *Describe finitely presented (finitely generated) groups acting freely on an arbitrary Λ-tree.*

Two principal cases:

- Λ archimedian
- Λ non-archimedian

Archimedian case

$\Lambda \hookrightarrow \mathbb{R}$. Groups acting on $\mathbb{R}$-trees are described by Rips' theorem:

Theorem. A finitely generated group acts freely on an $\mathbb{R}$-tree if and only if it is a free product of free abelian groups and surface groups (with exception of non- orientable groups of genus 1, 2, and 3)

Non-archimedian case

Conjecture. (Kharlampovich, Miasnikov, Serbin) A finitely presented group acting freely and regularly on Λ-tree can be embedded in a group acting freely on a $\mathbb{Z}^n$-tree.

$\mathbb{Z}^n$-free groups

Martino, O Rourke (2004), Guirardel (2004).

1. (MR) $\mathbb{Z}^n$-free groups are commutation transitive, and any abelian subgroup of a $\mathbb{Z}^n$-free group is free abelian of rank at most n.
2. (MR) $\mathbb{Z}^n$-free groups are coherent.
3. (G) $\mathbb{Z}^n$-free groups are hyperbolic relative to maximal abelian subgroups.
4. (MR) A finitely generated $\mathbb{Z}^n$-free group all of whose maximal abelian subgroups are cyclic is word hyperbolic (as are all its finitely generated subgroups).
5. (MR) Word Problem is decidable in any $\mathbb{Z}^n$-free group.
6. (MR) Class of Z^n-free (for some n) groups is closed under amalgamated products along maximal abelian subgroups.

The following is due to Chiswell and Myasnikov–Remeslennikov–Serbin $((1) \to (3))$.

Theorem. Let G be a finitely generated group. Then the following are equivalent:

1. there exists an embedding $G \hookrightarrow R^*(\mathbb{Z}^n, X)$,
2. G has a free Lyndon length function with values in $\mathbb{Z}^n$,
3. G acts freely on $\mathbb{Z}^n$-tree.

Action of G on a Λ-tree is called regular if, under corresponding $G \hookrightarrow R^*(\mathbb{Z}^n, X)$,

$$\forall f, g \in G \quad com(f, g) \in G.$$

In terms of action itself: action is branch-point transitive.

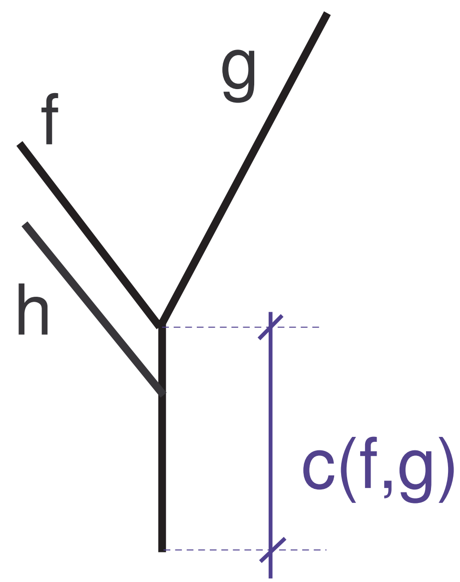
Length functions

A function $l : G \to \Lambda$ is called a (Lyndon) length function on G if:

(L1) $\forall\ g \in G:\ \ l(g) \geqslant 0$ and $l(1) = 0$;

(L2) $\forall\ g \in G:\ \ l(g) = l(g^{-1})$;

(L3) $\forall\ g, f, h \in G:\ \ c(g, f) > c(g, h) \to c(g, h) = c(f, h)$,
where $c(g, f) = \frac{1}{2}(l(g) + l(f) - l(g^{-1}f))$.



A length function $l : G \to \Lambda$ is called free if:

(L4) $\forall\, g, f \in G :\ c(g, f) \in \Lambda$.

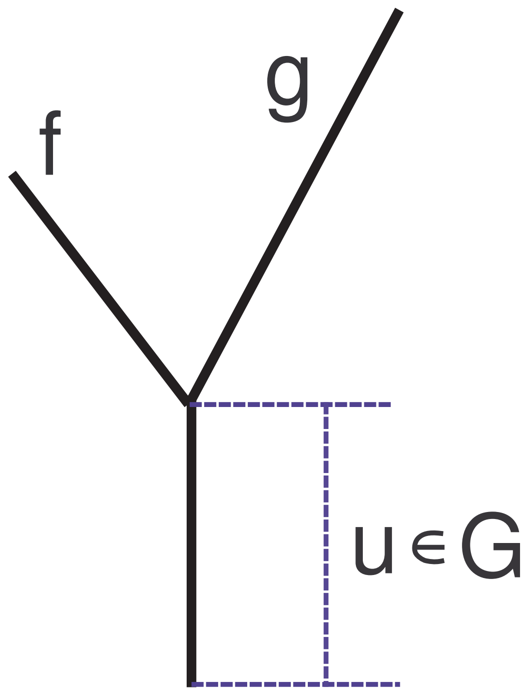
(L5) $\forall\, g \in G :\ g \neq 1 \to l(g^2) > l(g)$.

If $l(fg) = l(f) + l(g)$, we write $fg = f \circ g$.

A length function $l : G \to \Lambda$ is called regular if it satisfies the regularity axiom:

(L6) $\forall\ g, f \in G,\ \exists\ u, g_1, f_1 \in G :$

$$g = u \circ g_1 \ \&\ f = u \circ f_1 \ \&\ l(u) = c(g, f).$$



Example

Take $G \subseteq F(x, y)$, $G = y^{-1}\langle x\rangle y$. If

$$f = y^{-1}x^{100}y, \quad g = y^{-1}x^{10}y,$$

then

$$u = y^{-1}x^{10} \notin G,$$

so the free length function that F induces on G is not regular.

How to embed a group with free length function into a group with free regular length function: "cut up" elements into pieces until (L6) is satisfied.

Theorem. (Chiswell, Muller) Finitely generated group acting freely on a Λ-tree can be embedded in a group acting freely and regularly on a Λ-tree.

Theorem. (Kharlampovich, Miasnikov, Serbin) Finitely generated group acting freely on a $\mathbb{Z}^n$-tree can be embedded in a finitely generated group acting freely and regularly on a $\mathbb{Z}^n$-tree. Moreover, the embedding is (in certain sense) effective.

Theorem. (Kharlampovich, Myasnikov, Remeslennikov, Serbin) Finitely generated G has a regular free action on a Z^n-tree if and only if G can be represented as a union of a finite series of groups

$$G_1 < G_2 < \ldots < G_n = G,$$

where

1. G_i has a regular free action on a Z^i-tree (that is, G_1 is a free group),
2. G_{i+1} is obtained from G_i by finitely many HNN-extensions in which associated subgroups are maximal abelian and length-isomorphic.

Free groups:

1. $F(X)$ represented by reduced words in alphabet $X \cup X^{-1}$.
2. Graphs labeled by words in $X \cup X^{-1}$.
3. Stallings foldings, Stallings graph.
4. Solution to Membership problem and numerous other problems.

F.g. fully residually free groups:

1. A $g \in G$ represented by its reduced form $\pi(g)$. $G \hookrightarrow R(\mathbb{Z}^N, X)$.
2. Graphs labeled by special infinite words.
3. U-foldings, U-folded graphs.
4. Solution to Membership problem and numerous other problems.

Good intentions.

Given finitely generated $\mathbb{Z}^n$-free group G,

1. based on structure theorem and Britton's lemma, define normal form of elements of G,
2. build (not folded) graph labeled by infinite words that recognizes G,
3. "fold" it so that it accepts normal forms of elements of G,
4. enjoy solving algorithmic problems.

Good intention #1 fails.

Normal forms similar to ones in limit groups are unreasonably technically complicated. Instead of a unique normal form, for each $g \in G$ we define an infinite set of words $\Pi(g)$.

Denote in last theorem

$$G_n = \langle G_{n-1}, T_{n-1} \mid w^{-1} C_w w \stackrel{\phi_w}{=} D_w,\ w \in T_{n-1},\ \rangle.$$

As an infinite word, element w starts with "positive" infinite power of any element of C_w and ends with "positive" infinite power of any element of D_w.

Example:

$$C_w = \langle xy \rangle, \ D_w = \langle zx \rangle,$$

$$w = xyxy \cdots zxzx,$$

$$(x^{-1}z^{-1}x^{-1}z^{-1} \dots y^{-1}x^{-1}y^{-1}x^{-1})xy(xyxy \cdots zxzx) = zx.$$

Define finite alphabet $\mathcal{B}(G)$ to be union $X \cup T_1 \cup \ldots \cup T_{n-1}$.

Building folded $\mathcal{B}(G)$-graph.

Primary (short-term) goal:
build $\mathcal{B}(G)$-graph that can be used to solve subgroup membership problem.

Long-term goal:
build $\mathcal{B}(G)$-graph that can be reasonably used to solve other algorithmic problems.

Theorem. (Nikolaev, Serbin) For a fixed G, there exists algorithm that, given a $\mathcal{B}(G)$-graph Γ produces Γ', that recognizes the same group, with the following property:
if there exists path p in Γ' such that

$$o(p) = v_1, e(p) = v_2, \mu(p) = g,$$

then there exists path q such that

$$o(q) = v_1, e(q) = v_2, \mu(p) \in \Pi(g).$$

The latter for a given g can be checked effectively.

Good: Solved uniform subgroup membership problem (and power problem).

Bad: Solution to other algorithmic problems (even intersection problem) will be rather involved.