Automata and infinite words: applications in Group Theory

Denis Serbin

McGill University

Stallings' foldings in free groups

Let a graph Γ consist of a set of vertices $V(\Gamma)$, a set of edges $E(\Gamma)$, and two functions:

$$E \longrightarrow V \times V \ , \ e \longrightarrow (o(e), t(e)),$$

$$E \longrightarrow E \ , \ e \longrightarrow \bar{e},$$

which satisfy the following properties

$$\bar{\bar{e}} = e, \quad e \neq \bar{e}, \quad o(e) = t(\bar{e}).$$

That is, every edge e has an initial vertex $o(e)$, a terminal vertex $t(e)$, and a formal inverse $\bar{e}$.

An orientation of Γ is a subset $E_+ \subset E$ such that

$$E_+ \cap \bar{E}_+ = \emptyset, \quad E = E_+ \cup \bar{E}_+.$$

Edges from E_+ we call positively oriented.

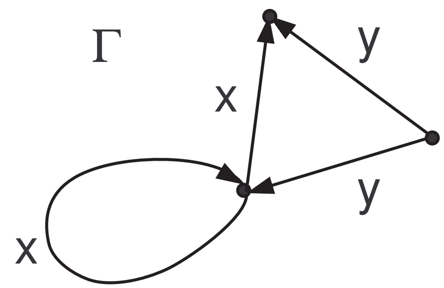
Let X be a finite alphabet. We can label positively oriented edges by

$$\mu : E_+ \longrightarrow X$$

and extend μ to $E = E_+ \cup \bar{E}_+$ by setting $\mu(\bar{e}) = \mu(e)^{-1}$ for every $e \in E_+$.

Hence, we obtain a directed X-labeled graph (X-digraph) Γ.

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



Observe that we draw only a positive edge e from each pair $\{e, \bar{e}\}$.

A path p in Γ is a sequence of edges $p = e_1, \ldots, e_k$, where $o(e_{i+1}) = t(e_i)$ for $i \in [1, k-1]$.

p has a naturally defined 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".

Obviously, $L(\Gamma, v) \subseteq (X \cup X^{-1})^*$. Note that words in $L(\Gamma, v)$ are not necessarily freely reduced.

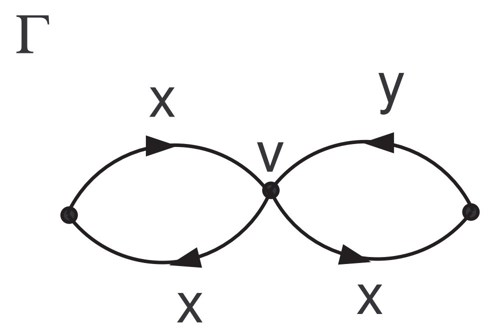
Fact. The set

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

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.



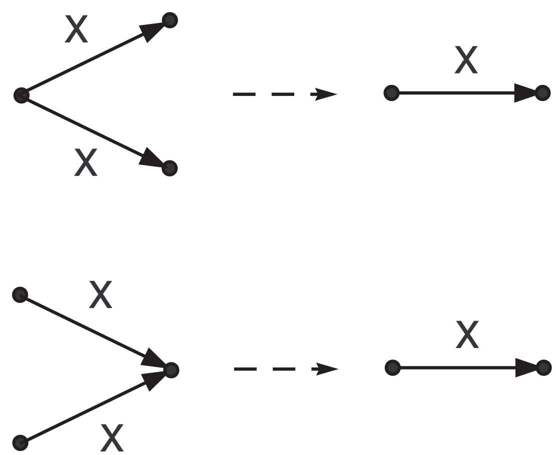
Obviously, $H = \overline{L(\Gamma, v)}$.

The idea to work with X-digraphs 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-digraph Γ is folded if there exist no edges $e_1 \neq e_2$ such that $o(e_1) = o(e_2)$, $\mu(e_1) = \mu(e_2)$. That is, the following situations are prohibited

Consider the following operations called foldings

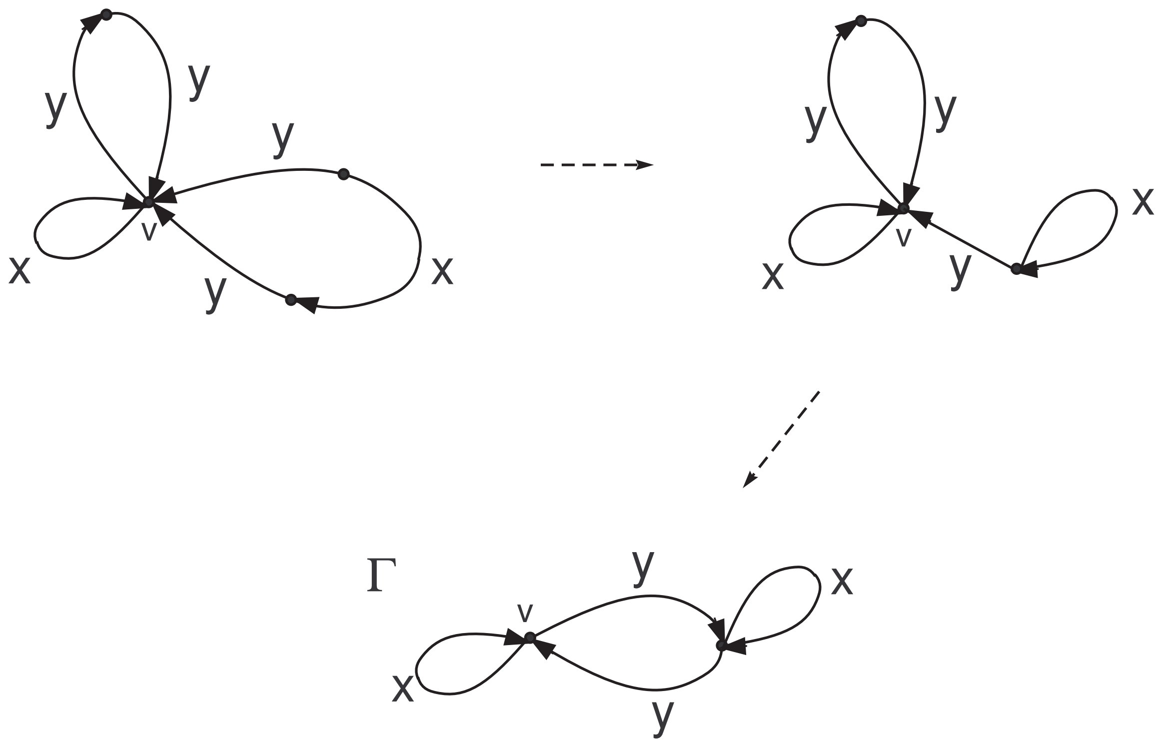


Fact. If Δ is obtained from Γ by a folding, so that $w \in V(\Delta)$ corresponds to $v \in V(\Gamma)$. Then $\overline{L(\Gamma, v)} = \overline{L(\Delta, w)}$.

Fact. For every finitely generated $H \leq F(X)$ there exists a folded X-digraph 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.

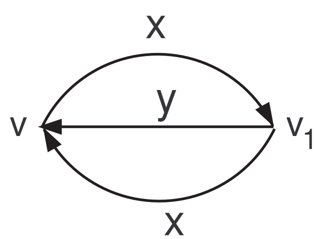
Let $H, K \leq F(X)$ and let Γ, Δ be folded X-digraphs such that $H = L(\Gamma, v),\ K = L(\Delta, w)$.

$$H \cap K = L(\Gamma, v) \cap L(\Delta, w) = L(\Gamma \times \Delta, v \times w),$$

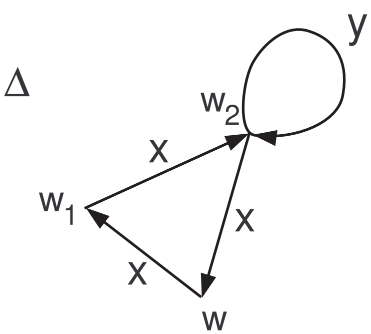
where $\Gamma \times \Delta$ is a product-graph of Γ and Δ. Hence, a solution of the Subgroup Intersection Problem.

Example: $H = \langle xy, y^{-1}x \rangle,\ K = \langle x^3, x^{-1}yx \rangle.$

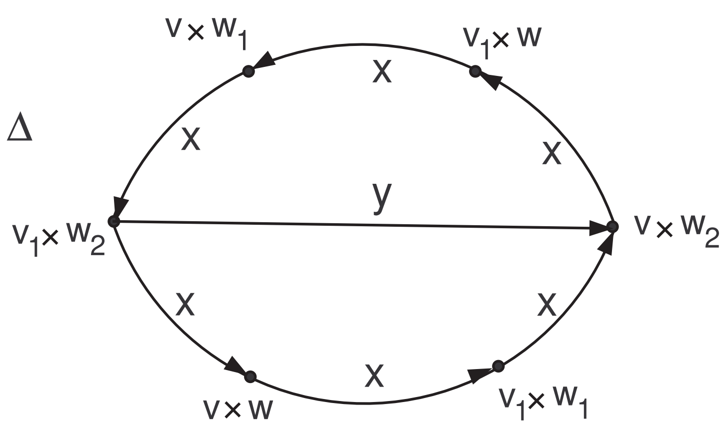
Γ



Δ



$\Gamma \times \Delta$



Question: Is it possible to generalize graph methods described above to groups whose elements can be represented by infinite words ?

Ordered abelian groups

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

Examples.

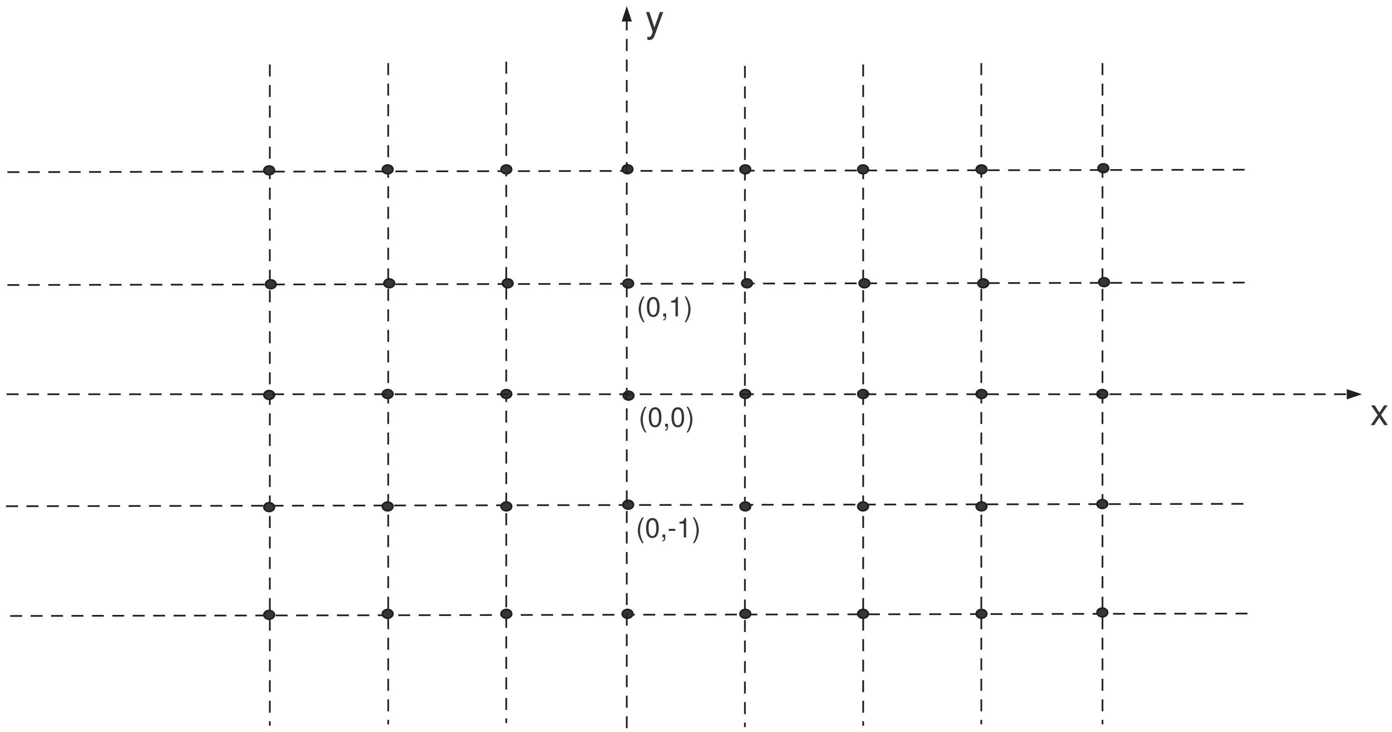
1. archimedean case: $A = \mathbb{R}$, $A = \mathbb{Z}$ with usual order.
2. non-archimedean case: $A = \mathbb{Z}^2$ with the right lexicographic order

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

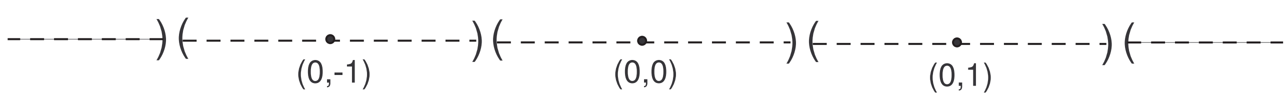
In particular,

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

$\mathbb{Z}^2$



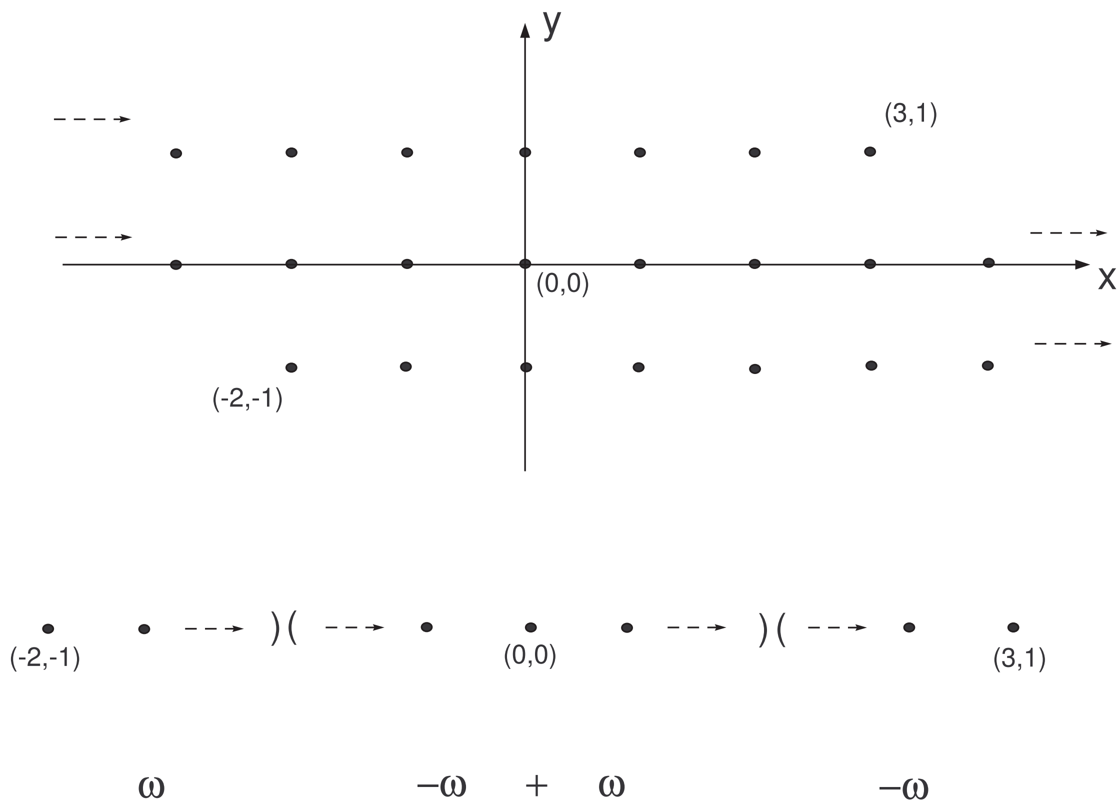
$\mathbb{Z}^2$ with the right lexicographic order



For $\alpha, \beta \in \mathbb{Z}^2$ the closed segment $[\alpha, \beta]$ is defined by

$$[\alpha, \beta] = \{\gamma \in \mathbb{Z}^2 \mid \alpha \leq \gamma \leq \beta \}.$$

Example. $[(-2, -1), (3, 1)]$



Infinite words

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

An A-word is a function of the type

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

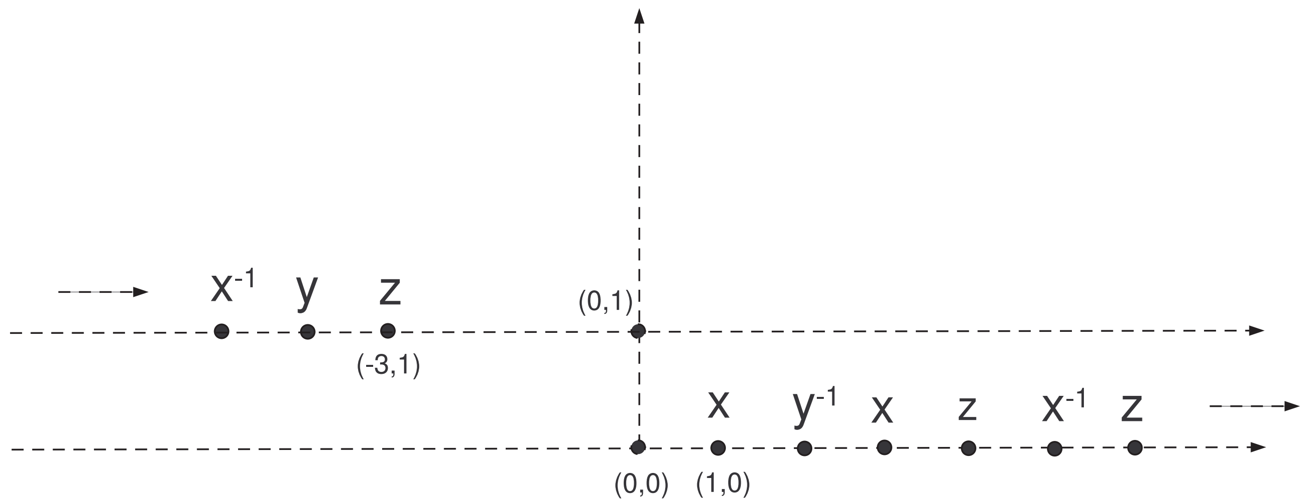
where $\alpha \geq 0$. The element α is called the length $|w|$ of w.

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

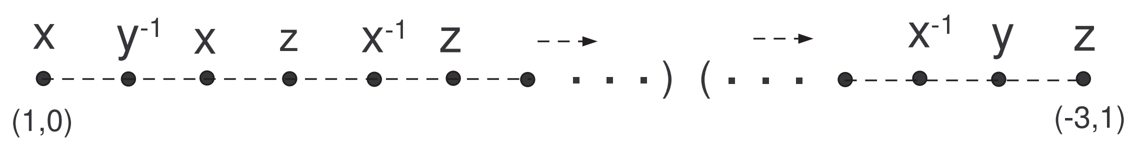
w is reduced $\Longleftrightarrow$ no subwords xx^{-1}, $x^{-1}x$ $(x \in X)$.

$R(A, X)$ = the set of all reduced A-words.

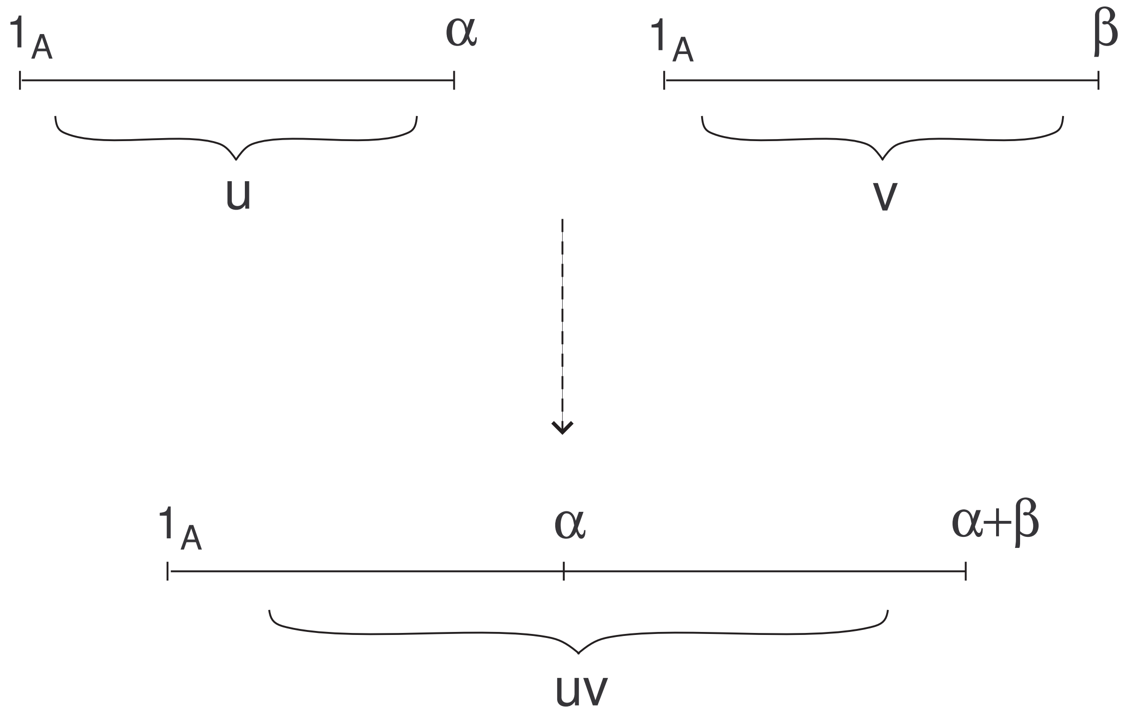
Example. $X = \{x, y, z\},\ A = \mathbb{Z}^2$



In "linear" notation

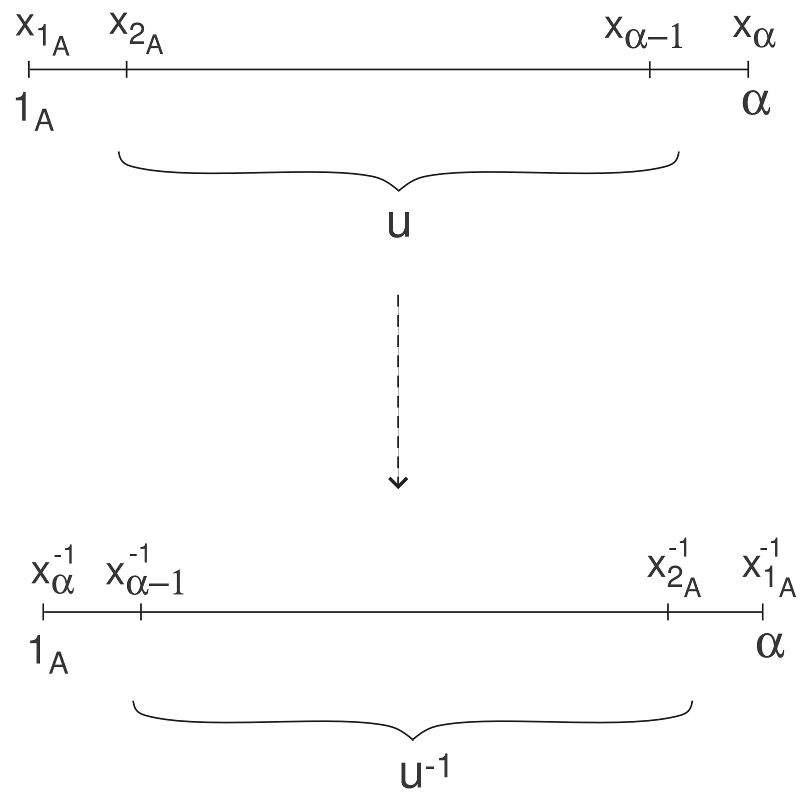


Concatenation of A-words

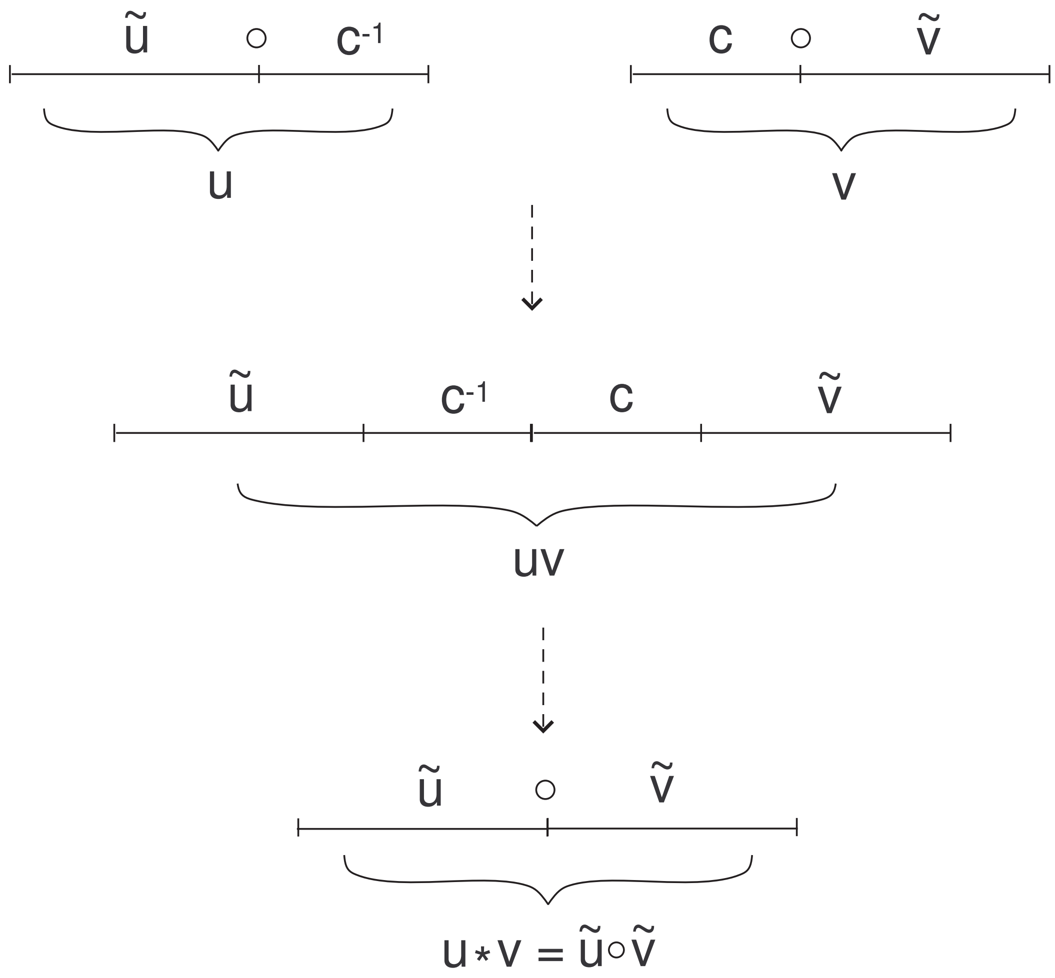


We write $u \circ v$ instead of uv in the case when uv is reduced.

Inversion of A-words



Multiplication of A-words



Multiplication of A-words

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

Suppose u and v can be represented in the form

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

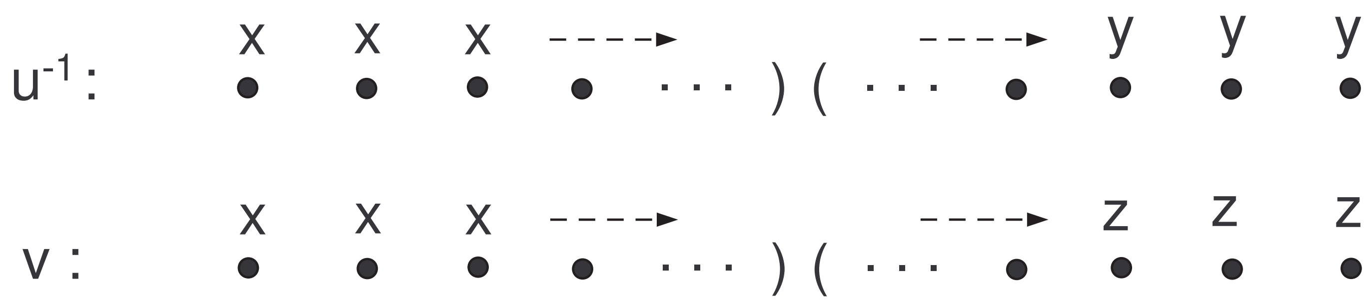
where $c \in R(A, X)$ is of maximal possible length.

Then define

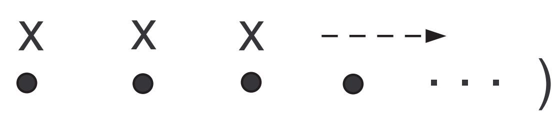
$$u * v = \tilde{u} \circ \tilde{v}.$$

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

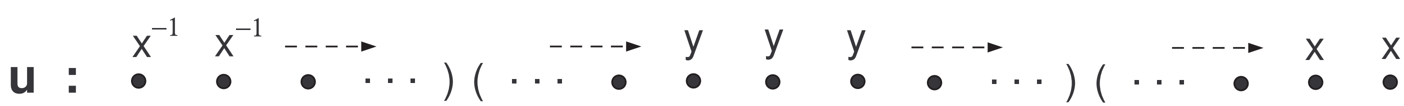
$v \in R(A, X)$ is cyclically reduced if $v(1_A)^{-1} \neq v(|v|)$.

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

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

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

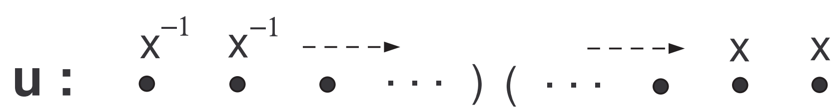
Example. $u \in R(\mathbb{Z}^2, X)$ does not admit a cyclic decomposition



Torsion

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

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



has order 2.

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

A non-standard free group

In 1960 R. Lyndon introduced a notion of a free $\mathbb{Z}[t]$-group. It can be defined as a union of the chain of groups

$$F = F_0 < F_1 < \cdots < F_n < \cdots,$$

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 $\alpha_i \in \mathbb{Z}[t]$.

Thus obtained group, denoted $F^{\mathbb{Z}[t]}$, is called Lyndon's free $\mathbb{Z}[t]$-group, or a $\mathbb{Z}[t]$-completion of a free group F.

Observe that for any $g \in F^{\mathbb{Z}[t]}$ and $\alpha \in \mathbb{Z}[t]$ there exists an element $g^\alpha \in F^{\mathbb{Z}[t]}$. That is, $F^{\mathbb{Z}[t]}$ admits $\mathbb{Z}[t]$-exponentiation.

$F^{\mathbb{Z}[t]}$ can be viewed as a non-standard free group. Besides standard exponents $\{g^n,\ n \in \mathbb{Z}\}$ of its elements it also contains non-standard ones $\{g^\alpha,\ \alpha \in \mathbb{Z}[t] \setminus \mathbb{Z}\}$.

Miasnikov and Remeslennikov (1996) gave an effective construction of $F^{\mathbb{Z}[t]}$ in terms of extensions of centralizers.

Let G be a group and $C_G(u) = \langle u \rangle$ a cyclic centralizer of $u \in G$. An extension of $C_G(u)$ by $\mathbb{Z}[t]$ is defined as the HNN-extension

$$H = \langle\ G, s_j \quad (j \in \mathbb{N}) \ \mid\ [u, s_j] = [s_j, s_k] = 1 \quad (j, k \in \mathbb{N})\ \rangle.$$

Observe that s_j corresponds to u^{t^j} which commutes with u, and $C_H(u) \simeq \mathbb{Z}[t]$

$F^{\mathbb{Z}[t]}$ is a union of the infinite chain of groups

$$F = G_0 < G_1 < \cdots < G_n < \cdots,$$

where G_{i+1} is obtained from G_i by extension of all cyclic centralizers in G_i.

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

Recall that $R^*(\mathbb{Z}[t], X)$ is the set of $\mathbb{Z}[t]$-words which admit cyclic decompositions.

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

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

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

Idea of the proof.

$F^{\mathbb{Z}[t]}$ is a union of the chain $F = G_0 < G_1 < \cdots < G_n < \cdots$.

Assume that an embedding $G_n \hookrightarrow R^*(\mathbb{Z}[t], X)$ is constructed (we identify G_n with its image).

Choose $C = \{u_i \mid i \in I\} \subset G_n$, the set of generators of proper cyclic centralizers in G_n (up to conjugacy and taking inverses).

Define a $\mathbb{Z}[t]$-exponentiation function

$$exp : (u, \alpha) \to u^{\alpha},$$

where $u \in C, \alpha \in \mathbb{Z}[t]$.

Finally, prove that $H = \langle\ G_n,\ \{u^{t^k} \mid u \in C, k \in \mathbb{N}\}\ \rangle$ is a subgroup of $R^*(\mathbb{Z}[t], X)$ isomorphic to G_{n+1}.

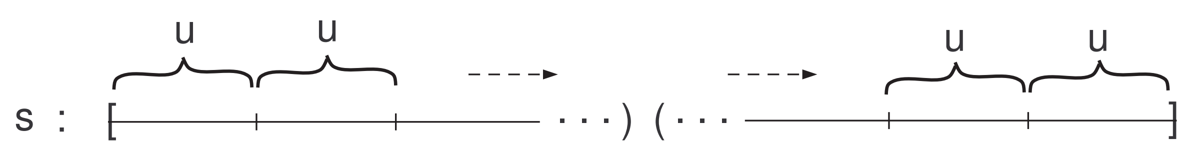
Example. Let $X = \{x, y\}, F = F(X)$. If $u \in F$ is cyclically reduced then

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

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

Indeed, $F \subset R^*(\mathbb{Z}^2, X)$ and we define s as a "non-standard" exponent of u

$$s = u^t, \ t = (0, 1).$$



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

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

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

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

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

Example. Let $F = F(X)$, $X = \{x, y\}$ and $G = \langle F, s \mid s^{-1}us = u\rangle$, where $u = xyx$ and $s = u^t$ is defined as before.

Take $g \in G$ to be $g = s^2yxs^3$. It follows that

$$g = u^{2t} \circ (yx) \circ u^{3t} = (xyx)^{2t} \circ (yx) \circ (xyx)^{3t}$$

is a representation of g as an infinite word.

But at the same time

$$g = u^{2t-1} \circ (xy) \circ u^{3t+1} = (xyx)^{2t-1} \circ (xy) \circ (xyx)^{3t+1}$$

is another representation of g as an infinite word.

The former one is characterized by a 2-tuple $(2t, 3t)$ of non-standard exponents involved, the latter one by $(2t-1, 3t+1)$, which is less than $(2t, 3t)$ in the left lexicographic order.

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

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

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

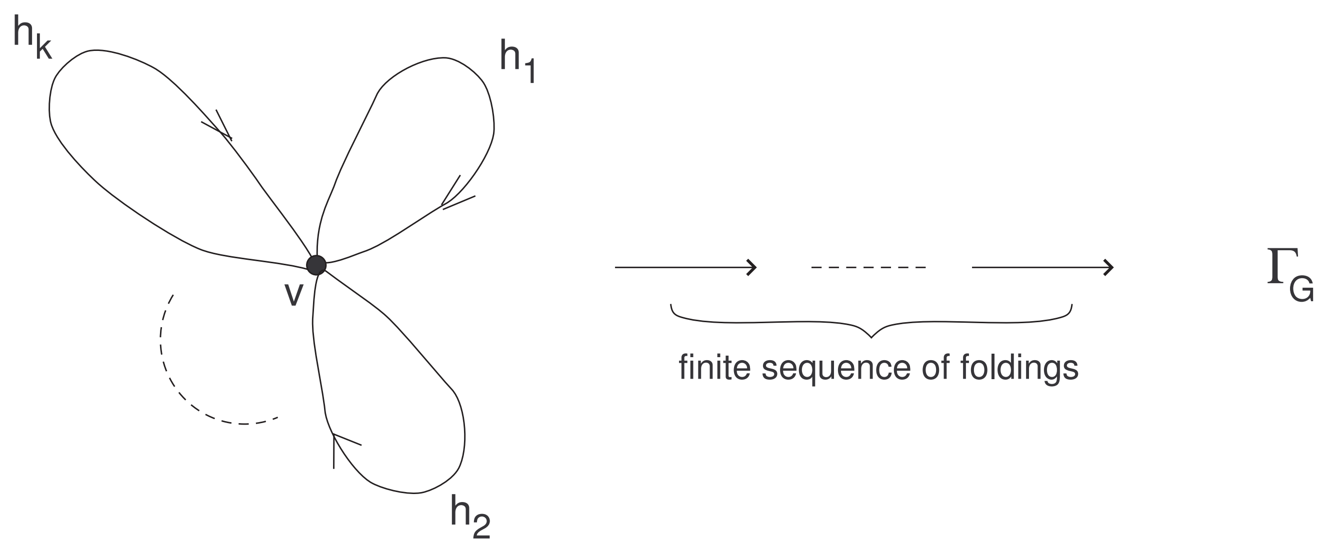
In other words Γ_G solves the Subgroup Membership Problem in $F^{\mathbb{Z}[t]}$. Moreover, Γ_G can be constructed effectively, given generators of G.

Edges of Γ_G are labeled by letters from the alphabet

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

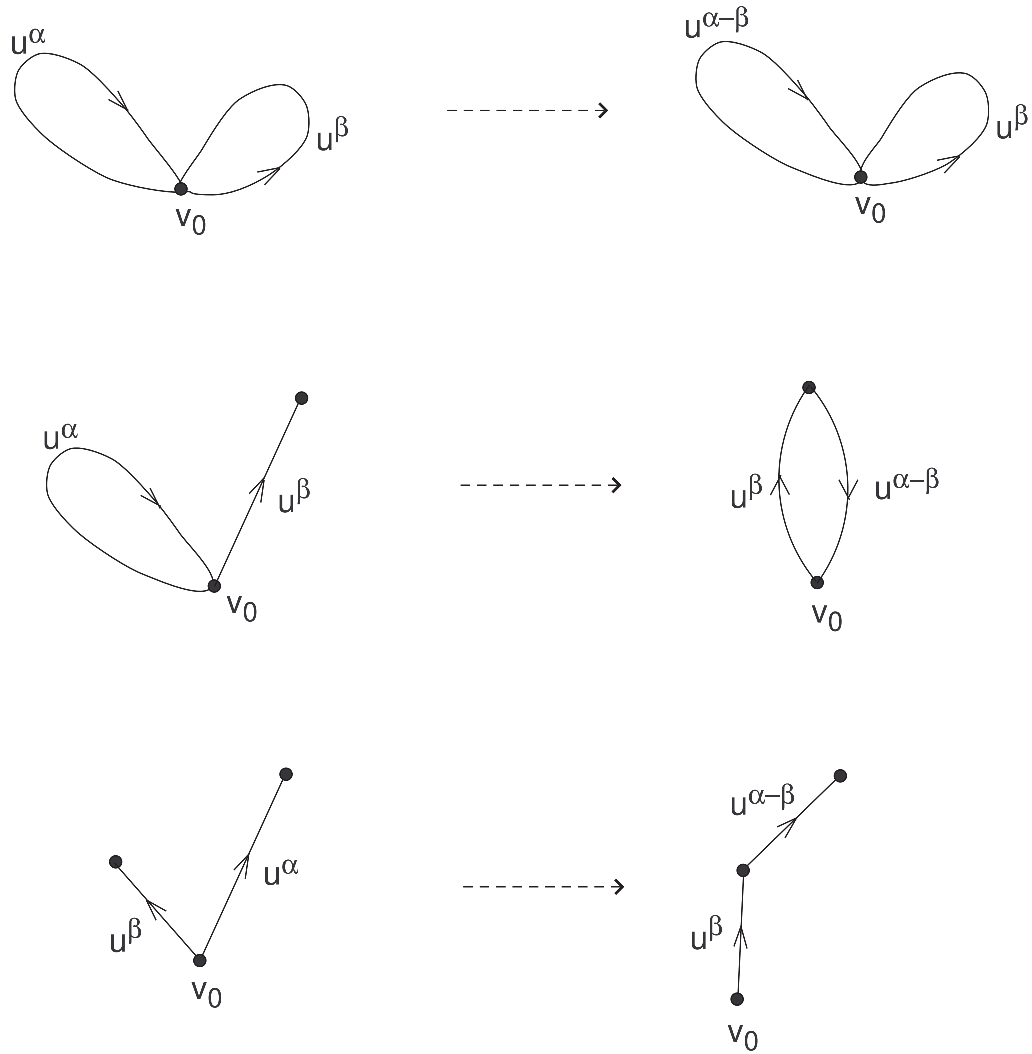
where U is a special subset of $F^{\mathbb{Z}[t]}$.

Let $G = \langle h_1, \ldots, h_k \rangle$.



$$\text{foldings} = \begin{cases} \text{standard Stallings' foldings} \\ U\text{-foldings} \end{cases}$$

U-foldings (assume $\alpha \geq \beta > 0$)



Theorem. (Kharlampovich, Miasnikov, Remeslennikov, S) The Subgroup Intersection Problem is decidable in $F^{\mathbb{Z}[t]}$. That is, there exists an algorithm which for any f.g. subgroups H and K of $F^{\mathbb{Z}[t]}$ effectively finds generators of $H \cap K$, which is finitely generated.

Theorem. (Kharlampovich, Miasnikov, Remeslennikov, S) There exists an algorithm which for any f.g. subgroups H and K of $F^{\mathbb{Z}[t]}$ effectively checks if there exists $g \in F^{\mathbb{Z}[t]}$ such that

$$H^g = K.$$

etc.

Applications to fully residually free (or limit) groups

A group G is called fully residually free if for any finitely many non-trivial elements $g_1, \ldots, g_n \in G$ there exists a homomorphism ϕ of G into a free group F, such that $\phi(g_i) \neq 1$ for $i = 1, \ldots, n$.

Fully residually free groups naturally arise from studying equations in free groups, and have a lot of nice properties.

Examples:

1. free groups,
2. surface groups (except for non-orientable surfaces of genus $1, 2, 3$),
3. extensions of centralizers of a free group.

Theorem (Kharlampovich-Myasnikov, 1998). Every f.g. fully residually free group is embeddable into a "non-standard" free group $F^{\mathbb{Z}[t]}$. Moreover, for a given finite presentation of a f.g. fully residually free group G one can effectively construct an embedding of G into $F^{\mathbb{Z}[t]}$.

Now, our solution of various algorithmic problems for subgroups of $F^{\mathbb{Z}[t]}$ implies the solution of the same problems for f.g. fully residually free groups.