On the decidability of the freeness problem in groups

Emir Melliti - ENS PSL
Emmanuel Breuillard - Mathematical Institute, University of Oxford

February - June 2024

I Introduction

1 Abstract

The free group is the fundamental object of combinatorial group theory that is the base used to define any group by generators and relations. It was at first mostly studied from a combinatorial point of view using Nielsen transformation [Nie21] one of the most important results being the Nielsen-Schreier theorem, stating that every subgroup of a free group is free (see for example [MKS04]). Some geometric tools appears to be very useful such as Van Kampen diagrams, Cayley graphs, and with the development of algebraic topology, groups described by presentations were identified as fundamental groups of 2-complexes. This point of view deeply studied by Stalling [Sta91] [Sta83] shows for example how to describe subgroup with covering map between complexes, or amalgamated sum with the Seifert-van Kampen theorem. The ideas of Stalling where then described in a more combinatorial way (e.g. in [KM02]), with object that we call here graph representations and that we use in this report to prove some classic theorems on free groups and to tackle a decision problem on groups: the freeness problem. While the problem of deciding if a finitely presented group is free is known as being undecidable by the Adian-Rabin theorem because it is a Markov property[Adi55] [Rab58], the freeness problem is the question asked in a fixed finitely presented group G, given some elements g_i, to determine if they freely generate the subgroup $< g_i >$. It can be decidable or not depending on the group G where it is stated. The main new result I found and that we prove here is that the class of groups where this problem is decidable (with a small but necessary additional hypothesis) is closed under free product.

Contents

2 The internship

The internship took place in the Mathematical Institute of the University of Oxford, in the heart of the city of Oxford, under the supervision of Pr. Emmanuel Breuillard.
I started the internship by reading articles and books around the subject of finitely presented groups, from both the combinatorial and geometrical points of view. Starting with recommendations of my supervisor Pr. Breuillard and jumping from references to others. Then, I gradually started to use my time to think of the decidability of the freeness problems in some kind of groups, at first with promising ideas but no complete answer, until I managed to tackle the details that were blocking me from getting the result presented here. I also spend some times coding to implement some of the algorithms I was working on and help visualizing their behavior.
The internship was punctuated by weekly meetings with my supervisor, where I presented my progress and my ideas, and where I received reading advice and we discussed about diverse problems around the subject.
The environnement in the Mathematical Institute, and more generally in Oxford, in sport activities for example, allowed me to meet a lot of people working on very diverse subjects from humanities to physics, and coming from all over the world.
I would like to thank Pr. Breuillard for his guidance and for sharing some of his interesting subjects of research with me, and the Mathematical Institute for the opportunity to work there and for the great environnement it offers.

II Decision Problems on groups

1 The word problem and the membership problem

A decision problem is a question asked on some input which answer is either yes or no. It is called decidable if there exists an algorithm, that given the input, outputs the right answer after a finite number of steps. It is called semi-decidable, or recursively enumerable if there exists an algorithm that given the input, outputs yes when the answer is yes, and can either never stop or answer no when the answer is no. A problem is decidable if and only if both him and its inverse are semi-decidable. While these concepts can be formalized either with Turing machine, either with recursion theory, we prefer here to think intuitively of the idea of algorithm.
We first introduce some decision problems on groups. The word problem is probably the most fundamental decision problem on groups, and it is the first one that was proved to be undecidable by Novikov and Boone [Boo58] [Nov55]. I worked on the proof of the undecidability of the word problem in [Rot95] that is based on HNN-extension, an important construction introduced in [HNN49] that is also at the heart of the Adian-Rabin theorem's proof.

Definition II.1 : Word Problem

> Let $G = (X, R)$ be a finitely presented group, i.e. X is a finite set of generators, and R is a finite set of relations (element of the free group $F(X)$), and G is the quotient of the free group $F(X)$ by the normal subgroup N generated by R.
> The word problem is to decide algorithmically given a word $w \in F(X)$ on the generators of G whether $w = 1$ in G, that is if $w \in N$.

The word problem is semi-decidable : given the word w on $X^{\pm 1}$, an algorithm can enumerate the elements of N as product of conjugates of elements of R and answer yes if it finds w. The inverse problem however (deciding if $w \neq 1$) is not always semi-decidable.
The existence of groups with undecidable word problem is one of the earliest examples of undecidability in mathematics. It played a crucial role in expanding the concept of undecidability beyond the realm of Turing machines. The undecidability of the word problem implies thanks to the Adian-Rabin theorem the undecidability of many problems on groups that consist on deciding if a finitely presented group has a certain "Markov property" [Adi55] [Rab58], such as being free, being finite, or even being trivial. An other interesting type of Markov property is having some decision problem decidable, the word problem itself for example, or the freeness problem, on which this report focus on. We will always work on groups where the word problem is decidable, in order to be able to talk about element of the groups without considering a particular word on the generator representing it.
Another classic decision problem of which we will use a restriction in the following is the membership problem.

Definition II.2 : Membership, free membership

> The membership problem is to decide given g_i elements of G, and $g \in G$, if $g \in < g_i >$. The free membership problem is the restriction of this problem when $\{g_i\}$ is free.

The membership problem is decidable in a (finitely generated) free group. It can be proved using the tools introduced in this report III.18, but it is not decidable in a direct product of free group because of a simple reduction to the word problem. If $G =< X, R >$ is a group with undecidable word problem, let $H \subset F(X) \times F(X)$ be the subgroup generated by (x, x) for $x \in X$ and $(1, r)$ for $r \in R$. It is easy to see that H is exactly the pairs (u, v) such that $uv^{-1} = 1$ in G, thus the problem

$(w, 1) \in H$ is equivalent to the word problem in G and is thus undecidable.

2 The freeness problem, first results

Here are some already known results on the decidability of the freeness problem.

Definition II.3 : Freeness Problem

Let G be a finitely presented group with decidable word problem. Given a family of elements $g_i, 1 \leq i \leq n$, the subgroup $< g_i >$ is the set of elements w than can be written as words on the $g_i^{\pm 1}$, i.e. : $w = g_{i_1}^{\varepsilon_1}, ..., g_{i_k}^{\varepsilon_k}$. Such a word is called reduced on the generators g_i if it does not contain sub-words $g_i g_i^{-1}$ or $g_i^{-1} g_i$.
The freeness problem is to decide, given the g_i, if there exist a reduced word w on the g_i such that $w = 1$ in G.

Another way to see this problem is in term of morphism from a free group to G. If $X = \{x_1, ...x_n\}$ is the set of generators of the free group $F(X)$, and $f : F(X) \to G$ is the only group morphism such that $f(x_i) = g_i$, then $\{g_i\}$ is free if an only if f is injective.
If this problem is decidable in a group G, then it is decidable in any subgroup H of G as long as we can compute an embedding. And it is always possible: given finite presentations of both groups $H \subset G$, we can enumerate all the possible writing of the generators of H in terms of the generators of G until we find one were the relation of H are indeed equal to 1 in G (we only need here the semi-decidability of the word problem in G).
Another easy result is that the decidability of the freeness problem in two groups G and H implies its decidability in the direct product $G \times H$ thanks to the following lemma.

Lemma II.4 : Intersection of normal subgroup

If A and B are normal subgroups of a free group F such that $A \cap B = \{1\}$, then $A = 1$ or $B = 1$.

Proof

Lets assume both $A \neq 1$, $B \neq 1$ and $A \cap B = \{1\}$. Let $a \in A$ and $b \in B$ be non trivial elements. Then $[a, b] = aba^{-1}b^{-1} \in A \cap B = \{1\}$ so a and b commute. But in a free group two elements commute if and only if they are powers of the same element, so there exists $c \in F$ and $p, q \in \mathbb{Z}$ such that $a = c^p$ and $b = c^q$. Then $1 \neq c^{pq} = a^q = b^p \in A \cap B$ which is a contradiction. □

To use this result, notice that a morphism f from $F(X)$ to $G \times H$ consists on two morphisms f_1, f_2 from $F(X)$ to G and H respectively, and that ker(f) =ker(f_1)∩ker(f_2), so a family is free in the direct product if and only if it is free after projection on one of the factor.
Less obvious and more interesting, the decidability of the freeness problem is stable by finite index extension. This is a consequence of the Redemeister Schreier process that implies in particular that a finite index normal subgroup of a finitely generated free group is finitely generated. If the freeness problem is decidable in a subgroup H of finite index in G, then $N = \bigcap_{g \in G} gHg^{-1}$ is normal and of finite index in G and has freeness problem decidable. We can then assume $H = N$ is normal in G. In the following commutative diagram, a freeness problem instance in G is equivalent to the injectivity of some f, which is equivalent to the injectivity of the restriction $\tilde{f}$ to ker$(\pi \circ f)$, which is equivalent to a freeness problem in N as long as the kernel of $\pi \circ f$ is finitely generated and a free basis can effectively be computed, and that is exactly what the Redemeister Schreier process gives

(see III.19 for a proof using representation graph).

$$\begin{array}{ccccc} \ker(\pi \circ f) & \hookrightarrow & F(X) & \xrightarrow{\pi\circ f} & \mathrm{Im}(f)/(N \cap \mathrm{Im}(f)) \\ \tilde{f}\downarrow & & \downarrow f & & \downarrow \\ N & \hookrightarrow & G & \underset{\pi}{\twoheadrightarrow} & G/N \end{array}$$

The goal of the following is to show the result if found during my research, that if the freeness problem is decidable in two group G and H, it is also decidable in the free product $G*H$. However, we will need an additional assumption on the groups G and H for this result to hold, that is the free membership problem to be decidable in G and H. The free membership problem naturally appears when trying to solve the freeness problem in the free product, and because of the following proposition, we can't get rid of this additional assumption.

Proposition II.5

Let G be a finitely presented group with freeness problem and word problem decidable.
Assume that for all finitely presented group H with freeness problem and word problem decidable, the freeness problem is decidable in $G * H$
Then G has free membership problem decidable.

Proof

Let $H =< h|h^2 >= \mathbb{Z}/2\mathbb{Z}$. H is finite so has both freeness problem and word problem decidable.
Let $g, \{g_1, ...g_n\}$ be an instance of the free membership problem in G.
Let $w_0 = hg$, and $w_i = g_i$ for $1 \leq i \leq n$ be elements of $G * H$
Then we claim that $\{w_0, ...w_n\}$ is free if and only if $g \in < g_i >$.
If $g \in < g_i >$, then there there is a reduced word on the g_i that is equal to g: $g = g_{i_1}^{\varepsilon_1}...g_{i_k}^{\varepsilon_k}$. Then $(w_{i_1}...w_{i_k}w_0^{-1})^2 = (g(hg)^{-1})^2 = (h^{-1})^2 = 1$ is a non trivial reduced relation on the w_i, so they are not free.
If $\{w_0, ...w_n\}$ is not free, there is a reduced relation $w = w_{i_1}^{\varepsilon_1}...w_{i_k}^{\varepsilon_k}$. such that $w = 1$
w_0 appears necessarily because $\{g_i\}$ is free. Moreover, there must be a non-empty sub-word of w that is in G or in H, and that is equal to 1.
It cannot be in h, because it means that the factor $w_0 w_0^{-1}$ appears in w. Then, it is in G, and it is either of the form u, gug^{-1}, gu or ug^{-1}, where u is a reduced word on the g_i.
It cannot be of the first to form, because it would mean that $u = 1$ which is impossible because $\{g_i\}$ id free. Thus, is either of the form gu or ug^{-1} and in both cases, we conclude that $g = u \in < g_i >$ or $g = u^{-1} \in < g_i >$. $\square$

We can now dive into the main object studied in this report, graph representations of subgroups.

III Graph representation of subgroup

1 Labelled graph and graph representation

We start by describing our formalism to describe graphs that we will use to encode subgroups. The ideas developed here are coming from algebraic topology, eliminating the "continuous" and focusing on the combinatorial part. We define here only 1-complexes, but we could add 2-cells to encode non-trivial relation and thus constructing topological spaces whose fundamental group are exactly the group they encode (see for example [LS01]). In the following, G is a group.

Definition III.1 : Labelled graph

A labelled graph Γ is given by a graph C, and a labelling μ, where $C = (V, E)$ with V a finite set, which elements are **vertices**, and a finite set E of **directed edges**, with functions $o, t : E \to V$ which give respectively the **origin** and **termination** of an edge. $o(e)$ and $t(e)$ are the **endpoints** of the edge e, and e is said to be incident to $o(e)$ and to $t(e)$. If $o(e) = t(e)$, then e is called a **loop edge**. We extend these functions to $E^{\pm 1} = E \sqcup E^{-1}$ by $\forall e \in E, o(e^{-1}) = t(e)$ and $t(e^{-1}) = o(e)$. Finally, a **labelling** of C is a map μ from E to G. We extend μ to E^{-1} by $\mu(e^{-1}) = \mu(e)^{-1}$.

Analogous to continuous map from $[0, 1]$ to a topological space and loop that constitute the fundamental group, path in the graph and cycle will encode element of a group in the graph.

Definition III.2 : Path

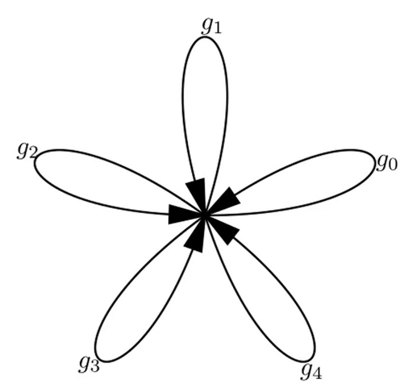
A **path** p in Γ is either a vertex $v \in V$ (it is then called trivial), either an ordered sequence of edges $e_1, ..., e_k \in E^{\pm 1}$ such that for all $1 \leq i < k, t(e_i) = o(e_{i+1})$. We will denote the set of path by $\mathcal{P}$. A path is **reduced** if it does not contain subpath ee^{-1}.
We extend o and t to paths by $o(p) = v$ if $p = v$ is trivial, and $o(p) = o(e_1)$ if $p = e_1...e_k$, and similarly for t. We will denote the set of path from x to y: $\mathcal{P}_{x \to y} = \{p \in \mathcal{P} | o(p) = x, t(p) = y\}$
We also define the **inverse** of a path, by $p^{-1} = v = p$ if p is trivial, or $p^{-1} = e_k^{-1}...e_1^{-1}$.
A path is called a **cycle** with base v if $o(p) = t(p) = v$, or if it is trivial $p = v$.
Paths p and q can be **concatenated** into pq in an obvious way if the endpoints are compatible $t(p) = o(q)$.
We extend μ to the set of path p by $\mu(p) = 1$ if p is trivial, and $\mu(p) = \mu(e_1)...\mu(e_k)$ if $p = e_1...e_k$.
We can see that μ behave with path inversion and concatenation as a group morphism.
Γ (or C) is **connected** if $\forall x, y \in V$, there is a path from x to y, i.e. $\mathcal{P}_{x \to y} \neq \emptyset$.

A path can be modified by adding subpath ee^{-1} without changing its label : this is the analog to homotopy between paths in a topological space. However, here, we can define a reduced path which is kind of a minimal member of a homotopy class.
The fundamental group of a topological space with a fixed base point corresponds to the following.

Definition III.3 : Subgroup represented by a graph

Let Γ be a labelled connected graph on a group G, and $v \in V$ a vertex.
We denote by $\mathcal{C}((\Gamma, v))$ the set of cycles with base v: $\mathcal{C}(\Gamma, v) = \mathcal{P}_{v \to v}$. It is closed under concatenation and inversion. Thus, $K = K(\Gamma, v) := \mu(\mathcal{C}(\Gamma, v))$ is a subgroup of G, and we say that (Γ, v) **represent** the group K

The rose, or bouquet of circles whose fundamental group is a free group can here encode any finitely generated group thanks to the additional data carried by the edges. As explained before, 2-cells corresponding to the relation of a finite presentations could be attached to the following example to build a topological space whose fundamental group is exactly the encoded group.



Example 1. If $(g_i)_{1 \leq i \leq n}$ are elements of G, then the graph with one vertex v, and n loops, each labelled with one of the g_i, is called the trivial representation of $< g_i >$ (associated to generators

g_i).

In the path-connected case, changing the base point to compute a fundamental group does not change the result. We investigate the effect in our combinatorial analog.

Proposition III.4 : Conjugates subgroup

Let Γ be a labelled connected graph on a group G, and p a path in G, and let $u = o(p), v = t(p)$, and $g = \mu(p)$.
Then $K(\Gamma, u) = \mu(p)K(\Gamma, v)\mu(p)^{-1}$

Proof

Let $h \in K(\Gamma, u)$. There exists a cycle q in Γ with base u such that $\mu(q) = h$. Then $p^{-1}qp$ is a cycle in Γ with base v, so $\mu(p)^{-1}h\mu(p) \in K(\Gamma, v)$, so $h \in \mu(p)K(\Gamma, v)\mu(p)^{-1}$, and thus $K(\Gamma, u) \subset \mu(p)K(\Gamma, v)\mu(p)^{-1}$. The other inclusion holds by symmetry because p^{-1} is a path from v to u. □

In terms of topological space, a tree is homotopical to a point. Thus, it can't encode any non-trivial element in our case, but it has some really interesting properties.

Proposition III.5 : Tree

If Γ is a labelled **tree**, i.e. it is connected with no reduced non-trivial cycle, then for all paths p, $\mu(p)$ only depends on $o(p)$ and $t(p)$
In particular, $K(\Gamma, v)$ is trivial for all $v \in V$.

Proof

If p_1, p_2 be paths with $o(p_1) = o(p_2)$ and $t(p_1) = t(p_2)$. Then $p = p_1p_2^{-1}$ is a cycle, and we only need to show that all cycles have label 1. By induction on the size of the cycle: If p has size 0, it is trivial so has label 1. If p has size n, then it is not trivial, thus not reduced by assumption on Γ, and it can be written $p = qee^{-1}r$. Then, by induction hypothesis, $\mu(qr) = 1$, and then $\mu(p) = \mu(q)\mu(e)\mu(e^{-1})\mu(r) = \mu(q)\mu(r) = 1$. □

2 Free and folded representation

In the following, we work, unless stated otherwise, in a graph representation (Γ, v) with label in G, with represented subgroup K, and notation as above. We define the notion of freeness for a graph representation which will coincide with the freeness of the generated group.

Definition III.6 : Free representation

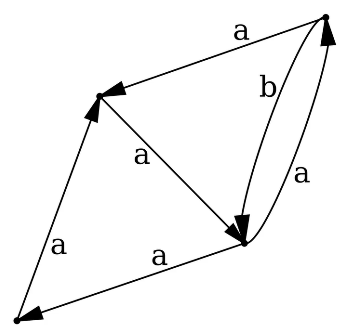
(Γ, v) is called a **free** representation of K if the only reduced cycle of $\mathcal{C}(\Gamma, v)$ that μ maps to 1 is the trivial path v.

A stronger property than free is being folded.

Definition III.7 : Folded graph

Γ is called **folded** if all reduced non-trivial path p has label $\mu(p) \neq 1$

If Γ is folded, then (Γ, v) is a free representation.



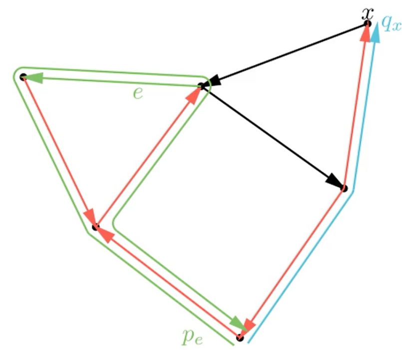
Example 2. A non-free representation.

A useful characterization of freeness uses the following result that uses trees to "decode" the graph and finds generators for the encoded group.

Definition - Theorem III.8 : Generators induced by a tree

Let T be a spanning tree of a representation (Γ, v), i.e. a sub-graph which is a tree, and has all the vertices of Γ. For each vertex $x \in V$ there exists a unique reduced path q_x from v to x in T.
For each $e \in E(\Gamma)\backslash E(T)$, let p_e defined by $q_{o(e)}eq_{t(e)}^{-1}$. It is a cycle with base v, and it is well known that a spanning tree has $|V|-1$ edges, so p_e are a set of $|E|-|V|+1$ cycles with base v.Then $\{\mu(p_e)\}$ generates $K(\Gamma, v)$, and the p_e are called the generator paths induced by the tree T.

Proof
Let $h \in K(\Gamma, v)$. There exists a cycle p with base v such that $\mu(p) = h$. Decompose $p = t_0e_1t_1...e_kt_k$ where $e_i \notin E(T)$ and t_i are paths in T. Because of proposition III.5, $\mu(t_0) = \mu(q_{o(e_1)})$, for $1 \leq i < k, \mu(t_i) = \mu(q_{t(e_i)}^{-1}q_{o(e_{i+1})})$, and $\mu(t_k) = \mu(q_{t(e_k)}^{-1})$ because they are edges in a tree with same endpoints. Thus, $\mu(p) = \mu(q_{o(e_1)})\mu(e_1)\mu(q_{t(e_1)}^{-1})...\mu(q_{t(e_k)}^{-1}) = \mu(p_{e_1})...\mu(p_{e_k})$ is generated by the $\mu(p_e)$. □



Example 3. Generator paths induced by a tree.

The very important characterization is the following.

Proposition III.9

Let $\{p_e\}$ be the set of generator path induced by a spanning tree T in the representation (Γ, v). Then $\{\mu(p_e)\}$ is free if and only if (Γ, v) is free.

Proof
Assume (Γ, v) is free. Let $g_e = \mu(p_e)$ for all $e \in E(\Gamma)\backslash E(T)$. Let $w = g_{e_1}^{\varepsilon_1}...g_{e_k}^{\varepsilon_k}$ be a reduced word on the g_e such that $w = 1$.
Then $p = p_{e_1}^{\varepsilon_1}...p_{e_k}^{\varepsilon_k}$ is a cycle of Γ with base v with label 1. Write $p = t_0e_1^{\varepsilon_1}t_1...e_k^{\varepsilon_k}t_k$ with t_i paths in T, and for each $0 \leq i \leq k$, let t'_i be the unique reduced path from $o(t_i)$ to $t(t'_i)$ in T. And let $p = t'_0e_1^{\varepsilon_1}t'_1...e_k^{\varepsilon_k}t'_k$. By the proposition III.5, p' is a cycle with base v and label 1. Moreover, if p' has a sub-path ee^{-1}, it cannot be a sub-path of t'_i because they are reduced, it cannot be an edge e_i with an edge of t'_i or t'_{i-1} because edges e_i are in $E(\Gamma)\backslash E(T)$ and the edges of t'_i are in $E(T)$. Then, it is necessarily of the form $e_i^{\varepsilon_i}e_{i+1}^{\varepsilon_{i+1}}$, with $t'_i = 1$, thus there is an i such that $e_i = e_{i+1}$ and $\varepsilon_i = -\varepsilon_{i+1}$, which contradict the fact that w is reduced on the g_e.
Thus, p' has no such factor so it is reduced, and then it is trivial because (Γ, v) is free, and so w is trivial and so $\{g_e\}$ is free.
Assume now $\{g_e\}$ is free. Let p be a reduced cycle with label 1 in Γ with base v.
Again, write $p = t_0e_1^{\varepsilon_1}t_1...e_k^{\varepsilon_k}t_k$ where $e_i \notin E(T)$ and t_i are paths in T.
With the previous notation, $\mu(t_0) = \mu(q_{o(e_1)})$, for $1 \leq i < k, \mu(t_i) = \mu(q_{t(e_i)}^{-1}q_{o(e_{i+1})})$, and $\mu(t_k) = \mu(q_{t(e_k)}^{-1})$ because they are edges in a tree with same endpoints.
Thus, $1 = \mu(p) = \mu(q_{o(e_1)})\mu(e_1)\mu(q_{t(e_1)}^{-1})...\mu(q_{t(e_k)}^{-1}) = g_{e_1}^{\varepsilon_1}...g_{e_k}^{\varepsilon_k}$.
This is a relation on the free generator g_e, so it can be reduced unless it is trivial.

If it can be reduced, then there is an i such that $e_i = e_{i+1}$ and $\varepsilon_i = -\varepsilon_{i+1}$.
Thus t_i is a cycle in T, and it is reduced, so it is trivial p has a sub-word $e_i^{\varepsilon_i} e_i^{-\varepsilon_i}$, but this contradict the fact that p is reduced. Then the relation on the g_e is trivial, and then p is trivial. Thus, (Γ, v) is free. □

As a corollary, we get an Euler characteristic formula that gives the rank of a group encoded in a free representation. We see here that the fundamental group of the 1-complex is indeed the group encoded.

Theorem III.10

(Γ, v) is a free representation of K if and only if K is a free group of order $|E| - |V| + 1$, i.e. the size of the set of generator paths induced by a spanning tree.

Then, we can also deduce that freeness does not depend on the base point.

Proposition III.11

Let $u \in V$
Then (Γ, v) is free if and only if (Γ, u) is free.

Proof
$K(\Gamma, v)$ and $K(\Gamma, u)$ are conjugate in G according to proposition III.4, so they are isomorphic. Thus, the characterization of theorem III.10 does not depend on the base point. □

Using the trivial example 1, we also get this classic theorem on free generators of a free group:

Theorem III.12

Let $\{w_1, ..., w_n\}$ be a set of element of a group G.
Then $\{w_1, ..., w_n\}$ is free if and only if $< w_i >$ is a free group of rank n.

Proof
Let Γ_0, v_0 be the trivial representation associated to $\{w_i\}$. A spanning tree is the one vertex graph v_0, and the associated path generators are the loops e_i with respective label w_i.
Then, $\{w_1, ...w_n\}$ is free if and only if Γ_0, v_0 is free by lemma III.9, if and only if $K(\Gamma_0, v_0) =< w_i >$ is a free group of order $|E| - |V| + 1 = n$ by theorem III.10. □

3 Decision problem in graph representation

Corollary III.13

G has freeness problem decidable, if and only if it is decidable to determine if a given graph representation (Γ, v) is free.

Proof
Given a presentations, compute a generating set as in the definition III.8 above. Then, (Γ, v) is free if and only if this generating set is free, which is decidable if G has freeness problem decidable. For the converse, given a set of element, compute the trivial representation 1 associated to it, and then determine if it is free. □

The semi-decidability of the freeness problem translates to the following in terms of graph representations.

Lemma III.14

If $G =< X, R >$ is finitely presented and x, y are vertices of the graph Γ such that there exists a path from x to y with label 1, then one can compute such path.
In particular, given a graph representation that is not free, one can compute a non-trivial reduced cycle with label 1

Proof
We can enumerate the paths p from x to y in Γ (for example by increasing length) and write their label $\mu(p)$ in terms of the generators, and we can enumerate the words $w \in F(X)$ equal to 1 in G. Enumerate the pairs p, w until the label $\mu(p)$ is the word w. If we know such a path exists, the algorithm will stop eventually. □

4 Free group graph

The simplest example of a graph representation is those of subgroups of free groups with edges labelled by the generators. These are the graph that are the more studied ([KM02]), and we will start by looking at this particular case that can be used to get many of the classic results on subgroups of free groups. We will then generalize the ideas to arbitrary graph representation and use them to tackle the freeness problem in a free product.

Definition III.15 : Freely reduced decomposition

Let $F(A)$ be the free group on the set of generators A.
A non trivial element of $F(A)$ can be written as a word $w = \alpha_1\alpha_2...\alpha_n$, where $\forall 1 \leq i \leq n$, $\alpha_i \in A^{\pm 1}$. We call such a decomposition **freely reduced** if it does not contain a sub-word aa^{-1} with $a \in A^{\pm 1}$.
Such decomposition is unique. This implies that the word problem is decidable in $F(A)$.

Definition III.16 : Free group graph

Let $F(A)$ be the free group on the set of generators A.
A free group graph is a labelled graph with labels in $A^{\pm 1}$.

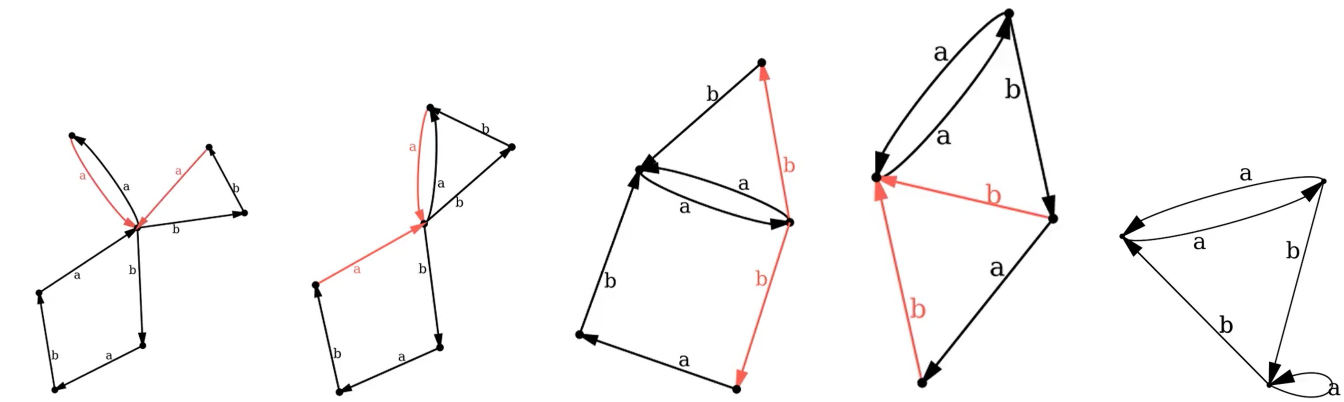
Proposition III.17 : Free group graph folding

Let Γ be a free group graph. Then Γ is folded if and only if it does not contain a pair of edges $e \neq f \in E^{\pm 1}$ with $o(e) = o(f)$ and $\mu(e) = \mu(f)$.

Proof
If Γ contain such edges e and f, then ef^{-1} is a non trivial path with label 1, then Γ is not folded.
If Γ is not folded, it contain a reduced path p with label 1. Write $p = e_1...e_n$. Then $1 = a_1...a_n$ where $a_i = \mu(e_i) \in A^{\pm 1}$, thus this word is not reduced and there is an i such that $a_i a_{i+1} = 1$, thus $o(e_{i+1}) = o(e_i^{-1})$ and $\mu(e_{i+1}) = a_{i+1} = a_i^{-1} = o(e_i)$.
□

Thus, any finite free group graph can be folded by founding such pair of edges, and merging

$t(e)$ and $t(f)$ if they are different (if they aren't then the graph is not free), and removing one of the two edges, until no such pair of edges exists. This process can effectively be executed algorithmically and does not change the freeness of the graph, neither the represented group, and this proves with proposition III.13 that the freeness problem is decidable in a free group. This process of merging two edges will be generalized in the following in order to be used not only in free group graph.



Example 4. Folding of the graph representing the group generated by $aa, bba, baba$.

Before, let's end this section with the promised proofs of two results: the decidability of the membership problem in a free group, and the Redemeister-Schreier process described above to prove that decidability of the freeness problem in a group is stable by finite index extension.

Proposition III.18 : Membership problem in folded free group graph

Let Γ, v be a free group graph representation of $K \subset F(X)$, and $w \in F(X)$. Then there is at most one path p with label w in Γ starting at v, and $w \in K$ if and only if there is such a path and it terminates at v.

Proof

If two distinct such paths exists say p and q, then r obtained by reducing pq^{-1} is not trivial but has label 1, but this is impossible since Γ is folded. The rest of the proposition follows by definition of K. $\square$

In order to solve the membership problem "$w \in < g_i >= H$?" in a free group, just compute the folded graph of $< g_i >$ and follow letter by letter the path corresponding to w as long as you can. If it reaches the end of w, check if you end up on v. In other words, Γ is a finite deterministic automaton (with v being both the initial and the only final state) and H is the recognized regular language. This point of view also shows how to find generators for the intersection of two finitely generated subgroup of a free group by computing the product automaton for the intersection (see for example section 9 in [KM02]).

Proposition III.19 : Redemeister-Schreier process

Let H be a normal subgroup of finite index m in a free group $F(X)$ with $|X| = k$.
Then H is a free group of rank $m(k-1)+1$, and a base can be computed algorithmically.

Proof

Let V be the finite set of cosets Hg for $g \in F(X)$, and let $E = V \times X$. Define $o(Hg, x) = Hg$, $t(Hg, x) = Hgx$ and, $\mu(Hg, x) = x$. To preserve these properties, inverse of edges can be defined by $(Hg, x)^{-1} = (Hgx, x^{-1})$. This defines the graph representation Γ, H and we claim it represents

H. One can recognize here the Cayley graph of G/H with generators X.
Let's show that $\mu(\mathcal{P}_{Ha,Hb}) \subset Ha^{-1}b$ for all $a, b \in F(X)$. We do it by induction on the length of the path p from Ha to Hb. If p is trivial, then $Hb = Ha$ and $ba^{-1} \in H$ so $\mu(p) = 1 \in H = ba^{-1}H$. If $p = qe$, where $e = (Hc, x)$, then $H = t(p) = t(e) = Hcx$ by definition of the graph, so $cxb^{-1} \in H$, and $\mu(p) = \mu(q)x$, but by induction hypothesis, $\mu(q) \in Ha^{-1}c$, so $\mu(p) \in Ha^{-1}cx = Ha^{-1}Hb = Ha^{-1}b$ because H is normal in $F(X)$
For the inverse inclusion, if $g = ha^{-1}b$ is such that $h \in H$, write g as a word on the element of $X^{\pm 1}$: $g = x_1^{\varepsilon_1}...x_k^{\varepsilon_k}$, and let $p = (Ha, x_1^{\varepsilon_1})(Hax_1^{\varepsilon_1}, x_2^{\varepsilon_2})...(Hax_1^{\varepsilon_1}...x_{k-1}^{\varepsilon_{k-1}}, x_k^{\varepsilon_k})$. Then p is a path from Ha to $Hag = Hb$ and $\mu(p) = g$.
Moreover, the representation is folded. Indeed, if $e, f \in E$ with same label and same origin, then $e = (Hg, x), f = (Hg, y)$, and $x = y$ so $e = f$, and if $e, f \in E$ with same label and same termination, then $e = (Hg, x), f = (Hh, x)$, and $Hgx = Hhx$ so $Hg = Hh$ so $e = f$.
Thus, H is a free group of rank $|E| - |V| + 1 = mk - m + 1 = m(k-1) + 1$. A base can be effectively computed with a spanning tree and the induced path generators. □

IV Graph representations transformations

1 Morphism and folding

Definition IV.1 : Morphism and folding

Let (Γ', v') be a graph representation (whose sets and function will be denoted with a prime), and let $\pi_V : V \to V', \pi_E : E \to \mathcal{P}'$ (we will only write π). We give notation for the following properties.
$(F0) : \pi(v) = v'$
$(F1) : \forall e \in E, o'(\pi(e)) = \pi(o(e)), t'(\pi(e)) = \pi(t(e))$, and $\mu'(\pi(e)) = \mu(e)$
$(F2) : \forall e' \in E'$, there exists $e \in E$ such that $\pi(e) = e'$
$(F3) : \forall x, y \in V$, if $\pi(x) = \pi(y)$, then there exists a path p from x to y with trivial label, i.e. $o(p) = x, t(p) = y, \mu(p) = 1$
If π satisfies $(F0-1)$, we say that π is a **morphism**.
If π satisfies $(F0-3)$, we say that π (and (Γ', v')) is a **folding** of (Γ, v)

In the case of topological spaces, one can find a correspondence between subgroup of the fundamental group and covering spaces (see for example [Mas89]). We investigate here how encoded groups behave with our definition above.

Lemma IV.2

If π is a morphism from (Γ, v) to (Γ', v') then for all vertices $x, y \in V, \mu(\mathcal{P}_{x\to y}) \subset \mu'(\mathcal{P}'_{\pi(x)\to\pi(y)})$.
In particular, if $K' := K(\Gamma', v')$, then $K \subset K'$

Proof
Let's first notice that π can be extended to paths: $\pi(p) = \pi(u)$ if $p = u$ is trivial, and $\pi(e_1...e_k) = \pi(e_1)...\pi(e_k)$. It is a path because $\forall 1 \le i < n, t'(\pi(e_i)) = \pi(t(e_i)) = \pi(o(e_{i+1})) = o'(\pi(e_{i+1}))$
With this extension, (1) also holds for paths. Thus, if $h \in \mu(\mathcal{P}_{x\to y})$, there exist a path p such that $o(p) = x, t(p) = y$, and $\mu(p) = h$. Define $p' = \pi(p)$, we then have $o'(p') = \pi(x), t'(p') = \pi(y)$ and $h = \mu(p) = \mu'(p')$. □

Lemma IV.3

> If π is a folding from (Γ, v) to (Γ', v') then for all vertices $x, y \in V, \mu(\mathcal{P}_{x\to y}) = \mu'(\mathcal{P}'_{\pi(x)\to\pi(y)})$.
> In particular, if $K' := K(\Gamma', v')$, then $K = K'$

Proof

We need to show the inverse inclusion $\mu'(\mathcal{P}'_{\pi(x)\to\pi(y)}) \subset \mu(\mathcal{P}_{x\to y})$.
Let $h \in \mu'(\mathcal{P}'_{\pi(x)\to\pi(y)})$, there exist a path p' such that $o'(p') = \pi(x), t'(p') = \pi(y)$ and $\mu'(p') = h$. If p' is trivial, then $h = 1$ and $\pi(x) = \pi(y)$, and we conclude immediately by condition $(F3)$. Otherwise, we can write $p' = e'_1...e'_k$. For all $1 \leq i \leq n$, let e_i given by condition $(F2)$ (such that $\pi(e_i) = e'_i$).
$\forall 1 \leq i < k$, we have $\pi(t(e_i)) = t'(e'_i) = o'(e'_{i+1}) = \pi(o(e_i))$. Then, thanks to condition $(F3)$, there exists a path q_i from $t(e_i)$ to $o(e_{i+1})$ with label $\mu(q_i) = 1$. We also have $\pi(o(e_1)) = o'(e'_1) = \pi(x)$, and $\pi(t(e_k)) = t'(e'_k) = \pi(y)$, thus there exists q_0 a path from x to $o(e_1)$, and q_k from $t(e_k)$ to y both with label 1 Let p be the path obtained by the inserting q_i between e_i and e_{i+1} : $p = q_0e_1q_1e_2...e_{k-1}q_{k-1}e_kq_k$. Then $p \in \mathcal{P}_{x\to y}$, and $\mu(p) = \mu(q_0)\mu(e_1)...\mu(e_k)\mu(q_k) = \mu(e_1)...\mu(e_k) = \mu'(\pi(e_1))...\mu'(\pi(e_k)) = \mu'(p') = h$. □

Remark :

Given π, if $(F2)$ holds, there is a unique way of defining o', t' and μ' such that $(F1)$ might holds: for $e' \in E$, $(F2)$ gives $e \in e'$ such that $\pi(e) = e'$. Then we have to set $o'(e') = \pi(o(e)), t'(e') = \pi(t(e))$ and $\mu'(e') = \mu(e)$. Thus, we don't need to explicitly give o', t' and μ'.

In the following, we will sometimes omit the prime for the functions o, t and μ when there is no ambiguity as to which graph Γ' the edge $e' \in E'$ it applies to belongs.

2 Folding transformations

Remark :

A folding of a folding of (Γ, v) is a folding of (Γ, v), the projection is given by the composition of the projections. The goal here is to generalize the process of folding two edges in a free group graph. This done by splitting the folding process into two steps : merging the vertex, then removing an edge. However, some details need to be considered precisely.

Lemma IV.4 : Vertex merging

> If x, y are two vertices of (Γ, v) linked by a path p with label 1, we define the graph (Γ', v') obtained by merging x and y into a new vertex z by the following: $E' = E$ with π_E the identity, $V' = (V\setminus\{x, y\}) \sqcup \{z\}$, $\pi(s) = s$ if $s \notin \{x, y\}$ and $\pi(x) = \pi(y) = z$, and o' and t' are determined according to the previous remark.
> Then, $\Gamma', \pi(v)$ is a folding of (Γ, v)

Proof

$(F0)$ is in the definition.
$(F2)$ is immediate because π_E is a bijection between E and E'
$(F1)$ is also immediate for the same reason with the right definition of o' and t' given by the remark.
$(F3)$ is immediate by construction. □

Merging the the vertices without touching to the edges creates in some sort a relation, a cycle with label 1. The idea is then to see this cycle as boundary of a surface, then contract one of its edges on the others. However, this can be done only if the edge appear only one time in the cycle.

Definition IV.5 : Unique edge in a path

Let $p = e_1...e_k$ be a non-trivial path in Γ.
Let $1 \leq i \leq n$. We say that e_i is unique in p if for all $j \neq i$, $e_i \neq e_j^{\pm 1}$.
We say that p has a **unique edge** if such an i exists.

Lemma IV.6 : Unique edge deletion

Let $p = e_1...e_k$ is a cycle such that $\mu(p) = 1$. Assume e_i is unique in p.
We define Γ' by setting $V' = V, \pi_V$ the identity on V, $E' = E \backslash \{e_i\}$, and $\pi_E(e) = e$ if $e \neq e_i$, and $\pi_E(e_i) = e_{i-1}^{-1}...e_1^{-1}e_k^{-1}...e_{i+1}^{-1}$. Finally, set $v' = v$
Then Γ', v' is a folding of Γ, v

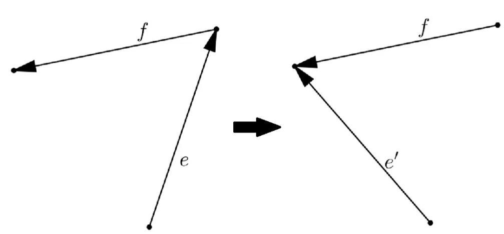
Proof
$(F0)$ is obvious.
$(F1)$ holds immediately for $e \neq e_i$, and $o'(\pi(e_i)) = o'(e_{i-1}^{-1}) = \pi(o(e_{i-1}^{-1}) = \pi(t(e_{i-1})) = \pi(o(e_i))$ (where e_{i-1} denotes e_k if $i = 1$), and similarly $t'(\pi(e_i)) = \pi(t(e_i))$.
$(F2)$ and $(F3)$ are immediate. □

Remark :
The fact that e_i is unique in p allows us to take the path $p' = e_{i-1}^{-1}...e_1^{-1}e_k^{-1}...e_{i+1}^{-1}$ in Γ'. Indeed, if e_i had appear more than once in p, p' wouldn't be a path of edges in E'

Lemma IV.7 : Short-cut transformation

Let ef be a 2-length path in Γ, i.e. $t(e) = o(f)$, with $e \neq f^{\pm 1}$.
We define Γ', the graph where e takes the short-cut ef, by the following:
We set $V' = V, v' = v, E' = E(\backslash\{e\}) \sqcup \{e'\}$.
For $a \neq e'$, we set $o'(a) = o(a), t'(a) = t(a), \mu'(a) = \mu(a)$.
Finally, we set $o'(e') = o(e), t'(e') = t(f), \mu'(e') = \mu(ef) = \mu(e)\mu(f)$.
We will denote the previous transformation as the "short-cut $e \to ef$.
Then, then for all vertices $x, y \in V, \mu(\mathcal{P}_{x\to y}) = \mu'(\mathcal{P}'_{\pi(x)\to\pi(y)})$ In particular, if $K' := K(\Gamma', v')$.
Then $K = K'$, and Γ' is a free representation if and only if Γ is also free.

Proof
The short-cut operation is symmetrical and mapping the edge e to $e'f^{-1}$ and the rest by identity is a morphism, so we can conclude with lemma IV.2. The quantity $|E| - |V| + 1$ is preserved, then so is freeness by theorem III.10. □

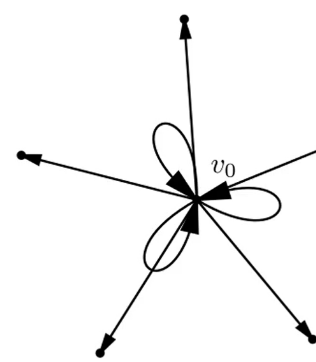


In order to get a folded graph, we need to eliminate the non-trivial paths with label 1. To do this, we want to use unique edge deletion after merging the endpoints of the paths. We thus need to have a unique edge in the path p. We use the following lemma.

Lemma IV.8

There exists (and one can compute) a sequence of short-cut transformation that transforms Γ into Γ', and such that all non-cyclic reduced paths in Γ' have a unique edge.

Proof
Choose an total ordering of the vertices. For all pairs of edges e, f such that $t(e) = o(f)$, with $e \neq f^{\pm 1}$, we say that the short-cut transformation $e \to ef$ is strictly decreasing if $t(f) < o(f)$.
When doing a strictly decreasing short-cut transformation exactly one endpoint strictly decrease in V. Thus, there can not be a infinite sequence of strictly decreasing short-cut transformation.
Then, by a finite sequence of strictly decreasing short-cut transformation, we can obtain a graph Γ' in which all possible short-cut transformation are not strictly decreasing.
In the resulting graph, let's show that all the vertices distinct from the vertex v_0 minimal for the order, have exactly one edge with other endpoint v_0
Let $u \neq v_0$ be an other vertex. Since Γ' is still connected, there is a path p from u to v_0 in Γ'. and we can assume it has minimal length. For all sub-path ef of p, we have $t(f) \geq o(f)$ otherwise their would be a possible strictly decreasing short-cut transformation with the path ef. Moreover, we have $t(e) \leq o(e)$ otherwise their would be a possible strictly decreasing short-cut transformation with the path $f^{-1}e^{-1}$. Thus, if we write $p = e_1 ... e_k$, all the interior edges e_i for $1 < i < k$ are loops, which is impossible because p has minimal length, thus p has length less than 2. If $p = ef$, since f is not a loop, and $t(f) = v_0 < o(f)$ which is impossible. Thus $p = e$ is an edge from u to v_0. If e' is another edge with $t(e') = u$, then $e'e$ is a possible path for a strictly decreasing short-cut, thus e is the only edge with incident to u.Now, because all vertices except v_0 have exactly one incident vertex, if p is a non-cyclic reduced path in Γ', all its edges except for the first and the last are loops based on v_0, and because it is non cyclic, at least its first edge or its last edge is not a loop. If both aren't, they can't be inverse from on another because it would make p cyclic, and they are thus unique, if only one isn't, it is obviously unique.



□

With the previous lemmas, we contract the transformation process that we intend to do in the following:

Lemma IV.9 : Full folding step

Let p be a non cyclic reduced path in Γ with label $\mu(p) = 1$.
The sub-graph generated by p is the sub-graph of Γ where we keep only the edges that appear in p.
Then one can execute a sequence of short-cut transformation that only modifies the sub-graph generated by p, then merge $o(p)$ and $t(p)$, and finally perform a unique edge deletion.
We call this sequence of transformation a full folding step, and the resulting graph representation is free if and only if Γ is free.

Proof
First, use the previous lemma on the sub-graph $\Delta \subset \Gamma$ generated by p to get Δ' and execute the sequence of short-cut on the whole graph Γ to get Γ', i.e., Γ where the sub-graph Δ is replaced by Δ'. Then, by the lemma IV.7, there is still a path p' from $o(p)$ to $t(p)$ in Δ' with label 1, and we can chose it to be reduced. Moreover, it has a unique edge because it is non cyclic and lies in Δ'.
Then, merge $o(p)$ and $t(p)$, to get Γ''. The path p' becomes a cycle p'' labelled by 1 that still has a unique edge. Thus, one can perform the unique edge deletion.
As previously, the quantity $|E| - |V| + 1$ and the group generated has not changed, so by theorem

III.10, the resulting graph representation is free if and only if Γ is free. □

V Freeness problem in free product of groups

1 Free product graph

In this section, $(G_a)_{a\in A}$ is a family of finitely presented group. The goal of this section is to show that if the freeness problem, and the membership free problem are both decidable in all G_a, then those two problems are decidable in the free product $\mathop{\ast}\limits_{a\in A} G_a$. Indeed, it is enough to show that for a free product $G * H$ of two free factor.

We first define an analogous notion of freely reduced decomposition as in definition III.15

Definition V.1 : Freely reduced decomposition for free product

A non trivial element of $\mathop{\ast}\limits_{a\in A} G_a$ can be written as a product $w = \alpha_1\alpha_2...\alpha_n$, where $\forall 1 \leq i \leq n$, $\alpha_i \neq 1$, and $\forall 1 \leq i < k$, we have $\alpha_i \in G_a$ and $\alpha_{i+1} \in G_b$ with $a \neq b$. We call such a decomposition **freely reduced**.

It may not be unique as a word on the generators of the G_a, but if $\beta_1...\beta_m = w$ is another freely reduced decomposition, then $n = m$ and $\beta_i = \alpha_i$ for all $1 \leq i \leq n$. And if the word problem is decidable in all G_a, we can decide if a decomposition is freely reduced, and if two freely reduced decomposition are given, we can decide if they represent the same element of $\mathop{\ast}\limits_{a\in A} G_a$. (i.e. the word problem is decidable in the free product).

Definition V.2 : Free product graph

A labelled graph Γ with labels in $\mathop{\ast}\limits_{a\in A} G_a$ is called a free product graph (with respect to the free factors G_a) if for all $e \in E$, there is an a such that $\mu(e) \in G_a$.

We can define E_{G_a} the set of edges $e \in E$ such that $\mu(e) \in G_a$, called G_a-edges. The only edges that lies in multiple G_a are the edges with label 1

We also define $\mathcal{P}_{G_a}$ the set of paths with all edges in E_{G_a}, we will call these G_a-paths.

For $x \in V$, we denote by $\Delta_{G_a}(x)$ the sub-graph of Γ defined as the connected component of x in the graph induced by the G_a-edges.

In the following, we consider a free product with two factors $G * H$

Example 5. Let $w_1, ..., w_n$ be elements of $G * H$.

Let v be a first vertex called the origin, and for each $1 \leq i \leq n$, write $\alpha_i^1...\alpha_i^{k_i}$ the freely reduced decomposition of w_i, and add a cycle of k_i edges starting from v with labels α_i^j.

Thus, the resulting graph is a bouquet of n cycles, attached on the vertex v, each one labelled by the freely reduced decomposition of one of the w_i.

The represented subgroup is $K =< w_i >$

We will denote this graph Γ_0, it is indeed a free product graph.

Because of theorem III.10, and because in $\Gamma_0 : |E| - |V| + 1 = n$, $\{w_i\}$ is free if and only if the representation Γ_0 is free.

The goal is now to transform the graph with full folding steps (which does not change freeness) in order to obtain either a folded graph, either find a cycle of label 1.

Remark :
In order to work with free product graph, it is important to notice that a full folding stepped performed on a path p whose edges are all in G (or all in H) preserves the propriety of being a free product graph. In the following, Γ is an arbitrary free product graph on $G * H$.
The following result is probably the fundamental statement that makes the free product preserve the decidability of the freeness and the free membership problems.

Lemma V.3

> If Γ is not folded, there exist a non-trivial reduced path that is a G-path or an H-path.

Proof
If Γ has an edge labelled 1, the lemma is obvious. Let's suppose it is not the case
Γ is not folded, so there exist a non-trivial reduced path p with $\mu(p) = 1$ Write $p = e_1...e_k$. Group the consecutive edges whose labels lies in the same free factor: $p = p_1...p_r$, with $p_i \in \mathcal{P}_G$ for i even, and $p_i \in \mathcal{P}_H$ for i odd, or the contrary. Now, notice that $1 = \mu(p) = \mu(p_1)\mu(p_2)...\mu(p_r)$ and each consecutive $\mu(p_i)$ are in different free factor. However, this can't be a freely reduced decomposition of 1, so there is necessarily a term $\mu(p_i)$ that is equal to 1. Thus, the corresponding path p_i is a non-trivial reduced path whose edges have labels all in the same free factor □

2 Decision problems in the free product

Lemma V.4

> If G has freeness problem decidable, then it is decidable, given a free product graph Γ and a vertex $x \in V$ to determine if there exist a non-trivial reduced cycle p from x to x with label 1 and edges in E_G.
> If the answer is no, we will say that x is G-free.

Proof
The word problem being decidable in both groups, we can determine given an edge if it lies in E_G.
Thus, we can compute the sub-graph $\Delta := \Delta_G(x)$
The non-trivial reduced G-cycles from x to x in Γ are exactly the non-trivial reduced cycles in Δ.
Thus, the problem is equivalent to decide if Δ is a free representation.
Since Δ is a representation with label in the graph G in which the freeness problem is decidable, then the freeness of Δ is decidable by corollary III.13 □

Lemma V.5

> If G has free membership problem decidable, then it is decidable, given a free product graph Γ, an element $g \in G$ and two vertices $x \neq y \in V$ such that x is G-free to determine if there exist a path p from x to y with label g and edges in E_G. (We will in particular us this result with $g = 1$)

Proof
As above, compute the graph Δ, the connected component of x in the sub-graph induced by G-edges. First, test if $y \in V(\Delta)$. If it's not, then there are no G-paths from x to y in Γ so the answer is no. Assume now that $y \in V(\Delta)$. Then we can find a path p_0 from x to y in Δ. Moreover, as in the previous lemma V.4, Δ, x is a free representation because x is assumed G-free. Thus, one can find

a set generator paths $\{p_i\}$ such that $\{\mu(p_i)\}$ is free and generates $K(\Delta, x)$ by lemma III.9. Let's show that the existence of a G-path from x to y in Γ label g is equivalent to $\mu(p_0)g^{-1} \in K(\Delta, x)$. First, the existence of a G-path from x to y with label g in Γ is equivalent to the existence of a paths from x to y with label g in Δ. If such a path exists, denoted p, then p_0p^{-1} is a cycle with base x and label $\mu(p_0)g^{-1}$, so $\mu(p_0)g^{-1} \in K(\Delta, x)$. If $\mu(p_0)g^{-1} \in K(\Delta, x)$, there exist a cycle p_1 in $\mathcal{C}(\Gamma, x)$ such that $\mu(p_1) = \mu(p_0)g^{-1}$, so $p = p_1^{-1}p_0$ is a path from x to y with label g. Thus, because the free membership problem is decidable, it is decidable whether $\mu(p_0)g^{-1} \in <\mu(p_i)>= K(\Delta, x)$, and so the existence of a path of label g from x to y in Γ is decidable. □

Corollary V.6

If G and H have both freeness problem, and free membership problem decidable, then there is an algorithm that decides, given a free product graph Γ if it is folded, and if it's not, finds a non trivial reduced G-path or H-path with label 1.

Proof

First, for each vertex $x \in V$, use the previous lemma to check if x is G-free and if x is H-free.
If it's not, let x be a vertex that is not G-free (or not H-free), and compute $\Delta := \Delta_G(x)$ (resp. $\Delta_H(x)$). Then Δ, x is not a free representation, and because the word problem is decidable in G (resp. in H), one can compute a non-trivial reduced cycle p with label 1 and base x in Δ, but then it is a G-path (resp. a H-path) in Γ. Assume now that all $x \in V$ are G-free and H-free. For all pairs of distinct vertices $x \neq y \in V$, check if there is a G-path (or an H-path) from x to y with label 1. This can be achieved according to lemma V.5 because G (and H) have free membership problem decidable. If such a path exists, it can be computed because word problem is decidable in G (in H), and it can be reduced. Assume now that for all pairs of distinct vertices $x \neq y \in V$, there is no G-path (and no H-path) from x to y with label 1.
Then conclude that Γ is folded. Indeed, if it was not, there would be a non-trivial reduced G-path or H-path with label 1 according to lemma V.3. □

Theorem V.7

Assume G and H have both freeness problem, and free membership problem decidable. Then, given Γ a free product graph and $v \in V$ then there is an algorithm that either transform Γ into a folded graph by a sequence of full folding process, or either shows that Γ is not free.
In particular, it is decidable whether (Γ, v) is a free representation.

Proof

Use corollary V.6 to decide if Γ is folded.
If it's not, let p be the G-path or H-path found by the algorithm of corollary V.6.
Notice p has label 1 and lies either in G, either in H.
If p is non cyclic, execute a full folding step on the path p, and because a full folding step preserves freeness of the representation, we can restart the algorithm on the obtained graph that has strictly less vertices, this way the algorithm can't run forever.
If p is cyclic conclude that (Γ, v) is not free. Indeed, $(\Gamma, o(p))$ is not, and so is Γ, v by corollary III.11 If Γ is, folded, stop the algorithm and wa can conclude that (Γ, v) is free. □

Theorem V.8

Assume G and H have both freeness problem, and free membership problem decidable. Then the freeness problem is decidable in the free product $G * H$.

Proof

Let $\{w_1, ..., w_n\}$ be an instance of the freeness problem in $G * H$.
Let Γ, v be the representation of example 5. Because $|E| - |V| + 1 = n$, combining theorem III.10 and theorem III.12, we get that $\{w_i\}$, is free if and only if Γ, v is a free representation, which is decidable according to theorem V.7. □

Theorem V.9

Assume G and H have both freeness problem, and free membership problem decidable. Then the free membership problem is decidable in the free product $G * H$.

Proof

Let w, $\{w_1, ..., w_n\}$ be an instance of the free membership problem in $G * H$.
Let (Γ, v) be the representation of example 5. Then, as above, Γ, v is free because $\{w_i\}$ is free. Thus, the algorithm of theorem V.7 can transform (Γ, v) into (Γ', v') that represent the same group $< w_i >$ and such Γ' is folded.
Let's show now that there is an algorithm to determine given to vertex x, y in V and a word $w' \in$ if there is a path from x to y with label w'.
Write $w' = \alpha_1 ... \alpha_k$ the freely reduced decomposition of w', and work by induction on k.
If $k = 0$ then $w = 1$ and the problem has a solution if and only if $x = y$ because Γ' is folded.
If $k \geq 1$, use lemma $V.5$ to determine if there exists a path p starting from x going to any other vertex with label α_1. If there is such vertex it is necessarily unique because Γ' is folded. Call it z, then the problem is equivalent as finding a path from z to y with label $\alpha_2 ... \alpha_k$, which is can be done by induction on the word length.
Use the previous algorithm with $x = y = v'$ and $w = w'$. □

VI Conclusion

While the first goal of the internship was to prove undecidability results concerning the freeness problem, these decidability results are a good starting point to study the freeness problem in some finitely presented groups. We have worked without complete success on other groups where the word problem in known to be decidable, such as right angled Artin groups (the result in this report allows us to work with RAAGs associated to connected graphs), but also in one relator group, and semi-direct product of free by cyclic groups, in the light of a recent result that one relator group with torsion are virtually (finite index extension of) one relator group [KL23].
The undecidability result we were hoping to prove is that of the freeness problem to be undecidable in a linear group $SL_n(Z)$ with sufficiently large n. A very simple open question in this area is the Lyndon-Ullman problem, asking if two parabolic linear fractional transformation are free [LU69]. This problems contains more arithmetic and not only combinatorial aspect. In that context, we worked on the solution of the 10nth Hilbert problem (see [Mat93]) with Francesco Ballini from the logic group of the department, mostly on the book [Smo91]. The undecidability result is here obtain in another way than reducing to another undecidable problem: it is proved that Diophantine equations yield the power of encoding all the semi-decidable problems. Maybe a similar approach can give a result for the freeness problem in linear groups.

References

[Adi55] SI Adian. "Algorithmic undecidability of problems of recognition of certain properties of groups". In: *Dokl. Akad. Nauk SSSR*. Vol. 103. 4. 1955, pp. 533–535.

[Boo58] William W. Boone. "The word problem*". In: *Proceedings of the National Academy of Sciences* 44.10 (Oct. 15, 1958). Publisher: Proceedings of the National Academy of Sciences, pp. 1061–1065. DOI: 10.1073/pnas.44.10.1061. URL: https://www.pnas.org/doi/abs/10.1073/pnas.44.10.1061.

[HNN49] Graham Higman, B. H. Neumann, and Hanna Neuman. "Embedding Theorems for Groups". In: *Journal of the London Mathematical Society* s1-24.4 (1949). _eprint: https://onlinelibra 24.4.247, pp. 247–254. ISSN: 1469-7750. DOI: 10.1112/jlms/s1-24.4.247. URL: https://onlinelibrary.wiley.com/doi/abs/10.1112/jlms/s1-24.4.247.

[KL23] Dawid Kielak and Marco Linton. *Virtually free-by-cyclic groups*. Mar. 16, 2023. DOI: 10.48550/arXiv.2302.11500. arXiv: 2302.11500[math]. URL: http://arxiv.org/abs/2302.11500.

[KM02] Ilya Kapovich and Alexei Myasnikov. "Stallings Foldings and Subgroups of Free Groups". In: *Journal of Algebra* 248.2 (Feb. 2002), pp. 608–668. ISSN: 00218693. DOI: 10.1006/jabr.2001.9033. URL: https://linkinghub.elsevier.com/retrieve/pii/S0021869301990337.

[LS01] Roger C. Lyndon and Paul E. Schupp. *Combinatorial Group Theory*. Vol. 89. Classics in Mathematics. Berlin, Heidelberg: Springer, 2001. ISBN: 978-3-540-41158-1. DOI: 10.1007/978-3-642-61896-3. URL: http://link.springer.com/10.1007/978-3-642-61896-3.

[LU69] R. C. Lyndon and J. L. Ullman. "Groups Generated by two Parabolic Linear Fractional Transformations". In: *Canadian Journal of Mathematics* 21 (Jan. 1969), pp. 1388–1403. ISSN: 0008-414X, 1496-4279. DOI: 10.4153/CJM-1969-153-1. URL: https://www.cambridge.org/core/journals/canadian-journal-of-mathematics/article/groups-generated-by-two-parabolic-linear-fractional-transformations/28707D1A0C9A75B813A983B77B6CC301.

[Mas89] William S. Massey. *Algebraic Topology: An Introduction*. Google-Books-ID: IX0dhDDHezgC. Springer New York, Oct. 19, 1989. 292 pp. ISBN: 978-0-387-90271-5.

[Mat93] Yuri V. Matiyasevich. *Hilbert's tenth problem*. Cambridge, MA, USA: MIT Press, Sept. 1993. 264 pp. ISBN: 978-0-262-13295-4.

[MKS04] Wilhelm Magnus, Abraham Karrass, and Donald Solitar. *Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations*. Courier Corporation, Jan. 1, 2004. 466 pp. ISBN: 978-0-486-43830-6.

[Nie21] J. Nielsen. "Om regning med ikke-kommutative faktorer og dens anvendelse i gruppeteorien. (Über das Rechnen mit nicht-vertauschbaren Faktoren und dessen Anwendung in der Gruppentheorie.)" In: *Matematisk Tidsskrift, B* 1921 (1921), pp. 78–94.

[Nov55] P. S. Novikov. *Über die algorithmische Unentscheidbarkeit des Wortproblems in der Gruppentheorie*. Published: Tr. Mat. Inst. Steklova 44, 140 S. (1955). 1955.

[Rab58] Michael O. Rabin. "Recursive Unsolvability of Group Theoretic Problems". In: *Annals of Mathematics* 67.1 (1958). Publisher: Annals of Mathematics, pp. 172–194. ISSN: 0003-486X. DOI: 10.2307/1969933. URL: https://www.jstor.org/stable/1969933.

[Rot95] Joseph J. Rotman. “The Word Problem”. In: *An Introduction to the Theory of Groups*. Ed. by Joseph J. Rotman. New York, NY: Springer, 1995, pp. 418–470. ISBN: 978-1-4612-4176-8. DOI: 10.1007/978-1-4612-4176-8_12. URL: https://doi.org/10.1007/978-1-4612-4176-8_12.

[Smo91] Craig Smoryński. *Logical Number Theory I*. Universitext. Berlin, Heidelberg: Springer, 1991. ISBN: 978-3-540-52236-2. DOI: 10.1007/978-3-642-75462-3. URL: http://link.springer.com/10.1007/978-3-642-75462-3 (visited on 06/19/2024).

[Sta83] John R. Stallings. “Topology of finite graphs”. In: *Inventiones Mathematicae* 71.3 (Mar. 1983), pp. 551–565. ISSN: 0020-9910, 1432-1297. DOI: 10.1007/BF02095993. URL: http://link.springer.com/10.1007/BF02095993.

[Sta91] John R. Stallings. “Foldings of G-trees”. In: *Arboreal Group Theory*. Ed. by Roger C. Alperin. New York, NY: Springer, 1991, pp. 355–368. ISBN: 978-1-4612-3142-4. DOI: 10.1007/978-1-4612-3142-4_14.