MASTER'S DEGREE THESIS

Master of Science in Advanced Mathematics and Mathematical Engineering

Title: Counting subgroups using Stallings automata and generalisations

Author: Paloma López Larios

Advisor: Jordi Delgado Rodríguez

Department: Departament de Matemàtiques

Academic year: 2022-2023

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

Universitat Politècnica de Catalunya
Facultat de Matemàtiques i Estadística

Master in Advanced Mathematics and Mathematical Engineering

Master's thesis

Counting subgroups using Stallings automata and generalisations

Paloma López Larios

Supervised by Jordi Delgado Rodríguez

September, 2023

First of all, I would like to thank my advisor Jordi Delgado for all the time he has dedicated to help me with this thesis, for his very useful insights and for his patience and kindness. I also want to thank him, as well as Enric Ventura, for encouraging me to attend the Barcelona Weekend in Group Theory and for discussing my master's thesis with me in Manresa.

Secondly, I want to thank all the people I have met during the master's degree at the FME. This year in Barcelona has been a great experience both academically and personally because of them.

Finally, I thank my family for always being there for me.

Abstract

The study of subgroups of the free group can be carried out using the theory developed by Stallings, in which a graphical representation encoding the algebraic properties of these subgroups is given in the form of Stallings automata. These automata can be used to solve many algorithmic problems for the free group, like the membership problem, the intersection problem or the finite index problem. In this work, we provide an overview of Stallings theory and apply it to prove a result by Hall that gives the number of finite index subgroups in the free group. Moreover, we present a generalisation of the theory of Stallings which gives a geometric representation of the subgroups of free times free-abelian groups using Stallings automata enriched with certain abelian labelling to account for the free-abelian part of these groups. Combining this theory with the result by Hall and an analogous result for free-abelian groups, we obtain a recursive formula giving the number of finite index subgroups in a free times free-abelian group.

Keywords

Free times free-abelian group, (enriched) Stallings automaton, (enriched) folding, finite index, finite index problem, decision problem.

Contents

1. Introduction

In 1983, J.R. Stallings published a paper [20] that set the foundations of the now celebrated Stallings automata theory, which gives a geometrical representation of the subgroups of the free group using certain type of automata. These so-called Stallings automata have proved to be very useful. Indeed, many algorithmic problems (like the finite index problem, the membership problem or the finite index problem) can be seen to be solvable for the free group thanks to techniques based on Stallings automata. In this work, we present the theory of Stallings following some recent references on the topic ([10] and [8]) and apply it to prove a result by M. Hall (see [15]), which gives a recursive formula for the number of finite index subgroups in the free group.

In [5] and [9], a study of free times free-abelian groups was recently carried out by developing a generalisation of Stallings theory for this more complicated family of groups. In this case, the subgroups of a free times free-abelian group are represented by Stallings automata enriched with certain abelian labelling. We will also give an account of this theory and we will use it to derive a formula for the number of finite index subgroups in a free times free-abelian group. To do this, we will also need to study the same problem for free-abelian groups, so some attention will be dedicated to that family of groups as well.

This work is structured as follows.

Section 2 is a brief collection of definitions and results of group theory with two aims: first, providing the basic background about groups (Section 2.1) and algorithmic problems (Section 2.2), and second, fixing the notation and terminology that we will use.

In Section 3, we focus on free-abelian groups. Being these groups one of the factors of free times free-abelian groups, the results exposed here will be relevant in Section 5. In Section 3.1, we give some basic general notions about free-abelian groups which are mainly oriented to obtain a bijection between the subgroups of a free-abelian group and certain matrices. This bijection is then used in Section 3.2 to obtain a formula for the number of finite index subgroups in a free-abelian group.

Section 4 is dedicated to the free group. In Section 4.1, the reader can find the definitions and results regarding these groups that will be essential in the rest of the work. After this, in Section 4.2, we give a quick overview of the classical Stallings theory, which provides a geometrical representation of the subgroups of the free group. In Section 4.3, we use the theory of Stallings to study the index of subgroups of the free group with some detail, which leads us to a reformulation in terms of Stallings automata of a result by Hall counting the number of finite index subgroups in the free group.

The central part of this work is Section 5, where we study free times free-abelian groups. In Section 5.1, we give the necessary algebraic background on these groups. In Section 5.2, we present a generalisation of the theory of Stallings that uses enriched automata to encode the information about subgroups of free times free-abelian groups. This description of subgroups using enriched automata is applied in Section 5.3 to study the index and, in particular, to derive a recursive formula for the number of finite index subgroups in a free times free-abelian group.

Finally, Section 6 draws attention to some possible continuations of the work developed in this thesis. These are based on the possibility of extending the results regarding the number of finite index subgroups to bigger families of groups, like free-abelian by free groups (see Section 6.1) and Droms groups (see Section 6.2).

1.1 Notation and terminology

With the aim of avoiding possible confusions, we include some clarification regarding the notation and terminology used in this work.

The set of natural numbers, which we denote by $\mathbb{N}$, does not include zero. The cardinal of a set S is denoted by $\#S$. By infinity we always mean countable infinity, and we denote it by ∞. We will write $[m, n] = \{k \in \mathbb{N} \cup \{0\} : m \leq k \leq n\}$, where m is a natural number and n might be a natural number or infinity. We will also sometimes write $[n] = \{1, 2, \ldots, n\}$ for $n \in \mathbb{N}$.

The last letters of the latin alphabet will usually represent symbols in formal alphabets $(x, y, \ldots)$ and formal words or elements of the free group $(u, v, w, \ldots)$. The first letters of the latin alphabet in bold $(\mathbf{a}, \mathbf{b}, \mathbf{c}, \ldots)$ will be used to denote elements of $\mathbb{Z}^m$. Uppercase letters in bold $(\mathbf{A}, \mathbf{B}, \mathbf{C}, \ldots)$ will be used to denote matrices.

Finally, it is important to note that functions act on the right. That is, we denote by $(x)\varphi$ (or just $x\varphi$) the image of an element x by the function φ. Accordingly, we will denote by $\phi\psi$ the composition $A \xrightarrow{\phi} B \xrightarrow{\psi} C$. We apply the same criterion for matrices acting on vectors by multiplication.

2. Preliminaries

In this section, we present briefly some standard concepts about group theory and algorithmic problems.

2.1 Basics of group theory

Let G be a non-empty set and let $\cdot : G \times G \to G$ be a binary operation assigning an element of G, denoted by $g_1 \cdot g_2$, to every pair (g_1, g_2), where $g_1, g_2 \in G$. If this binary operation is associative and has a (unique) neutral element (i.e., an element in G, which we will denote by 1_G or simply 1, such that $1_G \cdot g = g \cdot 1_G = g$, for all $g \in G$), then the pair $(G, \cdot)$ is said to be a *monoid*. If, in addition, every element $g \in G$ has a unique inverse g^{-1} with respect to this binary operation (that is, $g \cdot g^{-1} = g^{-1} \cdot g = 1_G$), then the pair $(G, \cdot)$ is called a *group*. In what follows, we will usually refer to the set G as a group, assuming the operation.

We say that $H \subset G$ is a *subgroup* of G, denoted by $H \leqslant G$, if H is also a group with the (restriction of the) operation $\cdot$.

Definition 2.1. Let G be a group and let S be a subset of G. We say that the smallest subgroup of G containing S is the subgroup *generated* by S and we denote it by $\langle S \rangle$. It is straightforward to check that

$$\langle S \rangle = \{s_{i_1}^{k_1} s_{i_2}^{k_2} \cdots s_{i_n}^{k_n} : n \in \mathbb{N} \text{ and } s_{i_j} \in S, k_j \in \mathbb{Z}, \text{ for } j = 1, 2, \dots, n\}.$$

Given a group G, we say that $S \subset G$ is a *generating set* for G if $\langle S \rangle = G$. We say that G is *finitely generated* if there exists a finite generating set for G. We will write $H \leqslant_{\mathrm{fg}} G$ meaning that H is a finitely generated subgroup of G.

Definition 2.2. The *rank* of a group G, which we denote by $\mathrm{rk}(G)$, is the minimum cardinality of a generating set for G, that is,

$$\mathrm{rk}(G) = \min\{\#S : S \subset G \text{ and } G = \langle S \rangle\}.$$

Remark 2.3. If H is a subgroup of G, it is not true in general that the rank of H is bounded by the rank of G. A representative example is the free group (see Section 4), whose subgroups may have a higher rank than the ambient group. But there also examples, like free-abelian groups (see Section 3) for which the rank of a subgroup can be at most the rank of the ambient group. This fact is a source of many interesting questions wondering about the rank of, for example, the subgroup of fixed points of an automorphism or the intersections of subgroups. With regard to intersections, we have the following important concept.

Definition 2.4. We say that a group G has the *Howson property* (or *is Howson*) if the intersection of any two finitely generated subgroups of G is again finitely generated (i.e., if $H, K \leqslant_{\mathrm{fg}} G$ implies that $H \cap K \leqslant_{\mathrm{fg}} G$).

In a group G, we define the *commutator* of two elements $x, y \in G$ as the element $[x, y] := x^{-1}y^{-1}xy$. The subgroup of G generated by all the commutators is called the *commutator subgroup of G* and is denoted by $[G, G] := \langle [x, y] : x, y \in G \rangle$.

Definition 2.5. A group G is *abelian* if $[g_1, g_2] = 1$ for every $g_1, g_2 \in G$, that is, if all the elements in G commute.

We say that a group G is *cyclic* if it can be generated by a single element, that is, if $G = \langle g \rangle$ for some $g \in G$. It is clear that cyclic groups are abelian.

Let G be a group and let H be a subgroup of G. For every $g \in G$ we may consider the sets

$$gH = \{gh : h \in H\} \text{ and } Hg = \{hg : h \in H\},$$

which we call the *left coset* of H by g and the *right coset* of H by g, respectively. It can be shown that the left and right cosets define respective partitions on G and, therefore, respective equivalence relations $\mathcal{L}_{\mathcal{H}}$ and $\mathcal{R}_{\mathcal{H}}$.

Definition 2.6. We call *index* of H in G, and denote it by $|G : H|$, the cardinal of the quotient set $G/\mathcal{L}_{\mathcal{H}}$ (which coincides with that of $G/\mathcal{R}_{\mathcal{H}}$), that is,

$$|G : H| = \#(G/\mathcal{L}_{\mathcal{H}}).$$

We write $H \leqslant_{\mathrm{fi}} G$ to denote that H is a finite index subgroup of G. Now, let $S \subset G$. We say that S is a left (right) *transversal* for H in G if every left (right) coset of H contains exactly one element of S.

In general, for a subgroup $H \leqslant G$, the left and right cosets by an element $g \in G$ may not coincide. But there are subgroups for which this does happen.

Definition 2.7. Let G be a group and $H \leqslant G$. We say that H is *normal* in G, and denote it by $H \lhd G$, if $gH = Hg$ for every $g \in G$.

For example, the commutator subgroup $[G, G]$ of a group G is an example of a normal subgroup in G.

Definition 2.8. Let G be a group and let S be a subset of G. The smallest normal subgroup of G containing S is called the *normal closure* of S and is denoted by $\langle\langle S \rangle\rangle$.

Notice that for a normal group K, the quotient sets $G/\mathcal{L}_{\mathcal{H}}$ and $G/\mathcal{R}_{\mathcal{H}}$ are the same and, in this case, we denote any of them by G/K. This is the crucial property of normality, which allows to give the quotient set a group structure.

Theorem 2.9. *Let G be a group. If $K \lhd G$, the quotient set G/K is a group with the operation*

$$(aK)(bK) = (ab)K, \text{ for all } aK, bK \in G/K.$$

In this case, G/K is called the quotient group.

For example, the quotient group $G/[G, G]$ is the largest abelian quotient of G, in the sense that if H is a normal subgroup of G, then G/H is abelian if and only if $[G, G] \leqslant H$. This quotient group is usually called the *abelianisation* of G, denoted by G^{ab}.

Definition 2.10. Let $(G_1, \cdot)$ and $(G_2, *)$ be two groups. A map $f : G_1 \to G_2$ is said to be a group *homomorphism* if $(g \cdot h)f = (g)f * (h)f$ for every $g, h \in G_1$. The *kernel* of a homomorphism $f : G_1 \to G_2$ is

$$\ker(f) := \{g \in G_1 : (g)f = 1_{G_2}\},$$

which is clearly a normal subgroup of G_1.

A very important result in group theory is the First Isomorphism Theorem, which we now state.

Theorem 2.11. *Let G_1 and G_2 be two groups. If $f : G_1 \to G_2$ is a homomorphism, then*

$$G_1/\ker(f) \cong Im(f).$$

In particular, if f is an epimorphism, then

$$G_1/\ker(f) \cong G_2.$$

A result which can be derived from the previous one and which we will use in this work is the Second Isomorphism Theorem, whose statement follows.

Theorem 2.12. *Let G be a group, let H be a subgroup of G and let N be a normal subgroup of G. Then,*

$$\frac{H}{H \cap N} \cong \frac{HN}{N}.$$

The First Isomorphism Theorem plays an important role (see Theorem 4.14) in the definition of a presentation for a group, which is a succinct way of presenting all the information about a group (see Definition 4.15 in Section 4.1).

The main objects of study of this work are direct products of free and free-abelian groups, we give the details of this product of groups now.

Definition 2.13. If $(H, \cdot)$ and $(K, *)$ are groups, then their external direct product, denoted by $H \times K$, is the group with elements all ordered pairs (h, k), where $h \in H$ and $k \in K$, and with operation

$$(h, k)(h', k') = (h \cdot h', k * k').$$

Proposition 2.14. *Let G be a group with normal subgroups H and K. If $HK = G$ and $H \cap K = 1$, then $G \cong H \times K$.*

A group HK like in the previous proposition is called the *internal direct product* of H and K. If we have a group $G \cong H \times K$, we say that H and K are *direct factors* of G.

2.2 Algorithmic problems

Between the years 1910 and 1914, the German-born mathematician Max Dehn published a series of papers on group theory and topology. The problems he posed and the techniques he developed have had a very strong influence in the study of combinatorial group theory. Among other significant contributions, Dehn posed three important problems, each one of them stemming from a specific topological question. Dehn's three problems are the following:

Definition 2.15. *Word problem, $WP(G)$*: Let G be a group given by a finite presentation $\langle X|R\rangle$. Decide, given a word $w \in (X^{\pm})^*$, whether $w \in \langle\langle R\rangle\rangle$.

Definition 2.16. *Conjugacy problem, $CP(G)$*: Let G be a group given by a finite presentation $\langle X|R\rangle$. Decide, given words $u, v \in (X^{\pm})^*$, whether there exists $w \in (X^{\pm})^*$ such that $w^{-1}uwv^{-1} \in \langle\langle R\rangle\rangle$.

Definition 2.17. *Isomorphism problem $IP(G)$:* Decide, given finite presentations $\langle X_1|R_1\rangle$ and $\langle X_2|R_2\rangle$, whether they present isomorphic groups.

A rigorous definition of an algorithm can be given using the concept of Turing machine. For our purposes, it will be enough to define an *algorithm* as a procedure, given by a finite number of instructions, that on a given input produces an unambiguous answer after a finite number of steps. If an algorithm outputting a correct yes/no answer exists for one of these problems, then we say that the problem is *solvable*.

In addition to the problems posed by Dehn, there are some other problems which will be of interest for us. For example we have the following generalisation of the word problem.

Definition 2.18. *Membership problem, $MP(G)$:* Let G be a group given by a finite presentation $\langle X|R\rangle$. Given words $u, v_1, \dots, v_k \in (X^{\pm})^*$, decide whether u represents an element in the subgroup generated by the elements represented by $v_1, \dots, v_k$.

Another problem of interest which is related to the Howson property we defined in the previous part is this one.

Definition 2.19. *Subgroup intersection problem, $SIP(G)$:* Let G be a group given by a finite presentation $\langle X|R\rangle$. Given two different finite families of words $u_1, \dots, u_l; v_1, \dots, v_k \in (X^{\pm})^*$, decide whether the intersection of the corresponding generated subgroups $\langle u_1, \dots, u_l\rangle \cap \langle v_1, \dots, v_k\rangle \leqslant G$ is finitely generated and, in the affirmative case, compute a generating set for the intersection.

Since in this work we are particularly interested in counting subgroups of finite index, the following problem will be quite relevant.

Definition 2.20. *Finite index problem, $FIP(G)$:* Let G be a group given by a finite presentation $\langle X|R\rangle$. Given a finite family $v_1, \dots, v_k \in (X^{\pm})^*$, decide if the subgroup $\langle v_1, \dots, v_k\rangle \leqslant G$ has finite index. And, in the affirmative case, compute a system of coset representatives.

3. Free-abelian groups

In this section we will focus on free-abelian groups. We will start by presenting some basic concepts and results regarding these groups, paying special attention to those results that allow us to study finite index subgroups in these groups. In this vein, Theorem 3.17 and Theorem 3.19 are probably the most important: the former gives a bijection between finite index subgroups of a free-abelian group and a certain kind of matrices and the latter exploits this bijection in order to count the number of subgroups of a given index in a free-abelian group. These results will be useful later in Section 5, since the groups we will study there are a direct product in which one of the factors is a free-abelian group.

3.1 Definition and properties of free-abelian groups

We will define the groups that we are going to study in this section in terms of the existence of a certain generating set.

Definition 3.1. Let G be an abelian group. We say that a subset $\mathcal{B} \subset G$ is an *abelian basis* for G if the following two conditions are satisfied:

(i) $G = \langle \mathcal{B} \rangle$ (that is, $\mathcal{B}$ generates G).

(ii) If for some $b_1, \dots, b_k \in \mathcal{B}$ and $n_1, \dots, n_k \in \mathbb{Z}$ we have that $n_1 b_1 + \cdots + n_k b_k = 0$, then $n_i = 0$ for all $i \in \{1, \dots, k\}$ (that is, $b_1, \dots, b_k$ are linearly independent).

If G is an abelian group which admits an abelian basis $\mathcal{B}$, we say that G is a *free-abelian group*.

If it is clear from the context, we will sometimes refer to abelian bases simply as bases.

Remark 3.2. In this work, we will restrict ourselves to the case of finitely generated free-abelian groups. From now on, every time we refer to a free-abelian group, the reader should take into account that we are referring to a finitely generated free-abelian group.

Remark 3.3. If G is a (finitely generated) free-abelian group, then every basis for G is finite. Indeed, by the previous remark, G admits a finite generating set $\mathcal{S} = \{s_1, \dots, s_p\}$. Now let $\mathcal{B}$ be an abelian basis for G. Since $s_i \in G = \langle \mathcal{B} \rangle$ for $i \in \{1, \dots, p\}$, each s_i can be written as an integer linear combination of a finite number of elements of $\mathcal{B}$. By considering the (finite) union of these elements of $\mathcal{B}$, we obtain a finite abelian basis $\mathcal{B}' \subset \mathcal{B}$ for G. If $\mathcal{B}' \neq \mathcal{B}$, there exists $b \in \mathcal{B} \backslash \mathcal{B}'$ which can be written as a linear combination of the elements in $\mathcal{B}'$, contradicting the fact that the elements in $\mathcal{B}$ are linearly independent. Thus, $\mathcal{B} = \mathcal{B}'$ is finite.

The prototypical example of a free-abelian group is $(\mathbb{Z}^m, +)$, whose elements are m-tuples of integers and whose operation is the component-wise addition. Indeed, an abelian basis for $\mathbb{Z}^m$ is $\mathcal{B} = \{\mathbf{e_i}\}_{i=1}^m$, where $\mathbf{e_i}$ denotes the tuple which consists of all zeros except for a one in the i-th position (this basis is usually called the *canonical basis* of $\mathbb{Z}^m$).

The following result collects a few basic properties about free-abelian groups, some of them concerning the cardinality of their bases and their rank (which turn out to be the same).

Proposition 3.4. *Let G and G' be groups. Then:*

(i) G is free-abelian if and only if $G \cong \mathbb{Z}^m$ for some $m \geq 0$.

(ii) If G is free-abelian, then any two bases of G have the same cardinality.

(iii) If G is free-abelian, then the cardinal of any abelian basis of G is equal to the rank of G.

(iv) If G and G' are free-abelian, then $G \cong G'$ if and only if $rk(G) = rk(G')$.

Proof. (i) If G is free-abelian and $\mathcal{B} = \{b_1, \dots, b_m\}$ is an abelian basis for G, the map

$$\begin{array}{rccc} f: & G & \to & \mathbb{Z}^m \\ & \sum_{i=1}^{m} x_i b_i & \mapsto & (x_1, \dots, x_m), \end{array}$$

where $x_i \in \mathbb{Z}$ for $i \in [m]$, is an isomorphism. Conversely, the canonical basis $\{\mathbf{e_i}\}_{i=1}^{m}$ is an abelian basis for $\mathbb{Z}^m$.

(ii) Let $\mathcal{B}$ and $\mathcal{B}'$ be finite bases of G with cardinals $\#\mathcal{B} = m$ and $\#\mathcal{B}' = m'$. By item (i), we have that $G \cong \mathbb{Z}^m \cong \mathbb{Z}^{m'}$. If we now consider the subgroup $H = \{2g : g \in G\}$, we have that

$$(\mathbb{Z}/2\mathbb{Z})^m \cong G/H \cong (\mathbb{Z}/2\mathbb{Z})^{m'},$$

so if we consider the cardinal of these isomorphic groups, we obtain

$$2^m = \#(\mathbb{Z}/2\mathbb{Z})^m = \#(G/H) = \#(\mathbb{Z}/2\mathbb{Z})^{m'} = 2^{m'},$$

which implies that $m = m'$.

(iii) By item (ii), all bases of G have the same cardinal. If we take any abelian basis of G, say $\mathcal{B}$, and we denote its cardinal $\#\mathcal{B} = m$, we have that $G \cong \mathbb{Z}^m$ by item (i). Arguing by contradiction, suppose that there exists a generating set S with cardinal $\#S < m$ for $\mathbb{Z}^m$. If we look at the elements of S in the $\mathbb{Q}$-vector space $\mathbb{Q}^m$, we also have that S generates $\mathbb{Q}^m$, but this contradicts the fact that $\mathbb{Q}^m$ is a vector space of dimension m. Therefore, $G \cong \mathbb{Z}^m$ has rank m.

(iv) This is a direct consequence of items (*i*) and (*iii*).

□

Since all free-abelian groups of rank m are isomorphic to $\mathbb{Z}^m$ by Proposition 3.4, we will usually denote any free-abelian group of rank m by $\mathbb{Z}^m$.

Remark 3.5. It is worth noting that a presentation for the free-abelian group of rank m, $\mathbb{Z}^m$, is given by

$$\langle t_1, \dots, t_m | t_i^{-1} t_j^{-1} t_i t_j, \forall i, j \in [m] \rangle.$$

In order to describe the subgroups of a free-abelian group and their rank, we will need the following lemma (we omit its proof, but it can be found in [16, Corollary 10.16]).

Lemma 3.6. *If $H \leqslant G$ and G/H is free-abelian, then $G = H \oplus K$, where $K \leqslant G$ and $K \cong G/H$.*

We can now use this lemma to prove that the property of being free-abelian is inherited by subgroups and to relate the rank of these subgroups with the rank of the ambient group.

Theorem 3.7. *Every subgroup H of a free-abelian group G of finite rank is itself free-abelian and, moreover, $rk(H) \leq rk(G)$.*

Proof. The proof is by induction on m, the rank of G. For the base case, if $m = 0$, the result is immediate because G is the trivial group. Also notice that if $m = 1$, then $G \cong \mathbb{Z}$. Since the subgroups of a cyclic group are cyclic as well, we have that either $H \cong \{0\}$ or $H \cong \mathbb{Z}$, and the result holds. For the inductive step, let $\{b_1, \ldots, b_{m+1}\}$ be an abelian basis of G. Define $G' = \langle b_1, \ldots, b_m \rangle$ and $H' = H \cap G'$. By induction, H' is free-abelian of rank $\leq m$. Applying Theorem 2.12, we have

$$H/H' = H/(H \cap G') \cong (H + G')/G' \leqslant G/G' \cong \mathbb{Z}.$$

By the case $m = 1$, either $H/H' = \{0\}$ or $H/H' \cong \mathbb{Z}$. In the first case, $H = H'$ and we are done; in the second case, Lemma 3.6 gives $H = H' \oplus \langle h \rangle$ for some element $h \in H$, where $\langle h \rangle \cong \mathbb{Z}$, and so H is free-abelian and $\text{rk}(H) = \text{rk}(H' \oplus \mathbb{Z}) = \text{rk}(H') + 1 \leq m + 1$. □

In Proposition 3.10, we will give a characterisation of finite index subgroups in terms of their rank and we will also show that the finite index problem is solvable for free-abelian groups. To do so, we first need to see how subgroups of $\mathbb{Z}^m$ can be described using integer matrices.

Given an integer matrix $\mathbf{A}$ of dimension $s \times m$, we will denote by $\langle \mathbf{A} \rangle$ the *row space* of the matrix $\mathbf{A}$, that is,

$$\langle \mathbf{A} \rangle = \{\mathbf{x}\mathbf{A} : \mathbf{x} \in \mathbb{Z}^s\}.$$

The elements in $\langle \mathbf{A} \rangle$ are integer linear combinations of the rows of $\mathbf{A}$, which are elements of $\mathbb{Z}^m$. Therefore, $\langle \mathbf{A} \rangle$ is the subgroup of $\mathbb{Z}^m$ generated by the rows of $\mathbf{A}$. Notice that, in general, the rows of $\mathbf{A}$ need not be an abelian basis of the subgroup $\langle \mathbf{A} \rangle$, they are just a generating set. However, if the matrix $\mathbf{A}$ has full row rank, then the rows of this matrix form an abelian basis of $\langle \mathbf{A} \rangle$.

An integral square matrix $\mathbf{U}$ of size m is called *unimodular*, $\mathbf{U} \in GL_m(\mathbb{Z})$, if $\det(U) = \pm 1$, that is, if the matrix is invertible in $\mathcal{M}_m(\mathbb{Z})$. The following lemma recalls some properties of unimodular matrices that we will use.

Lemma 3.8. *Let $\mathbf{A}$ and $\mathbf{A}'$ be integral matrices of dimension $s \times m$. If $\mathbf{A} = \mathbf{U}\mathbf{A}'$ for some unimodular matrix $\mathbf{U}$, then $\langle \mathbf{A} \rangle = \langle \mathbf{A}' \rangle$. Moreover, if $\mathbf{A}$ and $\mathbf{A}'$ have full row rank and $\langle \mathbf{A} \rangle = \langle \mathbf{A}' \rangle$, then $\mathbf{A} = \mathbf{U}\mathbf{A}'$ for some unimodular matrix $\mathbf{U}$.*

Proof. Suppose $\mathbf{A} = \mathbf{U}\mathbf{A}'$ for some unimodular matrix $\mathbf{U}$. If $\mathbf{a_i}$ and $\mathbf{u_i}$ are the i-th rows of $\mathbf{A}$ and $\mathbf{U}$ respectively, we have that $\mathbf{a_i} = \mathbf{u_i}\mathbf{A}' \in \langle \mathbf{A}' \rangle$ for $i \in \{1, \ldots, s\}$. Therefore, since $\langle \mathbf{A} \rangle$ is generated by the rows of $\mathbf{A}$, we have that $\langle \mathbf{A} \rangle \subset \langle \mathbf{A}' \rangle$. Given that $\mathbf{U}$ is unimodular, we also have that $\mathbf{A}' = \mathbf{U}^{-1}\mathbf{A}$ and can conclude similarly that $\langle \mathbf{A}' \rangle \subset \langle \mathbf{A} \rangle$.

Now, if $\mathbf{A}$ and $\mathbf{A}'$ have full row rank and $\langle \mathbf{A} \rangle = \langle \mathbf{A}' \rangle$, then the rows of $\mathbf{A}$ belong to $\langle \mathbf{A}' \rangle$ and we have that $\mathbf{A} = \mathbf{V}\mathbf{A}'$ for some integral matrix $\mathbf{V}$. Similarly, $\mathbf{A}' = \mathbf{W}\mathbf{A}$ for some integral matrix $\mathbf{W}$. This means that $\mathbf{A} = \mathbf{V}\mathbf{W}\mathbf{A}$ and, since $\mathbf{A}$ has full row rank, we may conclude that $\mathbf{V}\mathbf{W} = \mathbf{I}$ which implies that $\det(\mathbf{V}) = \det(\mathbf{W}) = \pm 1$. □

The following classical result (whose proof we omit but can be found in [1, Theorem 3.1, Section 5.3]) associates a matrix with a special form to every integer matrix. This matrix can be obtained from the original one multiplying it by suitable unimodular matrices.

Proposition 3.9. *For every $s \times m$ integral matrix $\mathbf{A}$, there exists a matrix, called the Smith Normal Form (SNF) of the matrix $\mathbf{A}$, with the same dimensions as $\mathbf{A}$ and which is of the form*

$$\mathbf{D} = diag(d_1, d_2, \ldots, d_r, 0, \ldots, 0),$$

where $d_1, \ldots, d_r$ are strictly positive integers satisfying that each of them divides the following one ($d_1 | d_2 | \cdots | d_r$) and $r \leq \min\{s, m\}$ such that

$$\mathbf{PA} = \mathbf{DQ},$$

for some $\mathbf{P} \in GL_s(\mathbb{Z})$ and $\mathbf{Q} \in GL_m(\mathbb{Z})$.

We now have all the ingredients to give the characterisation of finite index subgroups in a free-abelian group in terms of their rank.

Proposition 3.10. *A subgroup $L \leqslant \mathbb{Z}^m$ has finite index in $\mathbb{Z}^m$ if and only if it has maximum rank m.*

Proof. Let $\mathbf{a_1}, \ldots, \mathbf{a_s} \in \mathbb{Z}^m$ be a generating set for L. Consider the integral matrix $\mathbf{A}$ whose rows are the $\mathbf{a_i}'s$, which has dimension $s \times m$. We compute the SNF of $\mathbf{A}$, obtaining that

$$\mathbf{PA} = \mathbf{DQ},$$

for some $\mathbf{P} \in GL_s(\mathbb{Z})$, $\mathbf{Q} \in GL_m(\mathbb{Z})$ and $\mathbf{D} = \operatorname{diag}(d_1, d_2, \ldots, d_r, 0, \ldots, 0)$ where $d_1, \ldots, d_r$ are positive such that $d_1 | d_2 | \cdots | d_r$ and $r \leq \min\{s, m\}$ is the rank of $\mathbf{A}$.

Since the rows of $\mathbf{A}$ generate L, we have that L is also generated by the rows of $\mathbf{PA}$, due to Lemma 3.8. Since $\mathbf{PA} = \mathbf{DQ}$, L is generated by the image under the automorphism

$$\begin{array}{rccc} \mathbf{Q}: & \mathbb{Z}^m & \to & \mathbb{Z}^m \\ & \mathbf{v} & \mapsto & \mathbf{vQ} \end{array}$$

of the subgroup L' generated by the vectors $(d_1, 0, \ldots, 0), \ldots, (0, \ldots, 0, d_r, 0, \ldots, 0)$.

Observe that, given that $[d_1] \times \cdots \times [d_r] \times \mathbb{Z}^{m-r}$ is a transversal for $\mathbb{Z}^m / L'$, its image by the automorphism $\mathbf{Q}$ gives us a transversal for $\mathbb{Z}^m / L$. Moreover, notice that the index of L in $\mathbb{Z}^m$ is

$$|\mathbb{Z}^m : L| = d_1 \cdots d_r \cdot \#\mathbb{Z}^{m-r}. \tag{1}$$

Thus, it is clear that $|\mathbb{Z}^m : L|$ is finite if and only if $r = m$, i.e., if and only if L has maximum rank m. □

Corollary 3.11. *The finite index problem for $\mathbb{Z}^m$ is solvable, that is, if a subgroup L of $\mathbb{Z}^m$ is given by a finite set of generators, we can algorithmically decide whether L is of finite index in $\mathbb{Z}^m$, and effectively compute a transversal (and therefore the index $|\mathbb{Z}^m : L|$) if the index is finite.*

Proof. Maintaining the notation above, it is enough to observe that the finite index condition (having $r = m$) is algorithmically decidable just by counting the number of nonzero diagonal elements in the SNF of $\mathbf{A}$. Finally, to obtain a transversal in the case in which the index of L is finite, one simply has to multiply by $\mathbf{Q}$ the elements in $[d_1] \times \cdots \times [d_r]$. □

Suppose now that L is a finite index subgroup in $\mathbb{Z}^m$. Due to Proposition 3.10, it must have rank m and therefore we can take an abelian basis of L with cardinality m. If we denote by $\mathbf{A}$ the matrix whose rows are the elements of this abelian basis, we obtain a full rank square integer matrix satisfying that $\langle \mathbf{A} \rangle = L$. Observe that, because we may have different bases of L, there is not a unique square matrix whose row space is L. In what follows, we will define and prove the existence and unicity of a matrix with a certain special form (see Definition 3.12) having L as its row space. This will allow us to establish a bijection between finite index subgroups in $\mathbb{Z}^m$ and a certain set of matrices.

Definition 3.12. We say that a matrix $\mathbf{H} \in \mathcal{M}_{n,m}(\mathbb{Z})$ is in *Hermite normal form* (abbreviated HNF) if there exists $r \leq n$ and a strictly increasing map $f : [r] \to [m]$ satisfying the following conditions:

(i) The last $n - r$ rows of $\mathbf{H}$ are zero.

(ii) For $1 \leq i \leq r$, $h_{i,f(i)} > 0$, $h_{i,j} = 0$ if $j < f(i)$ and $0 \leq h_{j,f(i)} < h_{i,f(i)}$ if $j < i$.

The reader may find slightly different definitions for the previous concept from other authors (the definition we have presented is an adaptation of [4, Definition 2.4.2.]).

Remark 3.13. In the particular case in which $\mathbf{H} \in \mathcal{M}_m(\mathbb{Z})$ has full rank, we will have that $\mathbf{H}$ is in HNF if it satisfies the following properties (notice that in this case f is the identity):

(i) $h_{ij} = 0$ if $i > j$ (that is, $\mathbf{H}$ is an upper triangular matrix),

(ii) $h_{ii} > 0$ for all $i \in [m]$ (the elements in the diagonal are strictly positive),

(iii) For every $l < i, 0 \leq h_{li} < h_{ii}$ (the elements above h_{ii} are nonnegative and strictly upper-bounded by it).

Since we are interested in studying finite index subgroups of $\mathbb{Z}^m$, we will now focus on showing how to transform a full rank $m \times m$ integer matrix into a (unique) matrix in HNF with the same row space, which of course will be of the type specified in the previous remark.

Given an integer matrix $\mathbf{A}$, we can perform the so-called *elementary row operations*, which consist in premultiplying $\mathbf{A}$ by certain unimodular matrices and are the following:

(i) Swapping two rows R_i and R_j for $i \neq j$. We denote this operation by $R_i \leftrightarrow R_j$ and it is equivalent to premultiplying $\mathbf{A}$ by the unimodular matrix $\mathbf{U}$ obtained from the identity matrix by swapping its i-th and j-th rows.

(ii) Multiplying the i-th row R_i by -1, denoted by $R_i \leftarrow -R_i$. This is equivalent to premultiplying $\mathbf{A}$ by the unimodular matrix $\mathbf{U}$ resulting from multiplying the i-th row of the identity matrix by -1.

(iii) Adding an integer multiple of the j-th row to the i-th row. This operation is denoted by $R_i \leftarrow R_i + \alpha R_j$ with $\alpha \in \mathbb{Z}$ and it is equivalent to premultiplying $\mathbf{A}$ by the unimodular matrix $\mathbf{U}$ which is obtained from the identity matrix by adding α times the j-th column to the i-th column.

Notice that performing a finite sequence of these elementary row operations amounts to premultiplying the original matrix by a unimodular matrix (since the product of unimodular matrices is again a unimodular matrix). This means, by Lemma 3.8, that the row space of the matrix obtained after these operations is precisely that of the original matrix.

Theorem 3.14. *Let $\mathbf{A}$ be an integer $m \times m$ matrix of full rank, then it can be brought into HNF by a sequence of elementary row operations.*

Proof. We describe an algorithm converting $\mathbf{A}$ into a matrix in HNF. This algorithm constructs a sequence of matrices $\mathbf{A_0} = \mathbf{A}, \mathbf{A_1}, \mathbf{A_2}, \dots, \mathbf{A_m}$, where

$$\mathbf{A_k} = \begin{bmatrix} \mathbf{H_k} & \mathbf{C_k} \\ \mathbf{0} & \mathbf{D_k} \end{bmatrix},$$

and we have that $\mathbf{H_k}$ is a $k \times k$ matrix in HNF and $\mathbf{C_k}$ and $\mathbf{D_k}$ have dimensions $k \times (m-k)$ and $(m-k) \times (m-k)$ respectively. The matrix $\mathbf{A_{k+1}}$ is obtained from $\mathbf{A_k}$ as follows.

Step 1: Let $d_1, d_2, \dots, d_{m-k}$ be the entries in the first column of $\mathbf{D_k}$. By multiplying some of the rows by -1 if necessary, we may assure that all of these entries are nonnegative. Moreover, since the matrix $\mathbf{A}$ (and, therefore, all the matrices of the sequence) has full row rank, $d_l > 0$ for some $l \in [m-k]$. Now, if $d_i > d_j$ are two nonzero entries in the first column of $\mathbf{D_k}$, we perform the row operation $R_i \leftarrow R_i - \lfloor \frac{d_i}{d_j} \rfloor R_j$. We do this until we obtain that there is exactly one nonzero entry in the first column of $\mathbf{D_k}$ (we can assure that this will happen eventually because every time one of these row operations is performed, all the entries in the first column of $\mathbf{D_k}$ remain nonnegative but their total sum strictly decreases). If we denote by d the unique element in the first column of $\mathbf{D_k}$ different from zero and swap rows if necessary, we obtain that d is in the first row and first column of $\mathbf{D_k}$.

Step 2: It remains to ensure that all the entries in the first column of $\mathbf{C_k}$ are nonnegative and smaller than d. To do so, we perform the operation $R_i \leftarrow R_i - \lfloor \frac{c_i}{d} \rfloor R_{k+1}$ for each $i \in [k-1]$ (clearly, this does not affect the entries of $\mathbf{H_k}$).

Notice that when we compute $\mathbf{A_1}$ from $\mathbf{A_0}$, Step 2 is not necessary; and, when we compute $\mathbf{A_m}$ from $\mathbf{A_{m-1}}$, Step 1 can be omitted.

The matrix $\mathbf{A_m}$ is the claimed one, since it is in HNF. □

Theorem 3.15. *Two full rank square integer matrices* $\mathbf{H}$ *and* $\mathbf{H}'$ *in HNF satisfying that* $\langle \mathbf{H} \rangle = \langle \mathbf{H}' \rangle$ *must be equal.*

Proof. Suppose $\mathbf{H} = [h_{ij}]$ and $\mathbf{H}' = [h'_{ij}]$ are two full rank $m \times m$ matrices in Hermite normal form satisfying that $\langle \mathbf{H} \rangle = \langle \mathbf{H}' \rangle$ and $\mathbf{H} \neq \mathbf{H}'$. Choose $j \in [m]$ to be as small as possible satisfying $h_{ij} \neq h'_{ij}$ for some $i \in [m]$ and, without loss of generality, suppose $h_{ij} > h'_{ij}$.

If we denote by $\mathbf{h_i}$ and $\mathbf{h'_i}$ the i-th rows of $\mathbf{H}$ and $\mathbf{H}'$ respectively, we have that $\mathbf{h_i}, \mathbf{h'_i} \in \langle \mathbf{H} \rangle = \langle \mathbf{H}' \rangle$ and, therefore, $\mathbf{h_i} - \mathbf{h'_i} \in \langle \mathbf{H} \rangle$, which means that $\mathbf{h_i} - \mathbf{h'_i}$ can be expressed as an integer linear combination of the rows of $\mathbf{H}$.

Notice that, by the choice of j, $\mathbf{h_i} - \mathbf{h'_i}$ has zeros in its first $j-1$ components. This implies that $\mathbf{h_i} - \mathbf{h'_i}$ is an integer linear combination of rows $\mathbf{h_j}, \mathbf{h_{j+1}}, \dots, \mathbf{h_m}$. Indeed, suppose $\mathbf{h_i} - \mathbf{h'_i} = \sum_{k=1}^{m} \alpha_k \mathbf{h_k}$, with $\alpha_k \in \mathbb{Z}$. Since $\mathbf{h_1}$ is the only row of $\mathbf{H}$ whose first component is nonzero and the first component of $\mathbf{h_i} - \mathbf{h'_i}$ must be null, we have that $\alpha_1 = 0$. Now, out of $\mathbf{h_2}, \mathbf{h_3}, \dots, \mathbf{h_m}$, the only row whose second component is nonzero is $\mathbf{h_2}$, which implies that $\alpha_2 = 0$ because the second component of $\mathbf{h_i} - \mathbf{h'_i}$ is zero. Repeating this argument, we arrive at the conclusion that $\alpha_1 = \alpha_2 = \dots = \alpha_{j-1} = 0$.

Given that the only one of the rows $\mathbf{h_j}, \mathbf{h_{j+1}}, \dots, \mathbf{h_m}$ which has a positive element in the j-th position is $\mathbf{h_j}$, we have that $h_{ij} - h'_{ij} = z h_{jj}$ for some integer z. Now, taking into account that $h_{ij} < h_{jj}$ and $h'_{ij} < h_{ij} < h_{jj}$, we can see that $|h_{ij} - h'_{ij}| < h_{jj}$ and thus we must have $z = 0$. It follows that $h_{ij} = h'_{ij}$, which is a contradiction. □

Remark 3.16. The two previous results tell us that for any subgroup $L \leqslant \mathbb{Z}^m$ of rank m and any square full rank integer matrix $\mathbf{A}$ whose row space is L, there exists a unique matrix $\mathbf{H}$ in Hermite normal form satisfying that $\mathbf{H} = \mathbf{UA}$ for some unimodular matrix $\mathbf{U}$. The matrix $\mathbf{H}$ will be referred to as the *Hermite normal form of* $\mathbf{A}$. Moreover, observe that $\mathbf{H}$ is the only full rank square matrix in HNF whose row space is L. We will denote it by $(L)\mathbf{H}$.

We summarize the described situation in the result below.

Theorem 3.17. *There exists a bijection between finite index subgroups of $\mathbb{Z}^m$ and full rank $m \times m$ integer matrices in Hermite normal form.*

Proof. Given a subgroup $L \leqslant \mathbb{Z}^m$ of finite index, we know by Proposition 3.10 that L has rank m and therefore we can take an abelian basis for L of cardinality m. Now let $\mathbf{A}$ be the full rank $m \times m$ matrix whose rows are the elements of this basis. Computing the HNF of $\mathbf{A}$, we obtain $(L)\mathbf{H}$, which is the only full rank $m \times m$ matrix in HNF whose row space is L. Therefore, we can consider the following well-defined map:

$$\begin{array}{rccl} \mathbf{H}: & \{\text{f.i. subgroups of } \mathbb{Z}^m\} & \to & \{\text{ full rank } m \times m \text{ integer matrices in HNF}\} \\ & L & \mapsto & (L)\mathbf{H} \end{array}$$

Since the map $\langle \mathbf{M} \rangle \leftarrow\!\shortmid \mathbf{M}$ is clearly its inverse, we conclude that $\mathbf{H}$ is a bijection. □

This theorem that we have just proved together with the following result will be the keys for the proof of Theorem 3.19 in the next section.

Proposition 3.18. *Let L be a subgroup of finite index k in $\mathbb{Z}^m$, then* $\det((L)\mathbf{H}) = k$.

Proof. By Proposition 3.9, we know that there exist unimodular matrices $\mathbf{P}$ and $\mathbf{Q}$ such that $(L)\mathbf{H} = \mathbf{P}^{-1}\mathbf{D}\mathbf{Q}$, where $\mathbf{D}$ is the SNF of $(L)\mathbf{H}$. Since the determinant of unimodular matrices is -1 or 1 and the determinant of $(L)\mathbf{H}$ has to be positive, we have that

$$\det((L)\mathbf{H}) = \det(\mathbf{D}) = d_1 \cdots d_r = |\mathbb{Z}^m : L|,$$

where in the last step we have used the equality (1), taking into account that the rank of L is m because it has finite index. □

3.2 Counting finite index subgroups in free-abelian groups

The result in this section provides a recursive formula to obtain the number of subgroups of a given finite index in $\mathbb{Z}^m$. In general, for any group G, we will denote by $N_k(G)$ the number of subgroups of index k in the group G.

Theorem 3.19 (Bushnell-Reiner)**.** *Let $k \in \mathbb{N}$, then $N_k(\mathbb{Z}) = 1$ and*

$$N_k(\mathbb{Z}^m) = \sum_{s|k} N_s(\mathbb{Z}^{m-1}) \left(\frac{k}{s}\right)^{m-1}, \quad \text{for } m \geq 2.$$

Proof. By Theorem 3.17 and Proposition 3.18 , we have that every subgroup of index k in $\mathbb{Z}^m$ is uniquely represented by an $m \times m$ integral matrix in HNF whose determinant equals k. Therefore, $N_k(\mathbb{Z}^m)$ is the number of such matrices, which have the form:

$$\mathbf{H} = \begin{bmatrix} h_{11} & h_{12} & h_{13} & \cdots & h_{1m} \\ 0 & h_{22} & h_{23} & \cdots & h_{2m} \\ 0 & 0 & h_{33} & \cdots & h_{3m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & h_{mm} \end{bmatrix}, \tag{2}$$

where $h_{i,i} \geq 1$ for $i \in \{1, \dots, m\}$, $0 \leq h_{ij} < h_{jj}$ for $1 \leq i < j$ and $k = h_{11}h_{22}\cdots h_{mm}$. Let us count the number of these matrices.

Let $s = h_{mm}$ a divisor of k. To each of the elements $h_{1m}, h_{2m}, \dots, h_{(m-1)m}$ we can assign the values $0, 1, \dots, s-1$, which gives us s^{m-1} choices for the last column of the matrix. If we remove the last column and the last row, we obtain an $(m-1) \times (m-1)$ integral matrix in HNF whose determinant equals $\frac{k}{s}$, thus, there are $N_{\frac{k}{s}}(\mathbb{Z}^{m-1})$ choices for the rest of the matrix $\mathbf{H}$. Summing over all the positive divisors s of k gives the formula

$$N_k(\mathbb{Z}^m) = \sum_{s|k} N_{\frac{k}{s}}(\mathbb{Z}^{m-1}) s^{m-1},$$

which is equivalent to the desired formula if we take into account that $\frac{k}{s}$ runs over all divisors of k as s does. $\square$

In Table 1, we can find the number of subgroups of index k in $\mathbb{Z}^m$ for small values of k and m.

$m \backslash k$	1	2	3	4	5	6	7
1	1	1	1	1	1	1	1
2	1	3	4	7	6	12	8
3	1	7	13	35	31	91	57
4	1	15	40	155	156	600	400
5	1	31	121	651	781	3751	2801
6	1	63	364	2667	3906	22932	19608
7	1	127	1093	10795	19531	138811	137257
8	1	255	3280	43435	97656	836400	960800
9	1	511	9841	174251	488281	5028751	6725601

Table 1: Values of $N_k(\mathbb{Z}^m)$ for small m and k.

4. The free group

After studying free-abelian groups in the previous section, we will dedicate this section to the study of free groups, which are the other factor that makes up the groups that we will focus on in Section 5.

This section is structured in three parts: Sections 4.1 and 4.2 are meant to be a brief overview of the properties of the free group and the study of its subgroups using Stallings automata, which are fairly standard and well-known topics in group theory, whereas in Section 4.3 we will revisit a less well-known result related to finite index subgroups in free groups.

With more detail, in Section 4.1, we give the main properties of the free group that we will need in this work; in Section 4.2, we develop the celebrated theory of Stallings describing the subgroups of free groups as automata; finally, in Section 4.3, we will use the tools of Stallings theory to study the index of subgroups of free groups and provide a formula for counting the number of subgroups of a given finite index in the free group.

4.1 Definition and first properties

This section collects the basic definitions and results that we will need about free groups. Although different definitions of these groups can be given, the categorical approach is perhaps the best in order to highlight a crucial fact about free groups: the images of a certain subset (called a basis) of a free group uniquely determine a homomorphism to any other group, no matter what images we choose. To understand why this behaviour is special, notice that, in general, if we are trying to define a homomorphism between two groups G_1 and G_2 and $g, h \in G_1$ are two elements such that $g \cdot h = 1_{G_1}$, we are not free to choose their images $(g)f$ and $(h)f$ in any way we want, since they will have to satisfy that $(g)f * (h)f = (1_{G_1})f = 1_{G_2}$. This categorical definition will be the first one we present.

Definition 4.1. We say that a group F is *free* if there exists a subset $X \subset F$ (called a *basis*) such that for every group G and every map $f : X \to G$, there exists a unique homomorphism $\tilde{f} : F \to G$ making the following diagram commutative

$$\begin{array}{ccc} X & \hookrightarrow & F \\ & \underset{f}{\searrow} & \downarrow \tilde{f} \\ & & G. \end{array}$$

Notice that Definition 4.1 does not ensure the existence of the object we are defining. We will later give a constructive proof of the existence of a free group. But before this, it is convenient to give a second definition of free group (equivalent to the first one).

To present the second definition of the free group, some concepts and notation need to be introduced. Given a group G and a subset $X \subset G$, we will denote by $X^{-1} = \{x^{-1} : x \in X\}$ the set of elements in G which are inverses of elements in X. A product of elements of a group G in which 1_G does not appear as a factor and no element is adjacent to its inverse is said to be a reduced product (the empty reduced expression, which we denote by 1, represents the trivial element of G).

Definition 4.2. Let G be a group and $X \subset G$. We say that the subset X is *free* in G if the only reduced product of elements of $X \cup X^{-1}$ which yields the trivial element in G is the empty reduced expression.

Once these concepts have been established, we can give the second definition of free group.

Definition 4.3. Let F be a group and let $X \subset F$. We say that F is a *free group with basis* X if the subset X is free in F and it is a generating set of F.

The two definitions we have given for the free group (Definitions 4.1 and 4.3) are actually equivalent (see [10, Proposition 16] or [2, Theorem 3.6]).

The following corollary gives a useful characterisation of a basis of a free group.

Corollary 4.4. *F is a free group with basis $X \subset F$ if and only if every element in F can be written in a unique way as a reduced product of the elements in $X \cup X^{-1}$.*

In order to show that free groups exist, we proceed to construct them, specifying the set of elements of the group as well as an operation.

Definition 4.5. Let X be a nonempty set. The elements of X will be called *letters* and the set itself will be called an *alphabet*. Any ordered and finite sequence of letters in X, $w = x_1 x_2 \cdots x_n$ with $n \geq 0$ and $x_i \in X$ not necessarily distinct, is a *word* on X. A *subword* of a word will be any subsequence of consecutive letters. The *length* of a word w is the number of letters in the word and it will be denoted by $|w|$. We will follow the convention of denoting by 1 the empty word (the only word of length zero). The set of all words over X will be denoted by X^*. Notice that X^* is a free monoid with respect to the operation of concatenation. We define the set of formal inverses of X as $X^{-1} = \{x^{-1} : x \in X\}$ (notice that X and X^{-1} are disjoint). Moreover, we will use the notation $X^{\pm} = X \sqcup X^{-1}$.

Next, we define a congruence in the monoid $(X^{\pm})^*$ whose quotient will be the set for the free group we are building.

Definition 4.6. Let $u, v \in (X^{\pm})^*$. The words u and v are said to be equivalent, $u \sim v$, if there exists a finite sequence of words $u = w_1, w_2, \ldots, w_k = v$ such that every w_{i+1} can be obtained from w_i by insertion or deletion of subwords of the form xx^{-1} with $x \in X^{\pm}$.

We will consider the quotient $\mathbb{F}_X := (X^{\pm})^*/\sim$ and we will define an operation on it which yields a group. If we denote by $[w] \in \mathbb{F}_X$ the class of the word $w \in (X^{\pm})^*$, we can define the operation

$$[u] \cdot [v] := [uv], \tag{3}$$

where uv is the concatenation of u and v in $(X^{\pm})^*$.

Proposition 4.7. *The set $\mathbb{F}_X$ with operation (3) is a group.*

Proof. Associativity in $\mathbb{F}_X$ is a consequence of the associativity of concatenation in the monoid $(X^{\pm})^*$. The neutral element is $[1]$ and the inverse of a class $[x_{i_1}^{\epsilon_1} \cdots x_{i_n}^{\epsilon_n}] \in \mathbb{F}_X$ (where $\epsilon_j = \pm 1$) is the class $[x_{i_n}^{-\epsilon_n} \cdots x_{i_1}^{-\epsilon_1}]$. Therefore, $\mathbb{F}_X$ with operation (3) is a group. □

Once the group $\mathbb{F}_X$ is constructed, we still have to show that it is free with basis X. But let us introduce first the concept of reduced word.

Definition 4.8. A word $w \in (X^{\pm})^*$ is *reduced* if no letter in w is adjacent to its formal inverse.

The following result will allow us to reinterpret $\mathbb{F}_X$ in a more combinatorial and algorithm-friendly way.

Proposition 4.9. *Every equivalence class $[w] \in \mathbb{F}_X$ contains exactly one reduced word, denoted by $\overline{w}$.*

Proof. See [10, Proposition 12] or [2, Proposition 3.3]. □

Remark 4.10. Proposition 4.9 allows us to interpret the group $\mathbb{F}_X$ as the set of reduced words in $(X^{\pm})^*$ with the operation $u \cdot v = \overline{uv}$. In what follows, we will therefore think of elements of the free group as reduced words.

Proposition 4.11. *For any alphabet X, the group $\mathbb{F}_X$ is free with basis X.*

Proof. A corollary of Proposition 4.9 is the fact that the the map $\iota_X : X \to \mathbb{F}_X$ which takes $x \in X$ to $[x]$ is injective and this, in turn, gives the result (see [10, Corollary 14] for the details). □

We have shown that we can build a free group with basis any given set (if the set is empty, we have the free group of rank 0, $\mathbb{F}_0$, which is the trivial group). The following result tells us that the cardinal of a basis determines the free group up to isomorphism.

Proposition 4.12. *Let $\mathbb{F}$ be a free group with basis $X \subset \mathbb{F}$ and let $\mathbb{F}'$ be a free group with basis $X' \subset \mathbb{F}'$. Then, $\mathbb{F}$ and $\mathbb{F}'$ are isomorphic groups if and only if X and X' have the same cardinal.*

Proof. See [10, Theorem 17] or [2, Theorem 3.8 and Corollary 3.10]. □

Remark 4.13. If X is a basis of $\mathbb{F}$, we have that $rk(\mathbb{F}) = \#X$. Moreover, we will write $\mathbb{F}_n$ to denote the free group of rank n.

A fundamental trait of free groups is the fact that, in a way, they contain all the information about all existing groups. We make this statement precise below.

Theorem 4.14. *Every group G is a quotient of an appropriate free group. That is, for every group G, there exists a cardinal n and a normal subgroup $N \trianglelefteq \mathbb{F}_n$ such that $G \cong \mathbb{F}_n/N$.*

Proof. Let $X \subset G$ be a set of generators of G (we can always take $X = G$) and let $n = \#X$ be its cardinal. We consider the free group $\mathbb{F}_X$. If we let $\varphi : X \to G$ be the inclusion map, by the universal property, there exists a unique morphism of groups $\tilde{\varphi} : \mathbb{F}_X \to G$ such that $[x]\tilde{\varphi} = x$, for every $x \in X$. Given that X generates G, $\tilde{\varphi}$ is surjective and, by the First Isomorphism Theorem, $\ker \tilde{\varphi}$ is a normal subgroup of $\mathbb{F}_X$ satisfying that $\mathbb{F}_X / \ker \tilde{\varphi} \cong \mathrm{Im}(\tilde{\varphi}) = G$. □

Relying on Theorem 4.14, we give next the definition of presentation of a group, which is a compact way of encapsulating a group.

Definition 4.15. Let G be a group. A *presentation* for G is a pair (X, R) where X is an alphabet, R is a subset of $\mathbb{F}_X$ and $G \cong \mathbb{F}_X/\langle\langle R\rangle\rangle$. We usually write $G = \langle X|R\rangle$ and we call the elements of X the *generators* given by the presentation of G and, the elements in R, *relators* of the presentation of G.

Remark 4.16. Observe that the free group with basis X admits the presentation $\mathbb{F}_X = \langle X|-\rangle$, which is called the *canonical presentation* for $\mathbb{F}_X$.

Remark 4.17. Notice also that the presentation of a group is not unique. For example, $\langle a|-\rangle$ and $\langle a, b|ab^{-1}\rangle$ are both valid presentations for the group $\mathbb{Z}$.

Definition 4.18. We say that a presentation $\langle X|R\rangle$ is *finite* if both X and R are finite sets. Moreover, a group is said to be *finitely presented* if it admits a finite presentation.

Since finite presentations are finite ways to encode groups (which might be infinite), they are a specially convenient way of representing groups for algorithmic problems (see Section 2.2).

As a last piece of information about presentations, in the following result we state how a presentation for a direct product can be obtained from the presentations of its factors.

Proposition 4.19. *Let H and K be groups with respective presentations $\langle S_1|R_1\rangle$ and $\langle S_2|R_2\rangle$. Then $\langle S_1 \cup S_2|R_1 \cup R_2 \cup \{[s_1, s_2] : s_1 \in S_1, s_2 \in S_2\}\rangle$ is a presentation for the direct product $H \times K$.*

4.2 Stallings automata

In this section, we develop the Stallings theory representing subgroups of free groups as automata. The crucial idea is to understand the elements in a subgroup as labels of closed paths in these automata. We will develop this idea formally next, starting with some definitions that establish some basic concepts and notation regarding these mathematical objects.

Definition 4.20. Let X be an alphabet. A *(pointed) X-automaton* is a tuple $\Gamma = (V, E, \iota, \tau, \ell, \mathbf{b})$, where V and E are disjoint sets and V is nonempty, $\iota, \tau : E \longrightarrow V$ and $\ell : E \longrightarrow X$ are functions and $\mathbf{b} \in V$. The sets $V = V\Gamma$ and $E = E\Gamma$ are called the set of *vertices* and the set of *directed edges* or *arcs* of Γ, respectively. The function ι assigns to each edge $e \in E$ its *origin* $e\iota \in V$, while τ assigns its *end* $e\tau \in V$. The function ℓ assigns a label $(e)\ell \in X$ to each edge. The distinguished vertex $\mathbf{b}$ is called the *basepoint* of the X-automaton. If $e\iota = p$, $e\tau = q$ and $(e)\ell = x$, we write $e \equiv p \xrightarrow{x} q$ and we say that e is an x-arc. Finally, if we forget about the labelling and the basepoint, what remains is a directed graph (also called digraph) which we will call the *underlying digraph* of the automaton.

Definition 4.21. A *walk* of *length s* in an X-automaton Γ is a finite sequence $\gamma = p_0 e_1 p_1 \cdots e_s p_s$ with $p_i \in V\Gamma$, $e_i \in E$, $e_i\iota = p_{i-1}$ and $e_i\tau = p_i$ for $i = 1, \ldots, s$. We say p_0 and p_s are the *origin* and the *end* of γ respectively and we denote this by $\gamma\iota = p_0$ and $\gamma\tau = p_s$. We also say that γ is a walk from p_0 to p_s and we denote this by $\gamma : p_0 \rightsquigarrow p_s$. If $p_0 = p_s = p$, we say that γ is a *closed walk* and we also call it a *p-walk*. Note that walks of length 0 (called *trivial walks*) correspond to vertices in Γ.

Definition 4.22. An *involutive X-automaton* Γ is an $X^{\pm}$-automaton with a labelled involution on its arcs; i.e., to every arc $e \equiv p \xrightarrow{x} q$ we associate a unique arc $e^{-1} \equiv q \xrightarrow{x^{-1}} p$ such that $e^{-1} \neq e$ and $(e^{-1})^{-1} = e$. We say that e^{-1} is the *inverse* of e. We say that $E^+\Gamma = \{e \in E\Gamma : (e)\ell \in X\}$ is the set of *positive arcs* of Γ and that $E^-\Gamma = \{e \in E\Gamma : (e)\ell \in X^{-1}\}$ is the set of *negative arcs* of Γ. The *positive part* of an involutive automaton Γ is the automaton Γ^+ obtained after deleting all the negative arcs from Γ. If we remove the labelling and the basepoint of Γ, we obtain an involutive digraph and, if we identify the pairs of arcs which are inverse of each other (constituting an *edge*) we have the so-called *underlying graph* of Γ.

Remark 4.23. Note that an involutive automaton is fully characterised by its positive (or negative) part. We will make use of Γ^+ in order to represent the automaton Γ, following the implicit convention that the positive arcs $e \equiv p \xrightarrow{x} q$ can be crossed backwards (from q to p) reading the inverse label x^{-1}.

Let us now give some notions about graphs. These concepts refer to graphs like the ones we obtain when considering the underlying graph of an involutive automaton, but by extension we will use the same terms to refer to the involutive automata from which these graphs come from.

A *path* is a sequence of vertices and edges $v_0 e_0 v_1 e_1 \cdots e_{k-2} v_{k-1}$ without repetitions such that $v_i \in V\Gamma, e_i \in E\Gamma$, $e_i\iota = v_i$ and $e_i\tau = v_{i+1}$. If $P = v_0 e_0 v_1 e_1 \cdots e_{k-2} v_{k-1}$ is a path and $k \geq 3$, then the graph resulting from adding an edge between v_{k-1} and v_0 to P is a *cycle*.

A notion which will be of importance later on is that of connectivity. A non-empty graph Γ is called *connected* if any two of its vertices are linked by a path in Γ. A maximal connected subgraph of Γ is called a *connected component* of Γ. An edge of a graph Γ whose removal results in a disconnected graph is called a *bridge*.

A graph which does not contain any cycles is called a *forest* and a connected forest is called a *tree*. The *degree* of a vertex is the number of its incident edges. The vertices of degree 1 in a tree are its *leaves*. If T is a tree and u and v are two of its vertices, we say that v is at *T-distance d* of u if the length of the only path in T joining u and v has d edges. An edge e in the tree T is at T-distance d of u if its incident vertex closest to u is at T-distance d of u. Given a graph Γ, a *spanning forest* (*spanning tree*) of Γ is a subgraph of Γ which is a forest (tree) and whose vertices are all the vertices of Γ. The *graphical rank* of a graph Γ, $\mathrm{rk}(\Gamma)$, is the number of arcs outside a spanning forest. If Γ is finite, then

$$\mathrm{rk}(\Gamma) = \#E\Gamma - \#V\Gamma + \#C\Gamma,$$

where $C\Gamma$ is the set of connected components of Γ.

Remark 4.24. We will understand that the graphical rank of an automaton is the graphical rank of its underlying graph. Similarly, the degree of a vertex of an automaton will be that of the corresponding vertex in its underlying graph.

After giving these few notions for graphs, let us now go back to involutive automata. The labelling on the arcs of an involutive automaton Γ can be naturally extended to an $(X^{\pm})^*$-labelling of walks in the automaton simply by concatenating the corresponding labels of the arcs in the walk: if $\gamma = p_0 e_1 p_1 \cdots e_s p_s$ is a nontrivial walk, we define its label as $(\gamma)\ell = (e_1)\ell \cdots (e_s)\ell \in (X^{\pm})^*$. Moreover, we define its reduced label as $(\gamma)\overline{\ell} := \overline{(\gamma)\ell} \in \mathbb{F}_X$. The label and reduced label of a trivial walk are the trivial elements in the monoid $(X^{\pm})^*$ and the group $\mathbb{F}_X$ respectively (both will be denoted by 1). If $(\gamma)\ell = w \in (X^{\pm})^*$, we say that the walk γ *reads* w or that the word w *labels* the walk γ, and we write $\gamma : p_0 \overset{w}{\rightsquigarrow} p_s$.

Let Γ be an involutive and connected X-automaton and let $p \in V\Gamma$. One can observe that the set of reduced labels of p-walks in Γ,

$$\langle \Gamma \rangle_p = \{(\gamma)\overline{\ell} : \gamma \text{ is a } p\text{-walk of } \Gamma\},$$

is a subgroup of $\mathbb{F}_X$: indeed, the trivial element is a label for a trivial p-walk; the reduced label of the concatenation of two elements in $\langle \Gamma \rangle_p$ is the reduced label of the p-walk obtained from reading one p-walk after the other; and the inverse of the reduced label of a p-walk is the reduced label of the inverse walk (the walk with the reversed sequence) of this p-walk.

Definition 4.25. This subgroup $\langle \Gamma \rangle_p$ is called the *subgroup recognised by* Γ *at vertex* p. The subgroup recognised by Γ at the basepoint, $\langle \Gamma \rangle_{\mathbf{b}}$, will be denoted simply by $\langle \Gamma \rangle$ and we will call it the *subgroup recognised by* Γ.

The previous definition establishes a map between automata and subgroups of the free group, namely,

$$\begin{array}{rcl} \{\text{involutive } X\text{-automata}\} & \to & \{\text{subgroups of } \mathbb{F}_X\} \\ \Gamma & \mapsto & \langle \Gamma \rangle. \end{array} \tag{4}$$

Let us now remark that the map (4) is exhaustive. For any subgroup H of $\mathbb{F}_X$, we can consider a (possibly infinite) generating set S. Below, we present an automaton that recognises the subgroup H.

With the notation above, given an element (or reduced word) $w = x_{i_1} x_{i_2} \cdots x_{i_p} \in S$, the X-automaton consisting of the directed cycle reading the word w is called the *petal automaton* of w (see Figure 1). The

X-automaton obtained by identifying the basepoints of the different petal automata of all the words in S is called the *flower automaton* of S and is denoted by $\mathrm{Fl}(S)$ (see Figure 2).

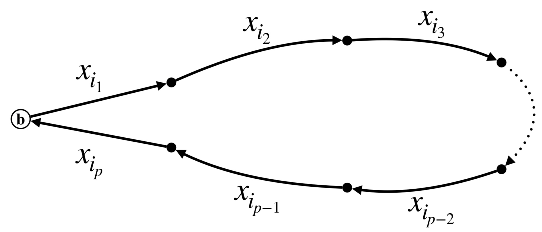

Figure 1: Petal automaton associated to the word $w = x_{i_1} x_{i_2} \cdots x_{i_p}$.

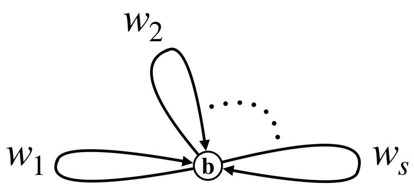

Figure 2: Flower automaton of $S = \{w_1, w_2, \ldots, w_s\}$

It is clear that $\mathrm{Fl}(S)$ is an automaton recognising H. Observe that an element $h \in H$ will be a product of the generators in S and their inverses. If we consider the concatenation of the **b**-walks around the petals of each of these generators in the same order that they appear in the expression of h as a product of elements of S, we obtain a **b**-walk whose label is h (notice that the orientation of the **b**-walk around each petal must be in concordance with the exponent $+1$ or -1 of each generator in the expression for h). Conversely, **b**-walks in the flower automaton have as reduced labels elements of the subgroup H, since S is a generating set. In consequence, the subgroup recognised by $\mathrm{Fl}(S)$ is H and we conclude that the map (4) is exhaustive. However, this map is not a bijection. For example, considering different generating sets gives different automata recognising the same subgroup.

With the goal of distinguishing a unique witness among all the automata recognising the same subgroup, we now focus on the sources of redundancy in the map (4) and present some properties of automata which will be relevant for the bijection.

Definition 4.26. Let Γ be an X-automaton. A vertex $p \in V\Gamma$ is *saturated* if for every letter $x \in X$ there is at least one x-arc with origin at p. An X-automaton Γ is said to be *saturated* if all of its vertices are saturated.

Remark 4.27. In the case of an involutive X-automaton (which is, in particular, an $X^{\pm}$-automaton), being saturated translates into having at least one x-arc going in and out of each vertex for each $x \in X$.

Definition 4.28. An X-automaton Γ is *deterministic at* a vertex $p \in V\Gamma$ if no two arcs with the same label depart from p (i.e., if $e\iota = e'\iota$ and $(e)\ell = (e')\ell$ implies that $e = e'$). We say that Γ is *deterministic* if it is deterministic at every vertex.

Definition 4.29. We say that a walk γ presents *backtracking* if it has two successive arcs inverse of each other. We say that γ is *reduced* if it presents no backtracking.

Definition 4.30. Let Γ be an involutive X-automaton. We say that a vertex in Γ is *alive* if it belongs to some reduced $\mathbf{b}$-walk, otherwise we say it is *dead*. Moreover, Γ is said to be *core* if it has no dead vertices. The *core of* Γ, denoted by $\mathrm{core}(\Gamma)$, is the maximal core subautomaton of Γ (containing the basepoint).

It is sometimes convenient to understand coreness in an alternative way. In order to present it, we need the following definition.

Definition 4.31. If the underlying graph of an automaton Γ can be obtained by identifying a vertex of some graph Δ with a vertex of some disjoint non-trivial tree T, then we say that T is a *hanging tree* of Γ.

Remark 4.32. An automaton will be core if it is connected and has no hanging trees which do not contain the basepoint. As a consequence, $\mathrm{core}(\Gamma)$ is what remains after choosing the connected component of Γ which contains the basepoint $\mathbf{b}$ and removing all the hanging trees which do not contain $\mathbf{b}$.

It is important to notice that $\langle \mathrm{core}(\Gamma) \rangle = \langle \Gamma \rangle$.

As we will see, automata which are both deterministic and core are the appropriate witnesses we are looking for.

Definition 4.33. An involutive X-automaton Γ is said to be *reduced* if it is deterministic and core.

Of course, in order to convert the map (4) into a bijection, we must distinguish reduced automata up to isomorphism. We formalise this notion below.

Definition 4.34. Let $\Gamma = (V, E, \iota, \tau, \ell, \mathbf{b})$ and $\Gamma' = (V', E', \iota', \tau', \ell', \mathbf{b}')$ be two X-automata. A *homomorphism of automata* from Γ to Γ' is a function $\theta : V \longrightarrow V'$ satisfying that $(\mathbf{b})\theta = \mathbf{b}'$ and that, for every pair of vertices $p, q \in V\Gamma$ and every $x \in X$, if there is an arc $p \xrightarrow{x} q$ in Γ then there is an arc $p\theta \xrightarrow{x} q\theta$ in Γ'.

The following result is key to establish the bijection, as it will later ensure that reduced automata recognising the same group will have to be the same up to isomorphism.

Proposition 4.35. *Let Γ and Γ' be reduced X-automata. Then, $\langle \Gamma \rangle \leqslant \langle \Gamma' \rangle$ if and only if there is a homomorphism $\Gamma \to \Gamma'$ and, in this case, the homomorphism is unique.*

Proof. The proof of this technical result can be found in [10, Proposition 42]. □

Corollary 4.36. *Two reduced X-automata recognise the same subgroup if and only if they are isomorphic (there exists a bijective homomorphism of automata between them). That is, if Γ and Γ' are reduced X-automata, then*

$$\langle \Gamma \rangle = \langle \Gamma' \rangle \Leftrightarrow \Gamma \cong \Gamma'.$$

Proof. If $\Gamma \cong \Gamma'$, we have homomorphisms $\phi : \Gamma \to \Gamma'$ and $\phi^{-1} : \Gamma' \to \Gamma$, so $\langle \Gamma \rangle \leqslant \langle \Gamma' \rangle$ and $\langle \Gamma' \rangle \leqslant \langle \Gamma \rangle$ by Proposition 4.35 and we conclude that $\langle \Gamma \rangle = \langle \Gamma' \rangle$.

Reciprocally, suppose $\langle \Gamma \rangle = \langle \Gamma' \rangle$. Equivalently, we have that $\langle \Gamma \rangle \leqslant \langle \Gamma' \rangle$ and $\langle \Gamma' \rangle \leqslant \langle \Gamma \rangle$, which implies (using again Proposition 4.35) that there exist homomorphisms $\phi : \Gamma \to \Gamma'$ and $\psi : \Gamma' \to \Gamma$. Notice that the compositions $\phi\psi$ and $\psi\phi$ are homomorphisms from Γ and Γ' to themselves respectively. Since it is clear that the identity is a homomorphism from any automata to itself, the unicity from Proposition 4.35 guarantees that $\phi\psi$ and $\psi\phi$ are the identity of Γ and Γ' respectively. Thus, $\Gamma \cong \Gamma'$. □

We will now define the Schreier automaton for a subgroup and, from it, the Stallings automaton for a subgroup, which will help us make the bijection in Theorem 4.44 more explicit.

Definition 4.37. Let G be a group, H a subgroup of G and $S \subset G$ a set of generators for G. The *(right) Schreier automaton of H with respect to S*, denoted by $\mathrm{Sch}_G(H, S)$ or $\mathrm{Sch}(H, S)$ if the group is clear by the context, is the S-automaton with set of vertices $H \backslash G$ (the set of right cosets of G mod H), an arc $Hg \xrightarrow{s} Hgs$ for every coset $Hg \in H \backslash G$ and every element $s \in S^{\pm}$, and the coset H as basepoint.

Since the vertices of the Schreier automaton are the cosets of the subgroup H, the index of H in G will be the number of vertices in this automaton. Some other of its properties are collected in the next proposition.

Proposition 4.38. *If H is a subgroup of $\mathbb{F}_X$, the following properties hold:*

(i) $Sch(H, X)$ is an involutive, deterministic and saturated X-automaton;

(ii) $Sch(H, X)$ is connected, but it may not be core;

(iii) $\langle Sch(H, X) \rangle = H$.

All points in the previous proposition are quite transparent, but it is worth providing an example to show that the Schreier automaton is not necessarily core.

Example 4.39. If we consider the subgroup $H = \langle x \rangle$ in $\mathbb{F}_2 = \langle x, y \mid - \rangle$, we have that $\mathrm{Sch}(H, \{x, y\})$ consist of an x-loop at the basepoint together with two hanging trees joined to the basepoint by respective b-arcs. This automaton is not core, due to the presence of hanging trees not containing the basepoint.

We will now add coreness to the Schreier automaton to reach a reduced automaton.

Definition 4.40. Let H be a subgroup of $\mathbb{F}_X$. The *Stallings automaton of H with respect to X*, denoted by $\mathrm{St}(H, X)$, is the core of $\mathrm{Sch}(H, X)$, that is $\mathrm{St}(H, X) = \mathrm{core}(\mathrm{Sch}(H, X))$.

The following result makes clearer the relation between the Schreier and the Stallings automata.

Proposition 4.41. *Let H be a subgroup of $\mathbb{F}_X$. Then, $St(H, X)$ is saturated iff $St(H, X) = Sch(H, X)$ iff $Sch(H, X)$ is core.*

Proof. To see this, we must simply take into account that $\mathrm{Sch}(H, X)$ is always saturated, $\mathrm{St}(H, X)$ is always core and $\mathrm{St}(H, X) = \mathrm{core}(\mathrm{Sch}(H, X))$. □

Before stating the result (Theorem 4.44) that gives us the bijection we are looking for, let us introduce certain transformations that will allow us to actually compute the Stallings automaton of a subgroup when it is given by a finite set of generators.

Definition 4.42. Let Γ be an involutive X-automaton and let e and f be two arcs breaking the determinism of Γ, that is, $e\iota = f\iota$ and $(e)\ell = (f)\ell$, but $e \neq f$. We define a *Stallings folding*, and denote it by $\Gamma \curvearrowright \Gamma'$, as the transformation which consists in identifying the arcs e and f (as well as their corresponding inverses) in Γ. If the arcs e and f are not parallel (i.e., $e\tau \neq f\tau$), we will refer to it as an *open folding* (see Figure 3); otherwise, we will say it is a *closed folding* (see Figure 4).

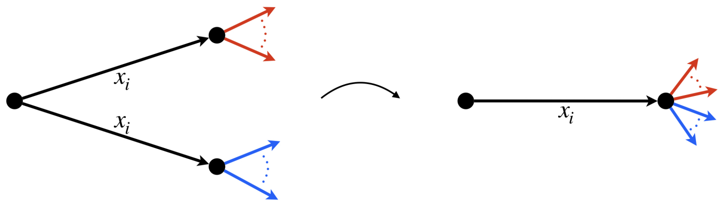

Figure 3: Open folding.

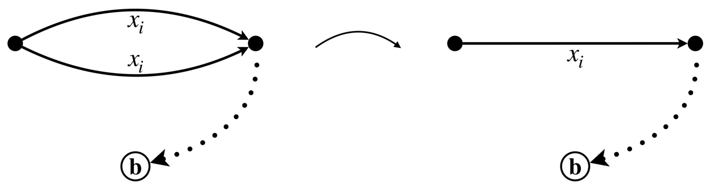

Figure 4: Closed folding.

Since the arcs involved in a Stallings folding have the same label, one can read the same reduced words in Γ before and after performing a Stallings folding. This observation gives the following lemma.

Lemma 4.43. *If $\Gamma \curvearrowright \Gamma'$ is a Stallings folding, then $\langle \Gamma \rangle = \langle \Gamma' \rangle$.*

All the previous concepts and results of this section crystallise into the following theorem, which gives a bijection between certain kind of automata and subgroups of the free group.

Theorem 4.44 (**Stallings**)**.** *The function*

$$\begin{array}{rcl} \{\textit{(isomorphic classes of) reduced } X\textit{-automata}\} & \to & \{\textit{subgroups of } \mathbb{F}_X\} \\ \Gamma & \mapsto & \langle \Gamma \rangle \end{array} \tag{5}$$

is a bijection with inverse $St(H, X) \hookleftarrow H$. Furthermore, finitely generated subgroups correspond precisely to finite automata and, in this case, the bijection is algorithmic.

Proof. Both maps are well-defined: indeed, for every Γ, $\langle \Gamma \rangle$ is a subgroup of $\mathbb{F}_X$; and $\mathrm{St}(H, X)$ is a reduced X-automaton for every $H \leqslant \mathbb{F}_X$. Also, the maps are inverse of each other: on the one hand, $\langle \mathrm{St}(H, X) \rangle = H$ because $\mathrm{Sch}(H, X)$ already recognised H and taking the core does not change the recognised subgroup; on the other hand, for Γ reduced, Corollary 4.36 ensures that $\mathrm{St}(\langle \Gamma \rangle, X) = \Gamma$.

We will now show that, if a subgroup H is given by a finite number of generators, then the map (5) is algorithmic. Suppose S is the given finite set of generators of $H \leqslant \mathbb{F}_X$. We can build $\mathrm{Fl}(S)$, the flower automaton of S. This automaton recognises H and it is core by construction (since we can assume the generators to be reduced words). However, this flower automaton may fail to be deterministic at the basepoint, since we can have two different generators starting by the same letter. To fix this, we can perform a series of Stallings foldings of the pairs of arcs which break the determinism.

By Lemma 4.43, we know that these Stallings foldings do not change the subgroup recognised by the automaton. During this process of folding, new nondeterministic situations to fix may arise. However, notice that with each folding we perform, the number of arcs in the automaton decreases by one and, since we start with a finite number of arcs because the initial automaton is finite, this folding process will eventually finish. As a result, we will obtain a deterministic X-automaton recognising H. Moreover, since the folding process can only produce hanging trees containing the basepoint, the final object is still core, and hence a reduced X-automaton recognising H, which must be $\mathrm{St}(H, X)$ (because we have already shown that (5) is a bijection). We emphasise that the bijectivity of (5) implies that the result of the folding process is independent of the order in which the foldings are performed as well as of the initial set of generators of H one starts with.

Since we have shown that one of the directions is algorithmic and we have a bijection, we also have that the map is algorithmic in the other direction. □

The following example illustrates how to perform Stallings foldings so as to obtain a Stallings automaton.

Example 4.45. Consider the subgroup $H = \langle x^2yx^{-1}, xy^{-1}xy \rangle \leqslant \mathbb{F}_2 = \langle x, y \mid - \rangle$. Figure 5 summarises a sequence of Stallings foldings which starts with the flower automaton of $S = \{x^2yx^{-1}, xy^{-1}xy\}$ and ends with $\mathrm{St}(H)$.

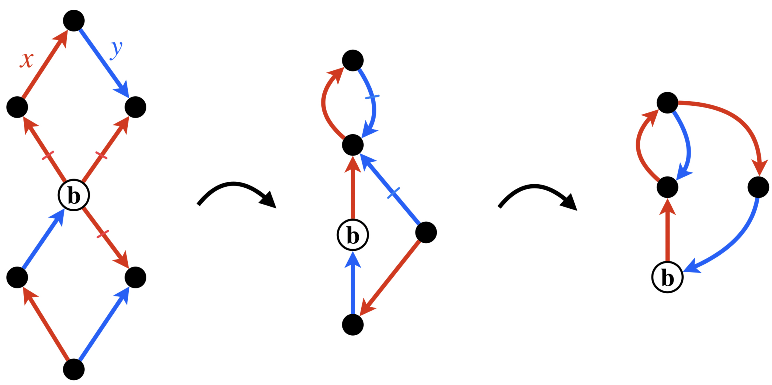

Figure 5: Sequence of Stallings foldings.

The following result is quite relevant because it gives an efficient way to compute the direction $\Gamma \mapsto \langle \Gamma \rangle$ of bijection (5). Moreover, it shows that an automaton encodes a basis for the group it recognises and that the rank of this subgroup can be interpreted graphically under certain assumptions.

Theorem 4.46. *Let Γ be a connected, pointed and involutive X-automaton, let T be a spanning tree of Γ, and let*

$$B_T = \{(\mathbf{b} \overset{T}{\rightsquigarrow} p \overset{e}{\to} q \overset{T}{\rightsquigarrow} \mathbf{b})\overline{\ell} : e \in E^+\Gamma \setminus ET\}$$

bet the set of reduced labels of positive T-petals (where $\overset{T}{\rightsquigarrow}$ means that the arcs in the corresponding part of the walk belong to T). Then,

(i) B_T is a generating set for $\langle \Gamma \rangle$,

(ii) if Γ is deterministic, then $\langle \Gamma \rangle$ is free with basis B_T,

(iii) if Γ is reduced, then $\langle \Gamma \rangle$ is finitely generated if and only if Γ is finite and, then,

$$rk(\langle \Gamma \rangle) = 1 - \#V\Gamma + \#E^+\Gamma = rk(\Gamma).$$

Proof. We will give an idea of the proof just for the first item (the rest of the proof can be seen in detail in [10, Proposition 54]). Let $w = (\gamma)\overline{\ell} \in \langle \Gamma \rangle$, where γ is a reduced $\mathbf{b}$-walk. We may write:

$$\gamma : \mathbf{b} \overset{T}{\rightsquigarrow} \bullet \xrightarrow{e_1^{\epsilon_1}} \bullet \overset{T}{\rightsquigarrow} \bullet \xrightarrow{e_2^{\epsilon_2}} \bullet \overset{T}{\rightsquigarrow} \bullet \cdots \bullet \overset{T}{\rightsquigarrow} \bullet \xrightarrow{e_l^{\epsilon_l}} \bullet \overset{T}{\rightsquigarrow} \mathbf{b},$$

where $e_1, \dots, e_l \in E^+\Gamma \backslash ET$ and $\epsilon_j = \pm 1$. And we can also consider:

$$\gamma' : \mathbf{b} \overset{T}{\rightsquigarrow} \bullet \xrightarrow{e_1^{\epsilon_1}} \bullet \overset{T}{\rightsquigarrow} \mathbf{b} \overset{T}{\rightsquigarrow} \bullet \xrightarrow{e_2^{\epsilon_2}} \bullet \overset{T}{\rightsquigarrow} \mathbf{b} \cdots \mathbf{b} \overset{T}{\rightsquigarrow} \bullet \xrightarrow{e_l^{\epsilon_l}} \bullet \overset{T}{\rightsquigarrow} \mathbf{b}.$$

It is clear that $w = (\gamma)\overline{\ell} = (\gamma')\overline{\ell} \in \langle B_T \rangle$. □

An immediate consequence of Theorem 4.46, is the following widely-known result.

Theorem 4.47. *(Nielsen-Schreier) Every subgroup of a free group is free.*

The theory of Stallings automata we have seen so far has many applications. For example, it can be used to derive results like the fact that bases of subgroups of free groups are generating sets of minimum cardinality (see [10, Proposition 72]) or to prove that $\mathbb{F}_n$ is Hopfian (see [10, Proposition 73]), that is, every exhaustive endomorphism of $\mathbb{F}$ is automatically injective. Another application of Stallings theory is to show that the membership problem is solvable for free groups (see [10, Proposition 69]). To see many other applications of this theory, we refer the interested reader to [8].

In the next section we will apply this theory to study the index of subgroups of free groups and, in particular, to count the number of subgroups of a given finite index.

4.3 Studying the index of subgroups in free groups

In this section, we will use Stallings automata to study questions related to the index of subgroups of free groups, including the finite index problem and the derivation of a formula giving the number of subgroups of a certain finite index in the free group. To start, we give a result which characterises finite index subgroups of free groups.

Proposition 4.48. *Let H be a finitely generated subgroup of a free group $\mathbb{F}_X$. Then, the index $|\mathbb{F}_X : H|$ is finite if and only if $St(H)$ is saturated and, in this case, $|\mathbb{F}_X : H| = \#VSt(H)$.*

Proof. Recall that the vertices of the Schreier automaton of H are the right cosets of H in $\mathbb{F}_X$. Then, if $|\mathbb{F}_X : H|$ is finite, $\mathrm{Sch}(H)$ is finite. If $\mathrm{St}(H)$ were not saturated, we would have to add to it hanging trees (with infinite vertices) at the vertices with a missing x-arc for some $x \in X^{\pm}$ to obtain $\mathrm{Sch}(H)$, which would mean that $\mathrm{Sch}(H)$ is infinite, yielding a contradiction. So $\mathrm{St}(H)$ must be saturated. Conversely, if $\mathrm{St}(H)$ is saturated, then $\mathrm{St}(H) = \mathrm{Sch}(H)$ by Proposition 4.41. Then, $\mathrm{Sch}(H)$ has a finite number of vertices because $\mathrm{St}(H)$ is finite due to the fact that H is finitely generated. Thus, $|\mathbb{F}_X : H|$ is finite. In consequence, the index $|\mathbb{F}_X : H|$ is finite if and only if $\mathrm{St}(H)$ is saturated and, in this case, since the Stallings and the Schreier automata of H are the same, we have that $|\mathbb{F}_X : H| = \#V\mathrm{St}(H)$. □

As a first consequence of this result, we may observe that $\mathbb{F}_X$ has a finite number of subgroups with a given finite index k, since there is a finite number of Stallings automata with k vertices. Later, in Theorem 4.55, we will obtain a formula to determine that number precisely. A second consequence is that we can solve $FIP(\mathbb{F}_X)$ for $\mathbb{F}_X$ a free group.

Corollary 4.49. *The finite index problem is solvable for free groups.*

Proof. The decidability of $FIP(\mathbb{F}_X)$ is a consequence of Proposition 4.48 and of the computability of the Stallings automaton in the finitely generated case. For the computation of a transversal when H is of finite index, take into account that $\mathrm{St}(H)$ is saturated and finite. Notice that any walk γ in $\mathrm{St}(H) = \mathrm{Sch}(H)$ starting at $\mathbf{b}$ satisfies that $\gamma\tau = Hw$, where $w = (\gamma)\ell \in \mathbb{F}_X$. Therefore, we can consider a family of representatives of the right cosets mod H simply by taking walks from the basepoint to each of the vertices of $\mathrm{St}(H)$ and taking their labels. □

We give below a formula relating the index and the rank of a subgroup of a free group, which will be used later on in Theorem 5.43.

Theorem 4.50. *(Schreier's Index Formula) Let $\mathbb{F}_n$ be a free group of rank n and let H be a finite index subgroup of $\mathbb{F}_n$. Then*

$$rk(H) - 1 = |\mathbb{F}_n : H|(n-1). \tag{6}$$

In particular, the subgroup H is finitely generated if and only if the ambient rank n is finite.

Proof. If H has finite index, then $\mathrm{St}(H)$ is saturated (so it is $2n$-regular) and $\#V\mathrm{St}(H) < \infty$. Therefore $\mathrm{rk}(\mathrm{St}(H)) < \infty$ (that is, there is a finite number of arcs outside any spanning tree) if and only if $n < \infty$. In particular, if n is infinite, then $\mathrm{rk}(H) = \infty$ and the formula (6) holds.

Let us suppose now that $n < \infty$. We know that H is finitely generated, so $\mathrm{St}(H)$ is finite. Let T be a spanning tree of $\mathrm{St}(H)$, then H has a basis with $\#(E^+\mathrm{St}(H)\setminus ET)$ elements. Taking this into account, we have

$$\begin{aligned} \mathrm{rk}(H) - 1 &= \#(E^+\mathrm{St}(H)\setminus ET) - 1 = \#E^+\mathrm{St}(H) - \#ET - 1 \\ &= \#E^+\mathrm{St}(H) - \#VT = n\#V\mathrm{St}(H) - \#V\mathrm{St}(H) \\ &= |\mathbb{F}_n : H|(n-1), \end{aligned}$$

where the second to last equality comes from the equality $2n\#V\mathrm{St}(H) = 2\#E^+\mathrm{St}(H)$, which is obtained by adding the degrees of all of the vertices. □

In the remaining of this section, we will obtain a recursive formula that gives the number of subgroups of a given finite index in a free group of finite rank. This result was initially obtained by Marshall Hall Jr. in a paper (see [15]) published in 1949. Here we revisit this result using the language of Stallings automata (whose theory was introduced in the previous section) in order to represent subgroups of the free group, instead of using a Schreier system and a certain function to do so (as it was done originally in [15]).

Taking into account the bijection presented in Theorem 4.44 and the characterisation of finite index subgroups given in Proposition 4.48, one can establish the following bijection:

$$\begin{array}{ccc} \mathcal{S}_k(X) & \to & \mathcal{H}_k(X) \\ \Gamma & \mapsto & \langle \Gamma \rangle, \end{array} \tag{7}$$

where $\mathcal{S}_k(X)$ denotes the set of (isom. classes of) saturated Stallings automata with k vertices and $\mathcal{H}_k(X)$ denotes the set of subgroups of index k of $\mathbb{F}_X$.

So, our task is to count the number of reduced and saturated X-automata with k vertices (taking $X = \{x_1, \ldots, x_n\}$ to be a set of n elements). In order to do so, it is convenient to use an alternative representation of Stallings automata in which the vertices of the automata are labelled. Propositions 4.52 and 4.53 give a one to one correspondence between the automata with labelled vertices and tuples of permutations, which will be easier to count. However, considering labelled automata raises the issue that, when counting subgroups, we will have to take into account that automata which are identical but for a change in the labels of the vertices actually represent the same subgroup.

We introduce now some notation that will be used in the remaining of this section. Firstly, we will denote by S_k the set of permutations of a set of k elements $V = \{v_1, v_2, \dots, v_k\}$. Secondly, for a fixed set $X = \{x_1, \dots, x_n\}$ we will denote by $\tilde{\mathcal{A}}_k(X)$ the set of all X-automata which are deterministic and saturated and which have k *labelled* vertices.

Remark 4.51. We make two observations:

(i) The automata in $\tilde{\mathcal{A}}_k(X)$ have no hanging trees. Indeed, if there was one, it would have to be finite and there would be a leaf, in contradiction with the fact that these automata are saturated (all vertices should have even degree).

(ii) The automata in $\tilde{\mathcal{A}}_k(X)$ need not be connected.

Proposition 4.52. *Let $X = \{x_1, \dots, x_n\}$ and $k \in \mathbb{N}$. Then there exists a bijection between $(S_k)^n$ and $\tilde{\mathcal{A}}_k(X)$.*

Proof. We will start by giving a map $\phi : (S_k)^n \to \tilde{\mathcal{A}}_k(X)$. Let $P = (\pi_1, \dots, \pi_n)$ be a tuple of permutations of a set $V = \{v_1, \dots, v_k\}$. We can build an X-automaton $\tilde{\Gamma}$ with (labelled) vertex set V, taking v_1 to be the basepoint and defining the set of arcs as follows: for each $i \in [n]$ and $j \in [k]$, if $(v_j)\pi_i = v_l$, add the edge $v_j \xrightarrow{x_i} v_l$ to $\tilde{\Gamma}$. This automaton satisfies that:

(i) It is deterministic: notice that $\tilde{\Gamma}$ is deterministic by construction, since π_i has a unique image for every element of V.

(ii) It is saturated: it is clear that for each label x_i we have an x_i-arc going out of each vertex and the fact that each π_i is surjective guarantees that there is also an x_i-arc arriving at each vertex.

Therefore, we have that $\tilde{\Gamma} \in \tilde{\mathcal{A}}_k(X)$ and we can set $(P)\phi = \tilde{\Gamma}$.

For the other direction of the bijection, let $\tilde{\Gamma} \in \tilde{\mathcal{A}}_k(X)$ with set of vertices $V = \{v_1, v_2, \dots, v_k\}$. Fix $i \in [n]$ and consider $j \in [k]$. Since $\tilde{\Gamma}$ is deterministic and saturated, there is a unique arc starting at vertex v_j with label x_i. Let us denote the end vertex of this arc by $v_j x_i$. Now, for every $x_i \in X$, we may define the map

$$\begin{array}{rccc} \pi_i : & V & \to & V \\ & v_j & \mapsto & v_j x_i, \end{array}$$

which is bijective because V is a finite set and we can show that the map is injective. Indeed, if we had $v_j x_i = v_l x_i$ for some $v_j, v_l \in V$ with $v_i \neq v_l$, there would be two different arcs labelled with x_i arriving at vertex $v_j x_i = v_l x_i$, contradicting the fact that $\tilde{\Gamma}$ is deterministic. Thus π_i belongs to $\mathrm{Sym}(V)$. If we define $(\tilde{\Gamma})\phi^{-1} = (\pi_1, \dots, \pi_n)$ for every $\tilde{\Gamma} \in \tilde{\mathcal{A}}_k(X)$, it is clear that ϕ^{-1} is indeed the inverse of ϕ. □

Proposition 4.53. *Let $X = \{x_1, \dots, x_n\}$. Then there exists a bijection between the subset of automata in $\tilde{\mathcal{A}}_k(X)$ which are connected and the set of tuples $P = (\pi_1, \dots, \pi_n)$ with $\pi_i \in Sym(V), \forall i \in \{1, \dots, n\}$, such that the action of the group $G = \langle P \rangle = \langle \pi_1, \dots, \pi_n \rangle$ on V is transitive.*

Proof. We will show that the restriction of the bijection ϕ given in the proof of Proposition 4.52 to the set

$$S = \{(\pi_1, \dots, \pi_n) \in (S_k)^n : \text{the action of } \langle \pi_1, \dots, \pi_n \rangle \text{ on } V \text{ is transitive}\}$$

is a bijection onto its image, which is nothing but the set of elements in $\tilde{\mathcal{A}}_k(X)$ which are connected.

Take $P = (\pi_1, \dots, \pi_n) \in S$ and consider two vertices $v_j, v_l \in V$ of the automaton $\tilde{\Gamma} = (P)\phi$. Given that the action of $G = \langle \pi_1, \dots, \pi_n \rangle$ on V is transitive, there exists $\sigma = \pi_{i_1}\pi_{i_2} \cdots \pi_{i_s} \in G$ such that $(v_j)\sigma = v_l$. By the way in which the automaton $\tilde{\Gamma}$ is built, this translates into a walk from v_j to v_l labelled by $x_{i_1}x_{i_2} \cdots x_{i_s}$, so it is clear that any two vertices in $\tilde{\Gamma}$ are connected.

Now suppose $\tilde{\Gamma} \in \tilde{\mathcal{A}}_k(X)$ is connected and consider the tuple $P = (\pi_1, \dots, \pi_n) = (\tilde{\Gamma})\phi^{-1}$. Observe that, since $\tilde{\Gamma}$ is connected, there is a walk from the basepoint to any other vertex u of the automaton with some label $x_{i_1} \cdots x_{i_s}$. If we now consider $\sigma = \pi_{i_1} \cdots \pi_{i_s} \in G = \langle \pi_1, \dots, \pi_n \rangle$, we have that σ is a permutation of V taking the basepoint to u. This implies that the orbit of the basepoint is the whole set V, so the action is transitive. $\square$

Notice that, given an automaton $\tilde{\Gamma} \in \tilde{\mathcal{A}}_k(X)$, it may not be connected and hence will not represent a (vertex-labelled) Stallings automaton. However, we can always obtain a reduced and saturated X-automaton with up to k labelled vertices simply by taking the basepoint component of $\tilde{\Gamma}$ (we assume it is the vertex with label v_1). If we denote by $\tilde{\Gamma}_{\mathbf{b}}$ the automaton obtained in this way, we can define the following map:

$$\begin{array}{rccc} f: & \tilde{\mathcal{A}}_k(X) & \to & \mathcal{C}_{\mathbf{b}}(\tilde{\mathcal{A}}_k(X)) \\ & \tilde{\Gamma} & \mapsto & \tilde{\Gamma}_{\mathbf{b}}, \end{array}$$

where $\mathcal{C}_{\mathbf{b}}(\tilde{\mathcal{A}}_k(X))$ denotes the set of connected components containing the basepoint (vertex with label v_1) of the automata in $\tilde{\mathcal{A}}_k(X)$. In terms of the permutations which are in bijection with $\tilde{\mathcal{A}}_k(X)$, what f does is to take the orbit of v_1 under the action of the group generated by the permutations. Restricted to this orbit, the action is transitive and, by Proposition 4.53, the corresponding automaton is a vertex-labelled Stallings automaton.

Remark 4.54. Notice that the automata in $\mathcal{C}_{\mathbf{b}}(\tilde{\mathcal{A}}_k(X))$ can have between 1 and k vertices. In addition, these automata are reduced.

Moreover, every (vertex-labelled) automaton $\tilde{\Gamma}_{\mathbf{b}}$ determines a (standard) Stallings automaton $\Gamma_{\mathbf{b}}$ simply by removing the labels of all vertices except the basepoint (in this context, the label v_1 is what differentiates it from the rest of vertices). Thus, we can define a map:

$$\begin{array}{rccc} g: & \mathcal{C}_{\mathbf{b}}(\tilde{\mathcal{A}}_k(X)) & \to & \bigcup_{j=1}^{k} \mathcal{S}_j(X) \\ & \tilde{\Gamma}_{\mathbf{b}} & \mapsto & \Gamma_{\mathbf{b}}, \end{array}$$

where $\bigcup_{j=1}^{k} \mathcal{S}_j(X)$ is the set of all possible saturated Stallings automata with up to k vertices.

These two maps f and g that we have just defined, together with Propositions 4.52 and 4.53, play an essential role in the proof of the following result which gives a recursive formula for $N_k(\mathbb{F}_n)$.

Theorem 4.55. *The number $N_k(\mathbb{F}_n)$ of subgroups of index k in $\mathbb{F}_n$ is given recursively by $N_1(\mathbb{F}_n) = 1$,*

$$N_k(\mathbb{F}_n) = k(k!)^{n-1} - \sum_{i=1}^{k-1} [(k-i)!]^{n-1} N_i(\mathbb{F}_n).$$

Proof. Let us consider the following composition of maps:

$$\begin{array}{ccccccccc} (S_k)^n & \overset{\phi}{\leftrightarrow} & \tilde{\mathcal{A}}_k(X) & \overset{f}{\to} & \mathcal{C}_{\mathbf{b}}(\tilde{\mathcal{A}}_k(X)) & \overset{g}{\to} & \bigcup_{j=1}^{k} \mathcal{S}_j(X) & \overset{\psi}{\leftrightarrow} & \bigcup_{j=1}^{k} \mathcal{H}_j(X) \\ P & \mapsto & \tilde{\Gamma} & \mapsto & \tilde{\Gamma}_{\mathbf{b}} & \mapsto & \Gamma_{\mathbf{b}} & \mapsto & \langle \Gamma_{\mathbf{b}} \rangle, \end{array}$$

where ϕ is the bijection described in the proof of Proposition 4.52, f and g are the maps defined above and ψ denotes a bijection whose restriction to subsets of automata in $\bigcup_{j=1}^{k} \mathcal{S}_j(X)$ with the same number of vertices is the bijection (7) for the corresponding value of the index.

Since all the maps involved are surjective, their composition $\varphi = \phi f g \psi$ is surjective as well. We may write

$$(S_k)^n = \bigsqcup_H (H)\varphi^{-1}, \tag{8}$$

where H runs over all possible subgroups of $\mathbb{F}_X$ of finite index lower or equal than k.

We will now determine the cardinal of the fiber of each element in the image of f and g respectively. In the case of f, the number of automata which have the same basepoint component as $\tilde{\Gamma} \in \tilde{\mathcal{A}}_k(X)$ (that is, the same orbit of v_1 in V under the action of the group generated by the elements of the tuple $(\tilde{\Gamma})\phi^{-1}$) is equal to the number of different ways in which n permutations can act on the vertices outside of this orbit. If the basepoint component of $\tilde{\Gamma}$ has r elements, there are $k-r$ vertices outside of the orbit of v_1, so there are exactly $[(k-r)!]^n$ automata in $\tilde{\mathcal{A}}_k(X)$ whose image by f is $(\tilde{\Gamma})f$. In the case of g, the number of preimages of an automaton $\Gamma_{\mathbf{b}} \in \bigcup_{j=1}^{k} \mathcal{S}_j(X)$ is equal to the number of different labellings that can be assigned to the vertices in $\Gamma_{\mathbf{b}}$ which are not the basepoint. If the number of vertices in the automaton is r, this is precisely $(k-1)(k-2)\cdots(k-(r-1))$.

So, we have seen that for a subgroup H of finite index r in $\mathbb{F}_X$, the cardinal of its fiber is determined by its index:

$$\#((H)\varphi^{-1}) = (k-1)(k-2)\cdots(k-(r-1))[(k-r)!]^n = (k-1)![(k-r)!]^{n-1}.$$

Therefore, by (8), we have that

$$(k!)^n = \sum_H \#((H)\varphi^{-1}) = \sum_{r=1}^{k} (k-1)![(k-r)!]^{n-1} N_r(\mathbb{F}_n),$$

where in the first sum H runs over the subgroups of indices from 1 to k in $\mathbb{F}_n$, and in the second equality we have stratified the sum according to the index of the subgroups. Dividing by $(k-1)!$ and separating the last term of the sum, we have

$$k(k!)^{n-1} = N_k(\mathbb{F}_n) + \sum_{r=1}^{k-1} [(k-r)!]^{n-1} N_r(\mathbb{F}_n),$$

and, isolating $N_k(\mathbb{F}_n)$, we obtain the desired formula. □

Table 2 shows the number of subgroups of index k in $\mathbb{F}_n$ for small values of k and n.

$n\backslash k$	1	2	3	4	5	6	7
1	1	1	1	1	1	1	1
2	1	3	13	71	461	3447	29093
3	1	7	97	2143	68641	3011263	173773153
4	1	15	625	54335	8563601	2228419359	893451975473
5	1	31	3841	1321471	1035045121	1611152548351	4514783110951681

Table 2: Values of $N_k(\mathbb{F}_n)$ for small n and k.

5. Free times free-abelian groups

In this section we will deal with free times free-abelian groups (FTFA groups, for short) which are the direct product of the two types of groups that we have seen in Sections 3 and 4, free groups and free-abelian groups.

Although at first sight one might be tempted to think that FTFA groups are just a simple combination of free and free-abelian groups, they turn out to be a more complicated family of groups than expected, since they exhibit certain behaviours that set them apart from their factors. One example of this unexpected behaviour is the fact that FTFA groups are not necessarily Howson, whereas it is known that both free groups and free-abelian groups are Howson. It is worth checking this fact with an example.

Example 5.1. Let $\mathbb{F}_2 \times \mathbb{Z} = \langle x, y | - \rangle \times \langle t | - \rangle$, and consider the finitely generated subgroups $H = \langle x, y \rangle$ and $K = \langle tx, y \rangle$. If we study the intersection of these two subgroups, we obtain

$$\begin{aligned} H \cap K &= \{w(x,y) : w \in \mathbb{F}_2\} \cap \{w(xt, y) : w \in \mathbb{F}_2\} \\ &= \{w(x,y) : w \in \mathbb{F}_2\} \cap \{w(x,y)t^{|w|_x} : w \in \mathbb{F}_2\} \\ &= \{w(x,y)t^0 : w \in \mathbb{F}_2, |w|_x = 0\} \\ &= \langle x^{-k} y x^k : k \in \mathbb{Z} \rangle = \langle\langle y \rangle\rangle, \end{aligned}$$

where $|w|_x$ denotes the sum of the exponents of every appearance of x in the word w and $\langle\langle y \rangle\rangle$ denotes the normal closure of y in $\mathbb{F}_2$. Since the Stallings automaton corresponding to $H \cap K = \langle\langle y \rangle\rangle$ is the one in Figure 6 and it has infinite graphical rank, we conclude that $H \cap K$ is not finitely generated (using Theorem 4.46, which relates the graphical rank of the automaton with the algebraic rank of the subgroup which it recognises).

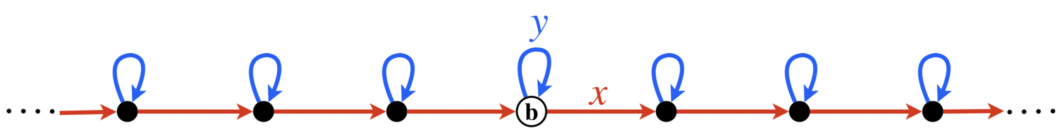

Figure 6: Stallings automaton of $H \cap K$.

As we can see, the sometimes unexpected behaviour of FTFA groups makes them an interesting object of study. Indeed, this family of groups has been the focus of several recent research papers (see [7, 19, 17, 18, 10, 3, 13, 6]) which investigate issues like, for example, the intersection of subgroups of FTFA groups or the endomorphisms of these groups.

The current section is structured as follows. In Section 5.1, we will present FTFA groups and derive some of their basic properties; in Section 5.2, an enriched version of Stallings automata suitable for the representation of subgroups of FTFA groups will be developed; and, in Section 5.3, we will obtain a formula for calculating the number of subgroups of a given finite index in a FTFA group. Since the study of FTFA groups using enriched automata is fairly recent (as opposed to the classical theory of Stallings automata for free groups presented in Section 4, whose origin may be traced back to 1983 with the publication of [20] by J.R. Stallings), the results in Sections 5.1 and 5.2 will include proofs in most cases and some will be illustrated with examples. For this part, we will follow closely [9] and [5].

5.1 Properties of FTFA groups

We call free times free-abelian groups (FTFA) the direct product of a finite rank free group $\mathbb{F}_n$ and a finitely generated free-abelian group $\mathbb{Z}^m$, that is, groups of the form $\mathbb{G} \cong \mathbb{F}_n \times \mathbb{Z}^m$. Therefore, by Proposition 4.19, we can consider the following standard presentation for them

$$\mathbb{G} \cong \mathbb{F}_n \times \mathbb{Z}^m = \left\langle \begin{array}{c} x_1, \ldots, x_n, \\ t_1, \ldots, t_m \end{array} \;\middle|\; \begin{array}{ll} t_i x_k = x_k t_i, & \forall i \in [m], \forall k \in [n] \\ t_i t_j = t_j t_i, & \forall i, j \in [m] \end{array} \right\rangle, \tag{9}$$

taking into account the presentations given for the direct factors in Remarks 4.16 and 3.5.

By definition, any element in $\mathbb{G}$ can be represented as a product of the generators x_i and t_j given in this presentation, but it is important to notice that, due to the fact that the t_j's commute with all the other generators, we can obtain different reduced words on these generators representing the same element of the group. However, every element of $\mathbb{G}$ admits a unique representation of the form $w(x_1, \ldots, x_n) t_1^{a_1} t_2^{a_2} \cdots t_m^{a_m}$, where $w(x_1, \ldots, x_n)$ is a word on $X = \{x_1, \ldots, x_n\}$ and $(a_1, a_2, \ldots, a_m) \in \mathbb{Z}^m$.

For economy in the notation, we will abbreviate this normal form writing it as

$$w t^{\mathbf{a}} = w(x_1, \ldots, x_n) t^{(a_1, a_2, \ldots, a_m)},$$

where t is a formal symbol with the only purpose of holding the vector $\mathbf{a} = (a_1, a_2, \ldots, a_m)$ in the exponent so that we can write the addition of elements in $\mathbb{Z}^m$ as a product. Indeed, in this manner, we can write the operation in $\mathbb{G}$ as $(ut^{\mathbf{a}})(vt^{\mathbf{b}}) = uvt^{\mathbf{a}+\mathbf{b}}$ using multiplicative notation, while the abelian part works additively, as usual, up in the exponent. With this convention, the trivial element of the group $\mathbb{G}$ is (represented by) $1 \cdot t^{\mathbf{0}}$ and $t_i = t^{\mathbf{e_i}}$, where $\mathbf{0} = (0, \ldots, 0) \in \mathbb{Z}^m$ and $\mathbf{e_i} = (0, \ldots, 1, \ldots, 0)$ is the all-zeros vector with a 1 in the i-th position, for $i \in [m]$.

Definition 5.2. For an element in normal form $wt^{\mathbf{a}}$, we say that $w \in \mathbb{F}_n$ is its *free part* and the vector $\mathbf{a} \in \mathbb{Z}^m$ is its *abelian part*. Moreover, we will denote by π the projection to the free part

$$\begin{aligned} \pi : \mathbb{G} &\to \mathbb{F}_n \\ wt^{\mathbf{a}} &\mapsto w, \end{aligned}$$

and by τ the projection to the abelian part

$$\begin{aligned} \tau : \mathbb{G} &\to \mathbb{Z}^m \\ wt^{\mathbf{a}} &\mapsto \mathbf{a}. \end{aligned}$$

Of course, two elements of $\mathbb{G}$ are equal if and only if their free and abelian parts coincide. And it is also worth noticing that both π and τ are homomorphisms. The following remark draws attention to a redundancy which might generate some confusion.

Remark 5.3. We must be careful in the case in which $n = 1$. In that case, $\mathbb{F}_n \times \mathbb{Z}^m \cong \mathbb{Z}^{m+1}$ is a free-abelian group and can be seen as $\mathbb{F}_0 \times \mathbb{Z}^{m+1}$ or as $\mathbb{F}_1 \times \mathbb{Z}^m$, a fact that gives rise to some ambiguity when defining π. We will think of these groups as $\mathbb{F}_0 \times \mathbb{Z}^{m+1}$. However, to avoid unnecessary confusions, in many cases we will choose to avoid this case $n = 1$, since free-abelian groups were already dealt with in Section 3.

As it is the case with free and free-abelian groups, subgroups of a FTFA group are again of the same kind (with the restrictions inherited from those of its factors). In order to prove this result, it is important to note that the group $\mathbb{G}$ fits in the middle of the natural short exact sequence

$$1 \longrightarrow \mathbb{Z}^m \xrightarrow{\ \iota\ } \mathbb{G} \xrightarrow{\ \pi\ } \mathbb{F}_n \longrightarrow 1, \tag{10}$$

where ι is the inclusion map and π is the projection to the free part.

Proposition 5.4. *Let H be a subgroup of $\mathbb{G} = \mathbb{F}_n \times \mathbb{Z}^m$. Then the subgroups of H are again free times free-abelian. In particular, for $n \geq 2$, H admits a decomposition*

$$H = H\pi\sigma \times (H \cap \mathbb{Z}^m) \cong \mathbb{F}_{n'} \times \mathbb{Z}^{m'}, \tag{11}$$

where σ is a splitting of (10), $m' \in [0, m]$ and $n' \in [0, \infty]$.

Proof. If we have $n = 0, 1$, then $\mathbb{G}$ is free-abelian and, therefore, any subgroup is free-abelian as well. Let us suppose in what follows that $n \geq 2$.

In the short exact sequence (10), we have that $\ker(\pi) = \operatorname{im}(\iota) = \{1\} \times \mathbb{Z}^m \cong \mathbb{Z}^m$. If we now restrict this short exact sequence to $H \leqslant \mathbb{G}$, we obtain

$$1 \longrightarrow \ker(\pi_{|H}) \xrightarrow{\ \iota\ } H \xrightarrow{\ \pi\ } H\pi \longrightarrow 1,$$

where $\ker(\pi_{|H}) = H \cap \ker(\pi) \cong H \cap \mathbb{Z}^m \leqslant \mathbb{Z}^m$ and $H\pi \leqslant \mathbb{F}_n$. In consequence, $\ker(\pi_{|H})$ is a free-abelian group and $H\pi$ is a free group. In order to obtain a splitting for $\pi_{|H}$, choose a basis for $H\pi$, say $\{u_i\}_{i \in I}$ for some countable set of indices I (recall that $H\pi$ need not be finitely generated). Consider the map that takes every u_i to an arbitrary preimage $u_i t^{\mathbf{a_i}} \in H$ for some $\mathbf{a_i} \in \mathbb{Z}^m$. Since the group $H\pi$ is free, this defines a splitting $\sigma : H\pi \mapsto H$. Moreover, we have that σ is injective, which implies that $H\pi\sigma \leqslant H$ is isomorphic to $H\pi$. We can now exhibit the following isomorphism of groups:

$$\begin{aligned} \varphi : H &\longrightarrow\ H\pi\sigma \times \ker(\pi_{|H}) \\ h &\longmapsto (h\pi\sigma, h(h\pi\sigma)^{-1}). \end{aligned}$$

Therefore $H = H\pi\sigma \times \ker(\pi_{|H}) \cong H\pi \times (H \cap \mathbb{Z}^m) \cong \mathbb{F}_{n'} \times \mathbb{Z}^{m'}$, where n' and m' are as indicated in the statement of the result, so H is free times free-abelian. □

Corollary 5.5. *A subgroup $H \leqslant \mathbb{F}_n \times \mathbb{Z}^m$ is finitely generated if and only if its projection $H\pi$ to the free part is finitely generated.*

The following result tells us how the rank of $\mathbb{G}$ is related to the ranks of its direct factors.

Proposition 5.6. *Let $H \leqslant \mathbb{F}_n \times \mathbb{Z}^m$, then*

$$rk(H) = rk(H\pi) + rk(H \cap \mathbb{Z}^m).$$

Proof. Let us denote $p = \operatorname{rk}(H\pi)$ and $q = \operatorname{rk}(H \cap \mathbb{Z}^m)$. From (11), we know that H is isomorphic to the direct product of $H\pi$ and $H \cap \mathbb{Z}^m$, so it can be generated by $p + q$ elements (the union of p generators of $H\pi$ and q generators of $H \cap \mathbb{Z}^m$) . Therefore $rk(H) \leq p + q$.

In general, if G^{ab} is the abelianisation of a group G, we have that $rk(G^{\mathrm{ab}}) \leq rk(G)$. Given that $H^{\mathrm{ab}} \cong (H\pi)^{\mathrm{ab}} \times (H \cap \mathbb{Z}^m)^{\mathrm{ab}} \cong \mathbb{Z}^p \times \mathbb{Z}^q$, we derive that $p + q = rk(H^{\mathrm{ab}}) \leq rk(H)$. Thus we conclude that $rk(H) = p + q$. □

Now, by considering respective bases for each of the factors of a subgroup $H \leqslant \mathbb{G}$ (that is, a basis for $H\pi\sigma$ and an abelian basis for $H \cap \mathbb{Z}^m$), we define a notion of basis for a subgroup of a FTFA group.

Definition 5.7. A *free-abelian basis* of a subgroup $H \leqslant \mathbb{F}_n \times \mathbb{Z}^m$ is a set of generators of H of the form

$$\{u_1 t^{\mathbf{a_1}}, \ldots, u_p t^{\mathbf{a_p}}; t^{\mathbf{c_1}}, \ldots, t^{\mathbf{c_q}}\},$$

where $\mathbf{a_1}, \ldots, \mathbf{a_p} \in \mathbb{Z}^m$, $\{u_1, \ldots, u_p\}$ is a free basis of $H\pi$, and $\{\mathbf{c_1}, \ldots, \mathbf{c_q}\}$ is an abelian basis of $L_H = H \cap \mathbb{Z}^m$. Notice that we might have $p = \infty$, since $H\pi$ could be a subgroup of infinite rank of $\mathbb{F}_n$. This does not happen with q, which will always be lower or equal than m (by Theorem 3.7).

Given an element $w \in \mathbb{F}_n$ and a subgroup $H \leqslant \mathbb{F}_n \times \mathbb{Z}^m$, we may wonder what elements of $\mathbb{Z}^m$ can "accompany" w as an abelian part in such a way that the resulting element belongs to H. This gives rise to the following concept.

Definition 5.8. Given a subgroup $H \leqslant \mathbb{G}$ and an element $w \in \mathbb{F}_n$, we define the *abelian completion of w in H* to be $C_H(w) = \{\mathbf{a} \in \mathbb{Z}^m : wt^{\mathbf{a}} \in H\}$. We also say that $\mathbf{a}$ is *an abelian completion* of w in H if $\mathbf{a} \in C_H(w)$.

Proposition 5.9. *The completion $C_H(u)$ is non-empty if and only if $u \in H\pi$ and, in this case, it is a coset of $L_H = H \cap \mathbb{Z}^m$ in $\mathbb{Z}^m$. In particular, if $\{u_1 t^{\mathbf{a_1}}, \ldots, u_p t^{\mathbf{a_p}}; t^{\mathbf{c_1}}, \ldots, t^{\mathbf{c_q}}\}$ is a free-abelian basis for $H \leqslant \mathbb{G}$ and $w \in \mathbb{F}_n$, then*

$$C_H(w) = \begin{cases} \varnothing, & \text{if } w \notin H\pi, \\ \boldsymbol{\omega}\mathbf{A} + L_H & \text{if } w \in H\pi, \end{cases}$$

where $\mathbf{A}$ is the $p \times m$ matrix having $\mathbf{a_i}$ as i-th row, $L_H = \langle \mathbf{c_1}, \ldots, \mathbf{c_q} \rangle \leqslant \mathbb{Z}^m$ and $\boldsymbol{\omega} = w\phi\rho$ is the abelianisation of the expression of w in the basis $\{u_1, \ldots, u_p\}$; that is, ϕ is the change of basis $w \mapsto \omega$ (w is originally represented by a word in the generators of the ambient $\mathbb{F}_n$ and $w = \omega(u_1, \ldots, u_p)$), and ρ is the abelianisation $\mathbb{F}_{u_1,\ldots,u_p} \cong \mathbb{F}_p \twoheadrightarrow \mathbb{Z}^p$, as it is represented in the following diagram:

$$\begin{array}{cccccccccc} \mathbb{F}_n & \geqslant & H\pi & \xrightarrow{\phi} & \mathbb{F}_p & \xrightarrow{\rho} & \mathbb{Z}^p & \xrightarrow{\mathbf{A}} & \mathbb{Z}^m & \xrightarrow{/L_H} & \mathbb{Z}^m/L_H \\ & & w & \longmapsto & \omega & \longmapsto & \boldsymbol{\omega} & \longmapsto & \boldsymbol{\omega}\mathbf{A} & \longmapsto & \boldsymbol{\omega}\mathbf{A} + L_H = C_H(w). \end{array}$$

Proof. For the first part, it is enough to take into account the definition of abelian completion, from which we deduce that $C_H(u) \neq \varnothing$ iff $\exists \mathbf{a} \in \mathbb{Z}^m : ut^{\mathbf{a}} \in H$ iff $u = (ut^{\mathbf{a}})\pi \in H\pi$. To see that, if $C_H(w) \neq \varnothing$, then it is a coset of L_H, let us assume that $\{u_1 t^{\mathbf{a_1}}, \ldots, u_p t^{\mathbf{a_p}}; t^{\mathbf{c_1}}, \ldots, t^{\mathbf{c_q}}\}$ is a basis for H. The fact that $C_H(w) = \boldsymbol{\omega}\mathbf{A} + L_H$ follows from this observation: if we take $wt^{\mathbf{a}} \in H$ and write it in terms of this basis, we will have

$$wt^{\mathbf{a}} = \omega(u_1 t^{\mathbf{a_1}}, \ldots, u_p t^{\mathbf{a_p}}) t^{\mathbf{b}}$$

for some $\mathbf{b} \in \langle \mathbf{c_1}, \ldots, \mathbf{c_q} \rangle$. Since the t's commute with everything, if we denote by $|\omega|_i$ the sum of the exponents of the different appearances of $u_i t^{\mathbf{a_i}}$ in $\omega(u_1 t^{\mathbf{a_1}}, \ldots, u_p t^{\mathbf{a_p}})$, we have that

$$wt^{\mathbf{a}} = \omega(u_1, \ldots, u_p) t^{(|\omega|_1, \ldots, |\omega|_p)\mathbf{A} + \mathbf{b}},$$

and thus, $\mathbf{a} = (|\omega|_1, \ldots, |\omega|_p)\mathbf{A} + \mathbf{b} \in \boldsymbol{\omega}\mathbf{A} + L_H$. □

A consequence of the previous result is this useful equivalence.

Corollary 5.10. *Let $wt^{\mathbf{a}} \in \mathbb{G}$ and $H \leqslant \mathbb{G}$ with basis $\{u_1 t^{\mathbf{a_1}}, \ldots, u_p t^{\mathbf{a_p}}; t^{\mathbf{c_1}}, \ldots, t^{\mathbf{c_q}}\}$, then*

$$wt^{\mathbf{a}} \in H \Leftrightarrow w \in H\pi \text{ and } \mathbf{a} \in w\phi\rho\mathbf{A} + L_H.$$

5.2 Enriched automata

In Section 4.2 we gave a graphical description of the subgroups of the free group using Stallings automata, and now we will extend this theory to the subgroups of FTFA groups. To achieve this goal, we will also use certain type of automata, but enriched with some additional information to encode the abelian part of these subgroups. We give a precise definition of these objects below.

Definition 5.11. A $\mathbb{Z}^m$*-enriched* X*-automaton* (or simply an enriched automaton) is a pointed involutive $(\mathbb{Z}^m \times X \times \mathbb{Z}^m)$-automaton, with a subgroup of $\mathbb{Z}^m$ attached to the basepoint. In more detail, an enriched automaton $\mathbf{\Gamma}$ consists of:

(i) an involutive pointed digraph $\Gamma = (V, E, \iota, \tau, \mathbf{b})$, which will be called the *underlying digraph* of $\mathbf{\Gamma}$;

(ii) an involutive labelling map $\ell = (\ell_1, \ell_X, \ell_2) : E \to \mathbb{Z}^m \times X^{\pm} \times \mathbb{Z}^m$ to which we refer as the *enriched labelling* of $\mathbf{\Gamma}$; in other words, for every arc $e \equiv p \to q$ with label $(\mathbf{a_1}, x, \mathbf{a_2})$, there exists a unique arc $e^{-1} \equiv q \to p$ with label $(-\mathbf{a_2}, x^{-1}, -\mathbf{a_1})$, which will be called the *inverse arc* of e. We will refer to $\mathbf{a_1}$ and $\mathbf{a_2}$ as *abelian labels* of e and to x as a *free label* of e.

(iii) a label for the basepoint, which is a subgroup $L_\Gamma \leqslant \mathbb{Z}^m$ which we call the *basepoint subgroup* of $\mathbf{\Gamma}$,

The result of removing from $\mathbf{\Gamma}$ the basepoint subgroup is what we call the *body* of $\mathbf{\Gamma}$ and we will denote it by $\mathbf{\Gamma}_*$. Removing not only the basepoint subgroup of $\mathbf{\Gamma}$ but also all the abelian labels gives as a result a standard X-automaton which we call the *skeleton* of $\mathbf{\Gamma}$, denoted by $\mathrm{sk}(\mathbf{\Gamma})$. An enriched X-automaton $\mathbf{\Gamma}$ is said to be deterministic (respectively, connected, core, reduced) if its skeleton $\mathrm{sk}(\mathbf{\Gamma})$ is so. We also define the core of an enriched automaton in terms of the core of its skeleton in the natural way.

We will follow the same convention as in the free case (see Remark 4.23), i.e., an involutive automaton is represented by its positive part.

We will write $e \equiv p \xrightarrow[x_j]{\mathbf{a_1} \quad \mathbf{a_2}} q$ to indicate that the arc $e \equiv p \to q$ has label $(\mathbf{a_1}, x_j, \mathbf{a_2})$. Recall that in the free case the labelling of arcs could be extended to walks in a natural way just by concatenating the labels of the arcs which formed the walk. We adapt this scheme to enriched automata:

(i) An enriched arc $e \equiv p \xrightarrow[x_j]{\mathbf{a_1} \quad \mathbf{a_2}} q$ is meant to be read $t^{-\mathbf{a_1}} x_j t^{\mathbf{a_2}} = x_j t^{\mathbf{a_2}-\mathbf{a_1}}$ when crossed forward (from the tail to the head of the arrow), while it should be read $t^{-\mathbf{a_2}} x_j^{-1} t^{\mathbf{a_1}} = x_j^{-1} t^{\mathbf{a_1}-\mathbf{a_2}} = (x_j t^{\mathbf{a_2}-\mathbf{a_1}})^{-1}$ when crossed backwards (from the head to the tail of the arrow).

(ii) Successive arcs in a walk read the product (in $\mathbb{G}$) of the labels of the arcs.

(iii) When at the basepoint, one can choose any element from $L_\Gamma \leqslant \mathbb{Z}^m \leqslant \mathbb{G}$ as a label.

Hence, if $\gamma = e_1 e_2 \cdots e_k$ is a non-trivial walk (every e_i is an arc and $k \geq 1$) in $\mathbf{\Gamma}$, an *enriched label* of γ will be

$$(\gamma)\ell := t^{-(e_1)\ell_1} (e_1)\ell_X t^{(e_1)\ell_2} \cdots t^{-(e_k)\ell_1} (e_k)\ell_X t^{(e_k)\ell_2} \in \mathbb{G}. \tag{12}$$

Moreover, due to rule (iii) above, we will consider that any walk $\gamma_{\mathbf{b}}$ that contains the basepoint has multiple enriched labels, namely, the product in $\mathbb{G}$ of $(\gamma_{\mathbf{b}})\ell$ and any element of the basepoint subgroup. In particular, we will follow the convention that any element in $L_{\mathbf{\Gamma}}$ is a possible enriched label of the trivial $\mathbf{b}$-walk (a walk beginning and ending at the basepoint).

Proposition 5.12. *The set of enriched labels of* $\mathbf{b}$*-walks in* $\mathbf{\Gamma}$ *is a subgroup of* $\mathbb{G}$.

Proof. The trivial element of $\mathbb{G}$ is an enriched label of the trivial $\mathbf{b}$-walk in $\mathbf{\Gamma}$. Moreover, if $g_1, g_2 \in \mathbb{G}$ are enriched labels of respective $\mathbf{b}$-walks γ_1 and γ_2, $g_1 g_2$ is an enriched label of the concatenation of γ_1 and γ_2, which is also a $\mathbf{b}$-walk. Finally, if $g \in \mathbb{G}$ is an enriched label of a $\mathbf{b}$-walk γ, g^{-1} is an enriched label of the inverse walk of γ, which is also a $\mathbf{b}$-walk. □

Definition 5.13. Let $\mathbf{\Gamma}$ be an enriched automaton. An element in the group $\mathbb{G}$ which is an enriched label of a $\mathbf{b}$-walk in $\mathbf{\Gamma}$ is said to be *recognised* by $\mathbf{\Gamma}$. The set of all elements recognised by $\mathbf{\Gamma}$, which we know is a subgroup of $\mathbb{G}$ by the previous result, is called the *subgroup recognised by* $\mathbf{\Gamma}$ and it is denoted by $\langle \mathbf{\Gamma} \rangle$.

The following lemma tells us how the subgroup recognised by $\mathbf{\Gamma}$ is related to the subgroups recognised by its skeleton and its core.

Lemma 5.14. *Let $\mathbf{\Gamma}$ be an enriched automaton. Then,*

(i) $\langle sk(\mathbf{\Gamma}) \rangle = (\langle \mathbf{\Gamma} \rangle)\pi$,

(ii) $\langle \mathbf{\Gamma} \rangle = \langle core(\mathbf{\Gamma}) \rangle$.

Proof. (i) If $u \in \langle \mathrm{sk}(\mathbf{\Gamma}) \rangle$, then u is the label of a $\mathbf{b}$-walk in $\mathrm{sk}(\mathbf{\Gamma})$ and, if we consider the enriched label of this walk in $\mathbf{\Gamma}$, we obtain an element $ut^{\mathbf{a}} \in \langle \mathbf{\Gamma} \rangle$ for some $\mathbf{a} \in \mathbb{Z}^m$ such that $(ut^{\mathbf{a}})\pi = u$. Reciprocally, if $u \in (\langle \mathbf{\Gamma} \rangle)\pi$, then there must exist some $\mathbf{a} \in \mathbb{Z}^m$ such that $ut^{\mathbf{a}}$ is a label of a $\mathbf{b}$-walk in $\mathbf{\Gamma}$ and it is clear that, if we ignore all the abelian information, u is a label of a $\mathbf{b}$-walk in $\mathrm{sk}(\mathbf{\Gamma})$.

(ii) The inclusion $\langle \mathrm{core}(\mathbf{\Gamma}) \rangle \subset \langle \mathbf{\Gamma} \rangle$ is clear. For the other inclusion, suppose v is a dead vertex in $\mathrm{Sk}(\mathbf{\Gamma})$ and let γ be a $\mathbf{b}$-walk containing v. The backtracking of this walk translates into a cancellation of the labels (both free and abelian) of the arcs in $\mathbf{\Gamma}$ which do not belong to $\mathrm{core}(\mathbf{\Gamma})$. Therefore, the labels (elements in $\mathbb{G}$) of $\mathbf{b}$-walks in $\mathbf{\Gamma}$ and $\mathrm{core}(\mathbf{\Gamma})$ coincide. □

Proposition 5.12 allows us to define a map which assigns a subgroup of $\mathbb{G}$ to every enriched automaton:

$$\begin{array}{rcl} \{\mathbb{Z}^m\text{-enriched } X\text{-automata}\} & \to & \{\text{subgroups of } \mathbb{G}\} \\ \mathbf{\Gamma} & \mapsto & \langle \mathbf{\Gamma} \rangle. \end{array} \qquad (13)$$

Recall that we are aiming to obtain a bijection between the set of subgroups of $\mathbb{G}$ and some set of enriched automata. For the map that we have just defined, which is a first step towards the bijection we seek, it is easy to prove its surjectivity by defining a FTFA version of the flower automaton we had in the free case.

Definition 5.15. Let $ut^{\mathbf{a}} \in \mathbb{G}$ where $u = x_{i_1} x_{i_2} \cdots x_{i_k} \neq 1$ and $x_{i_j} \in X^{\pm}$. We define the *canonical petal automaton* associated to $ut^{\mathbf{a}}$, denoted by $\mathrm{Fl}(ut^{\mathbf{a}})$, as the following enriched automaton:

$$\mathbf{b} \xrightarrow[x_{i_1}]{\mathbf{0} \quad \mathbf{0}} \bullet \xrightarrow[x_{i_2}]{\mathbf{0} \quad \mathbf{0}} \bullet \cdots \bullet \xrightarrow[x_{i_k}]{\mathbf{0} \quad \mathbf{a}} \mathbf{b}.$$

Moreover, given a finite subset $\mathcal{S} = \{u_1 t^{\mathbf{a_1}}, \ldots, u_p t^{\mathbf{a_p}}; t^{\mathbf{c_1}}, \ldots, t^{\mathbf{c_q}}\} \subset \mathbb{G}$, with $u_1, \ldots, u_p \neq 1$ and $\mathbf{a_1}, \ldots, \mathbf{a_p}$, $\mathbf{c_1}, \ldots, \mathbf{c_q} \in \mathbb{Z}^m$, we define the *enriched flower automaton* $\mathrm{Fl}(\mathcal{S})$ as the automaton obtained by identifying the basepoints of the petals of the first p elements of $\mathcal{S}$ and declaring the basepoint subgroup to be $L_{\mathbf{\Gamma}} = \langle \mathbf{c_1}, \ldots, \mathbf{c_q} \rangle$ (see Figure 7).

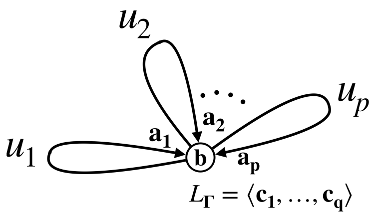

Figure 7: Enriched flower automaton.

Notice that in $\mathsf{Fl}(ut^{\mathbf{a}})$ we can read both $ut^{\mathbf{a}}$ and its inverse as enriched labels of a $\mathbf{b}$-walk, so $\langle \mathsf{Fl}(ut^{\mathbf{a}}) \rangle = \langle ut^{\mathbf{a}} \rangle$. The same argument (concatenating petals) proves that $\langle \mathsf{Fl}(\mathcal{S}) \rangle = \langle \mathcal{S} \rangle$. Indeed, enriched labels of $\mathbf{b}$-walks in $\mathsf{Fl}(\mathcal{S})$ are a product of elements of S and vice versa.

Given a subgroup $H \leqslant \mathbb{G}$, it is enough to consider a generating set of H, say $\mathcal{S}$, and build the flower automaton of $\mathcal{S}$ in order to obtain an enriched automaton which recognises the subgroup H, that is, $H = \langle \mathsf{Fl}(\mathcal{S}) \rangle$. This guarantees the surjectivity of the map (13).

However, a subgroup $H \leqslant \mathbb{G}$ can be recognised by infinitely many automata, so this map is not injective. The sources of this non-injectivity are:

(i) The redundancy inherited from the free part: since the skeleton of the flower automaton is a standard automaton, it may present non-determinism. We will have to adapt the classical Stallings foldings to enriched automata in order to fix this.

(ii) The presence of parallel enriched arcs with the same free label (situation depicted in Figure 8) generates redundancy due to the non-determinism of the free part (the kind of redundancy in item (i)), but also due to the abelian part. Indeed, looping around the two parallel arcs gives an abelian contribution which might not be included in the basepoint subgroup (we will specify this later in Lemma 5.27). Therefore, changing the basepoint label so that it includes said contribution gives an automaton with different basepoint label recognising the same subgroup. This source of non-injectivity will be dealt with by means of closed enriched foldings at the same time as (i).

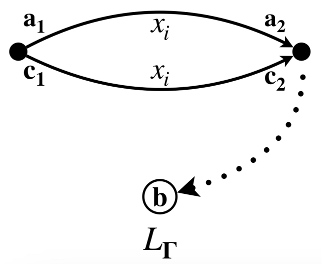

Figure 8: Parallel enriched arcs with the same free label.

(iii) Certain redistributions of abelian labels throughout the automaton do not change the recognised subgroup. For example, for any petal of the flower automaton, we could place the label $\mathbf{a}$ at the end of any of the arcs constituting the walk. To fix this source of redundancy we will introduce some transformations which will allow us to move the abelian labels around the automaton.

(iv) Every abelian label in the enriched automaton $\mathbf{\Gamma}$ works modulo $L_{\mathbf{\Gamma}}$. Indeed, suppose we have some $\mathbf{b}$-walk containing some arc with $\mathbf{a}$ as one of its abelian labels. Since the elements of $\langle \mathbf{\Gamma} \rangle$ are enriched labels of $\mathbf{b}$-walks in $\mathbf{\Gamma}$ and the product of an enriched label of a $\mathbf{b}$-walk by any element of $L_{\mathbf{\Gamma}}$ is another enriched label of the $\mathbf{b}$-walk, if we change some label $\mathbf{a}$ by $\mathbf{a}+\mathbf{l}$ with $\mathbf{l} \in L_{\mathbf{\Gamma}}$, the recognised subgroup does not change. This source of redundancy is inherent in the object that we are considering, so the way in which we deal with it is by absorbing it in the natural way, considering the labelling modulo the basepoint subgroup (which we will express writing mod $\mathbf{b}$).

In order to remove the previous sources of redundancy, we will ask for some extra properties that the representative automata must satisfy. Firstly, to remove the sources of redundancy (i) and (ii), we will consider reduced enriched automata.

Remark 5.16. Notice that if $\mathbf{\Gamma}$ is reduced, its skeleton $\mathrm{sk}(\mathbf{\Gamma})$ is a reduced X-automaton and, by Lemma 5.14, we have that $\langle \mathrm{sk}(\mathbf{\Gamma}) \rangle = (\langle \mathbf{\Gamma} \rangle)\pi = H\pi$. This implies that $\mathrm{sk}(\mathbf{\Gamma})$ is nothing but the classic Stallings automaton $\mathrm{St}(H\pi, X)$.

These reduced automata encode nicely many algebraic properties of the subgroup they recognise, like a basis for it.

Remark 5.17. Observe that, if T is a spanning tree of $\mathbf{\Gamma}$ and we call $\mathcal{B}_T = \{(\mathbf{b} \overset{T}{\rightsquigarrow} p \overset{e}{\to} q \overset{T}{\rightsquigarrow} \mathbf{b})\ell : e \in E^{+}\mathbf{\Gamma} \backslash ET\}$ (the set of enriched labels of positive T-petals in $\mathbf{\Gamma}$), we have that $(\mathcal{B}_T)\pi = B_T$ (the positive T-basis of $H\pi$).

The following lemma shows that $\mathcal{B}_T$ is a basis for the subgroup recognised by the body of $\mathbf{\Gamma}$ and can be completed so as to obtain a basis for H and it also shows that the basepoint subgroup of a reduced enriched automaton recognising H coincides with $H \cap \mathbb{Z}^m$.

Lemma 5.18. *Let $\mathbf{\Gamma}$ be a reduced enriched automaton recognising $H \leqslant \mathbb{G}$. Then, $H = \langle \mathbf{\Gamma}_* \rangle \times L_{\mathbf{\Gamma}}$, where $\langle \mathbf{\Gamma}_* \rangle$ is the image of a splitting of $\pi_{|H}$, and $L_{\mathbf{\Gamma}} = H \cap \mathbb{Z}^m$. Moreover, $\mathcal{B}_T$ is a free basis for $\langle \mathbf{\Gamma}_* \rangle$ which, joined to an abelian basis for $L_{\mathbf{\Gamma}}$, constitutes a basis for H.*

Proof. It is obvious by definition that $L_{\mathbf{\Gamma}} \leqslant \langle \mathbf{\Gamma} \rangle \cap \mathbb{Z}^m = H \cap \mathbb{Z}^m$. For the opposite inclusion, let $\mathcal{B}_T = \{u_i t^{\mathbf{a_i}}\}_i$, and suppose that $t^{\mathbf{a}} \in \langle \mathbf{\Gamma} \rangle \cap \mathbb{Z}^m = H \cap \mathbb{Z}^m$. Then, we may write $t^{\mathbf{a}} = w(u_i t^{\mathbf{a_i}}) t^{\mathbf{l}}$ for some $\mathbf{l} \in L_{\mathbf{\Gamma}}$, where $w(u_i t^{\mathbf{a_i}})$ denotes a reduced word on the $u_i t^{\mathbf{a_i}}$'s. Given that the free part of this element $t^{\mathbf{a}}$ is trivial and $\{u_i\}_i$ is freely independent, we must have that w is the trivial word and therefore $t^{\mathbf{a}} = t^{\mathbf{l}} \in L_{\mathbf{\Gamma}}$, as we wanted to see.

To prove that $H = \langle \mathbf{\Gamma}_* \rangle \times L_{\mathbf{\Gamma}}$, we consider the homomorphism $H\pi \to H$ given by $(\gamma_e^T)\ell_X \mapsto (\gamma_e^T)\ell$ for each arc $e \in E\mathbf{\Gamma} \backslash T$ and take into account the decomposition (5.4). □

Remark 5.19. We must point out here that, even though we always have $L_{\mathbf{\Gamma}} \leqslant H \cap \mathbb{Z}^m$, the opposite inclusion may not be true when $\mathbf{\Gamma}$ is not reduced. This is due to possible non-trivial relations among the free parts $u_1, \ldots, u_p$. We refer the reader to Example 5.37 to see an instance where $L_{\mathbf{\Gamma}} \neq H \cap \mathbb{Z}^m$.

Although reduced enriched automata are good representatives of subgroups of $\mathbb{G}$, there are still redundancies to care about. For this, we will consider the following kind of automata.

Definition 5.20. Let $\mathbf{\Gamma}$ be an enriched X-automaton and let T be a spanning tree of $\mathbf{\Gamma}$. We say that $\mathbf{\Gamma}$ is *T-normalised* if it is reduced and its abelian labelling satisfies these two conditions:

(i) $(e)\ell_1 = (e)\ell_2 = \mathbf{0}$ for all $e \in ET$ (the abelian labels in the arcs of T are all equal to zero),

(ii) $(e)\ell_1 = \mathbf{0}$ for all $e \in E\boldsymbol{\Gamma} \backslash ET$ (only the labels at the head of the arcs outside T might be nonzero).

Notice that if two T-normalised automata $\boldsymbol{\Gamma}$ and $\boldsymbol{\Gamma}'$ recognise the same subgroup $H \leqslant \mathbb{G}$, they will both have the same basepoint subgroup (indeed, by Proposition 5.18, $L_{\boldsymbol{\Gamma}} = H \cap \mathbb{Z}^m = L_{\boldsymbol{\Gamma}'}$). Because of this, we can compare $\boldsymbol{\Gamma}$ and $\boldsymbol{\Gamma}'$ modulo their basepoint subgroups, as we do in the next result.

Proposition 5.21. *For any given subgroup $H \leqslant \mathbb{G}$, and any given spanning tree T of St$(H\pi, X)$, every two T-normalised enriched automata $\boldsymbol{\Gamma}$ and $\boldsymbol{\Gamma}'$ recognising H are equal modulo $L_{\boldsymbol{\Gamma}} = L_{\boldsymbol{\Gamma}'} = H \cap \mathbb{Z}^m$.*

Proof. Observe that, by Remark 5.16, both $\boldsymbol{\Gamma}$ and $\boldsymbol{\Gamma}'$ have the same skeleton and, by Proposition 5.18, they also have the same basepoint subgroup. Notice as well that, because they are T-normalised, all the abelian labels in these automata are zero except for the ones placed at the endpoints of the arcs outside of the spanning tree. If we show that these labels coincide modulo $L_{\boldsymbol{\Gamma}}$, we will have the result. Take an arc e in $\mathrm{Sk}(\boldsymbol{\Gamma}) = \mathrm{Sk}(\boldsymbol{\Gamma}')$ and let us see if $(e)\ell_2$ takes the same value modulo $L_{\boldsymbol{\Gamma}}$ in both $\boldsymbol{\Gamma}$ and $\boldsymbol{\Gamma}'$. Suppose $(e)\ell_2 = \mathbf{a}$ in $\boldsymbol{\Gamma}$ and $(e)\ell_2 = \mathbf{c}$ in $\boldsymbol{\Gamma}'$. If we read the enriched label of the $\mathbf{b}$-walk containing the arc e whose other arcs all belong to T both in $\boldsymbol{\Gamma}$ and $\boldsymbol{\Gamma}'$, for some $w \in H\pi$ we will obtain that $wt^{\mathbf{a}} \in \langle \boldsymbol{\Gamma} \rangle = H$ and $wt^{\mathbf{c}} \in \langle \boldsymbol{\Gamma}' \rangle = H$. This implies that $t^{\mathbf{a}-\mathbf{c}} = (wt^{\mathbf{a}})(wt^{\mathbf{c}})^{-1} \in H \cap \mathbb{Z}^m = L_{\boldsymbol{\Gamma}} = L_{\boldsymbol{\Gamma}'}$. Therefore, the two automata coincide modulo the basepoint. □

Thanks to this result, once a spanning tree T is fixed, by considering the abelian labels modulo the basepoint subgroup, we have a unique object representing a given subgroup of $\mathbb{G}$: a T-normalised enriched automaton $\boldsymbol{\Gamma}$ modulo the basepoint subgroup, for some spanning tree T.

Definition 5.22. Let H be a subgroup of $\mathbb{G}$ and let T be a spanning tree of $\mathrm{St}(H\pi, X)$. Then, a T-normalised $\mathbb{Z}^m$-enriched X-automaton recognising H is said to be a *Stallings automaton* for H with respect to T. We will denote these automata by $\mathrm{St}_T(H, X)$ or simply $\mathrm{St}(H)$ when T and X are clear from the context.[1] When we consider the abelian labels of one of these automata modulo the basepoint subgroup (mod $\mathbf{b}$), we call this the *canonical Stallings automaton* for H with respect to T (which is a unique representative of the subgroup H), and we denote it by $\overline{\mathrm{St}}_T(H, X)$.

Remark 5.23. Notice that the existence of a Stallings automaton of a subgroup $H \leqslant \mathbb{G}$ is guaranteed. Indeed, we know that $\mathrm{St}(H\pi)$ exists and we can consider a spanning tree T. Now, at every arc e outside this spanning tree, we add as an abelian label (at the head of the arc) an element in the abelian completion of the element of $H\pi$ which labels the $\mathbf{b}$-walk $\mathbf{b} \overset{T}{\rightsquigarrow} p \overset{e}{\to} q \overset{T}{\rightsquigarrow} \mathbf{b}$. Then, we let the remaining labels in the automaton be zero. Finally, we set $H \cap \mathbb{Z}^m$ as the basepoint subgroup of the automaton. In this way, we obtain an enriched automaton which is a Stallings automaton for H.

In practice, we may work with any Stallings automaton for H (for example, when we solve some instance of the membership problem) and we will only need to consider the canonical Stallings automaton to have a bijection.

In order to establish a bijection between subgroups of $\mathbb{G}$ and these enriched automata, we will need to specify a uniform way to choose the spanning trees of reduced enriched automata.

Lemma 5.24. *Let $\boldsymbol{\Gamma}$ be a reduced enriched X-automaton. Let $\preccurlyeq$ be a well order in $X^{\pm}$ and consider the tree $T_{\preccurlyeq}(\boldsymbol{\Gamma})$ obtained in the following way:*

(i) First, declare that $\mathbf{b}$ *is a vertex of* $T_{\preccurlyeq}(\boldsymbol{\Gamma})$.

[1] Note that we are slightly abusing language here since $\mathrm{St}_T(H, X)$ might denote different automata (equal modulo the basepoint subgroup).

(ii) Recursively, add to $T_{\preccurlyeq}(\mathbf{\Gamma})$ the edge (together with its other incident vertex) with smallest possible label incident to the oldest vertex present in $T_{\preccurlyeq}(\mathbf{\Gamma})$ at the moment and not closing a path.

Then, $T_{\preccurlyeq}(\mathbf{\Gamma})$ is a spanning tree of $\mathbf{\Gamma}$.

Proof. The hypotheses in the statement of this result guarantee that step (ii) can always be performed. Indeed, since no two arcs with the same label can be incident in the same vertex (because the automaton is reduced), the edge with smallest possible label incident to the oldest vertex is well-defined. Given the fact that the automaton is connected (it is reduced) and the way in which new vertices are incorporated to the tree (first those at distance 1 from $\mathbf{b}$, then those at distance 2 from $\mathbf{b}$, etc.), all vertices of $\mathbf{\Gamma}$ will eventually be incorporated to $T_{\preccurlyeq}(\mathbf{\Gamma})$ and no cycle is generated, so it is a spanning tree. □

A Stallings automaton for $H \leqslant \mathbb{F}_n \times \mathbb{Z}^m$ with respect to a spanning tree obtained following the process in Lemma 5.24 will be denoted by $\mathrm{St}_{\preccurlyeq}(H, X)$ and we will refer to it as a $\preccurlyeq$-Stallings automaton when we want to emphasise the way in which the spanning tree has been chosen. Considering its labels modulo the basepoint subgroup, we obtain a canonical automaton which we denote by $\overline{\mathrm{St}}_{\preccurlyeq}(H, X)$

The main result of this section is the following bijection between subgroups of $\mathbb{G}$ and (uniformly chosen) enriched Stallings automata.

Theorem 5.25 (Delgado-Ventura)**.** *Let $\mathbb{F}_X$ be a free group with finite basis X, let $\mathbb{Z}^m$ be a finitely generated free-abelian group, and let $\preccurlyeq$ be a total order on $X^{\pm}$. Then, the map*

$$\begin{array}{rrcl} \overline{St}_{\preccurlyeq}: & \{\textit{subgr. of } \mathbb{F}_X \times \mathbb{Z}^m\} & \leftrightarrow & \{(\textit{isom. classes of}) \preccurlyeq\textit{-Stallings automaton} \;\; \textit{mod } \mathbf{b}\} \\ & H & \mapsto & \overline{St}_{\preccurlyeq}(H, X) \\ & \langle \mathbf{\Gamma} \rangle & \leftarrow\!\shortmid & \mathbf{\Gamma} \end{array} \tag{14}$$

is a bijection. Moreover, if we restrict it to finitely generated subgroups, this bijection is computable.

The fact that the map (14) is a bijection is a consequence of what we have discussed so far: the inverse map has been already shown to be well defined and surjective. On the other hand, if we consider $\preccurlyeq$-normalised Stallings automata modulo the basepoint subgroup, we have a unique representative for each subgroup in $\mathbb{G}$. In the remaining of this section, we will develop the theory necessary to show that if we restrict to finitely generated groups, the bijection (14) is algorithmic.

We will start by showing how to compute $\mathrm{St}_{\preccurlyeq}(H, X)$ when we are given a finite generating set S for a subgroup H. We start by constructing the enriched flower automaton for $\mathcal{S}$ in order to obtain an enriched automaton recognising H. Our goal now is to obtain a $\preccurlyeq$-normalised enriched automaton starting from the one we have. As it happened in the free case, the strategy is to introduce certain kinds of transformations on enriched automata that do not change the recognised subgroup and which will allow us to reach a reduced enriched automaton in finite time.

The idea is to adapt the folding process we had in the free case to the enriched case. Just like in the free case, here we will also have open and closed foldings, but with the extra information of the abelian labelling of the arcs. In the case of open foldings, we will perform an identification of two arcs like in the free case, but here we have the extra condition that the abelian labels (not only the free ones) must be the same for the arcs involved. On the other hand, for closed foldings the identification entails a possible abelian contribution to the basepoint subgroup. We formalise these two notions below.

Definition 5.26 (Enriched foldings)**.** Let us consider the following elementary transformations on enriched automata:

(i) *Open (enriched) foldings:* consisting in identifying a pair of nonparallel enriched arcs with exactly the same (free and abelian) labelling (see Figure 9).

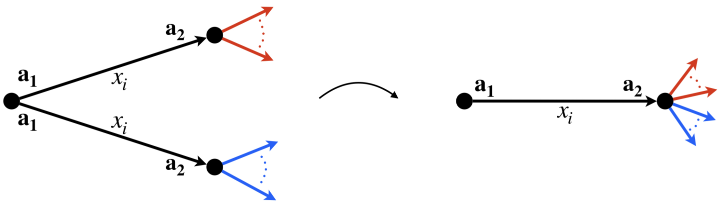

Figure 9: Open enriched folding.

(ii) *Closed (enriched) foldings:* consisting in identifying a pair of parallel enriched arcs with the same free label and updating the basepoint subgroup from L_Γ to $L_\Gamma + \langle \mathbf{c_1} - \mathbf{a_1} + \mathbf{a_2} - \mathbf{c_2} \rangle$ (see Figure 10).

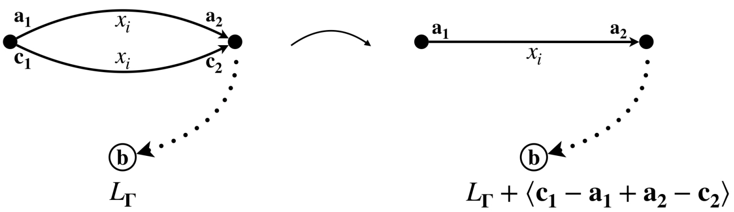

Figure 10: Closed enriched folding.

The following lemma guarantees that the previous transformations do not affect the subgroup recognised by an enriched automaton.

Lemma 5.27. *If* $\mathbf{\Gamma}$ *is an enriched* $\mathbb{Z}^m$*-automaton and* $\mathbf{\Gamma} \curvearrowright \mathbf{\Gamma'}$ *is an (open or closed) enriched folding, then the subgroups recognised by* $\mathbf{\Gamma}$ *and* $\mathbf{\Gamma'}$ *in* $\mathbb{G}$ *coincide, that is,* $\langle \mathbf{\Gamma} \rangle = \langle \mathbf{\Gamma'} \rangle \leqslant \mathbb{G}$.

Proof. Since the labels of both arcs involved in an open folding coincide, it is clear that one can read the same labels before and after the folding. As to closed foldings, the updating of the basepoint subgroup described in Definition 5.26 guarantees the invariance of the recognised subgroup, since it compensates the abelian contribution that looping around the closed folding creates. Indeed, when we have two parallel arcs with the same free label we can read the family of words $[(t^{-\mathbf{a_1}} x_i t^{\mathbf{a_2} - \mathbf{c_2}} x_i^{-1} t^{\mathbf{c_1}})^{\pm 1}]^*$, which (taking into account the commutativity between the t_i's with and the rest of the generators) corresponds to the abelian subgroup $\langle \mathbf{c_1} - \mathbf{a_1} + \mathbf{a_2} - \mathbf{c_2} \rangle$ in $\mathbb{G}$. By adding this abelian contribution to the basepoint subgroup, we ensure that we can remove one of the arcs involved without changing the recognised subgroup. □

Since open foldings require the two arcs involved to have the same enriched label, one may wonder what happens if we have an open folding situation in the skeleton of the enriched automaton but the abelian labels of the two arcs do not match. It is clear that we cannot apply an open enriched folding directly. This motivates the definition of certain *abelian transformations* which will allow us to change the distribution of the abelian labels in the automaton, again, without modifying the recognised subgroup. These transformations will not only help us to tranform any open folding situation in the skeleton into an enriched open folding situation, but they will also allow us to "move" the abelian labels out of the chosen spanning tree when we compute a $\preccurlyeq$-normalisation of our automaton.

Definition 5.28 (Abelian transformations)**.** Let us consider the following elementary abelian transformations on enriched automata:

(i) A *vertex transformation* consists in adding a vector $\mathbf{c} \in \mathbb{Z}^m$ to every abelian label in the neighbourhood of a vertex p (see Figure 11).

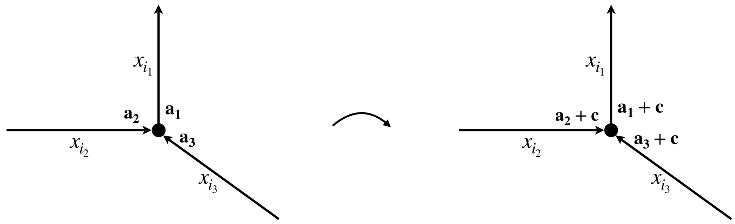

Figure 11: Vertex transformation.

(ii) An *arc transformation* consists in adding a vector $\mathbf{c} \in \mathbb{Z}^m$ to both the initial and final labels of an arc (see Figure 12).

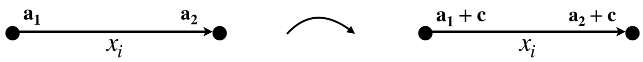

Figure 12: Arc transformation.

It is obvious that these transformations do not affect the skeleton of the automaton and, in the following result, we show that they do not affect the recognised subgroup either.

Proposition 5.29. *Abelian transformations do not change the recognised subgroup. That is, if* $\mathbf{\Gamma} \curvearrowright \mathbf{\Gamma}'$ *is a (vertex or arc) transformation, then* $\langle \mathbf{\Gamma} \rangle = \langle \mathbf{\Gamma}' \rangle$*.*

Proof. Let $\mathbf{\Gamma}$ be an enriched automaton and let $\mathbf{\Gamma}'$ and $\mathbf{\Gamma}''$ be the automata resulting from applying a vertex transformation and an arc transformation, respectively, to $\mathbf{\Gamma}$. We will prove that $\langle \mathbf{\Gamma} \rangle = \langle \mathbf{\Gamma}' \rangle = \langle \mathbf{\Gamma}'' \rangle$. To show that $\langle \mathbf{\Gamma} \rangle = \langle \mathbf{\Gamma}' \rangle$, we must simply observe that, if a $\mathbf{b}$-walk in $\mathbf{\Gamma}$ goes through a vertex p reading $x_{i_j} t^{\mathbf{a_j}} x_{i_k} t^{-\mathbf{a_k}} = x_{i_j} x_{i_k} t^{\mathbf{a_j} - \mathbf{a_k}}$, the corresponding $\mathbf{b}$-walk in $\mathbf{\Gamma}'$ will read $x_{i_j} t^{\mathbf{a_j} + \mathbf{c}} x_{i_k} t^{-\mathbf{a_k} - \mathbf{c}} = x_{i_j} x_{i_k} t^{\mathbf{a_j} + \mathbf{c} - \mathbf{a_k} - \mathbf{c}} = x_{i_j} x_{i_k} t^{\mathbf{a_j} - \mathbf{a_k}}$. Similarly, in order to prove that $\langle \mathbf{\Gamma} \rangle = \langle \mathbf{\Gamma}'' \rangle$, we need only realise that if an arc is read as $t^{-\mathbf{a}} x_i t^{\mathbf{b}} = x_i t^{\mathbf{b} - \mathbf{a}}$ in $\mathbf{\Gamma}$, the corresponding arc in $\mathbf{\Gamma}''$ is read as $t^{-\mathbf{a} - \mathbf{c}} x_i t^{\mathbf{b} + \mathbf{c}} = x_i t^{\mathbf{b} + \mathbf{c} - \mathbf{a} - \mathbf{c}} = x_i t^{\mathbf{b} - \mathbf{a}}$. □

By applying vertex and arc transformations, we can redistribute abelian labels throughout the automaton without changing the recognised subgroup. The proof of the following lemma may serve as an example of this.

Lemma 5.30. *The abelian labels in any bridge-arc in an enriched automaton do not affect the subgroup it recognises in* $\mathbb{F}_n \times \mathbb{Z}^m$*. In particular, we can remove all abelian labels from any bridge-arc.*

Proof. Let $e \equiv p \xrightarrow[x_j]{\mathbf{a_1} \quad \mathbf{a_2}} q$ be a bridge-arc and assume, without loss of generality, that p belongs to the component containing the basepoint when one removes the arc e (we may say p is the arc extreme closer to the basepoint). Firstly, we perform an arc transformation subtracting $\mathbf{a_2}$ to both abelian labels of e so as to obtain $e \equiv p \xrightarrow[x_j]{\mathbf{c} \quad \mathbf{0}} q$, where $\mathbf{c} = \mathbf{a_1} - \mathbf{a_2}$. Secondly, using a vertex transformation, we subtract $\mathbf{c}$ in each one of the vertices in the component containing the basepoint. In particular, the result of this transformation on e is to have $e \equiv p \xrightarrow[x_j]{\mathbf{0} \quad \mathbf{0}} q$. Notice that now all the abelian labels in the basepoint's component are shifted by $-\mathbf{c}$. We can restore their original labels by carrying out an arc transformation adding $\mathbf{c}$ to both the tail and the head of every arc in this component. □

As we had previously said, the idea is to use abelian transformations in order to reach (enriched) folding situations like the ones in Definition 5.26. The following result makes this clear.

Lemma 5.31. *A pair of arcs e and f in an enriched automaton $\boldsymbol{\Gamma}$ admit an open (resp. closed) enriched folding if and only if the corresponding arcs in $Sk(\boldsymbol{\Gamma})$ admit an open (resp. closed) folding.*

Proof. It is obvious that, if the enriched automaton admits an open folding then its skeleton does too. Suppose now that $\mathsf{Sk}(\boldsymbol{\Gamma})$ admits an open folding. If the abelian labels of the arcs coincide, the enriched automaton also admits an open folding. Otherwise, one can perform arc and vertex tranformations so as to obtain an enriched folding situation like in Definition 5.26. Indeed, if $e \equiv p \xrightarrow[x_j]{\mathbf{a_1} \quad \mathbf{a_2}} q$ and $f \equiv p \xrightarrow[x_j]{\mathbf{c_1} \quad \mathbf{c_2}} r$ are the two arcs which we want to identify, we can first apply an arc transformation to f adding $\mathbf{a_1} - \mathbf{c_1}$ to both of its abelian labels in order to obtain $(f)\ell_1 = (e)\ell_1 = \mathbf{a_1}$ and $(f)\ell_2 = \mathbf{c_2} - \mathbf{c_1} + \mathbf{a_1}$. Then, we perform a vertex transformation at r (notice that this will not affect the labelling of e because we have an open folding situation, that is, we have that $q \neq r$) adding $\mathbf{a_2} - \mathbf{c_2} + \mathbf{c_1} - \mathbf{a_1}$ to the abelian labels in its neighbourhood, which yields $(e)\ell_2 = (f)\ell_2$. After this preparation, all the abelian labels in e and f coincide, so we can perform the open folding. In the case of closed foldings, the double implication is clear, since there are no requirements on the abelian labels of the arcs involved. □

Remark 5.32. After seeing the proof of the previous proposition, one may wonder why in the case of closed enriched foldings we do not carry out a preparation process that makes the abelian labels match like in the open folding case. If this were possible, we might have defined closed enriched foldings as an identification of arcs like in the free case. However, if we try to adapt the argument we have used for open enriched foldings, we encounter that the vertex transformation at the endpoint of f would also affect the label $(e)\ell_2$ and we cannot obtain the same abelian labels in both arcs in this way. Given this situation, what we do is to fully remove f and update the basepoint to avoid changing the recognised subgroup. The reason behind this change in the basepoint is that want to ensure the recognised subgroup does not change (see the proof of Lemma 5.27).

As a consequence of Lemma 5.31, we have the following corollary.

Corollary 5.33. *Let $\boldsymbol{\Gamma}$ be an enriched automaton. Then $\boldsymbol{\Gamma}$ admits no more foldings if and only if $Sk(\boldsymbol{\Gamma})$ admits no more foldings.*

In order to prove the computability of the map (14) all we need to show is that we can transform our initial flower automaton for a generating set of a subgroup H into $\mathsf{St}(H)$.

Proposition 5.34. *Let $H \leqslant \mathbb{F}_n \times \mathbb{Z}^m$ be a subgroup given by a finite family of generators, then a Stallings automaton for H is computable.*

Proof. We will start by building an enriched flower automaton $\boldsymbol{\Gamma}$ for the given finite set of generators of H. This enriched automaton is core and we will show that it can be transformed into a reduced automaton without altering the subgroup it recognises (that is, H) by means of a finite sequence of transformations which may include abelian transformations and enriched foldings.

By classic Stallings automata theory, we know that there exists a finite sequence of foldings which convert the skeleton of $\mathbf{\Gamma}$ into the reduced automaton $\mathrm{St}(H\pi)$. Applying Lemma 5.31, it is clear that we can perform an enriched folding on $\mathbf{\Gamma}$ for each of the free foldings of the skeleton just by carrying out the necessary abelian transformations in the case of open foldings and by changing the basepoint subgroup suitably in the case of closed foldings. With this, we obtain a finite sequence of transformations which convert $\mathbf{\Gamma}$ into a reduced enriched automaton recognising H.

Suppose T is the chosen (by Lemma 5.24) spanning tree for the reduced enriched automaton we have obtained, which we will call $\mathbf{\Gamma}'$. We claim that we can normalise $\mathbf{\Gamma}'$ with respect to T by performing abelian transformations (which do not change the recognised subgroup) throughout the spanning tree in order to move the abelian labels out of T.

Suppose that we have removed all the abelian labels from every arc at T-distance at most $k-1$ from the basepoint $\mathbf{b}$. For every arc $e \equiv p_k \xrightarrow[x]{\mathbf{a}\quad \mathbf{c}} p_{k+1}$ in T at T-distance k from $\mathbf{b}$, perform an arc transformation removing the label $\mathbf{a}$ from the tail of e and then perform a vertex transformation in p_{k+1} to remove the obtained label (that is, $\mathbf{c}-\mathbf{a}$). Notice that the vertex transformation may also affect other arcs:

(i) it may modify the abelian labelling of an arc at distance $k+1$ from the basepoint,

(ii) it may modify the abelian labelling of an arc outside of T.

Since $\mathbf{\Gamma}'$ is finite, after a finite number of steps in this process, we will reach the arcs in T at maximum distance from $\mathbf{b}$. After performing the described transformations in these arcs, which may only modify the labelling of arcs outside of T because there are no arcs in T at a higher distance, we obtain that all nonzero abelian labels lie in arcs outside of T.

Finally, we can apply arc transformations to concentrate the abelian labels in the heads of the arcs outside of T so as to obtain a T-normalisation of $\mathbf{\Gamma}'$. Thus, $\mathrm{St}(H)$ is computable. ☐

We have shown how to compute $\mathrm{St}(H)$ for a finitely generated subgroup $H \leqslant \mathbb{G}$. We will now focus on describing an efficient way of computing the subgroup generated by a Stallings automaton (by giving a basis for it), showing the computability of the right-to-left direction of the bijection (14).

We already mentioned the idea that, as it happened in the free case, enriched Stallings automata encode a basis of the subgroups of $\mathbb{G}$ (see Remark 5.17 and Proposition 5.18).

Recall that we had seen that $\mathcal{B}_T = \{(\mathbf{b} \overset{T}{\rightsquigarrow} p \overset{e}{\rightarrow} q \overset{T}{\rightsquigarrow} \mathbf{b})\ell : e \in E^{+}\mathbf{\Gamma} \setminus ET\}$ is a basis for $\langle \mathbf{\Gamma}_* \rangle$. Taking this into account, we have that the union of an abelian basis of $L_{\mathbf{\Gamma}}$ and a basis of $\langle \mathbf{\Gamma}_* \rangle$ like $\mathcal{B}_T$ is a free-abelian basis for $\langle \mathbf{\Gamma} \rangle$. In case we have a finite $\preccurlyeq$-normalised enriched automaton, we can compute one of these bases. First, one must compute an abelian basis for $L_{\mathbf{\Gamma}}$, which can be done using linear algebra. Then, a basis of $\langle \mathbf{\Gamma}_* \rangle$ is obtained by reading the enriched labels of the T-petals in $\mathbf{\Gamma}$ (of which there is a finite number). Therefore, we have the following corollary.

Corollary 5.35. *Free-abelian bases of finitely generated subgroups of FTFA groups are computable.*

We will illustrate the computability of bijection (14) with two examples.

Example 5.36. Let us consider the subgroup

$$H_1 = \langle xyxt^{(1,2)}, x^{-1}yxt^{(4,0)}, yxyt^{(0,2)}, y^{-1}x^{-1}yt^{(1,1)}, t^{(3,0)}, t^{(0,6)} \rangle \leqslant \mathbb{F}_2 \times \mathbb{Z}^2.$$

We will obtain a $\mathrm{St}_{\preccurlyeq}(H_1)$, where the total order $\preccurlyeq$ that we are considering is $x^{-1} < x < y^{-1} < y$.

The first enriched automaton in Figure 13 is the flower automaton of the set

$$\{xyxt^{(1,2)}, x^{-1}yxt^{(4,0)}, yxyt^{(0,2)}, y^{-1}x^{-1}yt^{(1,1)}, t^{(3,0)}, t^{(0,6)}\}.$$

Notice that, in Figure 13, $L = \langle (3,0),(0,6)\rangle$ and the different automata represent the result we obtain after each of the five steps that we carry out.

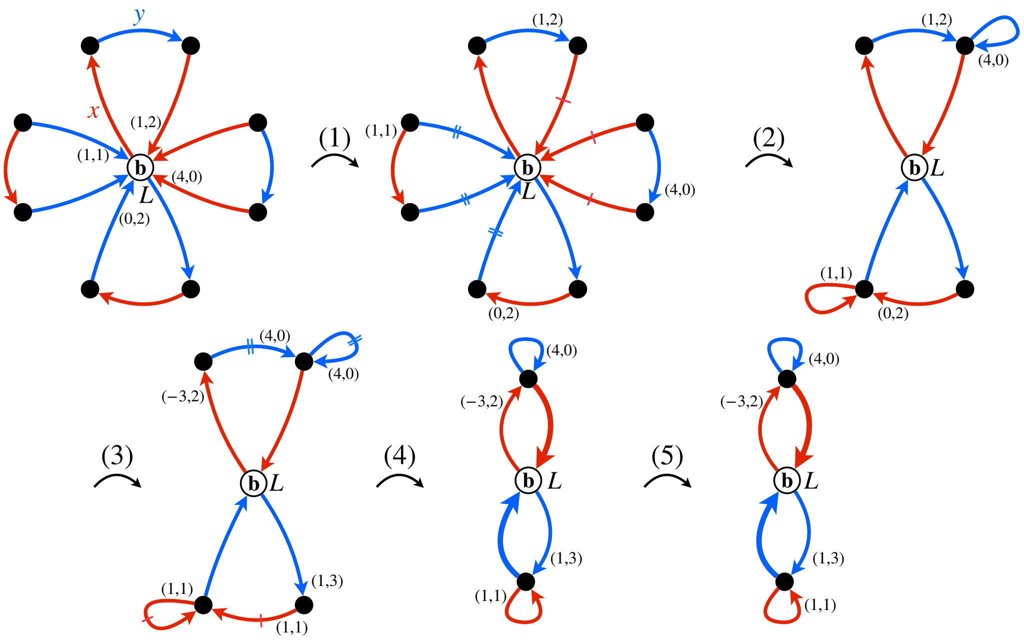

Figure 13: Steps in Example 5.36.

In step (1), we apply abelian transformations in order to obtain matching labels in the arcs that we will fold in the second step. For example, notice that to fold the red arc $e \equiv \bullet \xrightarrow[x]{(0,0)\quad (1,2)} \mathbf{b}$ with the other red arc below it, we need to perform the following abelian transformations: first, we apply an arc transformation to e adding $(-1,-2)$ and, afterwards, we perform a vertex transformation at $\bullet$ adding $(1,2)$. The enriched automaton we obtain after step (1) is the result of applying similar operations in the other petals.

In step (2), we fold the three red arcs whose heads are pointing at $\mathbf{b}$ (observe that all of them have zero abelian labels thanks to the preparation process carried out in step (1)) and we also fold the three blue arcs whose heads are pointing at $\mathbf{b}$.

In step (3), we perform the abelian transformations that are necessary before step (4). First, we apply an arc transformation to the blue arc $e \equiv \bullet \xrightarrow[x]{(0,0)\quad (1,2)} \bullet$ adding $(3,-2)$ so as to obtain $e \equiv \bullet \xrightarrow[x]{(3,-2)\quad (4,0)} \bullet$. Then, we perform a vertex transformation at the top left vertex adding $(-3,2)$. After this, we carry out an arc transformation at the red arc $f \equiv \bullet \xrightarrow[x]{(0,0)\quad (0,2)} \bullet$ adding $(0,-2)$ in order to have $f \equiv \bullet \xrightarrow[x]{(0,-2)\quad (0,0)} \bullet$. This is followed by applying a vertex transformation at the bottom right vertex adding $(1,3)$.

In step (4), we perform an enriched folding involving the two blue arcs on top and another one involving the two red arcs at the bottom. Notice that in the resulting automaton, the thicker arcs are those belonging to the spanning tree associated to the order we have chosen at the beginning.

In step (5), we apply an arc transformation to the red arc at the bottom adding $(-1,-1)$ so as to make sure that all nonzero abelian labels are placed at the heads of the arcs outside the spanning tree. This way, we obtain $\mathrm{St}(H_1)$.

Finally, from the Stallings automaton for H_1 that we have computed, we can obtain a basis for H_1, which is

$$\mathcal{B}_1 = \{x^2t^{(0,2)}, x^{-1}yxt^{(1,0)}, y^2t^{(1,3)}, y^{-1}xyt^{(1,1)}; t^{(3,0)}, t^{(0,6)}\}.$$

Notice that in this basis we have the same number of generators of $H_1\pi\sigma$ that we had at the beginning, which means that there were no nontrivial relations among the free parts of the original generators. This will not happen in the next example, in which there will be relations of this type among the given generators.

Example 5.37. In this second example, we will consider the subgroup

$$H_2 = \langle xyxt^{(1,2)}, x^{-1}y^2t^{(3,2)}, xy^3t^{(-1,4)}, t^{(2,0)}, t^{(0,4)}\rangle \leqslant \mathbb{F}_2 \times \mathbb{Z}^2.$$

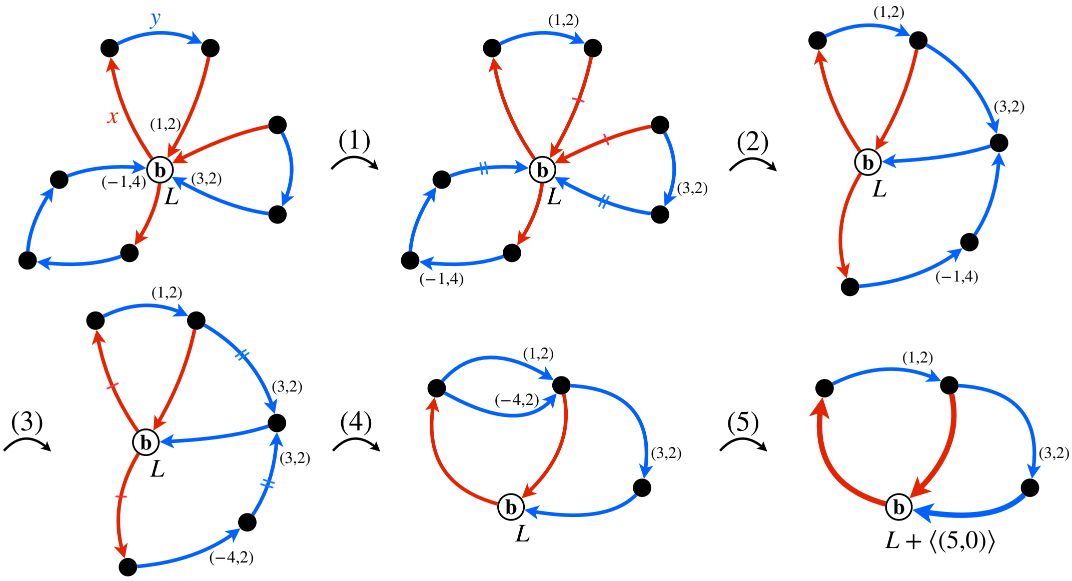

Figure 14: Steps in Example 5.37.

The first automaton in Figure 14 is the enriched flower automaton associated to the given generating set of H_2 and we have $L = \langle (2,0),(0,4)\rangle$. Since the transformations we apply are very similar to the ones in the previous example, we will only describe with detail the steps which present some difference. In step (1), we apply abelian transformations to redistribute the abelian labels. In step (2), we perform two open foldings involving the arcs marked with segments. In step (3), we apply abelian transformations to make the abelian labels of the pairs of arcs which are marked coincide. In step (4), we perform the two open foldings involving the arcs marked. In step (5), we perform a closed folding with the subsequent change of the basepoint subgroup, which consists in adding $(1,2)-(-4,2)=(5,0)$ to the basepoint subgroup. As before, the arcs which are thicker represent the spanning tree T that we choose to normalise the automaton (we have used the same order as in the previous example to obtain this tree). Since all non-zero abelian labels are placed at the head of the arcs outside T after the last folding, no more abelian transformations are needed. The resulting automaton is $\mathrm{St}(H_2)$.

Now, from the Stallings automaton for H_2 that we have computed, we can obtain a basis for H_2, which is

$$\mathcal{B}_2 = \{xyxt^{(1,2)}, x^{-1}y^2t^{(1,2)}; t^{(1,0)}, t^{(0,4)}\},$$

where we have used the fact that $\langle (2,0),(5,0),(0,4)\rangle = \langle (1,0),(0,4)\rangle$ to obtain a basis for the basepoint subgroup.

It is interesting to note that this example clarifies Remark 5.19: the enriched automaton that we have at the beginning recognises H_2, but its basepoint subgroup is not $H_2 \cap \mathbb{Z}^m$. Indeed, we have that $(xyxt^{(1,2)}) \cdot (x^{-1}y^2t^{(3,2)}) \cdot (xy^3t^{(-1,4)})^{-1} = t^{(5,0)} \in H_2 \cap \mathbb{Z}^m$, but it is clear that $t^{(5,0)} \notin L = \langle (2,0),(0,4)\rangle$. On the other hand, $\mathsf{St}(H_2)$ does have $H_2 \cap \mathbb{Z}^m$ as its basepoint subgroup (notice that during the process of folding, we have changed the basepoint subgroup when performing a closed folding).

An important consequence of the algorithmic behaviour of the bijection we have established is that the membership problem for FTFA groups is computable.

Proposition 5.38. *If $\mathbb{G}$ is a FTFA group, then the membership problem $MP(\mathbb{G})$ is computable.*

Proof. We may assume that all the input words are in normal form. Given elements $wt^{\mathbf{a}}, w_1t^{\mathbf{a}_1}, \ldots, w_kt^{\mathbf{a}_k} \in \mathbb{G}$, we will give a finite sequence of steps to show that it is possible to decide whether $wt^{\mathbf{a}}$ belongs to $H = \langle w_1t^{\mathbf{a}_1}, \ldots, w_kt^{\mathbf{a}_k}\rangle$.

Recall that any $\mathsf{St}(H)$ is an enriched automaton recognising H. This means, by the definition of recognised subgroup, that $wt^{\mathbf{a}} \in H$ if and only if it is an enriched label of a $\mathbf{b}$-walk in $\mathsf{St}(H)$. In particular, if $wt^{\mathbf{a}} \in H$, we must have that $w \in H\pi$ and this is equivalent to w being a label of a $\mathbf{b}$-walk in $\mathsf{Sk}(\mathsf{St}(H))$ (since by Proposition 5.14 we have that $\langle \mathsf{Sk}(\mathsf{St}(H))\rangle = H\pi$). Assuming that we can read w in the skeleton of $\mathsf{St}(H)$, we will still need to verify if $t^{\mathbf{a}} \in C_H(w)$ to decide if $wt^{\mathbf{a}} \in H$. When reading w in $\mathsf{St}(H)$, we also read an abelian completion $\mathbf{c_w} \in C_H(w)$. We will have that $wt^{\mathbf{a}}$ is an enriched label of a $\mathbf{b}$-walk in $\mathsf{St}(H)$ if and only if $t^{\mathbf{a}-\mathbf{c_w}} \in L_H$ (being L_H the basepoint subgroup of $\mathsf{St}(H)$). Taking this into account, we can decide whether $wt^{\mathbf{a}} \in H$ following these steps:

1. Compute a $\mathsf{St}(H)$.
2. Try to read the free part w of the word in the skeleton of $\mathsf{St}(H)$, keeping track of the abelian completion $\mathbf{c_w} \in \mathbb{Z}^m$ obtained in doing so. If this is not possible, it will mean that w is not the label of any walk in $\mathsf{Sk}(\mathsf{St}(H))$, so return NO; otherwise continue.
3. If the final vertex (after reading w in $\mathsf{Sk}(\mathsf{St}(H))$) is not the basepoint $\mathbf{b}$, then return NO (because this means that w is not the label of a $\mathbf{b}$-walk); otherwise continue.
4. Check whether $t^{\mathbf{a}}$ belongs to $\mathbf{c_w} + L_H$ using linear algebra methods over $\mathbb{Z}$. In the affirmative case, return YES; otherwise, return NO.

□

5.3 Finite index subgroups of FTFA groups

As an application of the description of subgroups of $\mathbb{F}_n \times \mathbb{Z}^m$ given by the bijection (14), in this section we will study the finite index subgroups of a FTFA group. We will first show how the index of a subgroup H of $\mathbb{G} = \mathbb{F}_n \times \mathbb{Z}^m$ is related to the indices of $H\pi$ in $\mathbb{F}_n$ and of $H \cap \mathbb{Z}^m$ in $\mathbb{Z}^m$ (Proposition 5.39). We will also show that the finite index problem is solvable for free times free-abelian groups (Proposition 5.42). And, finally, we will determine the number of finite index subgroups of a FTFA group.

Proposition 5.39. *Let $\mathbb{G}$ be a FTFA group, let H be a subgroup of $\mathbb{G}$, let $\{v_i\}_{i\in I}$ be a right transversal for $H\pi$ in $\mathbb{F}_n$, and let $\{\mathbf{c_j}\}_{j\in J}$ be a transversal for $L_H = H \cap \mathbb{Z}^m$. Then, $\{v_i t^{\mathbf{c_j}} : i \in I, j \in J\}$ is a right transversal for H in $\mathbb{G}$. Hence, $|\mathbb{G} : H| = |\mathbb{F}_n : H\pi| \cdot |\mathbb{Z}^m : L_H|$; in particular, the index $|\mathbb{G} : H|$ is finite if and only if both $|\mathbb{F}_n : H\pi|$ and $|\mathbb{Z}^m : L_H|$ are finite.*

Proof. We will first prove that the elements in $\{v_i t^{\mathbf{c_j}} : i \in I, j \in J\}$ all belong to different right cosets of H. Indeed, if $Hv_i t^{\mathbf{c_j}} = Hv_{i'} t^{\mathbf{c_{j'}}}$, then we can project to $\mathbb{F}_n$ in order to obtain $(H\pi)v_i = (H\pi)v_{i'}$ and, given that $\{v_i\}_{i\in I}$ is a right transversal for $H\pi$, we obtain that $i = i'$. Taking into account that $t^{\mathbf{c_j}}$ and $t^{\mathbf{c_{j'}}}$ commute with $v_i = v_{i'}$, it follows that $Ht^{\mathbf{c_j}} = Ht^{\mathbf{c_{j'}}}$. If we now intersect this with $\mathbb{Z}^m$, we obtain $L_H + \mathbf{c_j} = L_H + \mathbf{c_{j'}}$, and this implies that $j = j'$ because $\{\mathbf{c_j}\}_{j\in J}$ is a transversal for L_H. This shows that each of the right cosets represented by an element $v_i t^{\mathbf{c_j}}$ is different from the others. Now, to prove that these are all the right cosets of H in $\mathbb{G}$, we must simply prove that $\sqcup_{i\in I} \sqcup_{j\in J} Hv_i t^{\mathbf{c_j}} = \mathbb{F}_n \times \mathbb{Z}^m$. Let us take $wt^{\mathbf{a}} \in \mathbb{F}_n \times \mathbb{Z}^m$. For some $i \in I$ and $u \in H\pi$, we may write $w = uv_i$ and we can also choose $\mathbf{d} \in C_H(u)$ so that $ut^{\mathbf{d}} \in H$. Moreover, we may write $\mathbf{a} - \mathbf{d} = \mathbf{l} + \mathbf{c_j}$ for some $j \in J$ and $\mathbf{l} \in L_H$. With this, we have:

$$wt^{\mathbf{a}} = uv_i t^{\mathbf{a}} = ut^{\mathbf{a}} v_i = ut^{\mathbf{d}} t^{\mathbf{a}-\mathbf{d}} v_i = ut^{\mathbf{d}} t^{\mathbf{l}+\mathbf{c_j}} v_i = ut^{\mathbf{d}} t^{\mathbf{l}} v_i t^{\mathbf{c_j}},$$

where $ut^{\mathbf{d}} t^{\mathbf{l}} \in H$ because $ut^{\mathbf{d}} \in H$ and $t^{\mathbf{l}} \in L_H \subset H$, so $wt^{\mathbf{a}} \in Hv_i t^{\mathbf{c_j}}$ and this concludes the argument. □

Corollary 5.40. *Let H be a subgroup of a FTFA group $\mathbb{G}$ and let $St(H)$ be a Stallings automaton for H. Then, H has finite index k if and only if $St(H)$ is saturated, it has a finite number of vertices k_1 which is a divisor of k and has a basepoint subgroup of finite index $\frac{k}{k_1}$ in $\mathbb{Z}^m$.*

Example 5.41. To illustrate the two previous results, let us consider again the subgroups H_1 and H_2 in Examples 5.36 and 5.37.

In Example 5.36, we obtained a Stallings automaton which was saturated and had 3 vertices. This means that $|\mathbb{F}_2 : H_1\pi| = 3$. Now, since the basepoint subgroup of this automaton was $H_1 \cap \mathbb{Z}^2 = L_1 = \langle (3,0), (0,6) \rangle$, we have that $|\mathbb{Z}^2 : H_1 \cap \mathbb{Z}^2| = 3 \cdot 6 = 18$, where we have applied formula (1). With this, applying Proposition 5.39, we conclude that H_1 is a finite index subgroup with

$$|\mathbb{F}_2 \times \mathbb{Z}^2 : H_1| = |\mathbb{F}_2 : H_1\pi| \cdot |\mathbb{Z}^2 : H_1 \cap \mathbb{Z}^2| = 3 \cdot 18 = 54.$$

In Example 5.37, $\mathrm{St}(H_2)$ was not saturated, which means that H_2 does not have finite index in $\mathbb{F}_2 \times \mathbb{Z}^2$, in virtue of Corollary 5.40.

Proposition 5.39, together with the fact that the finite index problem is known to be solvable for each of the factors (free and free-abelian) of $\mathbb{G}$, give that $FIP(\mathbb{G})$ is solvable as a corollary.

Corollary 5.42. *Let $H \leqslant \mathbb{G}$ be a finitely generated subgroup given by a finite set of generators. Then, there is an algorithm to decide whether H is of finite index and, in the affirmative case, compute the index and a transversal for H. In other words, $FIP(\mathbb{G})$ is solvable.*

We will now combine the graphical description that we have obtained for finite index subgroups of FTFA groups with the formulas we obtained in 3.19 and 4.55 for free-abelian and free groups respectively in order to derive a formula for the number of subgroups of a given finite index in a FTFA group.

Theorem 5.43. *Let $\mathbb{G} = \mathbb{F}_n \times \mathbb{Z}^m$, then*

$$N_k(\mathbb{G}) = \sum_{k_1 | k} N_{k_1}(\mathbb{F}_n) \cdot N_{\frac{k}{k_1}}(\mathbb{Z}^m) \cdot \left(\frac{k}{k_1}\right)^{k_1(n-1)+1},$$

where $N_k(G)$ denotes the number of subgroups of index k in the group G and k_1 runs over all divisors of k.

Proof. By Corollary 5.40, it is clear that we must count the number of canonical Stallings automata which are saturated, have a finite number of vertices k_1 which is a divisor of k and have a basepoint subgroup of finite index $\frac{k}{k_1}$ in $\mathbb{Z}^m$.

Let us begin by fixing k_1, a divisor of k. To determine the number of enriched automata $\mathbf{\Gamma}$ with k_1 vertices satisfying the above properties, we will begin by studying how many choices we have for

(i) the skeleton of $\mathbf{\Gamma}$,

(ii) the basepoint subgroup of $\mathbf{\Gamma}$, and

(iii) the abelian labelling of the arcs of $\mathbf{\Gamma}$,

taking into account the restrictions coming from the mentioned properties.

We will first consider the skeleton of $\mathbf{\Gamma}$. Since $\mathbf{\Gamma}$ must be $\preccurlyeq$-normalised (in particular, reduced) and saturated and must have k_1 vertices, it is clear that $\mathsf{Sk}(\mathbf{\Gamma})$ must be the Stallings automaton of a subgroup of index k_1 in $\mathbb{F}_n$. Therefore, the number of possible choices that we have for $\mathsf{Sk}(\mathbf{\Gamma})$ is $N_{k_1}(\mathbb{F}_n)$, i.e., the number of subgroups of index k_1 in $\mathbb{F}_n$.

As to the basepoint subgroup of $\mathbf{\Gamma}$, since we need it to have index $\frac{k}{k_1}$ in $\mathbb{Z}^m$, the number of possible choices that we have for it is $N_{\frac{k}{k_1}}(\mathbb{Z}^m)$, i.e., the number of subgroups of index $\frac{k}{k_1}$ in $\mathbb{Z}^m$.

It remains to determine the number of distinct abelian labellings that we can have for the arcs of $\mathbf{\Gamma}$. The first thing one must notice is that, because $\mathbf{\Gamma}$ is $\preccurlyeq$-normalised, all abelian labels will be zero except maybe the ones situated at the heads of the arcs outside the spanning tree $T_{\preccurlyeq}(\mathbf{\Gamma})$. The number of arcs outside the spanning tree is the graphical rank of $\mathsf{Sk}(\mathbf{\Gamma})$, which coincides (by Theorem 4.46) with the rank of $\langle \mathsf{Sk}(\mathbf{\Gamma}) \rangle$. Using Schreier's formula (see Theorem 4.50), we can write the rank of $\langle \mathsf{Sk}(\mathbf{\Gamma}) \rangle$ in terms of its index. Indeed, $\mathrm{rk}(\langle \mathsf{Sk}(\mathbf{\Gamma}) \rangle) - 1 = |\mathbb{F}_n : \langle \mathsf{Sk}(\mathbf{\Gamma}) \rangle|(n-1) = k_1(n-1)$, so there are $k_1(n-1)+1$ labels whose value might be nonzero. Given that these abelian labels are considered modulo the basepoint subgroup, the number of possible choices for each of them is precisely the index of the basepoint subgroup in $\mathbb{Z}^m$, which we know is equal to $\frac{k}{k_1}$. Therefore, the number of possible abelian labellings for the arcs is $\left(\frac{k}{k_1}\right)^{k_1(n-1)+1}$.

Since the three elements listed above determine $\mathbf{\Gamma}$, for the value k_1 we had fixed, the product of the three numbers that we have obtained is the number of enriched automata with k_1 vertices which have the properties mentioned in the first paragraph of the proof. To finish the argument, we must simply sum the number we have obtained over all possible divisors k_1 of k and that yields the formula in the statement. □

We can see how many finite index subgroups of index k we have in $\mathbb{F}_n \times \mathbb{Z}^m$ for certain values of n, m and k in Table 3.

$(n,m)\backslash k$	1	2	3	4	5	6	7
$(0,3)$	1	7	13	35	31	91	57
$(2,0)$	1	3	13	71	461	3447	29093
$(2,1)$	1	7	22	111	486	3772	29142
$(2,2)$	1	15	49	255	611	4827	29485
$(2,3)$	1	31	130	799	1236	9232	31886
$(3,1)$	1	15	124	2431	68766	3025596	173773496
$(3,2)$	1	31	205	3263	69391	3057907	173775897
$(3,3)$	1	63	448	5951	72516	3139944	173792704

Table 3: Values of $N_k(\mathbb{F}_n \times \mathbb{Z}^m)$ for small n, m and k.

6. Future work

The work that we have presented so far has some possible continuations. Since FTFA groups can be thought of as members of larger families of groups, it is reasonable to think that the results that we have obtained for FTFA groups might be generalizable to these larger families. In this vein, two families of groups for which it is natural to try to obtain a formula for the number of subgroups of a given finite index are free-abelian by free groups (which we will present in Section 6.1) and Droms (which will be dealt with in Section 6.2).

6.1 Free-abelian by free groups

The groups we studied in Section 5, FTFA groups, which are the direct product of a free group and a free-abelian group, are actually a particular case of a more general notion which we present next.

Definition 6.1. Let $\mathbb{Z}^m = \langle t_1, \ldots, t_m | t_i t_j = t_j t_i, \forall i, j \in [m] \rangle$ be a free-abelian group of finite rank m with abelian basis $T = \{t_1, \ldots, t_m\}$, let $\mathbb{F}_n = \langle x_1, \ldots, x_n | - \rangle$ be a free group of rank n with basis $X = \{x_1, \ldots, x_n\}$ and let $\mathbf{A_j} \in GL_m(\mathbb{Z})$ for each $j \in \{1, \ldots, n\}$ be automorphisms of $\mathbb{Z}^m$. The semidirect product $\mathbb{G}_\mathbf{A} = \mathbb{F}_n \ltimes_{\mathbf{A}_\bullet} \mathbb{Z}^m$, with action the homomorphism given by

$$\begin{array}{rccl} \mathbf{A}_\bullet : & \mathbb{F}_n & \to & GL_m(\mathbb{Z}) \\ & x_j & \mapsto & \mathbf{A_j}, \end{array}$$

is called a *free-abelian by free group*, which we will abbreviate by FABF.

Remark 6.2. If $w = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} \cdots x_{i_p}^{\epsilon_p}$ is a word where $i_j \in \{1, \ldots, n\}$ and $\epsilon_j \in \{-1, +1\}$ for all $j \in \{1, \ldots, p\}$, we will write

$$\mathbf{A}_w := \mathbf{A}_{\mathbf{i_1}}^{\epsilon_1} \mathbf{A}_{\mathbf{i_2}}^{\epsilon_2} \cdots \mathbf{A}_{\mathbf{i_p}}^{\epsilon_p}$$

for the product of matrices obtained replacing each letter x_j in w by the corresponding matrix $\mathbf{A_j}$. Also, for a subgroup $H \leqslant \mathbb{F}_n$, we will write

$$\mathbf{A}_H := \{\mathbf{A}_w : w \in H\}.$$

With the notation above, a presentation for a FABF group $\mathbb{G}_\mathbf{A} = \mathbb{F}_n \ltimes_{\mathbf{A}_\bullet} \mathbb{Z}^m$ with a specified action is the following:

$$\mathbb{G}_\mathbf{A} = \mathbb{F}_n \ltimes_{\mathbf{A}_\bullet} \mathbb{Z}^m = \left\langle \begin{array}{c} x_1, \ldots, x_n, \\ t_1, \ldots, t_m \end{array} \middle| \begin{array}{cc} x_k^{-1} t_i x_k = t_i \mathbf{A_k}, & \forall i \in [m], \forall k \in [n] \\ t_i t_j = t_j t_i, & \forall i, j \in [m] \end{array} \right\rangle. \tag{15}$$

Remark 6.3. The case where the action is trivial (that is, $\mathbf{A_j} = \mathbf{I_m}$ for all $j \in \{1, \ldots, n\}$) corresponds to the direct product $\mathbb{F}_n \times \mathbb{Z}^m$, the family of groups studied in Section 5.

Given a word w on $(X \cup T)^\pm$, we can use the relations in (15) to move the t_i's orderly to the right and obtain a normal form for the element represented by w. Indeed, we define the normal form for the element of $\mathbb{G}_\mathbf{A}$ represented by the word w as

$$u t^\mathbf{a} = u(x_1, \ldots, x_n) \cdot t_1^{a_1} \cdots t_m^{a_m},$$

where u is the element of $\mathbb{F}_n$ represented by the free part of the element in $\mathbb{F}_n \ltimes_{\mathbf{A}_\bullet} \mathbb{Z}^m$ corresponding to the word w and $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{Z}^m$ is its abelian part. In addition, we will denote by $\pi : \mathbb{G}_\mathbf{A} \to \mathbb{F}_m$ the map assigning $u t^\mathbf{a} \mapsto u$.

With this notation, the semidirect conjugation relation in $\mathbb{G}_{\mathbf{A}}$ can be written as

$$u^{-1}t^{\mathbf{a}}u = t^{\mathbf{a}\mathbf{A}_u}, \text{ where } \mathbf{a} \in \mathbb{Z}^{\mathbf{m}} \text{ and } u \in \mathbb{F}_n.$$

Equivalently, we have the following multiplication rules:

$$t^{\mathbf{a}}u = ut^{\mathbf{a}\mathbf{A}_u} \text{ and } ut^{\mathbf{a}} = t^{\mathbf{a}\mathbf{A}_u^{-1}}u.$$

As it happened with free groups and FTFA groups, the subgroups of a FABF group are FABF as well. Moreover, a generalisation of the techniques developed in section 5 allow to establish again a bijection between subgroups and enriched automata (see [5]).

The enriched automata in this new bijection are the same objects presented in Definition 5.11. In this context, we will also have that the set of enriched labels of $\mathbf{b}$-walks in an enriched automata $\mathbf{\Gamma}$ is a subgroup in $\mathbb{G}_{\mathbf{A}}$, which we call the subgroup recognised by $\mathbf{\Gamma}$ and denote by $\langle \mathbf{\Gamma} \rangle_{\mathbf{A}}$. However, the way in which enriched arcs are meant to be read in the context of the semidirect product is a bit different from the FTFA case, since we must consider the action. Indeed, for a given action $\mathbf{A}_\bullet : \mathbb{F}_n \to GL_m(\mathbb{Z}^m)$, the arc $e \equiv p \xrightarrow[x_j]{\mathbf{a}_1 \quad \mathbf{a}_2} q$ is meant to be read as we indicate in Figure 15. And, taking this into account, enriched labels of walks in $\mathbf{\Gamma}$ are defined analogously to the FTFA case.

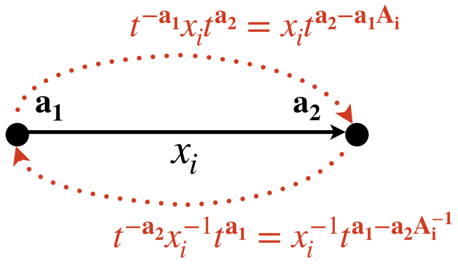

Figure 15: Reading of enriched labelling in FABF groups.

Another trait that differentiates the enriched automata in the FABF case is that we may obtain elements in $\mathbb{Z}^m$ which do not belong to the basepoint subgroup by conjugation. Let us clarify this. Suppose that $ut^{\mathbf{a}}$ is the label of a $\mathbf{b}$-walk γ in $\mathbf{\Gamma}$. If we read the inverse walk of γ, followed by an element $\mathbf{c} \in \mathbb{Z}^m$ belonging to the basepoint subgroup and then we read γ, what we obtain is

$$u^{-1}t^{-\mathbf{a}} \cdot t^{\mathbf{c}} \cdot ut^{\mathbf{a}} = u^{-1}t^{\mathbf{c}}t^{-\mathbf{a}}ut^{\mathbf{a}} = u^{-1}t^{\mathbf{c}}ut^{-\mathbf{a}\mathbf{A}_\mathbf{u}}t^{\mathbf{a}} = t^{\mathbf{c}\mathbf{A}_\mathbf{u}}t^{-\mathbf{a}\mathbf{A}_\mathbf{u}}t^{\mathbf{a}}.$$

Now, if we read just γ followed by its inverse, we have

$$u^{-1}t^{-\mathbf{a}}ut^{\mathbf{a}} = u^{-1}ut^{-\mathbf{a}\mathbf{A}_\mathbf{u}}t^{\mathbf{a}} = t^{-\mathbf{a}\mathbf{A}_\mathbf{u}}t^{\mathbf{a}}.$$

Thus, $t^{\mathbf{c}\mathbf{A}_\mathbf{u}}$ is an element of $\mathbb{Z}^m$ which belongs to the subgroup recognised by $\mathbf{\Gamma}$, but which may not belong to the basepoint subgroup. Thinking now about the whole basepoint subgroup, if we read the inverse of γ, the basepoint subgroup L and then γ, what we obtain is the conjugate of L by $ut^{\mathbf{a}}$, which is $(L)\mathbf{A}_\mathbf{u}$. This generates certain redundancy when trying to give a unique enriched automaton representing each subgroup, since we might take an enriched automaton with a bigger basepoint subgroup. This motivates the following definition.

Definition 6.4. Let $\mathbf{\Gamma}$ be a $\mathbb{Z}^m$*-enriched* X*-automaton* recognising a subgroup $H \leqslant \mathbb{G}_{\mathbf{A}}$. Then, the *closure* of the basepoint subgroup L in $\mathbf{\Gamma}$ with respect to $\mathbf{A}_\bullet$ is the subgroup

$$\overline{L} := (L)\mathbf{A}_{H\pi} \leqslant H \cap \mathbb{Z}^m.$$

The basepoint subgroup L of $\mathbf{\Gamma}$ is said to be *closed* (in $\mathbf{\Gamma}$ with respect to $\mathbf{A}_\bullet$) if it is equal to its own closure, that is, $\overline{L} = L$. An enriched automaton having a closed basepoint subgroup is called *closed*.

To eliminate the source of redundancy coming from conjugation that we were talking about before, we will need to consider closed enriched automata.

In spite of the complications in the basepoint subgroup that arise due to the effect of conjugation, it is possible to adapt foldings to this new situation and guarantee the computability of the basepoint subgroup in order to obtain a unique representative automaton. We now enunciate without proof the theorem that gives the bijection between FABF groups and certain enriched automata.

Theorem 6.5 (Delgado, Ventura)**.** *Let $\mathbb{F}_X$ be a free group with finite basis X, let $\mathbb{Z}^m$ be a finitely generated free-abelian group, and let $\preccurlyeq$ be a total order on $X^{\pm}$. Then, the map*

$$\begin{array}{rrcl} St_{\preccurlyeq}: & \{\textit{subgr. of } \mathbb{F}_X \ltimes_{\mathbf{A}_\bullet} \mathbb{Z}^m\} & \leftrightarrow & \{\textit{(isom. classes of) Stallings automata mod } \mathbf{b}\} \\ & H & \mapsto & St_{\preccurlyeq}(H,X) \\ & \langle \mathbf{\Gamma} \rangle_{\mathbf{A}} & \leftarrow\!\shortmid & \mathbf{\Gamma} \end{array} \tag{16}$$

is a bijection. Moreover, f.g. subgroups correspond to finite automata and the restriction of this bijection to f.g. subgroups is computable.

In the previous theorem, by Stallings automata we mean closed $\preccurlyeq$-normalised $\mathbb{Z}^m$-enriched X-automata, where the meaning of $\preccurlyeq$-normalised is the same as in the context of FTFA groups. As to $\mathrm{St}_{\preccurlyeq}(H,X)$, we will not give define it explicitely in the context of FABF groups. We simply observe that $\mathrm{St}_{\preccurlyeq}(H,X)$ is a closed enriched automaton.

Once we have this bijection, it is natural to ask whether it could be used to count finite index subgroups in $\mathbb{F}_X \ltimes_{\mathbf{A}_\bullet} \mathbb{Z}^m$ mimicking the approach that we followed for FTFA groups. The following two results, which are generalisations of Proposition 5.39 and Corollary 5.40 for FABF groups, suggest that this similar approach might work.

Proposition 6.6. *Let H be a subgroup of $\mathbb{G}_{\mathbf{A}}$, let $\{v_i\}_{i\in I}$ be a right transversal for $H\pi$ in $\mathbb{F}_n$, and let $\{\mathbf{c_j}\}_{j\in J}$ be a transversal for $L_H = H \cap \mathbb{Z}^m$. Then, $\{v_i t^{\mathbf{c_j}} : i \in I, j \in J\}$ is a right transversal for H in $\mathbb{G}_{\mathbf{A}}$. Hence, $|\mathbb{G}_{\mathbf{A}} : H| = |\mathbb{F}_n : H\pi| \cdot |\mathbb{Z}^m : L_H|$; in particular, the index $|\mathbb{G}_{\mathbf{A}} : H|$ is finite if and only if both $|\mathbb{F}_n : H\pi|$ and $|\mathbb{Z}^m : L_H|$ are finite.*

Corollary 6.7. *Let H be a subgroup of $\mathbb{G}_{\mathbf{A}}$. Then, H has finite index k if and only if the $St_{\preccurlyeq}(H,X)$ is saturated, it has a finite number of vertices k_1 which is a divisor of k and has a basepoint subgroup of finite index $\frac{k}{k_1}$ in $\mathbb{Z}^m$.*

It is clear from these results that, if we wish to determine the number of subgroups of index k in $\mathbb{G}_{\mathbf{A}}$, we will have to count the number of Stallings automata $\mathbf{\Gamma}$ which are saturated, have a finite number of vertices k_1 which is a divisor of k and have a basepoint subgroup of finite index $\frac{k}{k_1}$ in $\mathbb{Z}^m$. It is important to notice that, since Stallings automata are closed in this context, the basepoint subgroup must be closed in $\mathbf{\Gamma}$ with respect to $\mathbf{A}_\bullet$. That is, we are counting the same objects as in Theorem 5.43, but adding the extra condition that the basepoint subgroup L satisfies $L = (L)\mathbf{A}_{H\pi}$, where H is the subgroup recognised by $\mathbf{\Gamma}$.

If $\{u_1, \dots, u_p\}$ is a basis for $H\pi$, the extra condition $L = (L)\mathbf{A}_{H\pi}$ can be reformulated as

$$L = (L)\mathbf{A}_{\mathbf{u_i}}, \text{ for } i \in \{1, \dots, p\}. \tag{17}$$

Recall that, since L must be a finite index subgroup of $\mathbb{Z}^m$, we can associate to it a unique $m \times m$ integer matrix $\mathbf{L}$ of rank m in Hermite Normal Form (using the bijection in Theorem 3.17). Since the rows of $\mathbf{L}$ generate L, condition (17) can be written as

$$\exists \mathbf{X} \in GL_m(\mathbb{Z}) \text{ such that } \mathbf{L} \cdot \mathbf{A}_{\mathbf{u_i}} = \mathbf{X} \cdot \mathbf{L} \text{ for each } i \in \{1, \dots, p\}. \tag{18}$$

If we now regard $\mathbf{L}$ as a matrix over $\mathbb{Q}$ and take into account that its determinant is not zero (as it is the index of L in $\mathbb{Z}^m$, which we are assuming to be finite), we can consider its inverse $\mathbf{L}^{-1}$ and we can reformulate (18) as

$$\mathbf{L}\mathbf{A}_{\mathbf{u_i}}\mathbf{L}^{-1} \in \mathcal{M}_m(\mathbb{Z}) \text{ for all } i \in \{1, \dots, p\}. \tag{19}$$

From this, we can see that a first step to obtain the desired formula for this family of groups would be to determine, given $\mathbf{A} \in GL_m(\mathbb{Z})$, how many $m \times m$ full rank integer matrices in HNF satisfy that $\mathbf{LAL}^{-1}$ is an integer matrix.

Remark 6.8. Since we cannot expect $\mathbf{LAL}^{-1}$ to be an integer matrix for every $\mathbf{L}$ we consider (unless $\mathbf{A}$ is the identity matrix), it is clear that the number of subgroups of index k in a FABF group $\mathbb{F}_n \ltimes_{\mathbf{A}_\bullet} \mathbb{Z}^m$ will be at most $N_k(\mathbb{F}_n \times \mathbb{Z}^m)$.

6.2 Droms groups

Below, we present a second natural generalisation of the family of FTFA groups. The groups of this generalised family can be defined by giving a presentation for them that is encoded in a simple graph. Among these groups, we will focus on Droms groups, which will be defined later.

Definition 6.9. Given a finite simple graph Γ with vertex set $V(\Gamma)$, the corresponding *right-angled Artin group (RAAG)*, denoted by G_Γ, is given by the following presentation:

$$G_\Gamma = \langle V(\Gamma) | xy = yx \Leftrightarrow x \text{ and } y \text{ are adjacent vertices in } \Gamma \rangle.$$

Example 6.10. Some examples of RAAGs are the following:

(i) The free group of rank n, $\mathbb{F}_n$, is a RAAG whose associated graph consists of n isolated vertices.

(ii) The free-abelian group of rank m, $\mathbb{Z}_m$, is a RAAG associated to the complete graph with m vertices, K_m.

(iii) The FTFA group $\mathbb{F}_n \times \mathbb{Z}_m$ is a RAAG whose associated graph is the join of K_m and the graph with n isolated vertices. Recall that the join of two graphs is the result of connecting with edges all the vertices in one of the graphs with all the vertices of the other.

(iv) The group $\mathbb{F}_2 \times \mathbb{F}_2$ is a RAAG associated to the cycle of length 4.

The main theorem by Droms in [14] says that the graph describing a RAAG is unique in the sense of the following theorem.

Theorem 6.11. *Two RAAGs G_Γ and $G_{\Gamma'}$ are isomorphic if and only if the graphs Γ and Γ' are isomorphic.*

The behaviour of RAAGs can be quite wild; for example, the finite index problem for $\mathbb{F}_2 \times \mathbb{F}_2$ is not decidable, so we cannot expect to extend the results about the index to all RAAGs. This suggests that we will need to restrict to a smaller family. Another example of the complicated behaviour of RAAGs is the fact that the closure property that we had for free-abelian, free and FTFA groups (see Theorem 3.7, Theorem 4.47 and Proposition 5.4, respectively) does not hold in general, not all finitely generated subgroups of RAAGs are themeselves RAAGs. Droms provided a condition for a RAAG to have all of its subgroups again of this type, which we state next.

Theorem 6.12. *Every finitely generated subgroup of G_Γ is itself a RAAG if and only if no full subgraph of Γ is a cycle of length four (C_4) or a path of length three (P_4).*

The graphs satisfying this condition are called *Droms graphs* and their associated RAAGs are called *Droms groups*. The family of Droms groups admits a recursive construction with a neat algebraic interpretation.

Theorem 6.13. *The family of Droms graphs (resp., Droms groups) can be recursively defined as the smallest family of graphs $\mathfrak{D}$ (resp., groups $\mathcal{D}$) satisfying the following rules:*

(i) The empty graph, K_0, belongs to $\mathfrak{D}$. (The trivial group $\{1\}$ belongs to $\mathcal{D}$).

(ii) If $\Gamma_1, \Gamma_2 \in \mathfrak{D}$, then the disjoint union $\Gamma_1 \sqcup \Gamma_2$ belongs to $\mathfrak{D}$. (If $G_1, G_2 \in \mathcal{D}$, then their free product $G_1 * G_2$ belongs to $\mathcal{D}$).

(iii) If $\Gamma \in \mathfrak{D}$, the join $K_1 \vee \Gamma$ is a Droms graph. (If $G \in \mathcal{D}$, the direct product $\mathbb{Z} \times G$ is a Droms group).

The recursive description of Droms groups allows to combine Ivanov's graphs (which are a generalisation of Stallings graphs to study subgroups of a free product) and enriched graphs to understand Droms groups. This has already been done successfully in [12], where the intersection problem is solved and, in a work in progress [11], the same authors study and solve the finite index problem among other problems. This supports the possibility of counting finite index subgroups in this family.

References

[1] W. A. Adkins. *Algebra : an approach via module theory*. Graduate texts in mathematics; 136. Springer-Verlag, New York, 1992.

[2] O. V. Bogopolski. *Introduction to group theory.* EMS textbooks in mathematics. European Mathematical Society, 2008.

[3] A. Carvalho. On the dynamics of extensions of free-abelian times free groups endomorphisms to the completion. *Proceedings of the Edinburgh Mathematical Society*, 65(3):705–735, 2022.

[4] H. Cohen. *A Course in computational algebraic number theory*. Graduate texts in mathematics; 138. Springer-Verlag, Berlin, 1993.

[5] J. Delgado. Extensions of free groups: algebraic, geometric, and algorithmic aspects. 2017.

[6] J. Delgado, M. Roy, and E. Ventura. Intersection configurations in free and free times free-abelian groups, 2022.

[7] J. Delgado and E. Ventura. Algorithmic problems for free-abelian times free groups. *Journal of Algebra*, 391:256–283, 2013.

[8] J. Delgado and E. Ventura. A list of applications of Stallings automata. *Transactions on Combinatorics*, 11(3):181–235, 2022.

[9] J. Delgado and E. Ventura. Stallings automata for free-times-abelian groups: intersections and index. *Publicacions Matemàtiques*, 66(2):789 – 830, 2022.

[10] J. Delgado and E. Ventura. Autòmats de Stallings, un camí d'anada i tornada. *Butlletí de la Societat Catalana de Matemàtiques*, 37(1):5–59, 2023.

[11] J. Delgado, E. Ventura, and A. Zakharov. Yet more algorithmic problems for Droms groups. *(Work in progress)*.

[12] J. Delgado, E. Ventura, and A. Zakharov. Intersection problem for Droms RAAGs. *International Journal of Algebra and Computation*, 28, 09 2017.

[13] J. Delgado, E. Ventura, and A. Zakharov. Relative order and spectrum in free and related groups. *Communications in Contemporary Mathematics*, 2021.

[14] C. Droms. Isomorphisms of graph groups. 1987.

[15] M. Hall. Subgroups of finite index in free groups. *Canadian Journal of Mathematics*, 1(2):187–190, 1949.

[16] J. J. Rotman. *An Introduction to the theory of groups*. Graduate texts in mathematics; 148. Springer, New York, 4th ed. edition, 1995.

[17] M. Roy and E. Ventura. Fixed subgroups and computation of auto-fixed closures in free-abelian times free groups. *Journal of Pure and Applied Algebra*, 224(4):106210, 2020.

[18] M. Roy and E. Ventura. Degrees of compression and inertia for free-abelian times free groups. *Journal of Algebra*, 568:241–272, 2021.

[19] J. Sahattchieve. On convex hulls and the quasiconvex subgroups of $\mathbb{F}_m \times \mathbb{Z}^n$. *Groups Complexity Cryptology*, 7(1):69–80, 2015.

[20] J. R. Stallings. Topology of finite graphs. *Inventiones mathematicae*, 71:551–565, 1983.