

# DEPENDENCE OVER SUBGROUPS OF FREE GROUPS

AMNON ROSENMANN AND ENRIC VENTURA

ABSTRACT. Given a finitely generated subgroup  $H$  of a free group  $F$ , we present an algorithm which computes  $g_1, \dots, g_m \in F$ , such that the set of elements  $g \in F$ , for which there exists a non-trivial  $H$ -equation having  $g$  as a solution, is, precisely, the disjoint union of the double cosets  $H \sqcup Hg_1H \sqcup \dots \sqcup Hg_mH$ . Moreover, we present an algorithm which, given a finitely generated subgroup  $H \leq F$  and an element  $g \in F$ , computes a finite set of elements from  $H * \langle x \rangle$  (of the minimum possible cardinal) generating, as a normal subgroup, the “ideal”  $I_H(g) \trianglelefteq H * \langle x \rangle$  of all “polynomials”  $w(x)$ , such that  $w(g) = 1$ . The algorithms, as well as the proofs, are based on the graph-theoretic techniques introduced by Stallings and on the more classical combinatorial techniques of Nielsen transformations. The key notion here is that of dependence of an element  $g \in F$  on a subgroup  $H$ . We also study the corresponding notions of dependence sequence and dependence closure of a subgroup.

## 1. INTRODUCTION

The following is a basic question studied in classical algebra: given a *field extension*  $L/K$  ( $L$  over  $K$ ) and an element  $\alpha \in L$ , is  $\alpha$  *algebraic* over  $K$ , i.e., does there exist a non-trivial polynomial with coefficients in  $K$ , say  $p(x) \in K[x]$ , such that  $p(\alpha) = 0$ , or, otherwise, is  $\alpha$  *transcendental* over  $K$ ? Moreover, when  $\alpha$  is algebraic over  $K$ , it is interesting to study the set of all polynomials over  $K$  annihilating  $\alpha$ , namely  $I_K(\alpha) = \{p(x) \in K[x] \mid p(\alpha) = 0\} \subseteq K[x]$ . As is well known,  $I_K(\alpha)$  is a principal ideal of  $K[x]$ ,  $I_K(\alpha) = m_\alpha(x)K[x]$ , whose unique monic generator  $m_\alpha(x)$  is called the *minimal polynomial* of  $\alpha$  over  $K$ . An interesting algorithmic problem is then to compute  $m_\alpha(x)$  in terms of  $\alpha$ .

Analogous questions can be asked and studied in the context of group theory, where answers and algorithms turn out to be much more complicated. Here, we start with an *extension of groups*  $H \leq G$  and an element  $g \in G$ . The analog of the “ring of polynomials over  $K$ ” is the free product  $H * \langle x \rangle \simeq H * \mathbb{Z}$ , and the analog of the “ideal of polynomials annihilating  $\alpha$ ” is the normal subgroup  $I_H(g) \trianglelefteq H * \langle x \rangle$  of all “polynomials”  $w(x) \in H * \langle x \rangle$ , such that  $w(g) = 1$ . In the present paper, after some general considerations, we concentrate on extensions of free groups,  $H \leq F$ , where  $H$  is finitely generated, and analyze both the set of elements in  $F$  being algebraic over  $H$ , and the set of equations over  $H$  satisfied by a given  $g \in F$ . We give the precise definitions below.

Let  $G$  be a group and  $H \leq G$ . A univariate *equation over  $H$*  (or an  *$H$ -equation*, for short) is a “polynomial equation” of the form

$$(1.1) \quad w(x) = 1,$$

---

Key words and phrases: dependence in free groups, algebraic extension in free groups, equations over free groups, Stallings foldings, Nielsen transformations.

where  $w(x) \in H * \langle x \rangle$ , the free product of  $H$  and the free abelian group of rank 1 generated by the *variable*  $x$ . That is,  $w(x)$  is an expression of the form

$$(1.2) \quad w(x) = h_0 x^{\varepsilon_1} h_1 x^{\varepsilon_2} \cdots h_{d-1} x^{\varepsilon_d} h_d,$$

where  $\varepsilon_i = \pm 1$  and  $h_i \in H$ . We assume that the equation is *non-trivial*, i.e.,  $w(x) \in H * \langle x \rangle \setminus \{1\}$ , and that it is in *reduced form*, i.e.,  $\varepsilon_i = \varepsilon_{i+1}$  whenever  $h_i = 1$ , for  $i = 1, \dots, d-1$ . The *degree* of the equation  $w(x) = 1$  (or of the polynomial  $w(x)$ ), when written in reduced form, is  $d = \sum_{i=1}^d |\varepsilon_i|$ . The equation is *balanced* if  $\sum_{i=1}^d \varepsilon_i = 0$ . It is standard to group together into higher exponents the various possible consecutive occurrences of  $x$  with trivial elements in between; for example,  $h_1 x^2 h_2 x^{-2}$  stands for  $h_1 x 1 x h_2 x^{-1} 1 x^{-1}$ , a balanced equation of degree 4. An element  $g \in G$  is a *solution* to equation (1.1) if  $w(g) = 1$ , that is, the element of  $G$  resulting in substituting  $g$  for  $x$  in the expression (1.2) is the trivial group element.

The area of Group Theory studying equations and their solutions is known as *algebraic geometry over groups*; see [4]: the elements of  $H * \langle x \rangle$  (or, more generally, of  $H * \langle x_1, \dots, x_n \rangle$  in the case of multivariate equations) are the analog of non-commutative polynomials. Following the language from [4], a normal subgroup  $I \trianglelefteq H * \langle x_1, \dots, x_n \rangle$  is called an *ideal*, and the set of its common *zeros* (i.e., the subset of  $G^n$  of common solutions to the set of equations  $\{w(x) = 1 \mid w(x) \in I\}$ ) is an *algebraic set*. There is a vast body of literature about the general problem of solving equations (univariate or multivariate) in a group  $G$ ; see [4, 5, 11, 18, 19] and the references therein. A typical question is to decide, given an equation (or a system of equations), whether it has a solution in  $G$  or not and, in the positive case, to describe the set of all such solutions and its structure. Two of the main results in this direction are Makanin's and Razborov's theorems, which analyze the case of free groups: the first one (see Makanin [11]) solves the decidability part of the problem, while the second one (see Razborov [18, 19]) provides a kind of compact algorithmic description of *all* solutions, in case they exist. These are two very deep results, with intricate proofs, and having numerous important applications.

Here, we restrict ourselves to univariate equations and to free groups. In this particular case, the description of solution sets is much simpler: Bormotov, Gilman and Myasnikov [5] use reduction techniques from formal language theory to show that the solution set to a single equation of degree greater than 1 is either the whole group or a finite union of sets of the form  $\{g_1 g_2^n g_3 \mid n \in \mathbb{Z}\}$ . They also give a polynomial time algorithm for computing this solution set.

In contrast, we adopt here a kind of dual point of view. Instead of studying the solution set to a given equation in a group  $G$ , we fix a subgroup  $H \leq G$  and are interested in the set of all solutions in  $G$  of *all* possible equations over  $H$ . In addition, given an element  $g \in G$ , we study the set of equations over  $H$  satisfied by  $g$ , namely the ideal  $I_H(g) = \{w(x) \in H * \langle x \rangle \mid w(g) = 1\} \trianglelefteq H * \langle x \rangle$ : Is it trivial or not? And, if not, can we compute a finite set of generators for it (as a normal subgroup)? We shall answer and give algorithms for these and related questions, when the ambient group  $G$  is a free group.

The fundamental notion here is that of dependence of an element  $g \in G$  on a subgroup  $H \leq G$ , first introduced in Rosenmann [22]:

**Definition 1.1.** Let  $G$  be a group,  $H \leq G$  a subgroup, and  $g \in G$  an element. We say that  $g$  is *dependent on*  $H$  if there exists a non-trivial  $H$ -equation  $w(x) = 1$  that is satisfied by  $g$ . More generally,  $g$  is dependent on a subset  $S \subseteq G$  if it is dependent

on the subgroup  $H = \langle S \rangle$ . We denote by  $\text{dep}_G(H)$  the set of elements in  $G$  that depend on  $H$ , and by  $\text{Dep}_G(H) = \langle \text{dep}_G(H) \rangle$ , the subgroup they generate, called the *dependence* subgroup of  $H$ . When there is no risk of confusion, we shall delete the subscript  $G$  from the notation.

**Remark 1.2.** The notion of dependence, as given above, naturally suits free groups (as defined in [22], and as studied here). However, other possible definitions suit better in other contexts. For example, when  $G$  is an abelian group and  $1 \neq H \leq G$  then every  $g \in G$  satisfies the equation  $h x h^{-1} x^{-1} = 1$  (for each  $h \in H$ ) and so, it is dependent on  $H$ . Here, we may define an element  $g$  to be dependent on  $H$  if it satisfies an equation of the form  $x^n h = 1$ ,  $n \in \mathbb{Z} \setminus \{0\}$ ,  $h \in H$ . When  $G$  is free abelian and  $H$  is finitely generated then this definition is equivalent to  $\text{rk}(\langle H, g \rangle) \leq \text{rk}(H)$ . As seen below (Proposition 2.1), the latter is also equivalent to Definition 1.1 in the case of free groups.

**Remark 1.3.** Clearly,  $H \subseteq \text{dep}_G(H) \subseteq \text{Dep}_G(H) \leq G$  but, in general,  $\text{dep}_G(H)$  is not a subgroup. Also, when  $H \leq K \leq G$ , we have  $\text{dep}_K(H) = K \cap \text{dep}_G(H)$  and  $\text{Dep}_K(H) \leq K \cap \text{Dep}_G(H)$ , where the inclusion may be strict. We shall see examples of these situations in the free context; see Examples 2.2.

**Examples 1.4.** (i) If  $g \in H$  then  $g$  is dependent on  $H$ , satisfying the equation  $g^{-1}x = 1$  (also  $gx^{-1} = 1$ ) of degree 1.  
(ii) If  $g \notin H$  but  $H^g \cap H \neq 1$  then  $g$  is dependent on  $H$ , satisfying the balanced equation  $x^{-1}hxh'^{-1} = 1$  of degree 2, where  $h, h' \in H$  are such that  $g^{-1}hg = h'$ . It follows that if  $\{1\} \neq H \trianglelefteq G$  is a nontrivial normal subgroup of  $G$  then  $\text{dep}(H) = G$ . In particular, this is the case when  $\{1\} \neq H$  is a subgroup of the center  $Z(G)$  of  $G$ . It follows also that  $N_G(H) \subseteq \text{dep}(H)$ , where  $N_G(H) = \{g \in G \mid g^{-1}Hg = H\}$  is the normalizer of  $H$  in  $G$ .  
(iii) If  $H$  is of finite index in  $G$  then  $\text{dep}(H) = G$ : any  $g \in G$  satisfies the equation  $x^k h^{-1} = 1$ , where  $k \geq 1$  and  $h \in H$  are such that  $g^k = h$ .  
(iv)  $\text{dep}(\{1\})$  is, precisely, the set of torsion elements of  $G$ . This follows from the fact that the only equations of positive degree over the trivial subgroup are those of the form  $x^n = 1$ ,  $n \in \mathbb{Z} \setminus \{0\}$ .

Clearly, the notion of “ $g$  being dependent on  $H$ ” is a group-theoretic analog of “ $\alpha$  being algebraic over the field  $K$ ”. At this point, we can already observe a relevant initial difference with classical field theory: the sum and product of two algebraic elements over  $K$  are also algebraic over  $K$  while, here, the product of two dependent elements on a subgroup  $H$  may very well not be dependent on  $H$ ; see Example 2.2(i). So, one can expect the structure of the set  $\text{dep}(H)$  to be more complicated than its analog in the classical situation, where the algebraic elements over  $K$  just form an intermediate field between  $K$  and  $F$ . Here,  $\text{dep}(H)$  is not even a subgroup but, still, in the free group case, it will not be hard to understand its structure; see Theorem 4.1 below.

In order to describe the set of elements  $\text{dep}(H)$ , the following easy observation will be important:  $\text{dep}(H)$  is always the disjoint union of maybe infinitely many  $(H, H)$ -double cosets:

**Observation 1.5.** *Let  $G$  be a group and let  $H \leq G$ . If  $g \in \text{dep}(H)$  then all the elements of the double coset  $HgH$  depend on  $H$  as well. Moreover, they all satisfy an  $H$ -equation of the same minimal degree.*

*Proof.* Let  $w(x) = h_0x^{\varepsilon_1}h_1x^{\varepsilon_2}\cdots h_{d-1}x^{\varepsilon_d}h_d = 1$  be an  $H$ -equation satisfying  $w(g) = 1$ . Then, for every  $h, h' \in H$ , we have that the new equation

$$w'(x) = h_0(h^{-1}xh'^{-1})^{\varepsilon_1}h_1(h^{-1}xh'^{-1})^{\varepsilon_2}\cdots h_{d-1}(h^{-1}xh'^{-1})^{\varepsilon_d}h_d = 1$$

satisfies  $w'(hgh') = 1$ , showing that  $hgh' \in \text{dep}(H)$ . Since (after appropriate cancellations)  $w'(x) = 1$  has the same or smaller degree than  $w(x) = 1$ , it follows that all the elements of  $HgH$  satisfy an  $H$ -equation of the same minimal degree.  $\square$

The following is another elementary result. Its converse, however, is not true in general (see Example 2.2(iii) below).

**Observation 1.6.** *Let  $H \leq G$ ,  $g \in G$ , and  $k \in \mathbb{Z} \setminus \{0\}$ . If  $g^k \in G$  is dependent on  $H$  then  $g$  is dependent on  $H$  as well.*

*Proof.* If  $h_0x^{\varepsilon_1}h_1x^{\varepsilon_2}\cdots h_{d-1}x^{\varepsilon_d}h_d = 1$  is a non-trivial  $H$ -equation satisfied by  $g^k$  then,  $h_0x^{k\varepsilon_1}h_1x^{k\varepsilon_2}\cdots h_{d-1}x^{k\varepsilon_d}h_d = 1$  is a non-trivial  $H$ -equation satisfied by  $g$ .  $\square$

Two related notions are those of a dependence-closed subgroup and the dependence closure operator. The latter appeared first in Rosenmann [22] and it coincides with the notion of elementary-algebraic extension closure from Miasnikov–Ventura–Weil [16].

**Definition 1.7.** Let  $H \leq G$ . The subgroup  $H$  is called *dependence-closed* if  $\text{Dep}(H) = H$ , i.e., if the only elements  $g \in G$  which are solutions to non-trivial  $H$ -equations are those  $g \in H$ . For example, any free factor of  $G$  is clearly dependence-closed.

When  $H$  is not dependence-closed then  $\text{dep}(H)$ , the set of *all* dependent elements on  $H$ , strictly contains  $H$ . But then, when constructing the subgroup  $\text{Dep}(H)$  generated by these elements, new elements may arise, which depend on  $\text{Dep}(H)$  but not on  $H$ . We can then iterate this process of executing the dependence operator and ask ourselves whether the process finally stabilizes, that is, do we reach a dependence-closed subgroup after finally many steps, or can the process continue indefinitely? In Proposition 7.3, we show that when  $H$  is a finitely generated subgroup of a free group then the process indeed stabilizes after finitely many steps. However, the number of steps may be arbitrary large, even in the case of subgroups of the free group of rank 2, as shown in Example 7.1, but it is still bounded by the total length of the generators of  $H$  (see Proposition 7.3).

**Definition 1.8.** Let the ascending sequence of subgroups  $H_0 \leq H_1 \leq H_2 \leq \cdots \leq G$  be defined by  $H_0 = H$  and  $H_i = \text{Dep}(H_{i-1}) = \text{Dep}^i(H)$ , for  $i \geq 1$ . We define the *dependence closure* of  $H$  to be the subgroup

$$\widehat{\text{Dep}}(H) = \bigcup_{i \geq 0} H_i \leq G.$$

If this ascending sequence stabilizes after finitely many steps, we define the *dependence length* of  $H$  to be  $\text{depl}(H) = \min\{j \geq 0 \mid H_j = \widehat{\text{Dep}}(H)\}$ ; otherwise, we let  $\text{depl}(H) = \infty$ .

**Observation 1.9.** *For any subgroup  $H \leq G$ ,  $\widehat{\text{Dep}}(H)$  is the smallest dependence-closed subgroup of  $G$  containing  $H$ .*

*Proof.* Let  $g \in G$  be dependent on  $\widehat{\text{Dep}}(H)$ , i.e.,  $g$  is a solution to some non-trivial  $\widehat{\text{Dep}}(H)$ -equation  $w(x) = h_0 x^{\varepsilon_1} h_1 \cdots x^{\varepsilon_d} h_d = 1$ . Since  $h_0, h_1, \dots, h_d \in \widehat{\text{Dep}}(H)$ , there exists  $m \geq 0$ , such that  $h_0, h_1, \dots, h_d \in \text{Dep}^m(H)$ . Thus,  $w(x) = 1$  is also a non-trivial  $\text{Dep}^m(H)$ -equation and hence,  $g \in \text{Dep}^{m+1}(H) \leq \widehat{\text{Dep}}(H)$ . Therefore,  $\widehat{\text{Dep}}(H)$  is dependence-closed. The rest of the statement is clear.  $\square$

The following two propositions are straightforward, and we leave their proofs to the reader.

**Proposition 1.10.** *Let  $H \leq K \leq G$ . If  $H$  is dependence-closed in  $K$ , and  $K$  is dependence-closed in  $G$  then  $H$  is dependence-closed in  $G$ .*  $\square$

**Proposition 1.11.** *Let  $H \leq G$  be a dependence-closed subgroup of a group  $G$ . Then:*

- (i)  $H$  is malnormal in  $G$ :  $H^g \cap H = 1$  for every  $g \in G \setminus H$ ;
- (ii)  $H$  is pure in  $G$  (also called root-closed, radical-closed): if  $g^n \in H$ ,  $n \neq 0$ , then  $g \in H$ ;
- (iii) if  $H \leq K \leq G$  and  $H \neq K$  then  $|K : H| = \infty$ ;
- (iv) if  $K$  is a free factor of  $H$  then  $K$  is dependence-closed in  $G$ ;
- (v) if  $K \leq G$  is also dependence-closed in  $G$  then so is  $H \cap K$ .  $\square$

In the following and along the rest of the paper, when referring to morphisms, we adopt the notation with arguments on the left:  $x \mapsto (x)\varphi = x\varphi$ , and compositions denoted accordingly:  $x \mapsto x\varphi \mapsto x\varphi\phi$ .

Let us now look at  $H$ -equations from a different perspective. When  $H \leq G$  and  $g \in G$ , we can consider the group homomorphism

$$(1.3) \quad \begin{aligned} \varphi_{H,g}: H * \langle x \rangle &\rightarrow G, \\ h &\mapsto h, \forall h \in H, \\ x &\mapsto g, \end{aligned}$$

which is well defined by the universal property of free products. Then,  $(w(x))\varphi_{H,g} = w(g)$ . So, in this setting,  $g$  is a solution to  $w(x) = 1$  if and only if  $w(x) \in \ker \varphi_{H,g}$ . Thus, the set of  $H$ -equations satisfied by  $g$  is exactly

$$\{w(x) = 1 \mid w(x) \in \ker \varphi_{H,g}\},$$

and  $\ker \varphi_{H,g}$  is a normal subgroup of  $H * \langle x \rangle$ . Hence, a natural way to describe these  $H$ -equations is by giving a set of generators for the ideal  $I_H(g) = \ker \varphi_{H,g}$  as a normal subgroup of  $H * \langle x \rangle$ . This is what we do in the free case: we show that  $I_H(g)$  is always finitely generated (as a normal subgroup) and we provide an algorithm computing a set of generators for it, of the minimum possible cardinal; see Theorem 5.3.

**Organization of the paper.** After this section, where the basic notions and definitions corresponding to dependence on subgroups in general groups have been introduced, we restrict ourselves to free groups  $F$  for the rest of the paper. In Section 2 we exhibit basic results for free groups. In Section 3 we present a brief description of the well-known Stallings techniques for studying subgroups of a free group, which play a central role in the paper. Then, in Section 4, we examine closely the way we can use Stallings foldings in order to provide an explicit description of the set of elements that depend on a finitely generated subgroup  $H \leq F$ . This set is proved to have the form of a finite disjoint union of double cosets  $\text{dep}(H) = Hg_0H \sqcup Hg_1H \sqcup \cdots \sqcup Hg_nH$ ,

where  $g_0 = 1$  and the  $g_i$ 's are computable and generate  $\text{Dep}(H)$ ; see Theorem 4.1. In Section 5 we present two alternative algorithms for computing a minimal finite set of normal generators for the ideal (i.e., normal subgroup)  $I_H(g) \trianglelefteq H * \langle x \rangle$ , for a given fixed element  $g \in F$ ; see Theorem 5.3. The first algorithm is based on Nielsen transformations and the second one on Stallings graph-theoretic techniques providing, respectively, an algebraic and a geometric reason (in a way, complementary to one another) for such equations to exist. Finally, in Section 7 we study further the notion of a dependence-closed subgroup, and the corresponding closure operator within the context of free groups  $F$ , including examples of subgroups  $H \leq F_2$  with arbitrarily large dependence length. We close the paper highlighting a few interesting questions for further research.

A preliminary version of this paper was uploaded to arXiv on July 2021; see [24]. A year later, in the process of writing the present final version, we have been informed of a recent further development in this interesting topic: also applying Stallings techniques, Dario Ascari [2] has gone further and has analyzed the set of degrees of the polynomials in the ideal  $I_H(g)$ . Answering one of our questions from [24], he presented an algorithm that computes a non-trivial polynomial in  $I_H(g)$  of a minimal degree. Also, he exhibited an interesting example of a finitely generated subgroup  $H \leq F$ , whose corresponding ideal  $I_H(g)$  *cannot* be generated by its polynomials of minimal degree, even as a normal subgroup (providing another intriguing difference with the more classical field theory). See also Ascari [3] for a more language theoretically oriented exposition of similar results.

## 2. DEPENDENCE IN FREE GROUPS

For the rest of the paper we concentrate on free groups and study the above notions in this setting, both from the algebraic and the algorithmic points of view. We adopt the following notation: a free group is generally denoted by  $F$ ; also by  $F_r$ , if we want to emphasize its rank,  $\text{rk}(F_r) = r$ ; and by  $F(A)$ , if we want to emphasize a basis (a set of free generators)  $A \subseteq F$  for it. The notations  $H \leq_{\text{fg}} F$  and  $H \leq_{\text{ff}} F$  mean that  $H$  is a finitely generated subgroup, respectively, a free factor of  $F$ .

The next proposition follows from works by Nielsen and Schreier (see Rosenmann [22, Lemma 1.1], or Miasnikov–Ventura–Weil [16, Prop. 3.13]) and provides equivalent definitions for dependence of elements in the setting of free groups.

**Proposition 2.1.** *Let  $H \leq F$  and  $g \in F$ . The following statements are equivalent:*

- (a)  $g$  does not depend on  $H$ ;
- (b) the morphism  $\varphi_{H,g}: H * \langle x \rangle \rightarrow F, h \mapsto h, x \mapsto g$  is injective;
- (c)  $H$  is a proper free factor of  $\langle H, g \rangle$ ;
- (d)  $H$  is contained in a proper free factor of  $\langle H, g \rangle$ ;
- (e)  $\text{rk}(\langle H', g \rangle) = \text{rk}(H') + 1$  for every finitely generated subgroup  $H' \leq H$ ;
- (f)  $\text{rk}(\langle H', g \rangle) > \text{rk}(H')$  for every finitely generated subgroup  $H' \leq H$ .  $\square$

In view of Proposition 2.1, it is quite easy to decide, given  $H \leq_{\text{fg}} F$  and  $g \in F$ , whether  $g$  is dependent on  $H$  or not: we only need to compute the rank of  $\langle H, g \rangle$ . In case  $g$  is dependent on  $H$ , we can even find an explicit non-trivial  $H$ -equation  $w(x) = 1$ , such that  $w(g) = 1$ , by a brute force algorithm, enumerating all possible  $H$ -equations and checking for which one is  $g$  a solution. In the following sections we tackle more challenging problems:

- (i) in Section 4 we provide an effective algorithm which, given  $H \leq_{\text{fg}} F$ , computes a finite set of generators for  $\text{Dep}(H)$ ;
- (ii) in Section 5 we present two independent algorithms (both faster and more interesting than the brute force algorithm) which, given  $g \in \text{dep}(H)$ , results in a representation of *all* the  $H$ -equations having  $g$  as a solution.

**Examples 2.2.** Let  $F_2 = F(\{a, b\})$  be a free group of rank 2.

- (i) For  $H = \langle a^2, b^2 \rangle$ , we have  $a, b \in \text{dep}(H)$  (being solutions to the  $H$ -equations  $x^2 a^{-2} = 1$  and  $x^2 b^{-2} = 1$ , respectively) and so,  $\text{Dep}(H) = F_2$ . However,  $ab \notin \text{dep}(H)$  since  $\{a^2, b^2, ab\}$  is a freely independent subset of  $F_2$ . It follows that  $\text{dep}(H)$  is not a subgroup and thus, it is strictly contained in  $\text{Dep}(H)$ .
- (ii) When  $H = \langle a^2, b^2 \rangle$  and  $K = \langle a^2, b^2, ab \rangle \leq F_2$  then  $H \leq_{\text{ff}} K \leq F_2$ . It follows that  $\text{Dep}_K(H) = H$  and  $K \cap \text{Dep}_{F_2}(H) = K \cap F_2 = K$ , so that the inclusion  $\text{Dep}_K(H) \leq K \cap \text{Dep}_{F_2}(H)$  is strict.
- (iii) For  $H = \langle b, aba^{-1} \rangle \leq F_2$ , we have  $a \in \text{dep}(H)$ , whereas  $a^r \notin \text{dep}(H)$  for  $|r| \geq 2$ .
- (iv) Let  $F$  be a free group and  $g \in F$  not being a proper power. Then, for every  $0 \neq r \in \mathbb{Z}$ ,  $\text{dep}(\langle g^r \rangle) = \text{Dep}(\langle g^r \rangle) = \langle g \rangle$ . In particular,  $\langle g^r \rangle$  is dependence-closed if and only if  $r = \pm 1$ , i.e., the dependence-closed cyclic subgroups are, precisely, the maximal ones.
- (v) Let  $F$  be a free group,  $g \in F$ , and  $H, K \leq F$ , such that  $F = H * \langle g \rangle$  and  $H < K$  (strict inclusion). Then,  $\text{Dep}(K) = F$  because  $g$  is dependent on  $K$ .

When  $H \leq_{\text{fg}} F$  then  $\text{Dep}(H) \leq_{\text{fg}} F$  and, moreover,  $\text{rk}(\text{Dep}(H)) \leq \text{rk}(H)$ . This follows from results in Rosenmann [22] and Miasnikov–Ventura–Weil [16]; for completeness, we offer here a direct and elementary proof.

**Lemma 2.3.** *Let  $H_0 \leq_{\text{fg}} H_1 \leq_{\text{fg}} H_2 \leq_{\text{fg}} \dots$  be a non-decreasing sequence of finitely generated subgroups of a free group  $F$ , satisfying  $\text{rk}(H_i) \geq \text{rk}(H_{i+1})$ , for  $i \geq 0$ . Let  $H = \bigcup_{i \geq 0} H_i$ . Then  $\text{rk}(H) = \lim_{i \rightarrow \infty} \text{rk}(H_i)$  and, furthermore, there exists  $m$ , such that  $H = H_i$  for all  $i \geq m$ .*

*Proof.* Let  $r_i = \text{rk}(H_i)$ , for each  $i \geq 0$ , and let  $r_H = \text{rk}(H)$ . The sequence  $(r_i)_{i \geq 0}$  of natural numbers is monotone non-increasing and therefore eventually constant: there exists  $r \geq 0$  and  $m' \geq 0$  such that  $r_i = r$ , for all  $i \geq m'$ . Suppose now that  $r_H > r$ . It follows that there exists  $H' \leq_{\text{ff}} H$  of rank  $r + 1$ . But then,  $H' \leq H_{m''}$ , for some  $m''$ , and, in fact,  $H' \leq_{\text{ff}} H_i$ , for all  $i \geq m''$ , which is in contradiction to  $\text{rk}(H_i) = r$  for all  $i \geq m'$ . Therefore,  $r_H \leq r$  and there exists  $m$ , such that  $H_m$  contains a generating set of  $H$ , which implies that  $H = H_i$ , for all  $i \geq m$ , and  $r_H = r$ .  $\square$

**Proposition 2.4.** *Let  $H \leq_{\text{fg}} F$ . Then,  $\text{rk}(\text{Dep}(H)) \leq \text{rk}(H)$ .*

*Proof.* Being finitely generated,  $H$  is contained in a finitely generated free factor of  $F$  (even in the case that  $F$  is not countably generated). Therefore, there are only countably many elements in  $F$  depending on  $H$ , say  $(g_i)_{i \geq 1}$ . Let  $(H_i)_{i \geq 0}$  be the sequence of ascending subgroups of  $F$  defined by  $H_0 = H$  and  $H_{i+1} = \langle H_i, g_{i+1} \rangle$ , for  $i > 0$ . Since  $g_{i+1} \in \text{dep}(H)$  then  $g_{i+1} \in \text{dep}(H_i)$  and hence, by Proposition 2.1(vi),  $\text{rk}(H_{i+1}) \leq \text{rk}(H_i)$ , for each  $i$ . The result then follows by Lemma 2.3.  $\square$

**Proposition 2.5.** *Let  $H, K \leq G$ . Then,*

- (i)  $\text{Dep}(H \cap K) \leq \text{Dep}(H) \cap \text{Dep}(K)$  and the inclusion may be strict;
- (ii)  $\text{Dep}(\langle H, K \rangle) \geq \langle \text{Dep}(H), \text{Dep}(K) \rangle$  and the inclusion may be strict.

*Proof.* (i). The inclusion is immediate by definition. As an example for a strict inclusion, let  $F = F(\{a, b, c\})$ ,  $H = \langle a^{-1}ba, b \rangle$  and  $K = \langle a^{-1}ca, c \rangle$ . Then  $H \cap K = 1$  and so,  $\text{Dep}(H \cap K) = 1$ . However,  $\text{Dep}(H) = \langle a, b \rangle$ ,  $\text{Dep}(K) = \langle a, c \rangle$ , hence  $\text{Dep}(H) \cap \text{Dep}(K) = \langle a \rangle$ .

(ii) The inclusion is clear. As an example for a strict inclusion, let  $F = F(\{a, b\})$ ,  $H = \langle a^2b \rangle$  and  $K = \langle a^4b \rangle$ . By Example 2.2(iv),  $\text{Dep}(H) = H$  and  $\text{Dep}(K) = K$ . But  $\langle H, K \rangle = \langle a^2, b \rangle$  and so,  $\text{Dep}(\langle H, K \rangle) = F$ , which strictly contains  $\langle a^2, b \rangle = \langle \text{Dep}(H), \text{Dep}(K) \rangle$ .  $\square$

### 3. STALLINGS GRAPH-THEORETIC TECHNIQUES

Let  $A = \{a_1, \dots, a_r\}$  be an alphabet of  $r$  letters, let  $A^\pm = \{a_1, \dots, a_r, a_1^{-1}, \dots, a_r^{-1}\}$  be its formal involutive closure, and let  $F(A)$  be the free group on  $A$  (formally,  $F(A)$  is the free monoid  $(A^\pm)^*$  on  $A^\pm$ , modulo the equivalence relation generated by the elementary reductions  $a_i a_i^{-1} \sim a_i^{-1} a_i \sim 1$ ). In 1983, elaborating on previous ideas by several authors, Stallings [26] established the notion of so-called *Stallings A-automata*: oriented graphs (allowing loops and parallel edges) with labels from  $A^\pm$  at the edges, being *involutive* (i.e., for every edge  $e$  from  $p$  to  $q$  with label  $a \in A$  there is an edge  $e^{-1}$  from  $q$  to  $p$  labelled  $a^{-1}$ ;  $e$  and  $e^{-1}$  are said to be *inverse* to each other), with a selected vertex called the *basepoint* (denoted here  $\bullet$ ), and being connected, *deterministic* (there are no two different edges with the same label coming from, or into, the same vertex) and *trim* (every vertex appears in some reduced closed path through the basepoint). For the underlying oriented graph of an  $A$ -automaton we shall use the standard notation  $(V, E, \iota, \tau)$ , where  $V$  is the set of vertices,  $E$  is the set of edges, and  $\iota, \tau: E \rightarrow V$  are the incidence (initial and terminal) functions. A (nontrivial) *path* of length  $n \geq 1$  is a concatenation of edges  $\gamma = e_1^{\varepsilon_1} \cdots e_n^{\varepsilon_n}$ , such that  $\tau e_i^{\varepsilon_i} = \iota e_{i+1}^{\varepsilon_{i+1}}$  (the terminal vertex of an edge is the initial vertex of the following edge), for  $i = 1, \dots, n-1$ . The label of  $\gamma$  is  $\ell(\gamma) = (\ell(e_1))^{\varepsilon_1} \cdots (\ell(e_n))^{\varepsilon_n}$ , the product of the labels of the edges, understood as an element of  $F(A)$ . A path is *reduced* if it has no backtracking, i.e., if  $\varepsilon_i = \varepsilon_{i+1}$  whenever  $e_i = e_{i+1}$ . Note, that in the deterministic case, a path  $\gamma$  is reduced if and only if its label  $\ell(\gamma)$  is a reduced word of  $(A^\pm)^*$ . A path beginning and ending at vertex  $p$  is called a *closed path at p* (a *p-cycle*, for short). For later convenience, given a vertex  $p$  in a deterministic  $A$ -automaton  $\Gamma$  and given a reduced word  $u \in F(A)$ , we define  $pu$  to be the end of the unique possible path in  $\Gamma$  labelled  $u$  and starting at  $p$ ; in case no such path exists,  $pu$  remains undefined.

For the sake of brevity, we may only mention and depict the positive subautomaton of  $\Gamma$  (i.e., that formed by the edges labelled by letters in  $A$ ), denoted  $\Gamma^+$ , bearing in mind that, for each of such edges,  $\Gamma$  also contains its inverse (even if not depicted or mentioned). The *degree* of a vertex in  $\Gamma$  is the number of edges of  $\Gamma^+$  incident to it.

With this notion, Stallings [26] established a bijection between the set of (free) subgroups of  $F(A)$ , and the set of isomorphism classes of Stallings  $A$ -automata.

**Theorem 3.1** (Stallings, [26]). *The following is a bijection:*

$$\begin{array}{ccc} \text{St}: \{H \leq F(A)\} & \longrightarrow & \{\text{isom. classes of Stallings } A\text{-automata}\} \\ H & \mapsto & \Gamma_A(H), \\ \mathcal{L}(\Gamma) & \longleftarrow & \Gamma. \end{array}$$

Furthermore,  $H \leq_{\text{fg}} F_A$  if and only if  $\Gamma_A(H)$  is finite; in this case, both directions are computable.  $\square$

The map to the left consists of reading the *language* subgroup  $\mathcal{L}(\Gamma) \leq F(A)$  of a given Stallings  $A$ -automaton  $\Gamma$ , i.e., the set of labels of reduced  $\bullet$ -cycles in  $\Gamma$ . As for the map to the right, it assigns to each subgroup  $H \leq F(A)$  its *Stallings*  $A$ -automaton  $\Gamma_A(H)$ , being the core of the *Schreier coset graph* of  $H$  with respect to the basis  $A$  of  $F(A)$ , and with the trivial coset taken as the basepoint,  $\bullet = H1$ . By the *core* of an  $A$ -automaton  $\Gamma$ , denoted  $c(\Gamma)$ , we mean its largest trim subautomaton. It follows that  $\Gamma$  is trim if and only if  $c(\Gamma) = \Gamma$ . One can think of the Schreier coset graph of  $H \leq F(A)$  with respect to  $A$  as the covering graph of the  $A$ -bouquet  $\mathcal{F}(A)$  corresponding to the subgroup  $H$ ; and its *Stallings graph*  $\Gamma_A(H)$  as its core, i.e., the result of trimming all the hanging trees not containing the basepoint. For more details, see [6, 8, 16, 26].

For the purpose of the present paper, the important part of the bijection in Theorem 3.1 is when restricted to finitely generated subgroups on one side, and to finite Stallings  $A$ -automata on the other. In this case, the bijection becomes algorithmic friendly, i.e., there are fast algorithms for computing both directions, which we summarize in the following couple of paragraphs. Let us also mention that, in the finite and connected case, it is easy to see that an  $A$ -automaton  $\Gamma$  is trim if and only if no vertex in  $\Gamma$  has degree 1, except, possibly, for  $\bullet$ ; moreover, in this case, one can obtain  $c(\Gamma)$  from  $\Gamma$  by applying finitely many times the trim operation: removing a vertex of degree one different from  $\bullet$  (together with the incident edge).

In order to compute the map to the left, assuming that  $\Gamma$  is finite, we first construct a spanning tree  $T$  of  $\Gamma$  by removing a set of edges  $E' = \{e \in E\Gamma^+ \setminus ET\}$ . Then, for each  $e \in E'$ , consider the group element  $h_e = \ell(T[\bullet, \iota e] \cdot e \cdot T[\tau e, \bullet]) \in F(A)$ , where  $T[p, q]$  stands for the unique reduced path in  $T$  from vertex  $p$  to vertex  $q$  (the  $T$ -geodesic from  $p$  to  $q$ ). It is easy to see that, when  $\Gamma$  is deterministic, this is a free basis for  $\mathcal{L}(\Gamma) \leq F(A)$ , whose rank then coincides with the first Betti number (cyclomatic number) of  $\Gamma$ , namely  $\text{rk}(\mathcal{L}(\Gamma)) = 1 - |V\Gamma| + |E\Gamma|$  (in general, without determinism, we can only say that  $\{h_e \mid e \in E'\}$  generates  $\mathcal{L}(\Gamma)$  and so,  $\text{rk}(\mathcal{L}(\Gamma)) \leq 1 - |V\Gamma| + |E\Gamma|$ ).

In order to compute the map to the right, we need to use a key result in this setting: “for every  $H \leq F(A)$  there exists a unique  $A$ -automaton (up to isomorphism) which is deterministic, trim, and has language  $H$ ”; it is called the *Stallings*  $A$ -automaton for  $H$ , and is denoted  $\Gamma_A(H)$ . Given a set  $W = \{h_1, \dots, h_n\}$  of reduced words on  $A$ , we can construct the Stallings  $A$ -automaton  $\Gamma_A(H)$  for the subgroup  $H = \langle h_1, \dots, h_n \rangle \leq F(A)$  by applying the following procedure. First, for each  $h_i$ ,  $i = 1, \dots, n$ , we form the circular graph (called *petal*) whose  $A$ -label, when starting at the basepoint, spells the word  $h_i$  (or its inverse if traveled in the opposite direction). Then, we form the *wedge* of these circuits by identifying the  $n$  basepoints into a single one, denoted  $\bullet$ . The resulting  $A$ -automaton is called the *flower automaton*, denoted  $\mathcal{F}(W)$ . Note, that  $\mathcal{L}(\mathcal{F}(W)) = H$ . In order to gain determinism, we apply a finite series of *elementary foldings*: whenever two edges sharing the same initial

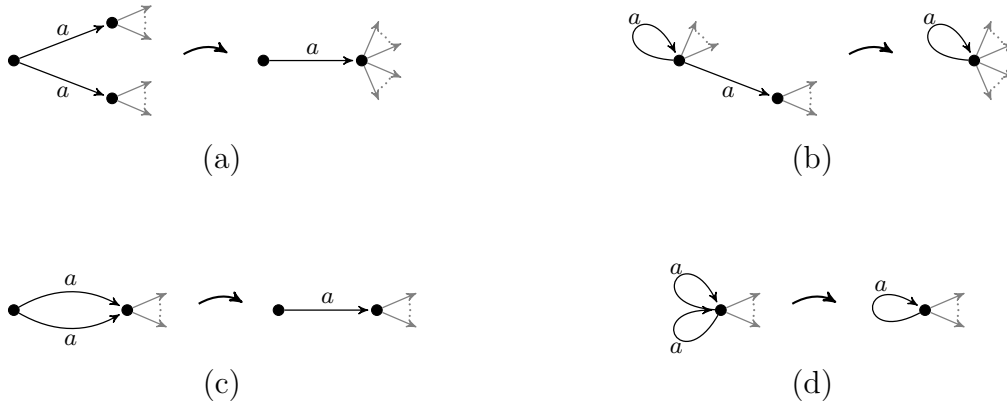


FIGURE 1. (a), (b) open (or homotopic) foldings; (c), (d) closed (or non-homotopic) foldings

(resp., terminal) vertex have the same label, we identify them into a single edge, together with their terminal (resp., initial) vertices. When the two terminal as well as the two initial vertices are the same, the elementary folding is called *closed* (or *non-homotopic*) (see Figure 1(c),(d)) and the first Betti number of the automaton reduces by one; otherwise, the folding is called *open* (or *homotopic*) (see Figure 1(a),(b)), and the first Betti number remains unchanged. In general, we denote such an elementary folding as  $\Gamma \rightsquigarrow \Gamma'$ . Note, that in a closed folding we identify two edges, whereas in an open folding we identify two edges as well as two vertices. In both cases, the language of the automaton remains unchanged. Of course, after performing an elementary folding, new possible foldings may emerge, but since at each step the number of edges strictly decreases, the process terminates after a finite number of steps. By construction, the resulting  $A$ -automaton is deterministic and has language  $H$ . It is also easy to see that it is trim (each vertex of the flower automaton, except possibly for the basepoint, has two incident edges of different labels, and they remain incident to that vertex throughout all the folding process). By the previous key result, the output of this process must be  $\Gamma_A(H)$ . In particular, this implies that the result of the folding process is independent from the specific sequence of foldings applied, and even of the set of generators for  $H$  we started with: it only depends on the subgroup  $H \leq F(A)$  (and on the ambient basis  $A$  chosen to work with).

Touikan [28] gave a more refined algorithm to compute  $\Gamma_A(H)$  in time  $\mathcal{O}(n \log^*(n))$ , where  $n$  is the sum of the lengths of the given generators for  $H$ , and  $\log^*(n)$  is the minimal number of successive applications of the log operator to  $n$  until reaching 1 or below.

Stallings bijection behaves well with respect to inclusions in the sense that, for any two subgroups  $H, K \leq F(A)$ , the inclusion  $H \leq K$  holds if and only if there is a (unique)  $A$ -homomorphism  $\theta_{H,K}: \Gamma_A(H) \rightarrow \Gamma_A(K)$  (sending vertices to vertices,  $\bullet_H$  to  $\bullet_K$ , and  $a$ -labelled edges to  $a$ -labelled edges, for each  $a \in A$ ). When  $H \leq K \leq F(A)$  and  $\Gamma_A(H)$  is a subautomaton of  $\Gamma_A(K)$ , that is, the map  $\theta_{H,K}$  is injective, then  $H$  is a free factor of  $K$  (take a spanning tree for  $\Gamma_A(H)$  and extend its image under  $\theta_{H,K}$  to a spanning tree for  $\Gamma_A(K)$ , resulting in extending the corresponding basis for  $H$  to a basis for  $K$ ), whereas the converse is far from true. Dually, the case where  $\theta_{H,K}$  is *onto*, at the level of edges, will be of central interest for our purposes. Here, we will be particularly interested in the case  $K = \langle H, g \rangle$ .

Let us finish with some technical details, which will be needed later. Given a finite  $A$ -automaton  $\Gamma$ , let us distinguish between the *language*  $\mathcal{L}(\Gamma) \leq F(A)$  of  $\Gamma$ , and its *fundamental group* at the basepoint  $\pi(\Gamma, \bullet)$  (namely the set of equivalence classes of  $\bullet$ -cycles modulo backtracking, endowed with the operation of concatenation). Of course, both are free groups and “reading the label” gives us an epimorphism  $\ell: \pi(\Gamma, \bullet) \twoheadrightarrow \mathcal{L}(\Gamma)$ ,  $\gamma \mapsto \ell(\gamma)$ ; in particular,  $\text{rk}(\pi(\Gamma, \bullet)) = b_1(\Gamma) = 1 - |V\Gamma| + |E\Gamma| \geq \text{rk}(\mathcal{L}(\Gamma))$ . Suppose now that  $\Gamma \curvearrowright \Gamma'$  is an elementary folding, identifying the edges  $e_1, e_2 \in E\Gamma$  with  $\iota e_1 = \iota e_2 = p$ ,  $\tau e_1 = q_1$ ,  $\tau e_2 = q_2$ , and  $\ell(e_1) = \ell(e_2) = a \in A$ . The natural map  $\varphi: \Gamma \rightarrow \Gamma'$  induces an epimorphism  $\varphi: \pi(\Gamma, \bullet) \twoheadrightarrow \pi(\Gamma', \bullet)$ , such that  $\varphi\ell = \ell$ , and  $\varphi$  is an isomorphism if and only if the folding is open (i.e.,  $q_1 \neq q_2$ ). Given a reduced path  $\gamma$  in  $\Gamma$ , the action of  $\varphi$  *projects*  $\gamma$  in a natural way to a path  $\gamma'$  in  $\Gamma'$  (which may not be reduced, e.g. when  $\gamma$  goes through  $e_1^{-1}$  and immediately through  $e_2$ , or through  $e_2^{-1}$  and immediately through  $e_1$ ).

In the other direction, when  $\gamma'$  is a reduced path in  $\Gamma'$ , then we can *lift*  $\gamma'$  to a path  $\gamma$  in  $\Gamma$ , but the lifting is not necessarily unique. When the folding  $\Gamma \curvearrowright \Gamma'$  is closed, then the lifting of  $\gamma'$  can simply be done in the following way: whenever we pass (in either direction) through the identified ( $e_1 = e_2$ )-edge, we choose between  $e_1$  and  $e_2$  to be in  $\gamma$ , while all the vertices and occurrences of other edges along the path stay the same. When the folding  $\Gamma \curvearrowright \Gamma'$  is open then it can happen that the path  $\gamma'$  goes through the identified vertex  $q_1 = q_2$  in such a way that, after the unfolding and separation of these vertices, it needs to enter the vertex  $q_1$  and immediately exit the vertex  $q_2$  (or the other way round). The remedy to this cut in the path is to connect  $q_1$  with  $q_2$  by inserting the segment  $e_1^{-1}e_2$  (or  $e_2^{-1}e_1$  in the reverse direction). At the level of labelling,  $\ell(\gamma)$  may thus not be reduced, even when  $\ell(\gamma')$  is reduced; however, both labels represent the same element in the free group  $F(A)$ .

Since 1983, Stallings bijection became a central tool for the modern understanding and study of the lattice of subgroups of a free group. With the development of these graph-theoretic techniques, many new results have been obtained about free groups and their subgroups. Also, most of the results known before Stallings [26] have been reproved using graph-theoretic techniques, usually with conceptually simpler and more transparent proofs.

#### 4. AN EXPLICIT DESCRIPTION OF THE SET OF DEPENDENT ELEMENTS

Let  $|A| < \infty$  be a finite alphabet and let  $H \leq_{\text{fg}} F(A)$  and  $1 \neq g \in F(A)$  be given. According to Proposition 2.1, in order to check whether  $g$  is dependent on  $H$ , we just have to check whether  $\text{rk}(\langle H, g \rangle) \leq \text{rk}(H)$ . One way to do this is by using classical Nielsen transformations; see [10]. Another way is within the Stallings graph theoretical setting. We start by computing  $\Gamma_A(H)$  and then we form the wedge of  $\Gamma_A(H)$  with a petal spelling the (reduced) word  $g$ . Let  $\Gamma_0$  be the resulting  $A$ -automaton. Clearly,  $\mathcal{L}(\Gamma_0) = \langle H, g \rangle$ . It is not necessarily deterministic but, after performing a maximal sequence of foldings to  $\Gamma_0$ , we obtain the Stallings automaton  $\Gamma_A(\langle H, g \rangle)$ :

$$(4.1) \quad \Gamma_0 \curvearrowright \Gamma_1 \curvearrowright \Gamma_2 \curvearrowright \cdots \curvearrowright \Gamma_s = \Gamma_A(\langle H, g \rangle)$$

(again, independent from the order in which we perform the foldings). Counting the first Betti numbers for these graphs, we have  $b_1(\Gamma_0) = b_1(\Gamma_A(H)) + 1 = \text{rk}(H) + 1$  and  $b_1(\Gamma_A(\langle H, g \rangle)) = \text{rk}(\langle H, g \rangle)$ . Since at each elementary folding  $\Gamma_i \curvearrowright \Gamma_{i+1}$  the

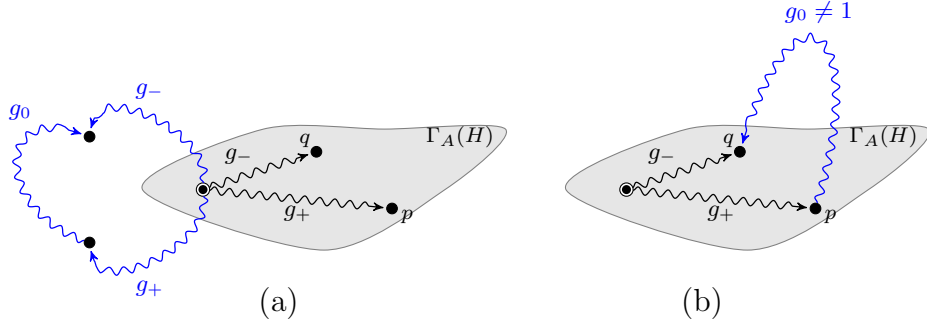


FIGURE 2. The  $A$ -automata (a)  $\Gamma_0$ ; and (b)  $\Gamma(\langle H, g \rangle)$  in case (i)

first Betti number either remains unchanged or decreases by one, we deduce that

$$\begin{aligned}
 g \text{ is dependent on } H &\Leftrightarrow \text{rk}(\langle H, g \rangle) \leq \text{rk}(H) \\
 &\Leftrightarrow b_1(\Gamma_A(\langle H, g \rangle)) \leq b_1(\Gamma_0) - 1 \\
 &\Leftrightarrow (4.1) \text{ contains at least one closed folding.}
 \end{aligned}$$

Let us look in more detail into the process of obtaining  $\Gamma_A(\langle H, g \rangle)$  from  $\Gamma_0$ . Since the result does not depend on the order of foldings, we can choose an order that suits our needs. We start at the basepoint and fold one by one the edges of the  $g$ -petal into those of the deterministic  $A$ -automaton  $\Gamma_A(H)$ , as long as this is possible. Let  $g = g_+g'$ , with  $g_+$  being the maximal initial segment of  $g$  that we managed to fold (where  $g_+$  or  $g'$  may be trivial), and let  $p$  be the vertex in  $\Gamma_A(H)$  at which the path spelling  $g_+$  ends. Note, that, by maximality of  $|g_+|$ , if  $g'$  is non-trivial then its first letter does not equal any of the labels of the edges in  $\Gamma_A(H)$  leaving  $p$ . In a similar way, we fold, edge by edge and backwards, into  $\Gamma_A(H)$  the longest possible terminal segment of the path spelling  $g'$ . Let  $g' = g_0g_-^{-1}$  be the corresponding decomposition of  $g'$ , with  $g_-$  spelling the label of a path from  $\bullet$  to a vertex, say  $q$ , in  $\Gamma_A(H)$ . Again, by maximality of  $|g_-|$ , if  $g_0$  is non-trivial then its last letter does not equal any of the labels of the edges in  $\Gamma_A(H)$  terminating at  $q$ ; see Figure 2(a). Note, that all the elementary foldings performed until now were open. At this stage we have the decomposition  $g = g_+g_0g_-^{-1}$ , with no cancellation among the three factors. Let us distinguish between the following three cases:

- (i)  $g_0 \neq 1$ . In this case the folding process is complete and the obtained  $A$ -automaton  $\Gamma_A(\langle H, g \rangle)$  consists of  $\Gamma_A(H)$  with an arc of positive length spelling  $g_0$  attached to it and going from  $p$  to  $q$ ; see Figure 2(b). In this case,  $b_1(\Gamma_A(\langle H, g \rangle)) = b_1(\Gamma_A(H)) + 1 = b_1(\Gamma_0)$  and so,  $g$  does not depend on  $H$ .
- (ii)  $g_0 = 1$  and  $p = q$ . In this case,  $g = g_+g_-^{-1}$  is the label of a genuine  $\bullet$ -cycle in  $\Gamma_A(H)$ . Thus,  $g \in H$  and  $\langle H, g \rangle = H$ . Clearly,  $g$  is dependent on  $H$  in this case.
- (iii)  $g_0 = 1$  and  $p \neq q$ . Here, as in case (i),  $g \notin H$ , but at this stage it is not clear yet whether  $g$  is dependent on  $H$  or not. At this moment, we have exhausted the original petal  $g$  and have identified the vertices  $p$  and  $q$ , obtaining the automaton  $\Gamma_A(H)/(p = q)$ . This automaton is not necessarily deterministic and further foldings may need to be performed until reaching  $\Gamma_A(\langle H, g \rangle)$ . In this case,  $g$  is dependent on  $H$  if and only if at least one closed folding occurs in this second part of the process.

Summarizing,  $g$  depends on  $H$  if and only if  $g \in H$ , or  $g$  goes into case (iii) with at least a closed folding occurring in the second part of the process. The above discussion leads us to an explicit description of *all* elements dependent on  $H$ .

**Theorem 4.1.** *Let  $F(A)$  be the free group with basis  $A$ . Given a finite set of generators of total length  $n$  for a subgroup  $H \leq_{\text{fg}} F(A)$ , one can algorithmically compute in time  $\mathcal{O}(n^3 \log^*(n))$  a finite set  $\{g_0 = 1, g_1, \dots, g_m\}$  of elements of  $F(A)$  that depend on  $H$ , and such that  $\text{dep}(H)$  is the disjoint union of the corresponding double cosets,  $\text{dep}(H) = H \sqcup Hg_1H \sqcup \dots \sqcup Hg_mH$ .*

*Proof.* Since  $H$  is finitely generated, there exists a finite subset  $A_0 \subseteq A$  (computable in linear time), such that  $H \leq_{\text{fg}} F(A_0) \leq_{\text{ff}} F(A)$ ; moreover,  $\text{dep}_{F(A)}(H) = \text{dep}_{F(A_0)}(H)$ . Thus, without loss of generality, we may assume that  $A$  is finite, say  $A = \{a_1, \dots, a_r\}$ .

First, we construct the finite Stallings  $A$ -automaton  $\Gamma_A(H)$ . Then, for each pair of distinct vertices  $p, q \in V = V\Gamma_A(H)$ , we form the graph  $\Gamma_A(H)/(p = q)$  by identifying these two vertices, and then we perform elementary foldings until reaching a deterministic  $A$ -automaton, say  $\Gamma_{p=q}$ . Let

$$(4.2) \quad R = \{(p, q) \in V \times V \mid p \neq q, b_1(\Gamma_{p=q}) \leq \text{rk}(H)\} \subseteq (V \times V) \setminus \Delta,$$

where  $\Delta = \{(p, p) \mid p \in V\}$  is the diagonal of  $V \times V$ . In other words,  $R$  is the set of pairs  $(p, q) \in (V \times V) \setminus \Delta$ , for which the sequence of elementary foldings from  $\Gamma_A(H)/(p = q)$  to  $\Gamma_{p=q}$  contains at least a closed folding. Note, that  $(p, q) \in R$  implies that  $(q, p) \in R$  and also  $(pa_i^\varepsilon, qa_i^\varepsilon) \in R$ , for all  $a_i \in A$  and  $\varepsilon \in \{1, -1\}$ , for which both  $pa_i^\varepsilon$  and  $qa_i^\varepsilon$  are defined.

Clearly, the discussion above tells us that

$$(4.3) \quad \text{dep}(H) = H \sqcup \bigcup_{(p,q) \in R} S_{(p,q)},$$

where  $S_{(p,q)}$  is the set of elements  $g \in F(A)$  that fall into case (iii) identifying  $p$  and  $q$ , that is, those of the form  $g = g_+g_-^{-1}$  where  $g_+$  labels some path from  $\bullet$  to  $p$ , and  $g_-$  labels some path from  $\bullet$  to  $q$ ,

$$S_{(p,q)} = \{g = g_+g_-^{-1} \mid g_+ = \ell(\gamma_p), g_- = \ell(\gamma_q), \iota\gamma_p = \iota\gamma_q = \bullet, \tau\gamma_p = p, \tau\gamma_q = q\}.$$

It only remains to observe that each of these sets  $S_{(p,q)}$  is the double coset  $S_{(p,q)} = Hg_{(p,q)}H$ , for some (any) representative  $g_{(p,q)} \in S_{(p,q)}$ . Since  $H$  is finitely generated,  $\Gamma_A(H)$  and  $R$  are finite, and so, the union in (4.3) is also finite. In addition, the coset representatives  $g_{(p,q)}$  are computable. Moreover, we can algorithmically check whether  $HuH = HvH$ , i.e.,  $uH \cap Hv \neq \emptyset$ , by using a solution to the coset intersection problem for free groups; see [6]. So, by writing  $g_{(\bullet,\bullet)} = 1$  and  $S_{(\bullet,\bullet)} = H$ , and keeping in the set  $\{g_{(p,q)} \mid (p,q) \in R\}$  only one representative of each double coset, we obtain the required elements  $g_0 = 1, g_1, \dots, g_m$ , such that:

$$\text{dep}(H) = \bigcup_{(p,q) \in R \sqcup \{(\bullet,\bullet)\}} S_{(p,q)} = H \sqcup Hg_1H \sqcup \dots \sqcup Hg_mH.$$

If  $n$  denotes the total length of the input generators,  $\Gamma_A(H)$  can be computed in time  $\mathcal{O}(n \log^*(n))$ ; see Touikan [28]. This  $A$ -automaton contains at most  $n$  vertices, and so,  $\mathcal{O}(n^2)$  pairs  $(p, q)$ . For each such pair  $(p, q)$ , we can check in time  $\mathcal{O}(n \log^*(n))$  whether, after identifying  $p$  with  $q$ , the elementary foldings towards  $\Gamma_{p=q}$  contain a closed folding. This makes a total time  $\mathcal{O}(n^3 \log^*(n))$  to compute the set  $R$ .

Finally, the process of removing from  $R$  the excessive pairs of vertices, so that no two pairs determine the same double coset, can be done in time  $\mathcal{O}(n^3)$ . In order to do it, we first compute a spanning tree  $T$  of  $\Gamma_A(H)$  (in time  $\mathcal{O}(n)$ ). Then, for each  $p \in V\Gamma_A(H)$ , we attach to  $\Gamma_A(H)$  a “hair”, labelled  $\ell(T[\bullet, p])$ , that ends at the basepoint  $\bullet$ . After making the necessary elementary foldings, we obtain a “hairy”  $A$ -automaton, denoted  $\Gamma'$ , with at most  $\mathcal{O}(n^2)$  vertices. Next, we compute the pull-back of  $\Gamma'$  with  $\Gamma_A(H)$ , which takes time  $\mathcal{O}(n^3)$ ; see [6]. For each pair of vertices  $p, q \in V\Gamma_A(H)$ , let  $u = \ell(T[\bullet, p])$  and  $v = \ell(T[\bullet, q])$ . Then,  $HuH = HvH$  if and only if  $uH \cap Hv \neq \emptyset$  if and only if  $(\bullet u^{-1}, \bullet)$  and  $(\bullet, q)$  belong to the same connected component of the pull-back.

Altogether, the whole process can be done in time  $\mathcal{O}(n^3 \log^*(n))$ .  $\square$

**Remark 4.2.** The complexity bound  $\mathcal{O}(n^3 \log^*(n))$  is rather high in practice. Here is a possible idea to reduce it: for each pair of vertices  $(p, q)$  in  $\Gamma_A(H)$ , each  $a \in A$  and each  $\varepsilon = \pm 1$  with  $pa^\varepsilon$  and  $qa^\varepsilon$  both defined, identifying  $p$  with  $q$  gives the final same result as identifying  $pa^\varepsilon$  with  $qa^\varepsilon$ , after the subsequent necessary foldings. Therefore, when following the algorithm provided in the previous theorem, we do not need to perform  $\mathcal{O}(n^2)$  checks, i.e., one for each vertex  $(p, q)$  in the pull-back  $\Gamma_A(H) \times \Gamma_A(H)$ , but only one for each connected components in  $\Gamma_A(H) \times \Gamma_A(H)$ . This could result into a significant improvement (which then goes multiplied by  $\mathcal{O}(n \log^*(n))$ ), although it is not clear how to quantify it: the dispersion of  $\Gamma_A(H) \times \Gamma_A(H)$  into more or less connected components strongly depends on the geometry of the Stallings automaton  $\Gamma_A(H)$ .

**Remark 4.3.** The algorithm for computing the representatives  $g_i$  of the double cosets whose union is  $\text{dep}(H)$  can also be done using Nielsen transformations. Suppose that  $u = \ell(T[\bullet, p])$  and  $v = \ell(T[\bullet, q])$ , as in the proof of Theorem 4.1. Let  $S = W \cup \{g\}$ , where  $W$  is a basis of  $H$  and  $g = uv^{-1}$ . Then, an occurrence of a closed elementary folding, after the identification of  $p$  with  $q$ , is equivalent to the trivial group element showing up at least once in a (any) sequence of Nielsen transformations leading from  $S$  to a basis for  $\langle H, g \rangle$ .

In fact, an identification of two edges of the same initial vertex and the same label  $a$  is the graphical counterpart to the reduction of a word in which the letter  $a^\varepsilon$  is followed by  $a^{-\varepsilon}$ .

Similar to performing Nielsen transformations but using a different representation is the following. We can represent each group element  $g = uv^{-1}$  as a *binomial*  $u - v$  in the group ring  $\mathbb{Z}_2 F$  of the free group  $F$  over the ring of integers modulo 2. Then, the analog of a Nielsen transformation is a reduction *à la Gröbner bases*, using, say, a *shortlex* order (comparing monomials by their length and using a lexicographic order for a tie-breaker); see [21, Sec. 7]. The advantage of this method is that it allows, in some cases, the generalization of theorems and algorithms from groups to group rings. On the other hand, Stallings graph-theoretic techniques, besides the new perspective and results they brought to the field of subgroups of free groups, show, in many cases, a simplified and unified approach: for example, the graph representation of the subgroup  $H \leq F$  does not depend on the generators of  $H$  but only on the chosen basis for  $F$ .

**Corollary 4.4.** *Given a finite set of generators of total length  $n$  for a subgroup  $H \leq_{\text{fg}} F(A)$ , a generating set for  $\text{Dep}(H)$  can be algorithmically computed in time  $\mathcal{O}(n^3 \log^*(n))$ .*

*Proof.* Clearly, if  $\{h_1, \dots, h_s\}$  are the given generators for  $H$ , then  $\text{Dep}(H) = \langle h_1, \dots, h_s, g_1, \dots, g_m \rangle$ , where  $g_1, \dots, g_m$  are the elements computed in Theorem 4.1. The result then follows.  $\square$

## 5. EQUATIONS FOR A DEPENDENT ELEMENT

Let  $H \leq_{\text{fg}} F(A)$  be a subgroup with  $\text{rk}(H) = n$ , and let  $g \in F(A)$  be an element dependent on  $H$ , i.e.,  $\text{rk}(\langle H, g \rangle) = m \leq n$ . In this section we present two algorithms for computing a finite set of polynomials generating  $I_H(g)$  (the ideal of all polynomials  $w(x)$ , such that  $w(g) = 1$ ) as a normal subgroup of  $H * \langle x \rangle$ : the first one is based on Nielsen transformations and the second one on Stallings graph theoretical techniques. The number of normal generators computed by these algorithms is  $n + 1 - m$ , which is the minimal possible number, as shown by the following observation.

**Observation 5.1.** *A lower bound to the number of normal generators of the ideal  $I_H(g)$  is  $n + 1 - m$ , where  $\text{rk}(H) = n$  and  $\text{rk}(\langle H, g \rangle) = m$ .*

*Proof.* Assume that  $I_H(g) = \langle\langle w_1(x), \dots, w_k(x) \rangle\rangle$ . We will show that  $k \geq n + 1 - m$ . Since the morphism  $\varphi_{H,g}: H * \langle x \rangle \rightarrow \langle H, g \rangle \leq F(A)$  is onto, the following is a presentation of the free group of rank  $m$ :

$$F_m \simeq \langle H, g \rangle \simeq H * \langle x \rangle / I_H(g) = \langle h_1, \dots, h_n, x \mid w_1(x), \dots, w_k(x) \rangle,$$

where  $\{h_1, \dots, h_n\}$  is a free basis for  $H$ . Abelianizing, we have

$$\begin{aligned} \mathbb{Z}^m &= \langle h_1, \dots, h_n, x \mid w_1(x), \dots, w_k(x), [h_i, h_j], [h_i, x] \quad (i, j = 1, \dots, n) \rangle \\ &= \langle h_1, \dots, h_n, x \mid w_1(x)^{\text{ab}}, \dots, w_k(x)^{\text{ab}} \rangle_{\text{ab}} \\ &= \mathbb{Z}^{n+1} / \langle w_1(x)^{\text{ab}}, \dots, w_k(x)^{\text{ab}} \rangle \end{aligned}$$

and so,  $m \geq n + 1 - k$ .  $\square$

Let us start with the easy case  $g \in H$ .

**Observation 5.2.** *For  $g \in H \leq_{\text{fg}} F(A)$ , we have  $I_H(g) = \langle\langle g^{-1}x \rangle\rangle \trianglelefteq H * \langle x \rangle$ .*

*Proof.* Clearly,  $g^{-1}x \in I_H(g)$ . Let now  $w(x) = 1$  be a reduced  $H$ -equation satisfying  $w(g) = 1$ . We will show, by induction on the degree  $d$  of  $w(x)$ , that  $w(x)$  is in the normal subgroup  $\langle\langle g^{-1}x \rangle\rangle = \langle\langle gx^{-1} \rangle\rangle$ . For  $d = 1$ , we have  $w(x) = h_0x^{\varepsilon_1}h_1$  and  $h_0g^{\varepsilon_1}h_1 = 1$ . So,  $g^{-\varepsilon_1} = h_1h_0$  and

$$w(x) = h_0x^{\varepsilon_1}h_1 = h_1^{-1}(h_1h_0x^{\varepsilon_1})h_1 = h_1^{-1}(g^{-\varepsilon_1}x^{\varepsilon_1})h_1 \in \langle\langle g^{-1}x \rangle\rangle.$$

Assume now that the statement holds for equations of degree  $d - 1$ , and let

$$w(x) = h_0x^{\varepsilon_1}h_1x^{\varepsilon_2} \dots h_{d-1}x^{\varepsilon_d}h_d = 1$$

be a reduced  $H$ -equation of degree  $d$  and satisfying  $w(g) = 1$ . Then,  $g$  clearly satisfies the  $H$ -equation

$$w'(x) = h_0x^{\varepsilon_1}h_1x^{\varepsilon_2} \dots x^{\varepsilon_{d-1}}(h_{d-1}g^{\varepsilon_d}h_d) = 1$$

of degree  $d - 1$ , and so, by the induction hypothesis,  $w'(x) \in \langle\langle g^{-1}x \rangle\rangle$ . It follows that

$$w(x) = (h_0x^{\varepsilon_1}h_1x^{\varepsilon_2} \dots x^{\varepsilon_{d-1}}h_{d-1}g^{\varepsilon_d}h_d)(h_d^{-1}g^{-\varepsilon_d}x^{\varepsilon_d}h_d) = w'(x)(g^{-\varepsilon_d}x^{\varepsilon_d})^{h_d},$$

which also belongs to  $\langle\langle g^{-1}x \rangle\rangle$ .  $\square$

**Theorem 5.3.** *Let  $H \leq_{fg} F(A)$  be a subgroup of rank  $n$ , and let  $1 \neq g \in F(A)$  be dependent on  $H$  and such that  $\text{rk}(\langle H, g \rangle) = m \leq n$ . Then, there exists an algorithm that, given a finite set of generators for  $H$ , computes a set of  $n + 1 - m$  normal generators of the ideal  $I_H(g) \trianglelefteq H * \langle x \rangle$ :*

$$I_H(g) = \langle\langle w_1(x), \dots, w_{n-m+1}(x) \rangle\rangle.$$

*Proof (using Nielsen transformations).* Let  $\{h_1, \dots, h_n\}$  be a set of free generators of  $H$ . As in (1.3), we consider the epimorphism

$$\begin{aligned} \varphi_{H,g}: H * \langle x \rangle &\twoheadrightarrow \langle H, g \rangle \leq F(A) \\ h_1 &\mapsto h_1, \\ &\vdots \\ h_n &\mapsto h_n, \\ x &\mapsto g. \end{aligned}$$

By applying a sequence of Nielsen transformations (each denoted by the symbol  $\varrho \rightarrow$ ), the tuple  $(h_1, \dots, h_n, g)$  can be transformed into the tuple  $(1, \dots, 1, b_1, \dots, b_m)$ , consisting of  $n - m + 1$  trivial elements, followed by a basis  $\{b_1, \dots, b_m\}$  of  $\langle H, g \rangle$ :

$$(h_1, \dots, h_n, g) \varrho \rightarrow \dots \varrho \rightarrow (1, \dots, 1, b_1, \dots, b_m).$$

Applying the same sequence of transformations to the tuple  $(h_1, \dots, h_n, x)$  results in a new basis  $\{w_1(x), \dots, w_{n+1}(x)\}$  of the free group  $H * \langle x \rangle$ . The epimorphism  $\varphi_{H,g}$ , expressed in this new basis, is

$$\begin{aligned} \varphi_{H,g}: H * \langle x \rangle &\twoheadrightarrow \langle H, g \rangle \\ w_1(x) &\mapsto 1, \\ &\vdots \\ w_{n-m+1}(x) &\mapsto 1, \\ w_{n-m+2}(x) &\mapsto b_1, \\ &\vdots \\ w_{n+1}(x) &\mapsto b_m. \end{aligned}$$

But  $\{b_1, \dots, b_m\}$  is a basis for  $\langle H, g \rangle$  so, the restriction of  $\varphi_{H,g}$  to  $\langle w_{n-m+2}(x), \dots, w_{n+1}(x) \rangle$  is injective, thus the kernel of  $\varphi_{H,g}$  is

$$\ker \varphi_{H,g} = \langle\langle w_1(x), \dots, w_{n-m+1}(x) \rangle\rangle,$$

the (normal) subgroup of  $H * \langle x \rangle$ , normally generated by  $w_1(x), \dots, w_{n-m+1}(x)$ .  $\square$

*Proof (using Stallings techniques).* An alternative way to obtain a set of normal generators for the ideal  $I_H(g)$  is through Stallings techniques. The basic case  $g \in H$  was already covered in Observation 5.2: in this case  $\langle H, g \rangle = H$ ,  $m = n$ ,  $n - m + 1 = 1$ , and  $I_H(g)$  is normally generated by the polynomial  $g^{-1}x$ .

So, let us assume that  $g$  is dependent on  $H$  and  $g \notin H$ , i.e.,  $g$  fits in case (iii) from the discussion at the beginning of Section 4. Let  $W = \{h_1, \dots, h_n\}$  be a free basis for  $H$  and let  $\mathcal{F}(W \cup \{g\})$  be the corresponding flower automaton. We will now perform a series of elementary foldings towards the deterministic  $A$ -automaton  $\Gamma_A(\langle H, g \rangle)$ , in a particular order that suits our needs. At the first stage we perform all possible folding among edges coming from  $W$  and leave the petal  $g$  untouched, obtaining the automaton  $\Gamma_0$  (as at the beginning of (4.1)) which is the wedge of  $\Gamma_A(H)$  with the petal labelled  $g$ :

$$\mathcal{F}(W \cup \{g\}) \curvearrowright \dots \curvearrowright \Gamma_0.$$

Note that, up to now, all the foldings are open because  $W$  is a free basis for  $H$ . In a second stage, we integrate  $g$  into  $\Gamma_A(H)$  through a series of elementary foldings as in (4.1), but doing *only open foldings*, until no more possible open foldings are available: first we fold the maximal initial and terminal segments of the petal labelled  $g$  until getting the automaton  $\Gamma_A(H)/(p = q)$ , and then we keep applying *open* foldings until no more are available; denote  $\Gamma_{p,q}$  the resulting automaton:

$$\Gamma_0 \curvearrowright \cdots \curvearrowright \Gamma_A(H)/(p = q) \curvearrowright \cdots \curvearrowright \Gamma_{p,q}.$$

The automaton  $\Gamma_{p,q}$  is not yet necessarily deterministic: it could contain several closed foldings to be done. But note that, after doing all of them, no more identifications of vertices are happening, no new foldings are introduced and so, we get directly the final deterministic output

$$(5.1) \quad \Gamma_{p,q} \curvearrowright \cdots \curvearrowright \Gamma_A(\langle H, g \rangle).$$

Let us introduce notation for this final step:  $\Gamma_{p,q}$  contains, say,  $r \geq 0$  blocks of edges (possibly loops) parallel to each other, namely  $\{e_{i,0}, e_{i,1}, \dots, e_{i,k_i}\}$  for  $i = 1, \dots, r$ , with  $\iota e_{i,0} = \iota e_{i,1} = \dots = \iota e_{i,k_i}$ , and  $\tau e_{i,0} = \tau e_{i,1} = \dots = \tau e_{i,k_i}$ , and  $\ell(e_{i,0}) = \ell(e_{i,1}) = \dots = \ell(e_{i,k_i})$ . Let us aggregate all these final closed foldings from (5.1) into a single final step denoted  $\widehat{\curvearrowright}$ : it is made of

$$\sum_{i=1}^r k_i = n - m + 1$$

closed foldings, and consists simply on identifying each block into a single edge; alternatively, we can think of it as deleting the edges  $e_{i,1}, \dots, e_{i,k_i}$  and leaving only  $e_{i,0}$  from each block. Summarizing, the whole folding process looks like this:

$$(5.2) \quad \mathcal{F}(W \cup \{g\}) \curvearrowright \cdots \curvearrowright \Gamma_0 \curvearrowright \cdots \curvearrowright \Gamma_A(H)/(p = q) \curvearrowright \cdots \curvearrowright \Gamma_{p,q} \widehat{\curvearrowright} \Gamma_A(\langle H, g \rangle).$$

Next, we will show how to construct  $n - m + 1$  non-trivial  $H$ -equations, each satisfied by  $g$ : one, say  $w_{i,j}(x) = 1$ , for each of the edges  $e_{i,j}$ ,  $i = 1, \dots, r$ ,  $j = 1, \dots, k_i$ . Then, we will prove that the polynomials  $w_{i,j}(x)$  generate the ideal  $I_H(g)$  as a normal subgroup of  $H * \langle x \rangle$ .

For each  $1 \leq i \leq r$ , one of the vertices  $\iota e_{i,0} = \dots = \iota e_{i,k_i}$  or  $\tau e_{i,0} = \dots = \tau e_{i,k_i}$  (or both) belong the same connected component of  $\Gamma_{p,q} \setminus \{e_{i,0}, \dots, e_{i,k_i}\}$  containing  $\bullet$ ; without loss of generality, we can assume it is the first one. Let then  $\gamma_i$  be a reduced path in  $\Gamma_{p,q}$  from  $\bullet$  to  $\iota e_{i,0} = \dots = \iota e_{i,k_i}$ , which does not contain any of the edges  $e_{i,0}, \dots, e_{i,k_i}$  nor their inverses. For each  $i = 1, \dots, r$  and for each  $j = 1, \dots, k_i$ , let now  $\gamma_{i,j}$  be the reduced non-trivial  $\bullet$ -cycle

$$\gamma_{i,j} = \gamma_i e_{i,j} e_{i,0}^{-1} \gamma_i^{-1}.$$

Let  $a_i^{\varepsilon_i} \in A^\pm$  be the common label of the edges  $e'_{i,j}$ 's. Then, the label of  $\gamma_{i,j}$  is

$$\ell(\gamma_{i,j}) = \ell(\gamma_i) a_i^{\varepsilon_i} a_i^{-\varepsilon_i} \ell(\gamma_i)^{-1} = 1;$$

this is capturing the algebraic essence of the closed folding determined by the pair of parallel edges  $e_{i,0}$  and  $e_{i,j}$ . In the next stage, we lift  $\gamma_{i,j}$  all the way up to  $\mathcal{F}(W \cup \{g\})$  by unfolding the open foldings from (5.2) in the reverse order, to obtain a (uniquely determined reduced)  $\bullet$ -cycle  $\widehat{\gamma}_{i,j}$ . This  $\bullet$ -cycle  $\widehat{\gamma}_{i,j}$  in  $\mathcal{F}(W \cup \{g\})$  is non-trivial and presents no backtracking. So, it spells a non-trivial, reduced word, denoted  $w_{i,j}(g)$ , on  $W \cup \{g\}$ , but reads the trivial element  $\ell(\widehat{\gamma}_{i,j}) = \ell(\gamma_{i,j}) = 1$ . Replacing the occurrences of  $g$  by  $x$  (and of  $g^{-1}$  by  $x^{-1}$ ) in  $w_{i,j}(g)$ , results in a reduced, non-trivial

polynomial  $w_{i,j}(x)$ , satisfying  $w_{i,j}(g) = 1$  (note, that  $x$  must occur in  $w_{i,j}(x)$  at least once, because  $W$  was chosen to be a free basis for  $H$ ).

Let us rename the  $n - m + 1$  polynomials  $w_{i,j}(x)$  obtained this way by  $w_1(x), \dots, w_{n-m+1}(x)$ . We finish the proof by showing that they generate normally the ideal  $I_H(g)$ . So, let  $w(x) \in I_H(g)$  be an arbitrary reduced polynomial over  $H$ , satisfying  $w(g) = 1$ . Then,  $w(x)$  corresponds to a reduced  $\bullet$ -cycle  $\gamma$  in the flower  $A$ -automaton  $\mathcal{F}(W \cup \{g\})$ . Note, that the condition  $w(g) = 1$  means that  $\ell(\gamma) = 1$ . We project  $\gamma$  down the open foldings in the cascade (5.2) until getting a reduced  $\bullet$ -cycle  $\gamma'$  in  $\Gamma_{p,q}$ , satisfying  $\ell(\gamma') = 1$ . We are going to prove our goal, namely  $w(x) \in \langle\langle w_1(x), \dots, w_{n-m+1}(x) \rangle\rangle$ , by induction on the number of occurrences, say  $s$ , of the duplicated edges  $e_{i,j}$ ,  $i = 1, \dots, r$ ,  $j = 1, \dots, k_i$ , in  $\gamma'$ . If  $s = 0$  then the same path  $\gamma'$  is, in fact, also a reduced  $\bullet$ -cycle in  $\Gamma_A(\langle\langle H, g \rangle\rangle)$  because the closed foldings do not affect it. But  $\Gamma_A(\langle\langle H, g \rangle\rangle)$  is a deterministic  $A$ -automaton and so,  $\ell(\gamma') = 1$  implies that  $\gamma'$  must be the trivial path. Therefore,  $\gamma$  is the trivial  $\bullet$ -cycle (from  $\mathcal{F}(W \cup \{g\})$ ) as well, meaning that  $w(x)$  is the trivial polynomial, obviously belonging to  $\langle\langle w_1(x), \dots, w_{n-m+1}(x) \rangle\rangle$ . This proves the base of the induction.

Suppose now that the result holds for equations determining paths with  $s$  occurrences of the duplicated edges  $e_{i,j}$  and let  $w(x) \in I_g(H)$  be an equation determining a path  $\gamma$  with  $s + 1 \geq 1$  such occurrences. Then, highlighting the first of such occurrences,  $\gamma$  can be written as  $\gamma = \alpha e_{i,j}^\varepsilon \beta$ , for some  $\varepsilon = \pm 1$ , some  $i = 1, \dots, r$ , some  $j = 1, \dots, k_i$ , and with  $\alpha$  containing no duplicated edge  $e_{i,j}$  in either direction. Next, we decompose  $\gamma$  in the following form:

$$\gamma = \begin{cases} \alpha e_{i,j} \beta = (\alpha \gamma_i^{-1})(\gamma_i e_{i,j} e_{i,0}^{-1} \gamma_i^{-1})(\gamma_i \alpha^{-1})(\alpha e_{i,0} \beta), & \text{if } \varepsilon = 1; \\ \alpha e_{i,j}^{-1} \beta = (\alpha e_{i,0}^{-1} \beta)(\beta^{-1} \gamma_i^{-1})(\gamma_i e_{i,0} e_{i,j}^{-1} \gamma_i^{-1})(\gamma_i \beta), & \text{if } \varepsilon = -1. \end{cases}$$

Lifting  $\gamma$  up to  $\mathcal{F}(W \cup \{g\})$ , we get

$$\widehat{\gamma} = \begin{cases} (\widehat{\gamma_i \alpha^{-1}})^{-1} \widehat{\gamma_{i,j}} (\widehat{\gamma_i \alpha^{-1}}) (\widehat{\alpha e_{i,0} \beta}), & \text{if } \varepsilon = 1; \\ (\widehat{\alpha e_{i,0}^{-1} \beta}) (\widehat{\gamma_i \beta})^{-1} \widehat{\gamma_{i,j}^{-1}} (\widehat{\gamma_i \beta}), & \text{if } \varepsilon = -1, \end{cases}$$

which, when translated back into  $H$ -polynomials, means that  $w(x)$  equals the product of a conjugate of one of the polynomials  $w_1(x)^\pm, \dots, w_{n-m+1}(x)^\pm$  and the polynomial corresponding to  $(\widehat{\alpha e_{i,0}^\varepsilon \beta})$ , say  $w'(x)$ . Observe that  $w'(g) = 1$  as well, and that the corresponding path has  $s$  occurrences of duplicated edges (since the first one,  $e_{i,j}^\varepsilon$ , was replaced by  $e_{i,0}^\varepsilon$ ). By the induction hypothesis, we have  $w'(x) \in \langle\langle w_1(x), \dots, w_{n-m+1}(x) \rangle\rangle$  and therefore, so does  $w(x)$ . This concludes the proof.  $\square$

**Corollary 5.4.** *Given  $H \leq_{\text{fg}} F$ , one can effectively compute an integer  $d$ , such that each  $g \in F$  dependent on  $H$  satisfies an equation over  $H$  of degree at most  $d$ .*

*Proof.* By Theorem 4.1, we can compute elements  $g_1, \dots, g_m \in F$  dependent on  $H$ , so that  $\text{dep}(H) = H \sqcup H g_1 H \sqcup \dots \sqcup H g_m H$ . Now, by Theorem 5.3, we can effectively compute an  $H$ -equation  $w_i(x) = 1$  of degree, say,  $d_i$  for each  $g_i$ ,  $i = 1, \dots, m$ . Since, by Observation 1.5, all the elements of the form  $h g_i h' \in H g_i H$  satisfy an  $H$ -equation of degree less than or equal to  $d_i$ , it follows that each dependent element satisfies an equation of degree at most  $d = \max\{d_1, \dots, d_m\}$ .  $\square$

**Remark 5.5.** We have seen that, when  $H \leq_{\text{fg}} F$ , the set of elements that depend on  $H$  is of the form  $\text{dep}(H) = H \sqcup Hg_1H \sqcup \cdots \sqcup Hg_mH$ . Let

$$J = \bigcup_{i=0}^m I_H(g_i) \subseteq H * \langle x \rangle,$$

where  $g_0 = 1$ . Then, the set of  $H$ -polynomials which are annihilated by some element dependent on  $H$  is the union, over the set of all automorphisms of  $H * \langle x \rangle$  that fix  $H$ , of images of  $J$ . This is because the  $H$ -equations satisfied by  $hg_ih'$  are, precisely, those of the form  $w(h^{-1}xh'^{-1}) = 1$ , for  $w(x) \in I_H(g_i)$ , and the elements  $h^{-1}xh'^{-1}$  are, precisely, all the images of  $x$  by the automorphisms of  $H * \langle x \rangle$  fixing  $H$ .

## 6. ON CERTAIN CLASSES OF SUBGROUPS

Let us look at some special classes of subgroups of a finitely generated free group  $F$  and see whether they are preserved under the dependence operator. These classes form a chain with respect to inclusion, where at the top of the chain are compressed subgroups and at the bottom free factors; see Figure 3.

A subgroup  $H \leq F$  is called *inert* if  $\text{rk}(H \cap K) \leq \text{rk}(K)$ , for every  $K \leq F$ , and it is called *compressed* when  $\text{rk}(H) \leq \text{rk}(K)$ , for every  $H \leq K \leq F$  (i.e., the same property as for inertness, required only for those subgroups  $K$  containing  $H$ ); see [7]. Of course, every inert subgroup of  $F$  is compressed, and it is an open problem whether compressed subgroups in free groups are inert. It is also clear that compressed subgroups of  $F$  cannot have rank larger than that of the ambient group  $F$ .

A subgroup  $H \leq F_r$  is an *echelon* subgroup if there exists an ordered basis  $A = \{a_1, \dots, a_r\}$  of  $F_r$ , such that  $0 \leq \text{rk}(H_i) - \text{rk}(H_{i-1}) \leq 1$  for  $i = 1, \dots, r$ , where  $H_0 = \{1\}$  and  $H_i = H \cap \langle a_1, \dots, a_i \rangle$ ,  $i = 1, \dots, r$  (we also say then that  $H$  is in *echelon form w.r.t. A*); see [23]. Note, that the inequality  $0 \leq \text{rk}(H_i) - \text{rk}(H_{i-1})$  always holds because  $H_{i-1} \leq_{\text{ff}} H_i$ . Clearly, every free factor of  $F$  is an echelon subgroup.

The family of echelon subgroups is a subclass of a broader class, called *1-gen-endo*, which was shown by Rosenmann [23] to be inert. A 1-gen-endo subgroup  $H$  is formed through a finite number of transformations. We start with a basis  $B_0$  of a free group  $F$  and let  $H_1$  be the subgroup generated by the elements of  $B_0$  except for some  $h \in B_0$  that is replaced by some element  $h' \in F$ . Suppose now that at step  $i$  we have a subgroup  $H_i \leq F$ . Then, in step  $i + 1$ , we form  $H_{i+1}$  by replacing some element  $h_j$  of a basis  $B_i$  of  $H_i$  by an element  $h'_j \in H_i$ . That is,  $H_{i+1}$  is the image of the  $H_i$ -endomorphism which sends  $h_j$  to  $h'_j$  and all other basis elements are mapped to themselves. We stop after finitely-many steps and the resulting subgroup is  $H$ . It is easy to see that every echelon subgroup can be formed through a finite number of such transformations.

We also note that the class of inert subgroups is still larger since e.g. every subgroup of rank 2 is inert, and there are subgroups of rank 2 that are not 1-gen-endo subgroups.

Let  $\text{Aut}(F)$  be the group of automorphisms of  $F$ . A subgroup  $H \leq F$  is called *1-auto-fixed* if  $H = \text{Fix}(\alpha)$ , the subgroup of elements of  $F$  fixed by  $\alpha$ , for some  $\alpha \in \text{Aut}(F)$ ; see [14]. Clearly, this class includes free factors of  $F$ . In Dicks–Ventura [7] it was proved that 1-auto-fixed subgroups of finitely generated free groups are inert (recently, this has been generalized to 1-endo-fixed subgroups by Antolín–Jaikin [1],

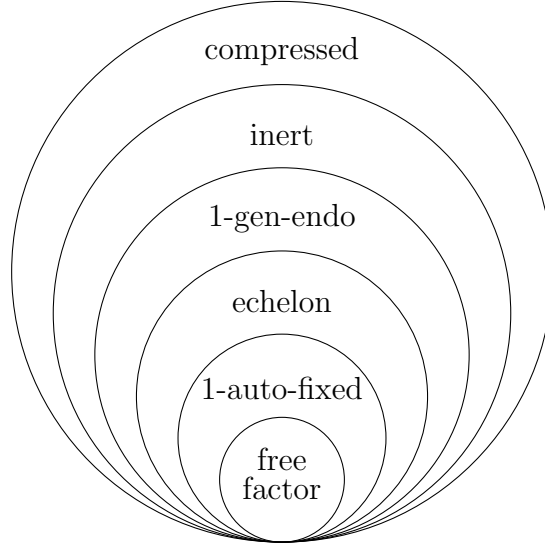


FIGURE 3. A chain of classes of subgroups of a free group

solving the inertia conjecture from [7]). Also, an explicit description of 1-auto-fixed subgroups of free groups was given in Martino–Ventura [15], and from this it follows that 1-auto-fixed subgroups are in echelon form w.r.t. an appropriate ambient basis; see also [23].

Next, we examine which of these classes are closed under the dependence operator. For some it is not difficult to give a positive answer: free factor, echelon and compressed. For the others, it seems to be an open problem.

**6.1. Free factors.** We start with the simplest class, that of free factors of  $F$ . Clearly, a subgroup which is a free factor is dependence-closed and so, it is invariant under the dependence operator. In the following proposition we are dealing with a somewhat more complex situation, where Stallings automata play an essential role in the proof.

**Proposition 6.1.** *Let  $F_1 = F(A_1)$ ,  $F_2 = F(A_2)$ , where  $A_1$  and  $A_2$  are disjoint alphabets, and let  $F = F(A_1 \sqcup A_2) = F_1 * F_2$ . Let  $H_1 \leq F_1$ ,  $H_2 \leq F_2$  and let  $H = \langle H_1, H_2 \rangle$ . Then,  $\text{Dep}_F(H) = \text{Dep}_{F_1}(H_1) * \text{Dep}_{F_2}(H_2)$ .*

*In particular, if  $H_1$  is dependence-closed in  $F_1$  and  $H_2$  is dependence-closed in  $F_2$ , then  $H$  is dependence-closed in  $F$ .*

*Proof.* It is clear that  $H = H_1 * H_2$ . The Stallings automaton  $\Gamma_{A_1 \sqcup A_2}(H)$  with respect to the basis  $A_1 \sqcup A_2$  of  $F$  is the disjoint union of  $\Gamma_{A_1 \sqcup A_2}(H_1) = \Gamma_{A_1}(H_1)$  and  $\Gamma_{A_1 \sqcup A_2}(H_2) = \Gamma_{A_2}(H_2)$ , with the basepoints  $\bullet_1$  and  $\bullet_2$  identified into a single one  $\bullet$ . Let  $R_1$ ,  $R_2$ , and  $R$  be the sets of pairs of vertices as in (4.2), respectively, from  $\Gamma_{A_1}(H_1)$ ,  $\Gamma_{A_2}(H_2)$ , and  $\Gamma_{A_1 \sqcup A_2}(H)$ . We claim that

$$R = R_1 \sqcup R_2.$$

Clearly,  $R \supseteq R_1 \sqcup R_2$  since each of the pairs  $(p, q)$  in  $R_1$  and in  $R_2$  results in a rank reduction after identifying  $p$  with  $q$  in the corresponding part. On the other hand, when we identify  $\bullet_1 \neq p \in \Gamma_{A_1}(H_1)$  and  $\bullet_2 \neq q \in \Gamma_{A_2}(H_2)$ , we already obtain a deterministic  $(A_1 \sqcup A_2)$ -automaton (by the fact that  $A_1 \cap A_2 = \emptyset$ ) and thus, no

folding occurs and the rank increases by 1, implying that  $(p, q) \notin R$ . It follows that

$$\text{dep}_F(H) = \bigcup_{(p,q) \in R_1 \sqcup R_2 \sqcup \{(\circ, \circ)\}} Hg_{(p,q)}H$$

and  $\text{Dep}_F(H) = \text{Dep}_{F_1}(H_1) * \text{Dep}_{F_2}(H_2)$ .  $\square$

**6.2. 1-auto-fixed subgroups.** In the following example we show that the dependence subgroup of  $H = \text{Fix}(\alpha)$ , for  $\alpha \in \text{Aut}(F)$ , is not necessarily fixed by  $\alpha$ . This does not exclude the possibility of  $\text{Dep}(H)$  being fixed by another automorphism, as is indeed the case in this particular example.

**Example 6.2.** Let  $F = F(a, b)$  and let  $\alpha: F \rightarrow F$  be the automorphism defined by  $a \mapsto a$ ,  $b \mapsto ba$ . Then,  $H = \text{Fix}(\alpha) = \langle a, bab^{-1} \rangle$ , and  $\text{Dep}(H) = F$  is not fixed by  $\alpha$ . However, clearly  $F$  is fixed by the identity automorphism.

**6.3. Echelon subgroups.** For the class of echelon subgroups, we show that it is closed under the dependence operator.

**Proposition 6.3.** *Let  $F(A)$  be the free group on  $A = \{a_1, \dots, a_r\}$ , and let  $H \leq_{\text{fg}} F(A)$  be an echelon subgroup w.r.t.  $A$ . Then,  $\text{Dep}(H)$  is also an echelon subgroup w.r.t.  $A$ .*

*Proof.* Let  $F_0 = \{1\}$  and  $F_i = \langle a_1, \dots, a_i \rangle \leq_{\text{ff}} F$ , for  $i = 1, \dots, r$ . Also, let  $H_i = H \cap F_i \leq_{\text{ff}} H$  and  $D_i = \text{Dep}(H) \cap F_i \leq_{\text{ff}} \text{Dep}(H)$ , for  $i = 0, \dots, r$ . Since  $F_{i-1} \leq_{\text{ff}} F_i$  then  $H_{i-1} \leq_{\text{ff}} H_i$ ,  $D_{i-1} \leq_{\text{ff}} D_i$  and  $\text{rk}(H_{i-1}) \leq \text{rk}(H_i)$ ,  $\text{rk}(D_{i-1}) \leq \text{rk}(D_i)$ , for  $i = 1, \dots, r$ . Moreover, observe that when  $\text{rk}(D_i) = \text{rk}(D_{i-1})$  then  $D_i = D_{i-1}$  and this implies that  $H_i = H_{i-1}$ . Now, suppose that  $H$  is in echelon form w.r.t.  $A$ , i.e.,  $0 \leq \text{rk}(H_i) - \text{rk}(H_{i-1}) \leq 1$ , for each  $i$ . Then  $\text{rk}(H)$  equals the number of times that  $\text{rk}(H_i) = \text{rk}(H_{i-1}) + 1$ . Since an equality in ranks,  $\text{rk}(D_i) = \text{rk}(D_{i-1})$ , implies  $H_i = H_{i-1}$ , we deduce that  $\text{rk}(D_i) - \text{rk}(D_{i-1}) \geq \text{rk}(H_i) - \text{rk}(H_{i-1})$ , for each  $i = 1, \dots, r$ . Therefore,

$$\text{rk}(\text{Dep}(H)) = \sum_{i=1}^r (\text{rk}(D_i) - \text{rk}(D_{i-1})) \geq \sum_{i=1}^r (\text{rk}(H_i) - \text{rk}(H_{i-1})) = \text{rk}(H).$$

But, by Proposition 2.4,  $\text{rk}(\text{Dep}(H)) \leq \text{rk}(H)$ . Hence, the above inequality is an equality and thus, for each  $i = 1, \dots, r$ ,

$$0 \leq \text{rk}(D_i) - \text{rk}(D_{i-1}) = \text{rk}(H_i) - \text{rk}(H_{i-1}) \leq 1.$$

Thus,  $\text{Dep}(H)$  is in echelon form w.r.t.  $A$ .  $\square$

#### 6.4. Compressed subgroups.

**Proposition 6.4.** *Let  $F$  be a free group and let  $H \leq_{\text{fg}} F$  be a compressed subgroup. Then,  $\text{Dep}(H)$  is compressed, with  $\text{rk}(\text{Dep}(H)) = \text{rk}(H)$ .*

*Proof.* By Proposition 2.4,  $\text{rk}(\text{Dep}(H)) \leq \text{rk}(H)$ , but since  $H \leq \text{Dep}(H)$  and  $H$  is compressed then  $\text{rk}(\text{Dep}(H)) = \text{rk}(H)$ . Let now  $K$  be an arbitrary subgroup with  $\text{Dep}(H) \leq K \leq F$ . Then, since  $H \leq K$  and  $H$  is compressed, we have

$$\text{rk}(K) \geq \text{rk}(H) = \text{rk}(\text{Dep}(H)),$$

which proves that  $\text{Dep}(H)$  is compressed.  $\square$

## 7. DEPENDENCE SEQUENCE AND DEPENDENCE CLOSURE

In this section we investigate further the dependence operator and the notion of dependence closure in the setting of a free group  $F$ . Recall that a subgroup  $H \leq F$  is dependence-closed in  $F$  if  $\text{Dep}_F(H) = H$ . For example, free factors  $H \leq_{\text{ff}} F$  are dependence-closed in  $F$ , but they are not the only ones (e.g.,  $H = \langle a^2 b^2 \rangle$  and  $K = \langle [a, b] \rangle$  are both dependence-closed in  $F(\{a, b\})$ ).

We provide here an example of a subgroup  $H \leq_{\text{fg}} F(a, b)$ , such that  $\text{Dep}(H)$  is *not* dependence-closed; that is, the process of adding to  $H$  *all* the elements that depend on  $H$  and constructing  $\text{Dep}(H)$ , itself creates new dependent elements. In fact, for every  $m \geq 1$ , we exhibit a finitely generated subgroup  $H_m \leq_{\text{fg}} F(a, b)$  with dependence length  $\text{depl}(H_m) = m$ , i.e., for which its dependence sequence has length exactly  $m$ ,  $H_m < \text{Dep}^1(H_m) < \text{Dep}^2(H_m) < \dots < \text{Dep}^m(H_m) = \widehat{\text{Dep}}(H_m)$ .

**Example 7.1.** For every  $m \geq 1$ , we construct a subgroup  $H_m \leq F = F(a, b)$  of dependence length  $m \geq 1$  in the following way (see Figure 4 for the case  $m = 4$ ).

Let  $p_1, p_2, p_3, \dots = 2, 3, 5, \dots$  be the ascending sequence of prime numbers. We define the elements  $A_n \in F$ ,  $n \geq 1$ , to be<sup>1</sup>

$$A_1 = a^2 b^3 a^5 b^7, \quad A_2 = a^{11} b^{13} a^{17} b^{19}, \dots, \quad A_n = a^{p_{4n-3}} b^{p_{4n-2}} a^{p_{4n-1}} b^{p_{4n}}.$$

Now, let  $H_m = \langle h_1, \dots, h_{m-1}, A_m^5, A_{m+1} \rangle \leq F$ , where

$$h_1 = A_2 A_3 A_1^5 A_3 A_2, \quad h_2 = A_3 A_4 A_2^5 A_4 A_3, \dots, \quad h_{m-1} = A_m A_{m+1} A_{m-1}^5 A_{m+1} A_m.$$

**Proposition 7.2.**  $H_m$  is of dependence length  $m$ .

*Proof.* We claim that

$$\begin{aligned} \text{Dep}(H_m) &= \langle h_1, \dots, h_{m-2}, A_{m-1}^5, A_m, A_{m+1} \rangle, \\ \text{Dep}^2(H_m) &= \langle h_1, \dots, h_{m-3}, A_{m-2}^5, A_{m-1}, A_m, A_{m+1} \rangle, \\ &\vdots \\ \text{Dep}^j(H_m) &= \langle h_1, \dots, h_{m-1-j}, A_{m-j}^5, A_{m-j+1}, \dots, A_{m+1} \rangle, \\ &\vdots \\ \text{Dep}^m(H_m) &= \langle A_1, A_2, \dots, A_{m+1} \rangle, \end{aligned}$$

where all the above generators are free generators.

The idea in constructing  $H_m$  is the following. Since  $H_m$  contains the element  $A_m^5$ , then, clearly,  $A_m \in \text{Dep}(H_m)$ . Consequently,  $A_{m-1}^5$  is “revealed” since  $\text{Dep}(H_m)$  contains  $A_{m+1}$ ,  $A_m$  and  $h_{m-1} = A_m A_{m+1} A_{m-1}^5 A_{m+1} A_m$ . Thus,  $A_{m-1}$  is a dependent element of  $\text{Dep}(H_m)$ . In the next step, we obtain  $A_{m-2}$  as a dependent element of  $\text{Dep}^2(H_m)$  through  $A_m$ ,  $A_{m-1}$  and  $h_{m-2} = A_{m-1} A_m A_{m-2}^5 A_m A_{m-1}$ , and so on. It follows that after (at most)  $m$  steps we end up with the subgroup  $\text{Dep}^m(H_m) = \langle A_1, A_2, \dots, A_{m+1} \rangle$ , which is dependence-closed.

It is, however, less clear that throughout the dependence sequence there are no more dependent elements besides the ones mentioned above, which can cause additional foldings in the graphs of the subgroups. So, let us examine the graph of the subgroup  $\text{Dep}^{m-j}(H_m)$ . It contains  $m+1$  simple cycles that are of (at most)

<sup>1</sup>The fact that the powers of  $a$  and  $b$  in the  $A_n$  are prime numbers may reduce the number of possible foldings in the graphs of the dependent subgroups, but it does not seem to be a necessary condition.

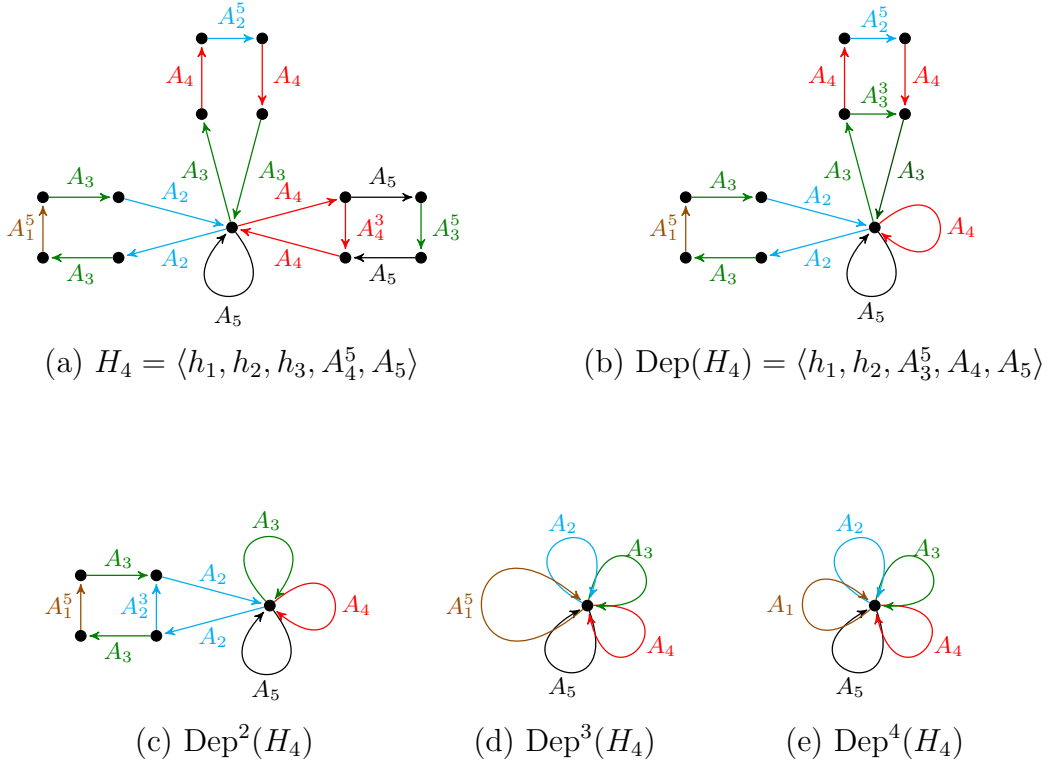


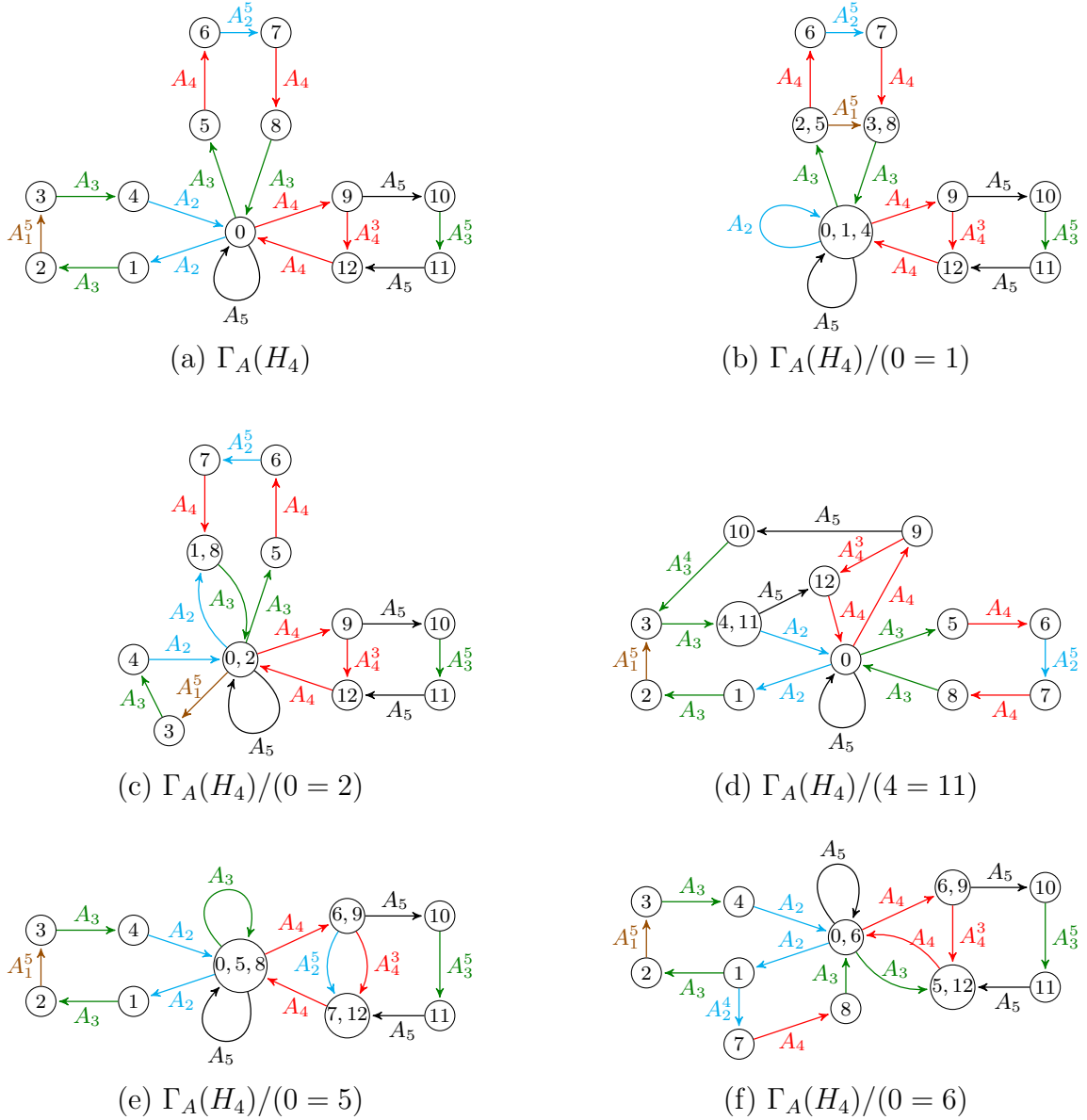
FIGURE 4. The dependence sequence of length 4 of the subgroup  $H_4$ , where  $h_j = A_{j+1}A_{j+2}A_j^5A_{j+2}A_{j+1}$ , for  $j = 1, 2, 3$ .

four types: the  $\odot$ -cycles  $h_i = A_{i+1}A_{i+2}A_i^5A_{i+2}A_{i+1}$ , for  $i = 1, \dots, j-1$ ,  $A_k$ , for  $k = j+1, \dots, m+1$ , and  $A_j^5$  (in addition to the cycle  $A_{j+1}A_{j-1}^5A_{j+1}A_j^{-3}$  which does not include the basepoint and is formed through  $h_{j-1}$  and  $A_j^5$ ). For convenience and without loss of generality, we will make use of the graph of  $H_4$  (Figure 5(a)) when checking the possible identifications of vertices. This graph contains cycles of all the above four types, and it is representative of the general case.

The fact that there are not many dependent elements is also due to the fact that the vertices are of low degrees. Most of the vertices are of degree 2, with outgoing pairs of edges labelled by  $(a, a^{-1})$ ,  $(b, b^{-1})$ ,  $(a, b^{-1})$  or  $(b, a^{-1})$ . Some vertices are of degree 3 (at most  $2(m+1)$  such vertices in  $\text{Dep}^i(H_m)$ ), with outgoing triples of edges labelled by  $(a, a^{-1}, b)$  or  $(b, b^{-1}, a^{-1})$ . The latter are to be found in the neighbourhood of the basepoint  $\odot$ , and two more vertices of degree 3 are located near the cycle that does not pass through  $\odot$  (near vertices 9 and 12 in Figure 5(a)).

Let us now look at the identification of any pair of possible vertices. We call a vertex at which an  $A_i$ -segment starts or terminates a *prime* vertex, and otherwise - a *secondary* vertex. When no prime vertex is involved in the identification (either directly or after the consequent foldings) then it takes place within some  $A_i$ . But clearly any such identification forms a loop that cannot be erased.

So, we can assume that the initial identification is of a prime vertex  $p$  and another vertex  $q$ . Suppose, first, that  $q$  is a secondary vertex. A  $p$ -cycle then starts with an  $A_i$ -segment (or an  $A_i^{-1}$ -segment), for some  $i$ , and ends with an  $A_j$ -segment (or an  $A_j^{-1}$ -segment), for some  $j$ . Let us assume, w.l.o.g. that it starts with an  $A_i$ -segment and ends with an  $A_j$ -segment. Given that  $A_i = a^{p_{4i-3}} b^{p_{4i-2}} a^{p_{4i-1}} b^{p_{4i}}$ , the  $p$ -cycle

FIGURE 5. Identifying vertices of  $\Gamma_A(H_4)$ 

begins with a sequence of  $a$ 's and ends with a sequence of  $b$ 's. The matching  $q$ -cycle then must also start and end with such sequences. Then, even if both  $a$ -sequences at the start of the cycles are completely matched, then the next sequence of  $b$ 's (of size  $p_{4i-2}$  in our case) in the  $p$ -cycle can be matched with a corresponding sequence of  $b$ 's in the  $q$ -cycle only when this  $b$ -sequence is part of an  $A_i$ -segment (the same  $i$  as in the  $p$ -cycle). This is because the size of the sequence of  $b$ 's that follows a sequence of  $a$ 's is unique to  $A_i$ . But then the previous sequence of  $a$ 's in the  $q$ -cycle should also be the first part of some  $A_i$ , which contradicts our assumption that  $q$  is a secondary vertex. Similarly, the last part of the  $p$ -cycle, consisting of a sequence of  $b$ 's that is preceded by an  $a$ -sequence, cannot be completely matched with a similar segment at the end of the  $q$ -cycle. It follows that the middle part of the  $p$ -cycle stays unfolded, and so the number of cycles cannot be reduced, and the identification of the vertices  $p$  and  $q$  does not produce a dependent element.

Let us now examine the case of identifying two prime vertices. Here it is clear that we can only match two paths both starting with an  $A_i$ -segment (the same  $i$ ) and ending with an  $A_j$ -segment (the same  $j$ ); otherwise, we cannot even match the first sequence of  $a$ 's or the last sequence of  $b$ 's.

It remains to look at an identification of two prime vertices  $p$  and  $q$  where both are incident to an  $A_i$ -segment or an  $A_j^{-1}$ -segment (the same  $i$  or  $j$ ). By the preceding discussion, we can look at the  $A_i$ -segments as single edges, representing free generators for the subgroups they generate (as in Figure 4(e)). So, let us examine such identifications in  $\Gamma(H_4)$  (Figure 5(a)). Clearly, the identification of vertex 0 (the basepoint  $\bullet$ ) with vertex 9 leads to the folding of the  $A_4^5$ -cycle into the  $A_4$ -segment and the result, after some more foldings, is seen in Figure 4(b). That is,  $A_4$  is obtained as a dependent element of  $H_4$ . We claim that all other identification of vertices (other than the ones that result with the same graph as in Figure 4(b)) increase the number of cycles. These are shown in Figure 5(b)-(f), where vertices of  $\Gamma_A(H_4)$  that are the initial or terminal vertices of an  $A_i$ -segment (the same  $i$  in both vertices) are identified. Not all possible identifications are shown, but the other identifications either lead to graphs that are of the same form as the graphs in Figure 5 (possibly with different vertex and edge labels) or are those in which it is clearly seen that they increase the number of cycles from 5 to 6.

The process of constructing the dependence sequence of  $H_m$  ends after  $m$  steps in the subgroup freely generated by the elements  $A_1, \dots, A_{m+1}$  and then no more dependent elements outside the subgroup exist. It follows that the dependence length of  $H_m$  is  $m$ .  $\square$

Despite the existence of these arbitrarily long dependence sequences, the dependence length,  $\text{depl}(H)$ , of a finitely generated subgroup  $H \leq_{\text{fg}} F$  is finite, and its dependence closure,  $\widehat{\text{Dep}}(H)$ , is always finitely generated. In addition, given a set of generators for  $H$ , one can algorithmically compute a set of generators for all the subgroups in the dependence sequence of  $H$ .

**Proposition 7.3.** *Let  $H \leq_{\text{fg}} F(A)$  and let  $n$  be the total length of the given generators of  $H$ . Then*

- (i)  $\text{depl}(H) \leq n$  and it is computable;
- (ii)  $\text{rk}(\widehat{\text{Dep}}(H)) \leq \text{rk}(H)$  and one can effectively compute a basis for  $\widehat{\text{Dep}}(H)$  in time  $\mathcal{O}(n^4 \log^*(n))$ .

*Proof.* (i) Consider the ascending sequence  $H \leq \text{Dep}^1(H) \leq \text{Dep}^2(H) \leq \dots$  of subgroups of  $F(A)$ . At each step, when passing from  $\text{Dep}^i(H)$  to  $\text{Dep}^{i+1}(H)$ , we identify at least one pair of vertices of the automaton  $\Gamma_A(\text{Dep}^i(H))$ , which does not result in an increase of rank. When no such pair exists anymore, the resulting dependence-closed subgroup is  $\widehat{\text{Dep}}(H)$ . Since the sum of the lengths of the given generators is  $n$ , the automaton  $\Gamma_A(H)$  has at most  $n$  vertices and so, the process consists of at most  $n$  steps, i.e.,  $\text{depl}(H) \leq n$ .

(ii) The fact that  $\text{rk}(\widehat{\text{Dep}}(H)) \leq \text{rk}(H)$  follows from Proposition 2.4 and from Lemma 2.3. By Corollary 4.4, given a set of generators for  $\text{Dep}^i(H)$ , we can compute a basis for  $\text{Dep}^{i+1}(H)$  in time  $\mathcal{O}(n^3 \log^*(n))$ . Since the dependence length is at most  $n$ , a basis for  $\widehat{\text{Dep}}(H)$  can be computed in time  $\mathcal{O}(n^4 \log^*(n))$ .

In fact, we can accelerate the process of computing a set of generators for  $\widehat{\text{Dep}}(H)$  (without getting generators for all the intermediate subgroups  $\text{Dep}^i(H)$ ) in the following way: whenever two vertices  $p$  and  $q$  are identified in an automaton  $\Gamma$  and, after performing all the subsequent foldings, the resulting automaton  $\Gamma'$  has rank not bigger than that of  $\Gamma$ , then we continue the identification of subsequent pairs of vertices from  $\Gamma'$  instead of  $\Gamma$ .  $\square$

When we are just interested in the question of deciding whether the subgroup  $H \leq_{\text{fg}} F(A)$  is dependence-closed then we only need to check if  $\text{Dep}(H) = H$ .

**Proposition 7.4.** *Let  $H \leq_{\text{fg}} F(A)$  and let  $n$  be the total length of the given generators of  $H$ . Then, it is algorithmically decidable in time  $\mathcal{O}(n^3 \log^*(n))$  whether  $H$  is dependence-closed or not.*

*Proof.* In order to decide whether  $\text{Dep}(H) \neq H$ , we only need to check (in the worst case) all pairs of distinct vertices  $(p, q)$  of the automaton  $\Gamma_A(H)$  and see whether, after identifying  $p$  with  $q$ , the following elementary foldings are all open. By Corollary 4.4, this can be done in time  $\mathcal{O}(n^3 \log^*(n))$ .  $\square$

## 8. OPEN PROBLEMS

We gather here some questions that we think are interesting for further research.

**Question 8.1** (answered by Dario Ascari [2]). Given  $H \leq_{\text{fg}} F$  and an element  $g \in F$  dependent on  $H$ , is it possible to find a non-trivial  $H$ -equation of minimal degree that is satisfied by  $g$ ? Is the ideal  $I_H(g)$  (of all polynomials  $w(x)$ , such that  $w(g) = 1$ ) generated (as normal subgroup of  $H * \langle x \rangle$ ) by (some of) its polynomials of minimal degree?

**Question 8.2.** Is the class of 1-auto-fixed subgroups closed under the dependence operator? And the class of 1-gen-endo subgroups? and that of inert subgroups?

**Question 8.3.** Can one extend the definitions and results in this paper to other classes of groups beside free groups? What are the “right” definitions of dependence in these cases (see Remark 1.2)?

**Question 8.4.** Is there a finitely presented group  $G$  where (some of) the above questions are algorithmically unsolvable? In the affirmative, construct such a group.

**Question 8.5.** Can one develop a similar theory for multi-variate equations over a subgroup  $H \leq_{\text{fg}} G$ ? Here, also, one has to find the “right” definition of dependence.

## ACKNOWLEDGMENTS

The first named author acknowledges the support of the Austrian Science Fund (FWF) project P29355-N35. The second named author acknowledges partial support from the Spanish Agencia Estatal de Investigación, through grants MTM2017-82740-P and PID2021-126851NB-100 (AEI/ FEDER, UE).

## REFERENCES

- [1] Y. Antolín, A. Jaikin-Zaipirain, “The Hanna Neumann conjecture for surface groups”, preprint available at <https://matematicas.uam.es/~andrei.jaikin/preprints/HNsurface.pdf>
- [2] D. Ascari, “Ideals of equations for elements in a free group and Stallings folding”, arXiv:2207.04759v1, July 2022.

- [3] D. Ascari, “Ideals of equations for elements in a free group and context-free languages”, to appear in *J. Algebra*, <https://www.sciencedirect.com/science/article/pii/S0021869323004192>
- [4] G. Baumslag, A. Myasnikov, V. Remeslennikov, “Algebraic geometry over groups. I. Algebraic sets and ideal theory”, *J. Algebra* **219**(1) (1999), 16–79.
- [5] D. Bormotov, R. Gilman, A. Myasnikov, “Solving one-variable equations in free groups Group”, *J. Group Theory* **12** (2009), 317–330.
- [6] J. Delgado, E. Ventura, “A list of applications of Stallings automata”, *Transactions on Combinatorics* **11**(3) (2022), 181–235.
- [7] W. Dicks, E. Ventura, “The group fixed by a family of injective endomorphisms of a free group”, *Contemporary Mathematics* **195**, American Mathematical Society, Providence, RI, 1996.
- [8] I. Kapovich, A. Myasnikov, “Stallings foldings and subgroups of free groups”, *Journal of Algebra* **248**(2) (2002), 608–668.
- [9] R. Lyndon, “Equations in free groups”, *Trans. Amer. Math. Soc.* **96** (1960), 445–457.
- [10] R. Lyndon, P. Schupp, “Combinatorial group theory”, *Classics in Mathematics*, Springer-Verlag, Berlin, Reprint of the 1977 edition.
- [11] G. Makanin, “Equations in a free group”, *Izv. Akad. Nauk SSSR Ser. Mat.* **46**(6) (1982), 1199–1273, 1344.
- [12] W. Magnus, A. Karrass, D. Solitar, “Combinatorial group theory: Presentations of groups in terms of generators and relations”, Interscience Publishers [John Wiley & Sons, Inc.], New York-London-Sydney, 1966.
- [13] S. Margolis, M. Sapir, P. Weil, “Closed subgroups in pro- $V$  topologies and the extension problems for inverse automata”, *Internat. J. Algebra Comput.* **11**(4) (2001), 405–445.
- [14] A. Martino, E. Ventura, “Examples of retracts in free groups that are not the fixed subgroup of any automorphism”, *J. Algebra* **269** (2003), 735–747.
- [15] A. Martino, E. Ventura, “A description of auto-fixed subgroups of a free group”, *Topology* **43** (2004) 1133–1164.
- [16] A. Miasnikov, E. Ventura, P. Weil, “Algebraic extensions in free groups”, *Trends Math.*, Birkhäuser, Basel (2007), 225–253.
- [17] D. Puder, “Primitive words, free factors and measure preservation”, *Israel J. Math.* **201**(1) (2014), 25–73.
- [18] A.A. Razborov, “On systems of equations in a free group”, *Izv. Akad. Nauk SSSR Ser. Mat.* **48**(4) (1984), 779–832; *Math. USSR-Izv.* **25**(1) (1985), 115–162.
- [19] A. Razborov, “On systems of equations in free groups”, *London Math. Soc. Lecture Note Ser.* (Cambridge Univ. Press, Cambridge) **204** (1995), 269–283.
- [20] A. Roig, E. Ventura, P. Weil, “On the complexity of the Whitehead minimization problem”, *Internat. J. Algebra Comput.* **17**(8) (2007), 1611–1634.
- [21] A. Rosenmann, “An algorithm for constructing Gröbner and free Schreier bases in free group algebras”, *J. Symb. Comput.* **16**(6) (1993), 523–549.
- [22] A. Rosenmann, “On rank, root and equations in free groups”, *Internat. J. Algebra Comput.* **11**(3) (2001), 375–390.
- [23] A. Rosenmann, “On the intersection of subgroups in free groups: echelon subgroups are inert”, *Groups Complex. Cryptol.* **5**(2) (2013), 211–221.
- [24] A. Rosenmann, E. Ventura, “Dependence and algebraicity over subgroups of free groups”, arXiv:2107.03154v1, July 2021.
- [25] P.V. Silva, P. Weil, “On an algorithm to decide whether a free group is a free factor of another”, *RAIRO - Theoretical informatics and applications - Informatique théorique et applications* **42**(2) (2008), 395–414.
- [26] J. Stallings, “Topology of finite graphs”, *Invent. Math.* **71**(3) (1983), 551–565.
- [27] M. Takahasi, “Note on chain conditions in free groups”, *Osaka Math. Journal* **3**(2) (1951), 221–225.
- [28] N. Touikan, “A fast algorithm for Stallings’ folding process”, *Internat. J. Algebra Comput.* **16**(6) (2006), 1031–1045.
- [29] E. Ventura, “On fixed subgroups of maximal rank”, *Comm. Algebra* **25** (1997), 3361–3375.

(A. Rosenmann) INSTITUT FÜR DISKRETE MATHEMATIK, TECHNISCHE UNIVERSITÄT GRAZ,  
AUSTRIA

*Email address:* `rosenmann@math.tugraz.at`

(E. Ventura) DEPARTAMENT DE MATEMÀTIQUES, UNIVERSITAT POLITÈCNICA DE CATALUNYA  
AND INSTITUT DE MATEMÀTIQUES DE LA UPC-BARCELONATECH, CATALONIA

*Email address:* `enric.ventura@upc.edu`