DEPENDENCE AND ALGEBRAICITY OVER SUBGROUPS OF FREE GROUPS

AMNON ROSENMANN AND ENRIC VENTURA CAPELL

Abstract. An element g of a free group F depends on a subgroup $H < F$, or is algebraic over H, if it satisfies a univariate equation over H. Equivalently, when H is finitely-generated, the rank of $\langle H, g\rangle$ is at most the rank of H. We study the elements that depend on subgroups of F, the subgroups they generate and the equations that they satisfy.

1. Introduction

Given a subgroup H of a free group F and an element $g \in F$, we say that g depends on H, or that g is algebraic over H, if it satisfies a univariate equation over H. Equivalently, when H is finitely-generated, the rank of $\langle H, g\rangle$ is at most the rank of H. When H is finitely generated then the set of elements that depend on H is a union of finitely-many double cosets. The subgroup generated by these elements is of rank at most the rank of H and a set of generators for this subgroup can be effectively computed. We also show that a dependence sequence of subgroups, i.e. when each subgroup is generated by the elements that depend on the previous subgroup, stabilizes after finitely-many steps in a subgroup which is dependence-closed.

When g depends on $H < F$ then the set of equations over H satisfied by g is a normal subgroup of the free product $H * \langle x\rangle$, and we show how one can compute a set of normal generators for this subgroup. We conclude by showing that there is a bound n, which can be effectively computed, such that every element g that depends on H satisfies an equation of degrees at most n over H.

2. The dependent subgroup

2.1. **Notation and definitions.** Throughout the paper, F denotes a free group. The free group on a set of free generators (a basis) $A = \{a_1, \dots, a_n\}$ is denoted $F = F(A)$ or $F = F(a_1, \dots, a_n)$. For a subgroup $H < F$ we write $H = \langle h_1, \dots, h_r\rangle$ when H is generated (not necessarily freely) by $h_1, \dots, h_r$. The rank of $H < K$, that is, the cardinality of a basis of H, is denoted by $\operatorname{rk} H$.

Key words and phrases: dependence on a subgroup of a free group, algebraic extension, dependence closure, equations over free groups.

When $H < F = F(A)$ then we denote by $\Gamma_A(H)$ the **Schreier coset graph** of H with respect to the basis $A = \{a_1, \dots, a_n\}$ of F, or just by $\Gamma(H)$ (see [MKS66]). Each vertex $v \in V(\Gamma_A(H))$ represents a right coset of H and is adjacent to $2n$ directed edges labelled $a_1^{\pm 1}, \dots, a_n^{\pm 1}$ going out of v. A directed edge e with initial vertex v and terminal vertex w that is labelled by a_j is labelled by a_j^{-1} in the opposite direction from w to v. The vertex labelled with 1 represents the coset $H1$ (1 being the trivial element of F) and is designated as the root of the graph. A vertex $v \in V(\Gamma_A(H))$ may be labelled with respect to the minimal path from the root to v, where "minimal" means of minimal length and with some lexical ordering on the letters of $A \cup A^{-1}$ as a tiebreaker. We also treat v according to its label as a group element of F (the minimal group element in its coset). If γ is a path starting at the root of $\Gamma_A(H)$ then the word $w = a_{i_1}^{\pm 1} \cdots a_{i_s}^{\pm 1}$ that is read off along the path represents an element of H if and only if γ is a closed path (a cycle) that terminates at the root. In general, two right cosets Hg and Hg' are equal if and only if the two paths in $\Gamma_A(H)$ that start at the root and with edge labels that form the two words g and g' end at the same vertex of $\Gamma_A(H)$.

The **core** of the graph $\Gamma_A(H)$ (or **Stallings subgroup graph** [Sta83]), denoted $C_A(H)$ or just $C(H)$, is the minimal connected subgraph containing the root and all non-trivial reduced cycles (the infinite hanging trees are chopped). As is known, $\operatorname{rk} H = b_1(\Gamma_A(H))$, the first Betti number, or the cyclomatic number (number of cycles), of $\Gamma_A(H)$ (or, equivalently, of $C_A(H)$). Note that $\operatorname{rk} H < \infty$ if and only if $C_A(H)$ is finite.

In [Ros01] the following notion was introduced.

Definition 2.1 (Dependence on a subgroup)**.** An element $g \in F$ **depends** on H if the following equivalent conditions hold:

(1) g satisfies a univariate equation $w(x) = 1$, where $w(x) \in H * F(x)$.
(2) The group homomorphism $\varphi_g : H * F(x) \to \langle H, g\rangle$, $h \mapsto h$ for $h \in H$ and $x \mapsto g$, is not injective.
(3) There exists a finitely-generated $H' < H$ such that $\operatorname{rk} \langle H', g\rangle \leq \operatorname{rk} H'$.

We denote by $\operatorname{dep} H$ the set of elements of F that depend on H. Note that $\operatorname{dep} H$ does not necessarily form a subgroup, e.g. when $H = \langle a^{10}, b^{10}\rangle$ then $a, b \in \operatorname{dep} H$ but $ab \notin \operatorname{dep} H$. We then denote by $\operatorname{Dep} H = \langle \operatorname{dep} H\rangle$ the **dependent subgroup** of H, i.e. the subgroup generated by the elements that depend on H. When $H, G < F$ then $\operatorname{Dep}_G H$ is the subgroup generated by all the elements of G that depend on H. We have $\operatorname{Dep}_G H < (\operatorname{Dep} H) \cap G$ and the inclusion may be strict.

Example 2.2. When $1 \neq H \lhd F$ or when H is of finite index in F then $\operatorname{Dep} H = F$.

When $H, G < F$ then $\operatorname{Dep}(H \cap G) < \operatorname{Dep} H \cap \operatorname{Dep} G$, and the inclusion may be strict, as shown in the following example.

Example 2.3. Let $F = F(a, b, c)$, $H = \langle aba^{-1}, b\rangle$, $G = \langle aca^{-1}, c\rangle$. Then $\mathrm{Dep}\, H = \langle a, b\rangle$, $\mathrm{Dep}\, G = \langle a, c\rangle$. Thus, $H \cap G = \mathrm{Dep}\,(H \cap G) = 1$ but $\mathrm{Dep}\, H \cap \mathrm{Dep}\, G = \langle a\rangle$.

In [KM02] the term **algebraic extension** was introduced (see also [MVW07]): when $H < G < F$ then G is an algebraic extension of H if there is no K such that $H < K < G$ and K is a (proper) free factor of G. Since g depends on H if and only if $\langle H, g\rangle$ is algebraic over H, we may say that an element g that depends on H is **algebraic** over H. In fact, when g depends on H then g is G-algebraic over H (i.e. every free factor of G that contains H contains also g) for every extension G of H, but the other way round does not necessarily hold. For example, when $H = \langle a^2b^2\rangle$ and $F = F(a, b)$ then F is an algebraic extension of H but $\mathrm{Dep}\, H = H$.

In [OHV16] the term **algebraic closure** is used in the more traditional sense to denote the set of all group elements that depend on H, similar to what we call $\mathrm{dep}\, H$ according to Definition 2.1 (1), but with the restriction that the corresponding equations should have only finitely-many solutions. Note, however, that when g is algebraic over H according to [OHV16] then the fact that it satisfies an equation over H with finitely-many solutions does not imply that $|\langle H, g\rangle : H| < \infty$, in contrast to the analogous simple algebraic extension in field theory, which is always a finite extension.

2.2. **The rank of the dependent subgroup.**

Lemma 2.4. *Let $(H_i)_{i\geq 0}$ be a sequence of finitely-generated subgroups of of a free group satisfying $H_i < H_{i+1}$ and $\mathrm{rk}\, H_i \geq \mathrm{rk}\, H_{i+1}$, for each i. Let $H = \cup_i H_i$. Then $\mathrm{rk}\, H = \lim_{i\to\infty} \mathrm{rk}\, H_i$ and furthermore, there exists m, such that $H = H_i$ for $i \geq m$.*

Proof. Let $r_i = \mathrm{rk}\, H_i$, for each i, and let $r_H = \mathrm{rk}\, H$. The sequence (r_i) is monotone decreasing and bounded, thus having a limit r. If $r_H > r$ there exists a free factor K of H of rank $r+1$. It follows that there exists l, such that for each $i \geq l$, $K < H_i$ and, moreover, K is a free factor of H_i. But then $r_i > r$, for $i \geq l$, in contradiction to $r = \lim_{i\to\infty} r_i$. Thus, $r_H \leq r$, and if S is a finite set of free generators of H, there exists m, such that $S \subset H_i$ for each $i \geq m$. Hence $H = H_i$ for each $i \geq m$ and $r_H = r$. □

For the next proposition we refer also to [Ros01].

Proposition 2.5. *Let $H < F$ be finitely-generated. Then $\mathrm{rk}\,\mathrm{Dep}\, H \leq \mathrm{rk}\, H$.*

Proof. There are countably-many elements $(g_i)_{i\geq 1}$ that depend on H. Let $(H_i)_{i\geq 0}$ be the sequence of subgroups satisfying $H_0 = H$ and $H_{i+1} = \langle H_i, g_{i+1}\rangle$, for $i > 0$. Since $g_{i+1} \in \mathrm{dep}\, H$ then $g_{i+1} \in \mathrm{dep}\, H_i$, hence $\mathrm{rk}\, H_{i+1} \leq \mathrm{rk}\, H_i$, for each i. That is, the sequence $(H_i)_{i\geq 0}$ is non-decreasing while the sequence $(\mathrm{rk}\, H_i)_{i\geq 0}$ is non-increasing. The result then follows by Lemma 2.4. □

2.3. **Computing a generating set for the dependent subgroup.**

Theorem 2.6. *Let $H < F$ be finitely-generated. One can effectively compute a finite set of generators for* $\operatorname{Dep} H$.

Proof. Since H is finitely-generated then it is a subgroup of a finitely-generated factor subgroup K of F and $\operatorname{Dep} H < K$. Thus, we may assume that F is also finitely-generated on some set $A = \{a_1, \ldots, a_n\}$.

Given $g \in F$, we want to check whether $\operatorname{rk}\langle H, g\rangle \leq \operatorname{rk} H$. One way to do it is through Nielsen-Schreier transformations [LS01]. Another way is in a graph-theoretic setting. We add to the root of the (finite) core $C(H) = C_A(H)$ of $\Gamma_A(H)$ a g-cycle. We then fold the graph by identifying edges of the same label that emerge from the same vertex, and finally we count the number of cycles in the resulting graph.

A necessary and sufficient condition for g to be in H is that the g-cycle maps into $C(H)$, possibly while forming loops. Otherwise, we check whether there exists a decomposition of g as $g = g_1 g_2^{-1}$ in reduced form (where g_1 or g_2 may be 1), such that both the g_1-path and the g_2-path start at the root and stay within $C(H)$. In order to find such a decomposition we first form the g_1-path by starting at the root and extending the path according to the letters of g as long as we can within $C(H)$. Suppose we end at the vertex u. We then form in a similar way the g_2-path where $g_2 = g^{-1} g_1$. Now there are two possible cases. If the g_2-path cannot stay within $C(H)$ then we know that a cycle labelled g that starts and ends at the root must stand out of $C(H)$, implying that $b_1(\Gamma(\langle H, g\rangle) = b_1(\Gamma(\langle H\rangle)) + 1$ and g does not depend on H. Otherwise, the g_2-path ends at a vertex $v \in C(H)$. What is left to do is to form a loop by identifying u with v, perform the necessary folding, and check whether the resulting graph $C(H))/(u = v)$, the induced quotient graph of $C(H)$, is of rank at most the rank of $C(H)$, and then g depends on H, or the rank increases, implying that g does not depend on H.

Let now

$$P = \{(u, v) \in V(C(H)) \times V(C(H)) : b_1(C(H)/(u = v)) \leq b_1(C(H))\}. \tag{2.1}$$

In fact, we may be satisfied with a smaller set P since identifying u with v is the same as identifying ua_i^{ε} with va_i^{ε}, $\varepsilon \in \{1, -1\}$, as long as ua_i^{ε} and va_i^{ε} are in $C(H)$. We claim that

$$\operatorname{Dep} H = \langle H, \{uv^{-1} : (u, v) \in P\}\rangle. \tag{2.2}$$

Indeed, if g is associated with the pair (u, v) as above then by the definition of a coset graph there exist $h_1, h_2 \in H$ such that $g = h_1 u (h_2 v)^{-1} = h_1 u v^{-1} h_2^{-1}$, an element of the double coset $Huv^{-1}H$, which is included in the above generated subgroup. $\square$

As we have seen, we can write the set of elements that depend on $H < F$ as a finite union of double cosets

$$\operatorname{dep} H = \bigcup_{(u,v)\in P} Huv^{-1}H, \tag{2.3}$$

where P is defined in (2.1). For example, the pair $(1, 1)$ represents the double coset $H1H = H$ and gives all the members of H as dependent on H.

The next proposition is about free products.

Proposition 2.7. *Let the free group F be factored as $F = F_1 * F_2$ and let $H = H_1 * H_2$, where $H_i < F_i$, for $i = 1, 2$. Let also*

$$\operatorname{dep} H_i = \bigcup_{(u_i,v_i)\in P_i} H_i u_i v_i^{-1} H_i,$$

for $i = 1, 2$. Then

$$\operatorname{dep} H = \bigcup_{(u,v)\in P_1\cup P_2} Huv^{-1}H.$$

Proof. Since $F = F_1 * F_2$ and $H_1 < F_1$, $H_2 < F_2$ then $C(H)$, the core of $\Gamma(H)$, is $C(H) = C(H_1) \wedge C(H_2)$, the wedge of the core graphs $C(H_1)$ and $C(H_2)$ with a common root 1. By (2.3), $\operatorname{dep} H = \bigcup_{(u,v)\in P} Huv^{-1}H$, where P is as in (2.1). Clearly $P_1 \cup P_2 \subseteq P$. On the other hand, when u and v do not belong to the same core $C(H_1)$ or $C(H_2)$, e.g. $1 \neq u \in C(H_1)$ and $1 \neq v \in C(H_2)$, then by identifying u and v we form a cycle and since the edges in $C(H_1)$ and $C(H_2)$ are of disjoint labels, no edges are identified and no folding occurs, so that the rank of the corresponding subgroup is greater than the rank of H. □

2.4. **Echelon subgroups.** In [DV96] the notion of an **inert subgroup** was introduced. A subgroup $H < F$ is inert if, for every $G < F$, $\operatorname{rk}(G \cap H) \leq \operatorname{rk}(G)$. When this property holds for every G that contains H then H is called **compressed** (see [DV96]). Of course, when H is inert then it is also compressed. An example of a subgroup which is inert is the fixed subgroup of an automorphism of a free group [DV96]. This subgroup is in an **echelon form** [Ros13]. Let $A = \{a_1, \ldots, a_n\}$, let $F = F(A)$, and let $F_i = \langle a_1, \ldots, a_i\rangle$, $i = 0, \ldots, n$, where $F_0 = \langle 1\rangle$. For $H < F$, let $H_i = H \cap F_i$, for each i. Then H is in echelon form with respect to (the ordered basis) A if for every i, $i = 1, \ldots, n$, we have $\operatorname{rk} H_i - \operatorname{rk} H_{i-1} \leq 1$.

Proposition 2.8. *If $H < F$ is in echelon form then so is* $\operatorname{Dep} H$.

Proof. Let F be freely generated by the ordered basis $A = \{a_1, \ldots, a_n\}$ and let F_i and H_i be as above. Let also $D_i = (\operatorname{Dep} H) \cap F_i$, for every i. Since $H < \operatorname{Dep} H$ then, as in the proof of Proposition 3.8 in [Ros13], for each i, $\operatorname{rk} H_i \leq \operatorname{rk} D_i$. But by Proposition 2.5, $\operatorname{rk} \operatorname{Dep} H \leq \operatorname{rk} H$, hence, for every i, $\operatorname{rk} H_i = \operatorname{rk} D_i$. It implies that $\operatorname{rk} D_i - \operatorname{rk} D_{i-1} \leq 1$ for every i, which means that $\operatorname{Dep} H$ is in echelon form. □

3. Dependence closure

The notion of dependence closure appears in [Ros01] and it equals the elementary algebraic closure of [MVW07].

Definition 3.1 (Dependence closure)**.** A subgroup H is **dependence-closed**, if $H = \operatorname{Dep} H$. Given $G < F$, we say that H_G is dependence-closed if no element of the set difference $G \setminus H$ depends on H.

Example 3.2. When H is a free factor of G then H_G is dependence-closed.

Example 3.3. Let $F = F(a, b)$. Then the subgroups $H = \langle a^2b^2\rangle$, and $G = \langle [a, b]\rangle$ are dependence-closed. However, since there is no proper factor of F which contains H or G then the algebraic closure (according to [MVW07]) of these subgroups is F itself.

The following three propositions are straightforward and the proofs are left to the reader.

Proposition 3.4. *Let $H < G < K$. If H_G is dependence-closed and G_K is dependence-closed then H_K is dependence-closed.*

Proposition 3.5. *If H_K is dependence-closed and G_L is dependence-closed then $(H \cap G)_{K\cap L}$ is dependence-closed.*

Proposition 3.6. *Let $\mathcal{DC} = \mathcal{DC}(F)$ be the set of dependence-closed subgroups of F. The following statements hold.*

1. *If $H \in \mathcal{DC}$ then H is malnormal: $H^g \cap H = 1$ for every $g \in F \setminus H$.*
2. *If $H \in \mathcal{DC}$ then H is pure (root-closed, radical-closed): if $g^n \in H$, $n \neq 0$, then $g \in H$.*
3. *If $H \in \mathcal{DC}$ and $H \lneq G$, then $|G : H| = \infty$.*
4. *If $H \in \mathcal{DC}$ and K is a free factor of H then $K \in \mathcal{DC}$.*
5. *If $H, G \in \mathcal{DC}$ then $H \cap G \in \mathcal{DC}$.*

The next proposition follows from Proposition 2.7.

Proposition 3.7. *For $i = 1, 2$, let F_i be a free group, let $H_i < F_i$ and let $\mathcal{DC}(F_i)$ be the set of dependence-closed subgroups of F_i. If $H_i \in \mathcal{DC}(F_i)$, $i = 1, 2$, then $H_1 * H_2 \in \mathcal{DC}(F_1 * F_2)$.*

Let $H_0 = H$ and let $(H_i)_{i\geq 0}$ be the dependence sequence of subgroups $H_{i+1} = \operatorname{Dep} H_i = \operatorname{Dep}^{i+1}(H)$. Let $\widehat{\operatorname{Dep}}\, H = \cup_i H_i$ be the **dependence closure** of H.

Proposition 3.8. *Let $H < F$ be finitely generated.*

1. *There exists a computable minimal $m \geq 0$, the **dependence length** of H, such that $\widehat{\operatorname{Dep}}\, H = \operatorname{Dep}^m(H)$.*
2. *$\operatorname{rk} \widehat{\operatorname{Dep}}\, H \leq \operatorname{rk} H$ and one can compute effectively a basis for $\widehat{\operatorname{Dep}}\, H$.*

Proof. The result follows from Lemma 2.4, Proposition 2.5 and Theorem 2.6. In fact, since the core graph $C(H)$ is finite and we form a sequence of quotient graphs by identifying vertices, as long as the number of cycles does not increase, then clearly this process is finite. □

Remark 3.9. The dependence closure $\widehat{\mathrm{Dep}}\,H$ is exactly the elementary algebraic extension closure of [MVW07].

Proposition 3.10. *For every $m \geq 0$ there exists a subgroup $H < F = F(a,b)$ with dependence length m.*

Proof. Let α_1 be the sequence of the first 10^{100} positive digits of π, ignoring the decimal point and the zeros, and let n_1 be the positive integer consisting of these digits:

$$\alpha_1 = (3, 1, 4, 1, 5, 9, ...).$$

$$n_1 = 314159\ldots$$

For $i \geq 2$, let α_i be the sequence of the next $10^{n_{i-1}}$ positive digits of π and let n_i be the integer consisting of the digits of α_i. Similarly, for $i \geq 0$, let the sequences β_i and the numbers l_i be formed from the positive digits of Euler's number e.

Given a sequence of positive integers $\alpha = (a_1, a_2, a_3, \ldots, a_{2r})$, we define a word in the variables y, z

$$w_\alpha(y,z) = y^{a_1} z^{a_2} y^{a_3} z^{a_4} \cdots y^{a_{2r-1}} z^{a_{2r}}.$$

Let us now form a sequence of elements h_i and g_i of F. Let

$$h_0 = g_0 = w_{\beta_0}(a,b) = a^2 b^7 a^1 b^8 a^2 b^8 \cdots .$$

For $i = 1, \ldots, m$, let

$$g_i = w_{\alpha_i}(a,b),$$

that is,

$$g_1 = w_{\alpha_1}(a,b) = a^3 b^1 a^4 b^1 a^5 b^9 \cdots ,$$

and so on. For $i = 1, \ldots, m$, let

$$h_i = w_{\beta_i}(g_i, g_{i-1}).$$

Note that the g_i, $i = 1, \ldots, m$, satisfy the equations

$$w_{\beta_i}(x, g_{i-1}) h_i^{-1} = 1. \tag{3.1}$$

Let now

$$H = \langle h_0, \ldots, h_m \rangle.$$

Clearly, $g_1 \in \operatorname{dep} H$ since it solves the equation $w_{\beta_1}(x, h_0) h_1^{-1} = 1$. Moreover, for $i = 1, \ldots, m$, by (3.1), by the lengths of the words and the randomness of the sequences that are used to build the group elements and by induction,

$$g_i \in \mathrm{Dep}^i(H) \setminus \mathrm{Dep}^{i-1}(H).$$

For example, for $i = 2$,

$$g_2 = w_{\alpha_2}(a, b),$$
$$h_2 = w_{\beta_2}(g_2, g_1),$$

and so $g_1 \in \operatorname{Dep} H \setminus H$ and $g_2 \in \operatorname{Dep}^2(H) \setminus \operatorname{Dep} H$. It follows that the dependence length of H is m. □

4. Equations for the dependent elements

Let $\mathbb{Z} = F(x)$ be the free abelian group of rank 1 generated by x. An **equation** in the variable x over a subgroup $H < F$ is an expression of the form $w(x) = 1$, where $w(x) \in H * \mathbb{Z}$ (see e.g. [Lyn60]). An element $g \in F$ is a **solution** of $w(x) = 1$ if $w(g) = 1$. A complicated algorithm for solving equations in free groups was developed by Makanin [Mak82] and Razborov [Raz87, Raz95].

For $g \in \operatorname{dep} H$, let $\mathrm{Eqn(H, g)}$ be the set of equations $w(x) \in H * \mathbb{Z}$ for which g is a solution. It is easy to see that $\mathrm{Eqn(H, g)}$ forms a normal subgroup of $H * \mathbb{Z}$.

When $w(x) = h_1 x^{i_1} h_2 x^{i_2} \cdots h_m x^{i_m} h_{m+1}$, where $h_j \in H$ for $j = 1, \ldots, m+1$, $h_j \neq 1$ for $j = 2, \ldots, m$, and $i_j \in \mathbb{Z} \setminus \{0\}$ for $j = 1, \ldots, m$, then the **degree** of $w(x)$ (or of $w(x) = 1$) is $\sum_{j=1}^{m} |i_j|$.

Theorem 4.1. *Given $H < F$ of rank r and an element $g \in \operatorname{dep} H$, one can effectively compute a normal basis of size $s \leq r$ for* $\mathrm{Eqn(H, g)}$.

Proof. Let $\{h_1, \ldots, h_r\}$ be a set of free generators for H and consider the group homomorphism $\varphi_g : H * \mathbb{Z} \to \langle H, g \rangle$ defined by $h_i \mapsto h_i$, $i = 1, \ldots, r$ and $x \mapsto g$. Then apply Nielsen-Schreier transformations to the elements $h_1, \ldots, h_r, g$ to compute a set $\{b_1, \ldots, b_s\}$ of size $1 \leq s \leq r$ of free generators for the subgroup $\langle H, g \rangle$. Assume also, without loss of generality, that $h_1, \ldots, h_s$ are transformed to $b_1, \ldots, b_s$, respectively, while $h_{s+1}, \ldots, h_r, g$ are reduced to 1. Now apply the same transformations to $h_1, \ldots, h_r, x$, where x replaces g, to compute a basis $\{w_1(x), \ldots, w_{r+1}(x)\}$ of $H * \mathbb{Z}$. The map φ_g applied to this basis is given by

$$\begin{aligned} w_1(x) &\mapsto b_1, \\ &\vdots \\ w_s(x) &\mapsto b_s, \\ w_{s+1}(x) &\mapsto 1, \\ &\vdots \\ w_{r+1}(x) &\mapsto 1. \end{aligned}$$

Since the restriction of φ_g to $\langle w_1(x), \ldots, w_s(x) \rangle$ is injective, the kernel of φ_g is

$$\ker \varphi_g = \langle\langle w_{s+1}(x), \ldots, w_{r+1}(x) \rangle\rangle,$$

the normal subgroup of $H * \mathbb{Z}$ generated by $w_{s+1}(x), \ldots, w_{r+1}(x)$.
It follows that $\{w_{s+1}(x), \ldots, w_{r+1}(x)\}$ is a normal basis for $\mathrm{Eqn(H, g)}$. □

Remark 4.2. When g_1, g_2 are two solutions of the same equation $w(x) = 1$ over H there is not necessarily an automorphism of $\langle H, g_1, g_2\rangle$ which sends g_1 to g_2 and fixes H. For example, let $F = F(a)$, $H = \langle a^3\rangle$ and $w(x) = axa^{-1}x^{-1}$. Then every element of F is a solution of $w(x) = 1$ but every automorphism that fixes H fixes the whole of F.

Theorem 4.3. *Given $H < F$ one can effectively compute an integer n, such that each $g \in F$ that depends on H satisfies an equation over H of degree at most n.*

Proof. One can compute a finite set of generators of $\operatorname{Dep} H$ by Theorem 2.6 and then an equation for each such generator by Theorem 4.1. Suppose now that $u, v \in P$ as in (2.1) and $w(x) = 1$ is an equation obtained for the element $uv^{-1} \in F$ that depends on H. If $g = h_1uv^{-1}h_2^{-1}$, where $h_1, h_2 \in H$, is another element that depends on H and is obtained by identifying the same u and v then, as seen in (4.1), g satisfies an equation of the same degree as the degree of $w(x)$. It follows that we only need to consider the finitely-many elements uv^{-1} for $u, v \in P$ and the result follows. □

We give now a description of all the equations over H which are satisfied by the elements that depend on H. We know how to construct a normal basis for the normal subgroup of all the equations for each of the generators of $\operatorname{Dep} H$ of the form uv^{-1}, where $u, v \in P$ as in (2.1). Let S be the finite union of these normal subgroups of $H * \mathbb{Z}$. Then, the equations for all the dependent elements on H are obtained as the union of the images of S by all the automorphisms of $H * \mathbb{Z}$ that fix H, because then x is mapped to an element of $HxH \cup Hx^{-1}H$ and when $w(x) = 1$ is an equation for uv^{-1} then $w(h_1^{-1}xh_2) = 1$ is an equation for $h_1uv^{-1}h_2^{-1}$.

4.1. **Computing the equations using Stallings folding.** As in the proof of Theorem 2.6, one can compute an equation for g over H also in the graph-theoretic setting. We begin with the core $C(H)$ of H and add to it a g-cycle. Since every cycle that starts and terminates at the root represents an element of H, it suffices to consider $g = g_1g_2^{-1}$ with both g_1 and g_2 forming a simple path within $C(H)$ that terminates at the vertex u, respectively v. Indeed, if $g = h_1uv^{-1}h_2^{-1}$, where $h_1, h_2 \in H$, then if uv^{-1} is a solution of $w(x) = 1$ then

$$w'(x) = w(h_1^{-1}xh_2) = 1 \tag{4.1}$$

is an equation satisfying $w'(g) = 1$ and of the same degree as the degree of $w(x)$.

Next we identify the vertices u and v. Then we start folding the graph whenever edges of the same label emerge from the same vertex. Since g depends on H, at some point some cycle $waa^{-1}w^{-1}$ collapses when identifying the two a-edges. We then lift $waa^{-1}w^{-1}$ all the way back to the starting graph. At the last step the cycle gets cut at all the places where the vertices u and v are separated. At this stage we reconnect the broken cycle by inserting $g_1^{-1}gg_2$ at all the places where the jump is from u to v, and inserting $g_2^{-1}g^{-1}g_1$ at all the places where the jump is from v to u. In this way, the words between consecutive appearances of $g^{\pm 1}$ start and end at the root and so are elements of H. Finally, replacing g by x and g^{-1} by x^{-1} gives an equation $w(x) = 1$ for which g is a solution.

5. Open problems

Problem 5.1. Is it possible to find an equation of minimal degree for an element g that depends on H?

Problem 5.2. When H is compressed then $\operatorname{Dep} H$ is also compressed (with $\operatorname{rk} H = \operatorname{rk} \operatorname{Dep} H$). Is it also true when H is inert? As shown in Proposition 2.8, it holds for echelon subgroups.

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 grant MTM2017-82740-P (AEI/ FEDER, UE).

References

[DV96] Warren Dicks and Enric Ventura. *The group fixed by a family of injective endomorphisms of a free group*, volume 195 of *Contemporary Mathematics*. American Mathematical Society, Providence, RI, 1996.

[KM02] Ilya Kapovich and Alexei Myasnikov. Stallings foldings and subgroups of free groups. *J. Algebra*, 248(2):608–668, 2002.

[LS01] Roger C. Lyndon and Paul E. Schupp. *Combinatorial group theory*. Classics in Mathematics. Springer-Verlag, Berlin, 2001. Reprint of the 1977 edition.

[Lyn60] Roger C. Lyndon. Equations in free groups. *Trans. Amer. Math. Soc.*, 96:445–457, 1960.

[Mak82] G. S. Makanin. Equations in a free group. *Izv. Akad. Nauk SSSR Ser. Mat.*, 46(6):1199–1273, 1344, 1982.

[MKS66] Wilhelm Magnus, Abraham Karrass, and Donald Solitar. *Combinatorial group theory: Presentations of groups in terms of generators and relations*. Interscience Publishers [John Wiley & Sons, Inc.], New York-London-Sydney, 1966.

[MVW07] Alexei Miasnikov, Enric Ventura, and Pascal Weil. Algebraic extensions in free groups. In *Geometric group theory*, Trends Math., pages 225–253. Birkhäuser, Basel, 2007.

[OHV16] Abderezak Ould Houcine and Daniele Vallino. Algebraic and definable closure in free groups. *Ann. Inst. Fourier (Grenoble)*, 66(6):2525–2563, 2016.

[Raz87] Alexander A. Razborov. *On systems of equations in a free group*. PhD thesis, Steklov Math. Institute, Moscow, 1987. In Russian.

[Raz95] Alexander A. Razborov. On systems of equations in free groups. In *Combinatorial and geometric group theory (Edinburgh, 1993)*, volume 204 of *London Math. Soc. Lecture Note Ser.*, pages 269–283. Cambridge Univ. Press, Cambridge, 1995.

[Ros01] Amnon Rosenmann. On rank, root and equations in free groups. *Internat. J. Algebra Comput.*, 11(3):375–390, 2001.

[Ros13] Amnon Rosenmann. On the intersection of subgroups in free groups: echelon subgroups are inert. *Groups Complex. Cryptol.*, 5(2):211–221, 2013.

[Sta83] John R. Stallings. Topology of finite graphs. *Invent. Math.*, 71(3):551–565, 1983.

(A. Rosenmann) Institut für Diskrete Mathematik, Technische Universität Graz, Austria
Email address: rosenmann@math.tugraz.at

(E. Ventura Capell) Departament de Matemàtiques, Universitat Politècnica de Catalunya and Institut de Matemàtiques de la UPC-BarcelonaTech, Spain
Email address: enric.ventura@upc.edu