The equation $w(x, y) = u$ over free groups: an algebraic approach

Nicholas W.M. Touikan
Department of Mathematics and Statistics, McGill University
Montréal, Québec, Canada
touikan@math.mcgill.ca

September 25, 2008

Abstract

Using the theory developed by Olga Kharlampovich, Alexei Miasnikov, and, independently, by Zlil Sela to describe the set of homomorphisms of a f.g. group $G$ into a free group $F$, we describe the solutions to equations with coefficients from $F$ and unknowns $x, y$ of the form $w(x, y) = u$, where $u$ lies in $F$ and $w(x, y)$ is a word in $\{x, y\}^{\pm 1}$. We also give an example of a single equation whose solutions cannot be described with only one “level” of automorphisms.

1 Introduction

Solving systems of equations over free groups has been a very important topic in group theory. A major achievement was the algorithm due to Makanin and Razborov [13, 15] which produces a complete description of the solution set of an arbitrary finite system of equations over a free group. In practice, however, the algorithm is quite complicated and does not readily imply the results of this paper.

Much has already been said about solutions to certain types of systems of equations. Solutions of systems of equations in one unknown over a free group were described in 1960 by Lyndon [11]. In 1971, Hmelevskii gave in [6] an algorithm to decide solvability as well as a description of the solutions of equations in unknowns $x, y$ with coefficients in a free group $F$ of the form $w(x, y) = u$, and $t(x, F) = u(y, F)$. In 1972 Wicks [21] also described a method for find all the the solutions of the equation $w(x, y) = u$. In his paper, Wicks gives a way to find a finite set of solutions to an equation and shows how to generate all the possible solutions from this finite set using automorphisms. It has also been shown by Laura Ciabaru in [4] that there is a polynomial time algorithm to determine if $w(x, y) = u$ has a solution. So far all the approaches have been combinatorial.

In this paper we tackle the equation $w(x, y) = u$ from a different point of view. We will use the theory developed by Olga Kharlampovich, Alexei Miasnikov, and, independently, by Zlil Sela to describe the set of homomorphisms
of a f.g. group $G$ into a free group $F$. We start by considering the fully residually $F$ groups (also called the Limit groups relative to $F$) corresponding to the equation $w(x, y) = u$. These groups were shown by Remeslennikov in [16] to be key in the study of systems of equations. We then systematically describe the possible canonical $F$-automorphisms of these groups and give the possible Hom (also called Makanin-Razborov) diagrams that arise.

In so doing we get an algebraic proof that solutions to equations of the form $w(x, y) = u$, can be parametrized by a finite set of minimal solutions and a group of canonical automorphisms, which gives us a very explicit description of the arising algebraic varieties (see Theorem 2.28). We also exhibit an equation $E(F, x, y) = 1$ whose solutions cannot be described this way (see Theorem 3.1). In particular, we recover some of the aforementioned results of Hmelevski˘ı and Wicks, but our description of the solutions is by far the most transparent. In our opinion this paper also serves as an illustration of some of the very important ideas and techniques that have recently been applied fully residually free (or limit) groups.

1.1 $F$-groups and Algebraic Geometry

A complete account of the material in this section can be found in [2]. Fix a free group $F$. An equation in variables $x, y$ over $F$ is an expression of the form

$$E(x, y) = 1$$

where $E(x, y) = f_1 z_1^{m_1} \ldots z_n^{m_n} f_{n+1}; f_i \in F, z_j \in \{x, y\}$ and $m_k \in \mathbb{Z}$. By an equation of the form $w(x, y) = u$ we mean an equation

$$z_1^{m_1} \ldots z_n^{m_n} u^{-1} = 1$$

where $u \in F, z_j \in \{x, y\}$.

We view an equation as an element of the group $F[x, y] = F \ast F(x, y)$. A solution of an equation is a substitution $x \mapsto g_1, y \mapsto g_2; g_i \in F$

so that in $F$ the product $E(g_1, g_2) = 1$. A system of equations in variables $x, y; S(x, y) = S$ is a subset of $F[x, y]$ and a solution of $S(x, y)$ is a substitution as in (1) so that all the elements of $S(x, y)$ vanish in $F$.

**Definition 1.1.** A group $G$ equipped with a distinguished monomorphism

$$i : F \hookrightarrow G$$

is called an $F$-group we denote this $(G, i)$. Given $F$-groups $(G_1, i_1)$ and $(G_2, i_2)$, we define an $F$-homomorphism to be a homomorphism of groups $f$ such that the following diagram commutes:

$$
\begin{array}{c}
G_1 \\
\downarrow{i_1} \\
F \\
\uparrow{i_2}
\end{array}
\xrightarrow{f} 
\begin{array}{c}
G_2 \\
\end{array}
$$

We denote by $\text{Hom}_F(G_1, G_2)$ the set of $F$-homomorphisms from $(G_1, i_1)$ to $(G_2, i_2)$.
In the remainder the distinguished monomorphisms will in general be obvious and not explicitly mentioned. It is clear that every mapping of the form \( F \) induces an \( F \)-homomorphism \( \phi(g_1, g_2) : F[x, y] \to F \); it is also clear that every \( f \in \text{Hom}_F(F[x, y], F) \) is induced from such a mapping. It follows that we have a natural bijective correspondence

\[
\text{Hom}_F(F[x, y], F) \leftrightarrow F \times F = \{(g_1, g_2) | g_i \in F\}
\]

**Definition 1.2.** Let \( S = S(x, y) \) be a system of equations. The subset

\[
V(S) = \{(g_1, g_2) \in F \times F | x \mapsto g_1, y \mapsto g_2 \text{ is a solution of } S\}
\]

is called the algebraic variety of \( S \).

We have a natural bijective correspondence

\[
\text{Hom}_F(F[x, y]/\text{ncl}(S), F) \leftrightarrow V(S)
\]

**Definition 1.3.** The radical of \( S \) is the normal subgroup

\[
\text{Rad}(S) = \bigcap_{f \in \text{Hom}_F(F[x, y]/\text{ncl}(S), F)} \ker(f)
\]

and we denote the coordinate group of \( S \)

\[
F_{R(S)} = F[x, y]/\text{Rad}(S)
\]

It follows that there is a natural bijective correspondence

\[
\text{Hom}_F(F[x, y]/\text{ncl}(S), F) \leftrightarrow \text{Hom}_F(F_{R(S)}, F)
\]

so that \( V(S) = V(\text{Rad}(S)) \). We say that \( V(S) \) or \( S \) is reducible if it is a union

\[
V(S) = V(S_1) \cup V(S_2); V(S_1) \subseteq V(S) \supseteq V(S_2)
\]

of algebraic varieties. An \( F \)-group \( G \) is said to be fully residually \( F \) if for every finite subset \( P \subseteq G \) there is some \( f_P \in \text{Hom}_F(G, F) \) such that the restriction of \( f_P \) to \( P \) is injective.

**Theorem 1.4** ([2]). \( S \) is irreducible if and only if \( F_{R(S)} \) is fully residually \( F \).

**Theorem 1.5** ([2]). Either \( F_{R(S)} \) is fully residually \( F \) or

\[
V(S) = V(S_1) \cup \ldots \cup V(S_n)
\]

where the \( V(S_i) \) are irreducible and there are canonical epimorphisms \( \pi_i : F_{R(S)} \to F_{R(S_i)} \) such that each \( f \in \text{Hom}_F(F_{R(S)}, F) \) factors through some \( \pi_i \).

**Corollary 1.6.** If \( F[x, y]/\text{ncl}(S) \) is fully residually \( F \) then \( F_{R(S)} = F[x, y]/\text{ncl}(S) \).
1.2 Rational Equivalence

Definition 1.7. An $F$-automorphism of $F[x, y]$ is an automorphism
\[ \phi : F[x, y] \to F[x, y] \]
such that the restriction $\phi|_F$ is the identity. Two systems of equations $S, T$ are said to be rationally equivalent if $\phi(S) = T$, for some $\phi \in \text{Aut}_F(F[x, y]).$

Proposition 1.8. (i) $\text{Aut}_F(F[x, y])$ is generated by the elementary Nielsen transformations on the basis $\{F, x, y\}$ that fix $F$ elementwise.

(ii) If $S, T$ are rationally equivalent via $\phi \in \text{Aut}_F(F[x, y])$, then the natural map $\phi$ in the commutative diagram below is an isomorphism.

\[
\begin{array}{ccc}
F[x, y] & \xrightarrow{\phi} & F[x, y] \\
\downarrow \cong & & \downarrow \cong \\
F_{R(S)} & \xrightarrow{\bar{\phi}} & F_{R(T)}
\end{array}
\]

Proposition 1.9. Suppose $w(x, y)$ is a primitive (by primitive we mean an element that belongs to some basis) element of $F(x, y)$, then there exist words $X(u, z), Y(u, z)$ such that the set of solutions of $w(x, y) = u$ correspond to the set of pairs
\[(x, y) = (X(u, z), Y(u, z))\]
where $z$ takes arbitrary values in $F$.

Proof. Let $S = \{w(x, y)u\}$. By assumption there is $\phi \in \text{Aut}_F(F[x, y])$ that sends $w(x, y)$ to $x$ and $\phi$ extends to an $F$ automorphism of $F[x, y]$. This means that $S$ is rationally equivalent to $T = \{xu^{-1}\}$. The first thing to note is that $F_{R(T)}$ is a free group, hence so is $F_{R(S)}$. $\text{Hom}_F(F_{R(T)}, F)$ is given by
\[ V(T) = \{(x, y) \in F \times F | x = u, y \in F \} \]
the result now follows by precomposing with $\bar{\phi}^{-1}$, as defined in Proposition 1.8.

Lemma 1.10. Suppose the free group $F(x, y)$ on generators $\{x, y\}$ admits a presentation
\[ F(x, y) = \langle \xi, \zeta, p | \xi, \zeta | p^{-1} \rangle \]
where $\xi, \zeta, p \in F(x, y)$. Then the mapping $\phi(\xi) = x, \phi(\zeta) = y, \phi(p) = [x, y]$, extends to an automorphism $\phi : F(x, y) \to F(x, y)$.

Proof. Notice that the basis elements $x, y$ of $[x, y]$ obviously satisfy the identity $[x, y]^{-1} = y$ so the mapping $\phi$ gives an automorphism.

1.3 Splittings

We assume the reader is familiar with Bass-Serre theory, so we only describe enough to explain our notation.
Definition 1.11. A graph of groups \( \mathcal{G}(A) \) consists of a connected directed graph \( A \) with vertex set \( VA \) and edges \( EA \). \( A \) is directed in the sense that to each \( e \in EA \) there are functions \( i : EA \to VA, t : EA \to VA \) corresponding to the initial and terminal vertices of edges. To \( A \) we associate the following:

- To each \( v \in VA \) we assign a vertex group \( G_v \).
- To each \( e \in EA \) we assign an edge group \( G_e \).
- For each edge \( e \in EA \) we have monomorphisms

  \[ \sigma_e : G_e \to G_{i(e)}, \tau_e : G_e \to G_{t(e)} \]

we call the maps \( \sigma_e, \tau_e \) boundary monomorphisms and the images of these maps boundary subgroups.

A graph of groups has a fundamental group denoted \( \pi_1(\mathcal{G}(A)) \). We say that a group splits as the fundamental group as a graph of groups if \( G = \pi_1(\mathcal{G}(A)) \) and refer to the data \( D = (G, \mathcal{G}(A)) \) as a splitting.

Definition 1.12 (Moves on \( \mathcal{G}(A) \)). We have the following moves on \( \mathcal{G}(A) \) that do not change the fundamental group.

- Change the orientation of edges in \( \mathcal{G}(A) \), and relabel the boundary monomorphisms.
- Conjugate boundary monomorphisms, i.e. replace \( \sigma_e \) by \( \gamma_g \circ \sigma_e \) where \( \gamma_g \) denotes conjugation by \( g \) and \( g \in G_{t(e)} \).
- Slide, i.e. if there are edges \( e, f \) such that \( \sigma_e(G_e) = \sigma_f(G_f) \) then we change \( X \) by setting \( i(f) = t(e) \) and replacing \( \sigma_f \) by \( \tau_e \circ \sigma_e^{-1} \circ \sigma_f \).
- Folding, i.e. if \( \sigma_e(G_e) \leq A \leq G_{t(e)} \), then replace \( G_{t(e)} \) by \( G_{t(e)} \ast_{\sigma_e(G_e)} A \), replace \( G_e \) by a copy of \( A \) and change the boundary monomorphism accordingly.
- Collapse an edge \( e \), i.e. for some edge \( e \in EA \), take the subgraph \( \text{star}(e) = \{i(e), e, t(e)\} \) and consider the quotient of the graph \( A \), subject to the relation \( \sim \) that collapses \( \text{star}(e) \) to a point. The resulting graph \( A' = A/\sim \) is again a directed graph. Denote the equivalence class \( v' = [\text{star}(e)] \in A' \), then we have \( G_{v'} = G_{t(e)} \ast_{\sigma_e} G_{i(e)} \) or \( G_{i(e)} \ast_{\sigma_e} G_{t(e)} \) depending whether \( i(e) = t(e) \) or not. For each edge \( f \) of \( A \) incident to either \( i(e) \) or \( t(e) \), we have boundary monomorphisms \( G_f \to G_{v'} \) given by \( \sigma_f' = i \circ \sigma_f \) or \( \tau_f' = i \circ \tau_f \), where \( i \) is the one of the inclusion \( G_{t(e)} \subset G_{v'} \) or \( G_{i(e)} \subset G_{v'} \).
- Conjugation, i.e. for some \( g \in G \) replace all the vertex groups by \( G_v^g \) and postcompose boundary monomorphisms with \( \gamma_g \) (which denotes conjugation by \( g \)).

1.4 The cyclic JSJ decomposition

Definition 1.13. An elementary cyclic splitting \( D \) of \( G \) is a splitting of \( G \) as either a free product with amalgamation or an HNN extension over a cyclic subgroup. We define the Dehn twist along \( D \), \( \delta_D \), as follows.

- If \( G = A \ast_{\langle \gamma \rangle} B \) then
  \[ \delta_D(x) = \begin{cases}  
x & \text{if } x \in A \\
\gamma x\gamma^{-1} & \text{if } x \in B
\end{cases} \]
• If $G = \langle A, t | t^{-1} \gamma t = \beta \rangle$, $\gamma, \beta \in A$ then
  \[
  \delta_D(x) = \begin{cases} 
  x & \text{if } x \in A \\
  t\beta & \text{if } x = t
  \end{cases}
  \]

A Dehn twist generates a cyclic subgroup of $\text{Aut}(G)$. A splitting such that all the edge groups are nontrivial and cyclic is called a cyclic splitting.

We can generalize the notion of a Dehn twist to arbitrary cyclic splittings.

**Definition 1.14.** Let $D$ be a cyclic splitting of $G$ with underlying graph $A$ and let $e$ be an edge of $A$. Then a Dehn twist along $e$ is an automorphism that can be obtained by collapsing all the other edges in $A$ to get a splitting $D'$ of $G$ with only the edge $e$ and applying one the applicable automorphisms of Definition 1.13.

**Definition 1.15.**

1. A subgroup $H \leq G$ is elliptic in a splitting $D$ if $H$ is conjugable into a vertex group of $D$, otherwise we say it is hyperbolic.
2. Let $D$ and $D'$ be two elementary cyclic splittings of a group $G$ with boundary subgroups $C$ and $C'$, respectively. We say that $D'$ is elliptic in $D$ if $C'$ is elliptic in $D$. Otherwise $D'$ is hyperbolic in $D$.

A splitting $D$ of an $F$-group is said to be modulo $F$ if the subgroup $F$ is contained in a vertex group.

The following is proved in [17]:

**Theorem 1.16.**

1. Let $G$ be freely indecomposable (modulo $F$) and let $D', D$ be two elementary cyclic splittings of $G$ (modulo $F$). $D'$ is elliptic in $D$ if and only if $D$ is elliptic in $D'$.
2. Moreover if $D'$ is hyperbolic in $D$ then $G$ admits a splitting $E$ such that one of its vertex groups is the fundamental group $Q = \pi_1(S)$ of a punctured surface $S$ such that the boundary subgroups of $Q$ are puncture subgroups. Moreover the cyclic subgroups $\langle d \rangle, \langle d' \rangle$ corresponding to $D, D'$ respectively are both conjugate into $Q$.

**Definition 1.17.** A subgroup $Q \leq G$ is a quadratically hanging (QH) subgroup if for some cyclic splitting $D$ of $G$, $Q$ is a vertex group that arises as in item (ii) of Theorem 1.16.

Not every surface with punctures can yield a QH subgroup. By Theorem 3 of [8], the projective plane with puncture(s) and the Klein bottle with puncture(s) cannot give QH subgroups. It has also been noted that surfaces that can give QH subgroups must admit pseudo-Anosov homeomorphisms.

**Definition 1.18.**

1. A QH subgroup $Q$ of $G$ is a maximal QH (MQH) subgroup if for any other QH subgroup $Q'$ of $G$, if $Q \leq Q'$ then $Q = Q'$.
2. Let $D$ be a splitting of $G$ with $Q$ be a QH vertex subgroup and let $C$ be a splitting of $Q$ with boundary subgroup $\langle c \rangle$ then there is a splitting $D'$ of $G$ called a refinement of $D$ along $C$ such that $D$ is obtained from a collapse of $D'$ along an edge whose corresponding group is $\langle c \rangle$.

**Definition 1.19.** A splitting $D$ is almost reduced if vertices of valency one and two properly contain the images of edge groups, except vertices between two MQH subgroups that may coincide with one of the edge groups.
(ii) A splitting $D$ of $G$ is unfolded if $D$ can not be obtained from another splitting $D'$ via a folding move (See Definition 1.12).

**Theorem 1.20** (Proposition 2.15 of [10]). Let $H$ be a freely indecomposable modulo $F$ f.g. fully residually $F$ group. Then there exists an almost reduced unfolded cyclic splitting $D$ called the cyclic JSJ splitting of $H$ modulo $F$ with the following properties:

1. Every MQH subgroup of $H$ can be conjugated into a vertex group in $D$; every QH subgroup of $H$ can be conjugated into one of the MQH subgroups of $H$; non-MQH [vertex] subgroups in $D$ are of two types: maximal abelian and non-abelian [rigid], every non-MQH vertex group in $D$ is elliptic in every cyclic splitting of $H$ modulo $F$.

2. If an elementary cyclic splitting $H = A * C B$ or $H = A * C$ is hyperbolic in another elementary cyclic splitting, then $C$ can be conjugated into some MQH subgroup.

3. Every elementary cyclic splitting $H = A * C B$ or $H = A * C$ modulo $F$ which is elliptic with respect to any other elementary cyclic splitting modulo $F$ of $H$ can be obtained from $D$ by a sequence of moves given in Definition 1.12.

4. If $D_1$ is another cyclic splitting of $H$ modulo $F$ that has properties (1)-(2) then $D_1$ can be obtained from $D$ by a sequence of slidings, conjugations, and modifying boundary monomorphisms by conjugation (see Definition 1.12.).

**Definition 1.21.** (For simplicity we consider only the case where $F_{R(S)}$ is freely indecomposable modulo $F$.) Given $D$, a cyclic JSJ decomposition of $F_{R(S)}$ modulo $F$, we define the group $\Delta$ of canonical $F$-automorphisms of $F_{R(S)}$ to be generated by the following:

- Dehn twists along edges of $D$; or by Dehn twists along edges $e'$ obtained from refinements of $D$ along cyclic splittings of MQH subgroups; that fix $F \leq F_{R(S)}$.
- Automorphisms of the abelian vertex groups that fix edge groups.

The following Theorem is proved in [9, 18].

**Theorem 1.22.** If $F_{R(S)} \neq F$ and is freely indecomposable (modulo $F$) then it admits a non trivial cyclic JSJ decomposition modulo $F$.

### 1.5 The Structure of Hom$_F(F_{R(S)}, F)$

**Definition 1.23.** A Hom diagram for Hom$_F(G, F)$, denoted $\text{Diag}_F(G, F)$, consists of a finite directed rooted tree $T$ such that the root, $v_0$, has no incoming edges and otherwise every vertex has at most one incoming edge along with the following data:

- To each vertex, except the root, $v$ of $T$ we associate a fully residually $F$ group $F_{R(S,v)}$.
- The group associated to each leaf of $T$ is a free product $F * H_1 * \ldots * H_n$, where the $H_i$ are isomorphic to subgroups of $F$. (The $H_i$ can be thought as free variables)
Figure 1: Hom diagrams corresponding to cases 1, 2, and 3 of Corollary 2.12. \( \pi_1, \pi_2, \pi_3 \) are given in Proposition 2.14.

- To each edge \( e \) with initial vertex \( v_i \) and terminal vertex \( v_t \) we have a proper \( F \)-epimorphism \( \pi_e : F \times F(S_{v_1}) \to F \times F(S_{v_2}) \).

We point out that in the work of Sela, the Hom diagram is called a Makanin-Razborov diagram (relative to \( F \)) and that our fully residually \( F \) groups are limit groups (relative to \( F \)). The following theorem gives a finite parametrization of the solutions of systems of equations over a free group.

**Theorem 1.24** ([9, 18]). For any system of equations \( S(x_1, \ldots, x_n) \) there exists a Hom diagram \( \text{Diag}_F(F \times F(S), F) \) such that for every \( f \in \text{Hom}_F(F \times F(S), F) \) there is a path

\[
v_0, e_1, v_1, e_2, \ldots, e_{m+1}, v_{m+1}
\]

from the root \( v_0 \) to a leaf \( v_{m+1} \) such that

\[
f = \rho \circ \pi_{v_{m+1}} \circ \sigma_{v_m} \circ \ldots \circ \sigma_{v_1} \circ \pi_{e_1}
\]

where the \( \sigma_{v_j} \) are canonical \( F \)-automorphisms of \( F \times F(S_{v_j}) \), the \( \pi_j \) are epimorphisms \( \pi_j : F \times F(S_{v_j}) \to F \times F(S_{v_{j+1}}) \) inside \( \text{Diag}_F(F \times F(S), F) \), and \( \rho \) is any \( F \)-homomorphism \( \rho : F \times F(S_{v_{m+1}}) \to F \) from the free group \( F \times F(S_{v_{m+1}}) \) to \( F \).

### 2 The system of equations \( S = \{ w(x, y)u^{-1} \} \)

**Definition 2.1.** Let \( \phi \) be a solution of \( S \), then the rank of \( \phi \) is the rank of the subgroup \( \langle \phi(x), \phi(y) \rangle \leq F \).

If all solutions of \( S \) are of rank 1, then \( V(S) \) is easy to describe and is given in Section 2.1. If \( S \) has solutions of rank 2, then there will be infinitely many such solutions. For this case we will prove that \( \text{Diag}_F(F \times F(S), F) \) correspond to one of three cases (see Figure 1). We will moreover describe the possible splittings of \( F \times F(S) \) and the associated canonical automorphisms. This description along with Theorem 1.24 will enable us to describe \( V(S) \) as a set of pairs of words in \( F \) (see Theorem 2.28).
2.1 Easy Cases and Reductions

By Proposition 1.9 we need only concern ourselves with the case where \( w(x, y) \) is not primitive. We state some results that enable us to simplify matters:

**Lemma 2.2.** The equation \( w(x, y) = 1 \) doesn’t admit any rank 2 solutions.

Let \( \sigma_x(w) \) and \( \sigma_y(w) \) be the exponents sums of \( x \) and \( y \) respectively in the word \( w(x, y) \). Then it is easy to see that

\[
V(S) = \{ (r^{n_1}, r^{n_2}) \in F \times F | r \in F; \ n_1\sigma_x(w) + n_2\sigma_y(w) = 0 \} \quad (2)
\]

In this case we have that

\[
F \cong V(S) \quad \text{and the mapping} \quad F \langle x, y \rangle / \text{ncl}(S) \rightarrow F \cong V(S)
\]

is given by the mapping

\[
\begin{align*}
\{ f \mapsto f, f \in F \\
x \mapsto t^x \\
y \mapsto t^y
\end{align*}
\]

where \((r_x, r_y)\) is a generator of the subgroup \( \{(a, b) \in \mathbb{Z} \oplus \mathbb{Z} | a\sigma_x(w) + b\sigma_y(w) = 0 \} \).

**Lemma 2.3.** If \( w(x, y) = v(x, y)^n, \ n > 1 \) then either the variety \( V(\{ w(x, y)^{-1} \}) \) is empty or \( u = r^n \) for some \( r \in F \) and we have the equality \( V(\{ w(x, y)^{-1} \}) = V(\{ v(x, y)^{-1} \}) \).

We will always assume that \( w(x, y) \) is not a proper power. Although this may seem somewhat contrived, our reason for doing so is twofold: firstly, requiring that an element is primitive is not enough; in our theorems we want to exclude the case where \( w(x, y) \) is a proper power of a primitive element as, again, solutions are easy to describe. Secondly, if \( w(x, y) = v(x, y)^n \) with \( n \) maximal, then in the cyclic JSJ splitting of \( F \) modulo \( F \), the edge group will be generated by \( v(x, y) \) and not \( w(x, y) \). For the next result we need the following theorem:

**Theorem 2.4 (Main Theorem of [1]).** Let \( w = w(x_1, x_2, \ldots, x_n) \) be an element of a free group \( F \) freely generated by \( x_1, x_2, \ldots, x_n \) which is neither a proper power nor a primitive. If \( g_1, g_2, \ldots, g_n, g \) are elements of a free group connected by the relation

\[
w(g_1, g_2, \ldots, g_n) = g^m \quad (m > 1)
\]

then the rank of the group generated by \( g_1, g_2, \ldots, g_n \) is at most \( n - 1 \).

**Corollary 2.5.** Suppose that \( w(x, y) \) is neither primitive nor a proper power. If \( u = r^n, \ n > 1 \) is a proper power then the equation \( w(x, y) = u \) doesn’t have any rank 2 solutions.

**Proof.** Suppose not then there is a solution \( \phi : F \cong V(S) \rightarrow F \) such that \( \phi x = r \) and \( \phi y = r \) which means that \( \langle \phi x, \phi y \rangle \neq 1 \) which means that \( \langle \phi x, \phi y \rangle \) is free group of rank two. But we have the identity \( w(\phi x, \phi y) = r^n \) which by Theorem 2.4 implies that rank of \( \langle \phi x, \phi y \rangle \) is at most one – contradiction. \( \square \)
2.2 Possible cyclic JSJ splittings of $F_{R(S)}$ and canonical automorphisms

Lemma 2.6. Suppose that $w(x, y)$ is neither primitive nor a proper power. If $w(x, y) = u$ has a rank 2 solution then the group

$$F[x, y]/ncl(S) \approx F *_{u=w(x, y)} \langle x, y \rangle$$

is fully residually $F$ and, in particular, we have that

$$F_{R(S)} = F *_{u=w(x, y)} \langle x, y \rangle$$

Proof. Let $(\mathfrak{a}, \mathfrak{b})$ be a rank 2 solution. Let $F_1 = \langle F, t | t^{-1}ut = u \rangle$, $F_1$ is a rank one free extension of a centralizer of $F$, and therefore is fully residually $F$. By definition $F$–subgroups are also fully residually $F$. Let $H = (\mathfrak{a}, \mathfrak{b}) \leq F$ and let $H' = t^{-1}Ht$. By Britton’s Lemma we see that $H' \cap F = \langle u \rangle$ and that

$$(F, H) \approx F_{u=w(x, y)}H' \approx F *_{u=w(x, y)} \langle x, y \rangle$$

so this gives an $F$–embedding

$$F *_{u=w(x, y)} \langle x, y \rangle \hookrightarrow F_1$$

so $F *_{u=w(x, y)} \langle x, y \rangle$ is fully residually $F$. By Corollary 1.6 we obtain the equality

$$F_{R(S)} = F[x, y]/ncl(S)$$

--

Lemma 2.7. If $w(x, y)$ is not primitive nor a proper power then $F_{R(S)} = F *_{u=w(x, y)} \langle x, y \rangle$ is freely indecomposable modulo $F$.

Proof. Suppose not. Since $\langle x, y \rangle$ is a free group of rank 2, if it splits freely with nontrivial factors, then it must split as a free product of two cyclic groups. Since any splitting of $F_{R(S)}$ modulo $F$ must also be modulo $w(x, y)$ we have that $w(x, y)$ must lie in one of these free cyclic factors, contradicting the hypotheses of the lemma.

Given this first decomposition as an amalgam, we wish to see how it can be refined to a cyclic JSJ decomposition modulo $F$. By the Freiheitssatz, the subgroup $\langle x, y \rangle \leq F_{R(S)}$ is free of rank 2. So to investigate cyclic JSJ decomposition modulo $F$, we must first look at the possible cyclic splitting of $\langle x, y \rangle$. Our main tool will be the following theorem of Swarup:

Theorem 2.8 (Theorem 1 of [20]). (A) Let $G = G_1 * H G_2$ be an amalgamated free product decomposition of a free group $G$ with $H$ finitely generated. Then, there is a non-trivial free factor $H'$ of $H$ such that $H'$ is a free factor of either $G_1$ or $G_2$.

(B) Let $G = J *_{H, J} H$ be an HNN decomposition of a free group $G$ with $H$ finitely generated. Then there are decompositions $H = H_1 * H_2$, $J = J_1 * J_2$ with $H_1$ non trivial such that $H_1$ is a free factor of $J_1$ and $t^{-1}H_1t$ is conjugate in $J$ to a subgroup of $J_2$.

Corollary 2.9. If $G = G_1 *_{(?)} G_2$ is an amalgamated free product decomposition of a free group over a nontrivial cyclic subgroup, then $\text{rank}(G) = \text{rank}(G_1) + \text{rank}(G_2) - 1$. 

10
Lemma 2.10. Let $G$ be a free group of rank 2 and let $w \in G$ be non-primitive, and not a proper power. Then the only possible almost reduced (see Definition 1.19) nontrivial cyclic splittings of $G$ as the fundamental group of a graph of groups with $w$ elliptic are as

(i) a star of groups, specifically a graph of groups whose underlying graph is simply connected, consisting of a center vertex $v_c$ and a collection of peripheral vertices $v_1, \ldots, v_m$ connected to $v_c$ by an edge. The group associated to $v_c$, called the central group, is free of rank 2 and each edge group is nontrivial, cyclic and is a proper finite index subgroup of the associated “peripheral” vertex group; or

(ii) as an HNN extension

$$G = \langle H, t | t^{-1}pt = q \rangle; p, q \in H - \{1\}$$

where $w \in H$ and $H$ is another free group of rank 2. Moreover we have that $H = \langle p \rangle * \langle q \rangle$ i.e. $G = \langle p, t \rangle$.

Proof. Let $D$ be a splitting of $G$. If $G$ splits as a free product with amalgamation $G = G_1 * \langle \gamma \rangle * G_2$ then if $\gamma$ is not trivial, Corollary 2.9 forces one of the factors to be cyclic. Since we are assuming almost reducedness we must have that the edge group is a finite index subgroup of one of the cyclic factors. Suppose $G_2$ is a cyclic factor and let $z$ be a generator of $G_2$. Then the free group $G$ is obtained by adjoining the $n^{th}$ root $z$ of the element $\gamma \in G_1$, which is a free group of rank 2. It is however impossible to have a further splitting $G_1 * \langle \gamma \rangle * G_2 * \langle \gamma' \rangle * G_3$ with $G_2$ and $G_3$ cyclic and with $\langle \gamma \rangle, \langle \gamma' \rangle$ proper finite index subgroups of $G_2, G_3$ (resp.) since then, by an easy computation using normal forms, it would be possible to get a counter example to commutation transitivity, which must hold in a free group. The general star case follows.

If the underlying graph of $D$ is simply connected and one of the edge groups is trivial, then we can collapse $D$ to a free product $G_1 * G_2$ with nontrivial factors, and with $w$ lying in one of the vertex groups, by Grushko’s Theorem we must have rank($G_1$) = rank($G_2$) = 1 and our assumption that $w$ is elliptic in $D$ and not a proper power forces $w$ to be primitive – contradiction. We have therefore covered the case where the underlying graph is simply connected.

If the underlying graphs have two cycles (and a nontrivial vertex group), then we would have a proper epimorphism $G \twoheadrightarrow F(a, b)$ which contradicts the Hopf property.

Claim: If $G = \langle H, t | t^{-1}pt = q \rangle$, then $H$ is a free group of rank 2. By Theorem 2.8 (B) and conjugating boundary monomorphisms we can arrange so that

$$H = H_1 * H_2$$

with $p \in H_1$ and $q \in H_2$ (3)

Theorem 2.8 (B) moreover gives us that without loss of generality we can assume that $\langle q \rangle$ is a free factor of $H_2$. This means that

$$H_2 = H_2' * \langle q \rangle$$

(4)

Letting $H' = H_1 * H_2'$ we get that $H = H' * \langle q \rangle$ so combining (3) and (4) gives us a presentation $G = \langle H', t, q | t^{-1}pt = q \rangle$ which via a Tietze transformation gives us

$$G = \langle H', t | \emptyset \rangle$$

(5)
which forces $H'$ to be cyclic which means that $H$ has rank 2. Moreover, we see immediately that $H = \langle p \rangle * \langle q \rangle$.

We denote by $\Delta$ the group of canonical $F$–automorphisms of $F_{R(S)}$ (see Definition 1.21).

**Convention 2.11.** Whenever we have a “star” splitting of the subgroup $\langle x, y \rangle$, as given in item (i) in the statement of Lemma 2.10 we will collapse the whole splitting to a single vertex group. The first reason being that the Dehn twists around the edge groups fixing the central group act trivially. Secondly, by uniqueness of $n^{th}$ roots in a free group, we see that any mapping of the central group into a free group has at most a unique extension to the whole group. It follows that to describe solutions to the equation, the collapsed splitting is sufficient.

**Corollary 2.12.** There are three possible classes of cyclic JSJ decomposition modulo $F$ of $F_{R(S)}$:

1. $F_{R(S)} \cong F \ast_{w(x,y)} \langle x, y \rangle$ and $\Delta = \langle \gamma_w \rangle$, where $\gamma_w$ is the automorphism that extend the mapping:
   $$\gamma_w : \begin{cases} f \mapsto f; & f \in F \\ z \mapsto w^{-1}zw; & z \in \langle x, y \rangle \end{cases}$$

2. The subgroup $\langle x, y \rangle$ splits as a cyclic HNN-extension:
   $$\langle x, y \rangle = \langle H, t \rangle | t^{-1}pt = q \rangle$$
   with $w(x,y) \in H$ so that $F_{R(S)} \cong F \ast_{w(x,y)} \langle H, t \rangle | t^{-1}pt = q \rangle$ and $\Delta = \langle \gamma_w, \tau \rangle$ where these are the automorphisms that extend the mappings:
   $$\gamma_w : \begin{cases} f \mapsto f; & f \in F \\ z \mapsto w^{-1}zw; & z \in \langle x, y \rangle \\ t \mapsto tq; & t \in \langle F, H \rangle \end{cases}$$

3. $F_{R(S)} \cong F \ast_{w(x,y)} Q$ where $Q$ is a QH subgroup and, up to rational equivalence, $Q = \langle x, y, w | [x, y]w^{-1} \rangle$. $\Delta$ is generated by the automorphisms extending the mappings:
   $$\gamma_w : \begin{cases} x \mapsto yx; & \text{identity on } F \cup \{ y \} \\ t \mapsto tq; & t \in \langle F, H \rangle \end{cases}$$
   $\delta_x : \begin{cases} y \mapsto xy; & \text{identity on } F \cup \{ x \} \end{cases}$

**Proof.** Suppose first that the cyclic JSJ decomposition of $F_{R(S)}$ modulo $F$ has a QH subgroup $Q$. Then $Q$ must be a subgroup of $\langle x, y \rangle$, in particular there must be a splitting of $\langle x, y \rangle$ modulo $w$ such that $Q$ is one of its vertex groups. By Lemma 2.10 we must either have that $Q = \langle x, y \rangle$, or $\langle x, y \rangle$ is an HNN extension of $Q$. Either way we must have that $Q$ is a free group of rank 2. The possible punctured surfaces $S$ such that $\sigma_1(S)$ is a free group of rank 2 are the once punctured torus or the once punctured Klein bottle, the latter is not allowed (see Theorem 3 of [8].) Moreover, we see that if $\langle x, y \rangle$ is an HNN extension of $Q$ then the associated subgroups must be conjugate in $Q$, which would imply that $\langle x, y \rangle$ contains an abelian free group of rank 2 – contradiction. It follows from Corollary 1.10 that, up to rational equivalence, the only possibility is as in case 3. of the statement.

The rest of the statement follows immediately from Lemma 2.10 and Definition 1.21.

12
2.3 Solutions of rank 1

We now consider solutions of rank 1. Although everything can easily be described in terms of linear algebra, it is instructive to explain this in terms of Hom diagrams and canonical automorphisms, because as we shall see these provide examples of canonical epimorphisms that are not strict (see [13] for a definition.)

As we saw earlier, rank 1 solutions occur when we are solving \( w(x, y) = 1 \). More generally a rank 1 solution occurs if and only if \( w(x, y) = u = v^d \) where \( d = \gcd(\sigma_x(w), \sigma_y(w)) \); \( \sigma_x(w), \sigma_y(w) \) denote the exponent sums of \( x, y \) in \( w(x, y) \). Corollary 2.5 states that if \( d > 1 \), but \( w(x, y) \) not primitive and not a proper power, then all solution of \( w(x, y) = u \) have rank 1. If \( d = 1 \) then \( w(x, y) = u \) may have both rank 1 and rank 2 solutions.

Let \( S_1 = \{ w(x, y)u^{-1}, [x, y] \} \), then all rank 1 solutions must factor through \( F_{R(S_1)} \). If \( d > 1 \) then, since all solutions are rank 1, we must have in fact have \( \text{Rad}(\{ w(x, y)u^{-1} \}) = \langle w(x, y)u^{-1}, [x, y] \rangle \). As a set, these solutions are easy to describe:

\[
V(S_1) = \{(u^{n_1}, w^{n_2}) \in F \times F| n_1 \sigma_z(w) + n_2 \sigma_y(w) = d\}
\] (6)

Let \( p, q \) be integers such that

\[
p \sigma_x(w) + q \sigma_y(w) = d
\] (7)

then doing some linear algebra we have that \( n_1, n_2 \) in (6) are given by

\[(n_1, n_2) = (p, q) + m(\sigma_y(w), -\sigma_z(w)); \ m \in \mathbb{Z}\] (8)

We now investigate the situation where \( w(x, y) = u \) has rank 1 and rank 2 solutions, i.e \( V(S) \supseteq V(S_1) \). We first want to understand \( F_{R(S_1)} \).

**Lemma 2.13.** Suppose that \( w(x, y) \) is not primitive nor a proper power and suppose moreover that \( w(x, y) = u \) admits rank 1 and rank 2 solutions. Then there \( F_{R(S_1)} \) is isomorphic to \( \langle F, s| [u, s] = 1 \rangle = F_1 \). The \( F \)-morphism \( \pi_1 : F_{R(S_1)} \to F_1 \) given by

\[
\pi_1(x) = u^p s^{\sigma_x(w)} = \mathfrak{f}, \ \pi_1(y) = u^q s^{\sigma_y(w)} = \mathfrak{g}
\] (9)

where \( p, q \) are as in equation (7), realizes this isomorphism.

**Proof.** Consider the \( F \)-epimorphism \( \pi_1 : F_{R(S_1)} \to \langle F, s| [u, s] = 1 \rangle = F_1 \) given by (9) On one hand we see that \( \pi_1 \) is surjective which gives an injection

\[
\text{Hom}_F(F_1, F) \hookrightarrow \text{Hom}_F(F_{R(S_1)}, F)
\] (10)

via pullbacks \( f \mapsto f \circ \pi_1 \). On the other hand \( F_1 \), a free rank 1 extension of a centralizer, is fully residually free. On the third hand the group \( \Delta_1 \) of canonical \( F \) automorphisms of \( F_1 \) is generated by the automorphism given by:

\[
\delta : \begin{cases}
  s \mapsto su \\
  f \mapsto f & f \in F
\end{cases}
\]
and if we consider the \( F \)-epimorphism \( \pi_2 : F_1 \to F \) given by \( \pi_2(s) = u \) then we immediately see that the set

\[
V = \{ (\pi_2(\sigma^m(\mathfrak{f})), \pi_2(\sigma^m(\mathfrak{g})) \in F \times F| \sigma \in \Delta_1 \}
\]
of images of \((x, y)\) via the mappings \(\pi_2 \circ \sigma \circ \pi_1, \sigma \in \Delta_1\) coincides with \(\mathcal{V}(S_1)\). And since \(\text{Hom}_F(F_1, F) = \{\pi_2 \circ \sigma | \sigma \in \Delta_1\}\) we get that the correspondence (10) is in fact a bijective correspondence. It follows that \(F_{R(S_1)} \approx F_{F_1}\). \(\square\)

**Proposition 2.14.** Let \(w(x, y)\) be non primitive and not a proper power. Suppose moreover that \(w(x, y) = u\) has rank 1 and rank 2 solutions. Then

(i) if \(F_{R(S)}\) is as in 1. in Corollary 2.12, then \(\mathcal{V}(S_1)\) is represented by the following branch in \(\text{Diag}_F(F_{R(S)}, F)\): 

\[
\begin{array}{ccc}
F_{R(S)} & \xrightarrow{\sigma} & F_1 \\
\sigma_1 \circ & \sigma_2 & \\
\end{array}
\]  

(11)

where \(\sigma \in \Delta_1\).

(ii) If \(F_{R(S)}\) is as in 2. in Corollary 2.12, then \(\mathcal{V}(S_1)\) is represented by the following branch in \(\text{Diag}_F(F_{R(S)}, F)\): 

\[
\begin{array}{ccc}
F_{R(S)} & \xrightarrow{\sigma} & F_1 \\
\pi_3 & \pi_2 & \\
\end{array}
\]  

(12)

where \(\sigma \in \Delta\) and \(\pi_3 = \pi_2 \circ \pi_1\)

Where \(\pi_1, \pi_2\) and \(\Delta_1\) were defined in the previous proof.

**Proof.** We first note that if \(F_{R(S)}\) corresponds to case 3. of Corollary 2.12 then the equality (7) is impossible. In both possible cases we have epimorphisms 

\[
\begin{array}{ccc}
F_{R(S)} & \xrightarrow{\pi_1} & F_1 \\
\pi_2 & \pi_2 & \\
\end{array}
\]  

(13)

We saw that all solutions rank 1 solutions factor through \(\pi_1\). If \(F_{R(S)}\) is as in 1. in Corollary 2.12 then \(\Delta\) is generated by \(\gamma_w\), now since \(\pi_1 \circ \gamma_w = \pi_1\) we have that solutions in \(\mathcal{V}(S_1)\) must factor through \(F_1\) and are parametrized by \(\Delta_1\).

If \(F_{R(S)}\) is as in 2. in Corollary 2.12 then \((x, y)\) splits as

\[\langle H, t | t^{-1}pt = q\rangle; p, q \in H\]

, moreover by Lemma 2.10 we have that \((x, y) = \langle p, t \rangle\). We consider this basis of \((x, y)\). Let \(\pi_1(t) = \xi, \pi_1(p) = \eta\), then the subgroup \(\mathbb{Z} \oplus \mathbb{Z} \approx A = \langle u, s \rangle \leq F_1\) is generated by \(\eta, \xi\). We note that in \(F_{R(S)}\), as written as a word in \(\{p, t\}^\pm, w(x, y) = w(p, t) = u\) has exponent sum zero in the letter \(t\). Since \(A\) is the abelianization of \((x, y)\), we have that in \(A, u = \eta^0 + n\eta\) and since \(u\) lies in a minimal generating set of \(A\) we must have \(n = \pm 1\). It therefore follows that for the Dehn twist \(\tau\), which sends \(t \mapsto tq\), we have \(\pi_1 \circ \tau = \delta \circ \pi_1\), where \(\delta\) is the generator of \(\Delta_1\). It follows that the canonical \(F\)-automorphisms of \(F_1\) in (13) can be “lifted” to \(F_{R(S)}\) and the branch (12) gives us a parametrization of \(\mathcal{V}(S_1)\). \(\square\)
2.4 Solutions of rank 2

Before being able to make our finiteness arguments we need some preliminary setup. We will study more closely mappings \( F(x, y) \rightarrow F \).

**Definition 2.15.**

(i) Let \((f_1, f_2)\) be a pair of words in a free group, then an elementary Nielsen move (e.N.m.) is a mapping of the form

\[
(f_1, f_2) \mapsto (f_1, (f_1^\epsilon_1 f_2^\epsilon_2)^\epsilon_3)
\]

with \(\epsilon_1, \epsilon_3 \in \{-1, 1\}\) and \(\epsilon_2 \in \{-1, 0, 1\}\).

(ii) For \(F(x, y)\), the free group on the basis \(\{x, y\}\), an elementary Nielsen transformation (e.N.t.) is an element of \(Aut(F(x, y))\) that is defined by the mappings:

\[
\begin{align*}
x &\mapsto (x^\epsilon_1 y^\epsilon_2)^\epsilon_3 \\
y &\mapsto y
\end{align*}
\]

with \(\epsilon_1, \epsilon_3 \in \{-1, 1\}\) and \(\epsilon_2 \in \{-1, 0, 1\}\).

**Lemma 2.16.** Suppose \(\phi, \) given by \((x_0, y_0) \in F \times F\), is a rank 2 solution of \(w(x, y) = u\), let

\[
(x_0, y_0) \xrightarrow{m_1} \ldots \xrightarrow{m_n} (x_n, y_n)
\]

be a sequence of e.N.m. then

(i) there is a corresponding sequence of e.N.t \(t_1, \ldots, t_n\) such that letting \(w_0(x, y) = w(x, y)\) and \(w_{j+1}(x, y) = t_{j+1}(w_j(x, y))\) we have the equalities

\[
u = w_0(x_0, y_0) = \ldots = w_n(x_n, y_n)
\]

(ii) Let \(\alpha = t_n \circ \ldots \circ t_1 \in Aut(F(x, y))\)

then the mapping \(\phi' = \phi \circ \alpha^{-1} : F(x, y) \rightarrow F\) is given by the pair

\((x_n, y_n)\)

**sketch of proof.** Noting that a rank 2 solution isomorphically identifies the subgroup \(\langle x, y \rangle \leq F_{R(S)}\) with a rank 2 subgroup of a free group, the proof is essentially the same as the proof that elementary Nielsen transformations generate the automorphisms of a f.g. free group (See Proposition I.4.1. of \([12]\)).

The reader can look at Section I.2 of \([12]\) for the necessary background for the next lemma.

**Lemma 2.17.** Fix a basis \(X\) of \(F\), then to any subgroup \(H \leq F\) of rank \(n\) we can canonically associate an ordered set of Nielsen reduced generators \((j_1, \ldots, j_n)\), moreover this ordered set can be obtained from any ordered \(n\) – tuple of generators \((h_1, \ldots, h_n)\) via a sequence of e.N.m.

We now give names to all of these:

**Definition 2.18.** Let \(\phi, \) given by \((x_0, y_0)\), be a solution of \(w(x, y) = u\). Let

\[
(x_0, y_0) \xrightarrow{m_1} \ldots \xrightarrow{m_n} (x_n, y_n)
\]

be the sequence of e.N.m. that brings the pair \((x_0, y_0)\) to the canonical pair \((x_n, y_n)\) of generators of \(\langle x_0, y_0 \rangle\) guaranteed by Lemma 2.17. Then we have:
• The pair \((x_n, y_n)\) is called the terminal pair of \(\phi\) (denoted \(tp(\phi)\)).

• The word \(w_n(x, y) \in \langle x, y \rangle\) in \(\mathbb{F}\) is called the terminal word of \(\phi\) (denoted \(tw(\phi)\)).

• The automorphism \(\alpha \in Aut(F(x, y))\), is the automorphism associated to \(\phi\) (denoted \(\alpha_{\phi}\)).

**Proposition 2.21.** Let \(S = \{w(x, y) = u\}\) and let \(U \subset V(S)\) be the open subvariety of rank 2 solutions, then there are only finitely many possible terminal pairs and terminal words that can be associated to solutions \(\phi \in U\).

**Proof.** Fix a basis \(X\) of \(F\), we first show finiteness of possible terminal pairs.

Let \(\phi\) be a solution, given by \((x_0, y_0)\) and let \(H = (x_0, y_0) \leq F\) and let \(\Gamma\) be the Stallings graph for \(H\) (See, for instance, \([19]\)) Then there is a path in \(\Gamma\) with label \(u\). We also have that Nielsen generators can be read directly off \(\Gamma\) (see \([7]\)) as labels of simple closed paths. If we define the radius of \(\Gamma\) to be the distance between the basepoint of \(\Gamma\) and the “farthest” vertex, then we see that the length of Nielsen the generators \((x_n, y_n)\) is bounded by two times the radius. Moreover since \(w(x, y)\) is neither primitive nor a proper power in \(F(x, y) \approx H\), \(u\) is primitive nor a proper power in \(H\). It follows that the reduced path in \(\Gamma\) labeled \(u\) must cover the whole graph which means \(|u|\) is at least twice the radius, hence

\[ |x_0|, |y_0| \leq |u|\]

so the number of possible terminal pairs is bounded.

Consider now the terminal word \(w_n(x, y)\). Since \((x_n, y_n) \in F \times F\) is a Nielsen reduced pair we have that

\[ |w_n(x, y)|_{\langle x, y \rangle} \leq |w_n(x_0, y_0)|_X = |u|_X\]

which bounds the number of terminal words. \(\square\)

We now connect all these ideas to solutions of equations. The next observation is obvious but critical.

**Lemma 2.20.** Let \(F_{R(S)}\) be the coordinate group of \(w(x, y) = u\), with \(w(x, y)\) not primitive, not a proper power and such that \(w(x, y)\) has a rank 2 solution. Then the group of \(F\)-automorphisms of \(F_{R(S)}\) are induced by the automorphisms of the free subgroup \(\langle x, y \rangle\) that fix \(w(x, y)\).

**Proposition 2.21.** Suppose that \(\phi\) and \(\phi'\) are solutions \(F_{R(S)} \rightarrow F\) of \(w(x, y) = u\). And suppose moreover that \(tp(\phi) = tp(\phi')\) and \(tw(\phi) = tw(\phi')\), then there is an automorphism \(\beta \in Aut_F(F_{R(S)})\) such that \(\phi' = \phi \circ \beta\).

**Proof.** Let \(\phi\) be given by \((x_0, y_0)\) and let \(\phi'\) be given by \((x'_0, y'_0)\). Then we have a sequence of e.N.m.

\[
(x_0, y_0) \xrightarrow{m_1} \cdots \xrightarrow{m_n} tp(\phi) = tp(\phi') \xrightarrow{m'_1} \cdots \xrightarrow{m'_k} (x'_0, y'_0)
\]

And we have automorphisms \(\alpha_{\phi}, \alpha_{\phi'}\) such that \(\alpha_{\phi}(w(x, y)) = \alpha_{\phi'}(w(x, y)) = tw(\phi)\). On one hand we have that \(\beta = \alpha^{-1}_{\phi} \circ \alpha_{\phi'} \in \text{stab}(w)\), so, by Lemma 2.20 \(\beta \in Aut(F(x, y))\) extends to an automorphism of \(F_{R(S)}\). We moreover
have by Lemma 2.16 we have that the mappings $F(x, y) \to F, \phi' \circ \alpha_{\phi}^{-1} = \phi \circ \alpha_{\phi}^{-1}$ which means that
\[ \phi' = \phi \circ \alpha_{\phi}^{-1} \circ \alpha_{\phi'} = \phi \circ \beta \]

So we have proved that all rank 2 solutions are obtained from a finite family $\phi_1, \ldots, \phi_N$ of solutions and precomposition with $F$-automorphism of $F_{R(S)}$. Nothing so far has been said about canonical automorphisms.

**Definition 2.22.** Let $\Delta \leq \text{Aut}(F_{R(S)})$ be the group of canonical $F-$automorphisms of $F_{R(S)}$ associated to a cyclic JSJ decomposition modulo $F$. Let $\phi, \phi' \in \text{Hom}_F(F_{R(S)}, F)$, we say $\phi \sim_{\Delta} \phi'$ if there is a $\sigma \in \Delta$ such that $\phi \circ \sigma = \phi'$. $\phi \in \text{Hom}_F(F_{R(S)}, F)$ is minimal if after fixing a basis $X$ of $F$ the quantity $l_f = |\phi(x)| + |\phi(y)|$ is minimal among all $F$-morphisms in $\phi$'s $\sim_{\Delta}$ equivalence class.

We wish to show that there are only finitely many $\Delta$-minimal rank 2 solutions to $w(x, y) = u$. In light of Proposition 2.21, this is equivalent to the statement $|\text{stab}(w) : \Delta| < \infty$.

### 2.4.1 Proving finite index

In [3], it is proved that for freely indecomposable fully residually free groups, the subgroup canonical automorphism is of finite index in the group of outer automorphisms. Unfortunately, the result as formulated does not cover the case involving only automorphisms modulo $F$. We therefore prove this fact directly. What we will essentially show is that the internal $F$-automorphisms are of finite index in the whole group of $F$-automorphisms. The main pillars of the argument are that the JSJ decomposition is canonical in the sense of (4) of Theorem 1.20 and the following Theorem:

**Theorem 2.23** (Corollary 15.2 of [10]). Let $G$ be a nonabelian fully residually free group, and let $A = \{A_1, \ldots, A_n\}$ be a finite set of maximal abelian subgroups of $G$. Denote by $\text{Out}(G; A)$ the set of those outer automorphisms of $G$ which map each $A_i \in A$ onto a conjugate of itself. If $\text{Out}(G; A)$ is infinite, then $G$ has a nontrivial abelian splitting, where each subgroup in $A$ is elliptic. There is an algorithm to decide whether $\text{Out}(G; A)$ is finite or infinite. If $\text{Out}(G; A)$ is infinite, the algorithm finds the splitting. If $\text{Out}(G; A)$ is finite, the algorithm finds all its elements.

This next lemma follows immediately from the fact that in free groups $n^{th}$ roots are unique and centralizers of elements are cyclic.

**Lemma 2.24.** Let $(x, y)$ be a free group and suppose
\[ (x, y) = \langle H, t | t^{-1} pt = q; p, q \in H - \{1\} \rangle \]

Suppose that for some $g \in (x, y)$ we have the equality
\[ g^{-1}pg = q \]

then $g = tq^j$ for some $j \in \mathbb{Z}$.

**Proposition 2.25.** $\Delta \leq \text{Aut}(F(x, y))$ is of finite index in $\text{stab}(w)$
Proof. If \( w \) is conjugate to either \([x, y]\) or \([y, x]\) then the result follows immediately since the \( \text{stab}(w) \) coincides with the automorphisms given in Corollary 2.24 (see, for instance, [13]). We first concentrate on the case where the JSJ of \( F_{R(S)} \) is as in case 2. of Corollary 2.22.

Suppose the induced splitting of \([x, y]\) is of the form

\[
\langle x, y \rangle = \langle H, t \rangle t^{-1} pt = q, p \in H - \{1\}
\]

Let \( \alpha \in \text{stab}(w) \leq \text{Aut}(\langle x, y \rangle) \), then we can extend \( \alpha \) to \( \tilde{\alpha} : F_{R(S)} \to F_{R(S)} \).

We wish to understand the action of \( \tilde{\alpha} \) on \( F_{R(S)} \). First note that \( \tilde{\alpha} \) restricted to \( F \) is the identity and \( \tilde{\alpha}(\langle x, y \rangle) = \langle x, y \rangle \). On the other hand, \( \tilde{\alpha} \) gives another cyclic JSJ decomposition \( D_1 \) modulo \( F \):

\[
F_{R(S)} = F *_{u = w(x, y)} \langle \tilde{\alpha}(H), \tilde{\alpha}(t)\tilde{\alpha}(t)^{-1}\tilde{\alpha}(p)\tilde{\alpha}(t) = \tilde{\alpha}(q) \rangle
\]

with \( w \in \tilde{\alpha}(H) \). By Theorem 1.20 (4), \( D_1 \) can be obtained from \( D \) by a sequence of slidings, conjugations and modifying boundary monomorphisms.

\( \tilde{\alpha}(H) \cap F = \langle w \rangle \), and \( H \) must be obtained from \( \tilde{\alpha}(H) \) as in (4) of Theorem 1.20 i.e. by slidings, conjugating boundary monomorphisms and conjugations. The only inner automorphism of \( F_{R(S)} \) that fixes \( w \) is conjugation by \( w^k, k \in \mathbb{Z} \); (use Bass-Serre theory and properties of free groups) and since \( \tilde{\alpha}(H) \) and \( H \) are attached to \( F \) at \( \langle w \rangle \), slidings will have no effect. It follows that \( \tilde{\alpha}(H) = H \). Applying Theorem 1.20 again forces \( p, q \) to be conjugate in \( H \) to \( \tilde{\alpha}(p), \tilde{\alpha}(q) \) [respectively or in the other order]. We now have strong information enough on the dynamics of \( \text{stab}(w) \) to apply Theorem 2.23.

Indeed since \( \tilde{\alpha}(H) = H \), we have a natural homomorphism \( \rho : \text{stab}(w) \to \text{stab}(w) \leq \text{Aut}(H) \) given by the restriction \( \alpha \mapsto \alpha|_H \). Moreover we see that any almost reduced cyclic splitting of \( H \) modulo \( \{\langle w \rangle, \langle p \rangle, \langle q \rangle \} \) must be trivial, otherwise contradicting Lemma 2.10. Let \( \pi : \text{Aut}(H) \to \text{Out}(H) \) be the canonical map (i.e. quotient out by \( \text{Inn}(G) \), the subgroup of inner automorphisms). It therefore follows from Theorem 2.23 that the image \( \pi \circ \rho(\text{stab}(w)) = \text{stab}(w) \) must be finite.

First note that \( \text{Inn}(H) \cap \text{stab}(w) = \langle \gamma_w \rangle \) which means that

\[
\text{stab}(w) \approx \text{stab}(w)/\langle \gamma_w \rangle
\]

and this isomorphism is natural. Let \( \alpha \in \ker \rho \) then we must have that \( \alpha|_H = 1 \). In particular we have

\[
\alpha(t)^{-1}pt\alpha(t) = q
\]

which by Lemma 2.24 implies that \( \alpha(t) = tq^i \) it follows that \( \ker(\rho) \leq \langle \tau \rangle \). The other inclusion is obvious so

\[
\ker(\rho) = \langle \tau \rangle
\]

There is a bijective correspondence between subgroups \( K \) of \( \text{stab}(w) \) and subgroups of \( \text{stab}(w) \) that contain \( \langle \tau \rangle \) given by \( K \mapsto \rho^{-1}(K) \). Moreover this correspondence sends normal subgroups to normal subgroups. It follows that \( \ker(\pi \circ \rho) = \langle \tau, \gamma_w \rangle \) and so we get:

\[
\text{stab}(w)/\langle \tau, \gamma_w \rangle \approx \text{stab}(w)
\]
which is finite. It follows that \(|\text{stab}(w) : \langle \tau, \gamma_w \rangle| < \infty\).

In the case where \(D\), the cyclic JSJ of \(F_{R(S)}\) modulo \(F\) is as in case 1. of Corollary 2.12 then again elements of \(\alpha \in \text{stab}(w)\) will give new splittings \(F_{R(S)} = F *_{u=w(x,y)} \widehat{\alpha}(H)\). Arguing as before, we get that \(\widehat{\alpha}(H) = H\) and we can apply Theorem 2.23 with \(A = \{\langle w \rangle\}\). We get that \(\text{Out}(H; A) \approx \text{stab}(w)/\langle \gamma_w \rangle\) must be finite, otherwise \(H\) could split further, contradicting the fact that \(D\) was a JSJ splitting, and the result follows.  

By Lemma 2.20 Propositions 2.10 2.21 and 2.25 we get the second half of our main result:

Proposition 2.26. Suppose that \(w(x,y)\) is not a proper power, nor is it primitive. Then there are finitely many \(\Delta\)-minimal rank 2 solutions to the equation \(w(x,y) = u\).

2.5 The description of \(V(\{w(x,y)u^{-1}\})\)

These next two results now follows immediately from Proposition 2.26, 2.14 Corollary 2.12, Lemma 2.10 and Theorem 1.24.

Theorem 2.27. Suppose that \(w(x,y) = u\) has rank 2 solutions and that \(w(x,y)\) is not a power of a primitive element. Then the possible Hom diagrams are given in Figure 4.

Theorem 2.28. Suppose that \(w(x,y) = u\) has rank 2 solutions and that \(w(x,y)\) is neither primitive nor a proper power. Let \(\{\phi_i | i \in I\}\) be the collection of \(\Delta\)-minimal solution. Then \(V(S) = V(S_1) \cup V'\), where \(V' = V(S) - V(S_1)\), is given by the following:

1. \(F_{R(S)} \approx F *_{u=w(x,y)} \langle x, y \rangle\), let \(\phi_i(x) = x_i, \phi_i(y) = y_i\), then \(V(S) = V(S_1) \cup V'\) where 
   
   \[V' = \{(u^{-n}x_iu^n, u^{-n}y_iu^n)| i \in I \text{ and } n \in \mathbb{Z}\}\]

   and if the exponent sums \(\sigma_x(w), \sigma_y(w)\) of \(x, y\) respectively in \(w\) are relatively prime, then \(V(S_1)\) is non empty and is given by (D).

2. \(F_{R(S)} \approx F *_{u=w(x,y)} \langle H, t^{-1}pt \rangle = \langle p, q \rangle\) and we can write \(x, y \in \langle x, y \rangle\) as words \(x = X(p, q, t), y = Y(p, q, t)\). Let \(\phi_i(p) = p_i, \phi_i(q) = q_i, \phi_i(t) = t, \) then we have that \(V(S) = V(S_1) \cup V'\) where
   
   \[V' = \{(X(u^{-n}p_iu^n, u^{-n}q_iu^n, u^{-n}t_iq_i^m u^n), Y(u^{-n}p_iu^n, u^{-n}q_iu^n, u^{-n}t_iq_i^m u^n)) | i \in I, n, m \in \mathbb{Z}\}\]

   and if the exponent sums \(\sigma_x(w), \sigma_y(w)\) of \(x, y\) respectively in \(w\) are relatively prime, then \(V(S_1)\) is non empty and is given by (D).

3. \(F_{R(S)} \approx F *_{u=w(x,y)} Q\) where \(Q\) is a QH subgroup and, up to rational equivalence, \(Q = \langle x, y, w|x, y|w^{-1}\rangle\). Then \(V(S_1)\) is empty. Let \(\phi_i(x) = x_i, \phi_i(y) = y_i\) then
   
   \[V(S) = \{(X_\sigma(x_i, y_i), Y_\sigma(x_i, y_i)| \sigma \in \Delta}\]

   where the words \(\sigma(x) = X_\sigma(x, y), \sigma(y) = Y_\sigma(x, y) \in \langle x, y \rangle\).

   We finally note that unless \(w(x,y) = u\) is orientable quadratic, then solutions are given by “one level parametric” words (see [11] for a definition.)
3 An Interesting Example

The Hom diagrams given for \( w(x, y) = u \) were very simple. In particular, modulo the slight technicalities of Theorem 2.28 item 1, we can say that; unless \( w(x, y) \) is a power of a primitive element; there are only finitely many minimal solutions to \( w(x, y) = u \) with respect to a group of canonical automorphisms. This translates as the Hom diagram having only one “level”. This also means that all fundamental sequences or strict resolutions of \( F_{R(S)} \) have length 1 (see [9] or [18], respectively for definitions.) It is natural to ask this holds true for general equations in two variables. We answer this negatively:

**Theorem 3.1.** Let \( F = F(a, b) \) then the Hom diagram associated to the equation with variables \( x, y \)

\[
[a^{-1}ba[b, a][x, y]^2x, a] = 1 \tag{17}
\]

has branches corresponding to rank 2 solutions that have length at least 2.

**Proof.** First note that via Tietze transformations, we have the following isomorphism:

\[
\langle F, x, y \rangle[a^{-1}ba[b, a][x, y]^2x, a] = 1 \\
\approx \langle F, x, y, t \rangle[x, y]^2x = [a, b][a^{-1}b^{-1}at; \{t, a\} = 1]
\]

Let \( w(x, y) = [x, y]^2x \) and let \( u = [a, b]a^{-1}b^{-1}at. \) We now embed \( G = \langle F, x, y, t | w(x, y) = u, \{t, a\} = 1 \rangle \) into a chain of extensions of centralizers. Let \( F_1 = \langle F, t | \{t, a\} = 1 \rangle \) and let \( F_2 = \langle F_1, s | u, s \rangle = 1 \). Let \( \overline{F} = b^{-1}t \) and \( \overline{G} = b^{-1}ab. \) First note that

\[
[x, y]^2 \overline{F} = ((t^{-1}b[(b^{-1}a^{-1}b)(b^{-1}t)(b^{-1}ab)^2][b^{-1}t]) = [a, b][a^{-1}b^{-1}at = u
\]

We now form a double, i.e. we set \( x = \overline{x}, y = \overline{y} \) and let \( H = \langle x, y \rangle = \langle \overline{x}, \overline{y} \rangle. \)

By Britton’s Lemma we have that \( H \cap \overline{F}_1 = \{u\} \) and it follows that \( \langle F, x, y \rangle \) is isomorphic to the amalgam \( F_1 *_{\{u\}} H = G. \) Since chains of extensions of centralizers of \( F \) are fully residually \( F. \) We have that our equation (17) is an irreducible system of equations, we write \( F_{R(S)} = G. \) We note that we have the nontrivial cyclic splitting

\[
D : F_{R(S)} \approx F_1 *_{\{u = w(x, y)\}} \langle x, y \rangle
\]

moreover since \( w(x, y) = [x, y]^2x \) cannot belong to a basis (see [5]) of \( \langle x, y \rangle \) we have that \( F_{R(S)} \) is freely indecomposable modulo \( F_1. \) On the other hand, if we take the Grushko decomposition of \( F_{R(S)} \) modulo \( F \)

\[
F_{R(S)} = \overline{F} * K_1 * \ldots K_n; \ F \leq \overline{F}
\]

we see that we must have \( F_1 \leq \overline{F} \) since \( \{t, a\} = 1 \Rightarrow t \in \overline{F}. \) It follows that \( F_{R(S)} \) is actually freely indecomposable modulo \( F. \) It follows that \( D \) can be refined to a cyclic JSJ decomposition modulo \( F. \)

Suppose towards a contradiction that all branches of the Hom diagram for \( \text{Hom}_x(F_{R(S)}, F) \) corresponding to rank 2 solutions had length 1. This means that there are finitely many minimal rank 2 solutions \( \phi : F_{R(S)} \to F. \)
On one hand the element $t$ must be sent to arbitrarily high powers of $a$, since $F_{R(S)}$ is fully residually $F$. On the other hand, for there to be a canonical automorphism of $F_{R(S)}$ that sends $t \mapsto ta^n$, there must be a splitting $D'$ of $F_{R(S)}$ with some conjugate of $\langle a \rangle$ as a boundary subgroup, but $u$ would have to be hyperbolic in such a splitting, and since $\langle a \rangle$ is elliptic in $D$, we would have an elliptic-hyperbolic splitting which by Theorem 1.1 would contradict free indecomposability modulo $F$.

We now provide some illustration. We determined that $F_{R(S)} = \langle x, y \rangle$ with $u = [a, b]ab^{-1}a^{-1}t$. Now the mapping $x \mapsto x^n$ and $y \mapsto y^n$ extends to a canonical automorphism of $F_{R(S)}$ and along some branch there must be another canonical automorphism that maps $t \mapsto ta^n$. By checking directly we see that $\phi : F_{R(S)} \mapsto F$ given by $x = b^{-1}a, y = b^{-1}ab$ is a solution, so we can get the family of solutions:

$$x = ([a, b]ab^{-1}a^{-1}a^n)^m(b^{-1}a)([a, b]ab^{-1}a^{-1}a^n)^{-m}$$

$$y = ([a, b]ab^{-1}a^{-1}a^n)^m(b^{-1}ab)([a, b]ab^{-1}a^{-1}a^n)^{-m}$$

with $n, m$ in $\mathbb{Z}$. Notice that no precomposition by a canonical automorphism of $F_{R(S)}$ can affect the $n$ parameter. It follows that the set of solution of (17) can not be given by precomposing a finite collection of maps $\phi_1, \ldots, \phi_n : F_{R(S)} \mapsto F$ with canonical automorphisms.

References

[1] Gilbert Baumslag. Residual nilpotence and relations in free groups. J. Algebra 2 (1965), 271–282

[2] Gilbert Baumslag, Alexei Myasnikov, and Vladimir Remeslennikov. Algebraic geometry over groups. I. Algebraic sets and ideal theory. J. Algebra 219 (1999), no. 1, 16–79

[3] Inna Bumagin, Olga Kharlampovich, and Alexei Miasnikov. The isomorphism problem for finitely generated fully residually free groups. J. Pure Appl. Algebra 208 (2007), no. 3, 961–977

[4] Laura Ciobanu. Polynomial-time complexity for instances of the endomorphism problem in free groups. Internat. J. Algebra Comput. 17 (2007), no. 2, 289–328

[5] M. Cohen, Wolfgang Metzler, and A. Zimmermann. What does a basis of $F(a, b)$ look like? Math. Ann. 257 (1981), no. 4, 435–445

[6] Ju. I. Hmelevskii. Systems of equations in a free group. I, II. Izv. Akad. Nauk SSSR Ser. Mat. 35 (1971), 1237–1268; ibid. 36 (1972), 110–179

[7] Ilya Kapovich and Alexei Myasnikov. Stallings foldings and subgroups of free groups. J. Algebra 248 (2002), no. 2, 608–668

[8] O. Kharlampovich and A. Myasnikov. Irreducible affine varieties over a free group. I. Irreducibility of quadratic equations and Nullstellensatz. J. Algebra 200 (1998), no. 2, 472–516, 1998.

[9] O. Kharlampovich and A. Myasnikov. Irreducible affine varieties over a free group. II. Systems in triangular quasi-quadratic form and description of residually free groups. J. Algebra, 200 (1998), no. 2, 517–570
[10] Olga Kharlampovich and Alexei G. Myasnikov. Effective JSJ decom positions. In *Groups, languages, algorithms*, volume 378 of *Contemp. Math.*, pages 87–212. (Amer. Math. Soc., Providence, RI, 2005).

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

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

[13] G. S. Makanin. Equations in a free group. *Izv. Akad. Nauk SSSR Ser. Mat.* 46 (1982), no. 6, 1199–1273, 1344.

[14] A. I. Mal’cev. On the equation $zxy^{-1}y^{-1}z^{-1} = aba^{-1}b^{-1}$ in a free group. *Algebra i Logika Sem.* 1 (1962), no. 5, 45–50.

[15] A Razborov. On systems of equations in a free group. PhD thesis. Steklov Math. Institute, Moscow, (1987).

[16] V. N. Remeslennikov. 3-free groups. *Sibirsk. Mat. Zh.* 30 (1989), no. 6, 193–197.

[17] E. Rips and Z. Sela. Cyclic splittings of finitely presented groups and the canonical JSJ decomposition. *Ann. of Math. (2)* 146 (1997), no. 1, 53–109.

[18] Zlil Sela. Diophantine geometry over groups. I. Makanin-Razborov diagrams. *Publ. Math. Inst. Hautes Études Sci.* (2001), no. 93, 31–105.

[19] John R. Stallings. Topology of finite graphs. *Invent. Math.* 71 (1983), no. 3, 551–565.

[20] G. A. Swarup. Decompositions of free groups. *J. Pure Appl. Algebra* 40 (1986), no1, 199–102.

[21] M. J. Wicks. A general solution of binary homogeneous equations over free groups. *Pacific J. Math.* 41 (1972), 543–561.

22