

**Algorithmic and combinatorial methods
for enumerating the relators of a group
presentation**

Carmelo Vaccaro

Abstract

The main achievement of this thesis is an algorithm which given a finite group presentation and natural numbers n and k , computes all the relators of length and area up to n and k respectively. The complexity of this algorithm is less by a factor of at least $a^{k^2} a^{kn}$ than those of the classical methods using van Kampen diagrams (a is a constant).

Contents

Introduction	3
Overview of the results	4
Structure of the thesis	9
1 Finite and infinite presentations of groups	10
1.1 Words and presentations	10
1.2 Decision problems for groups	15
1.3 Tietze transformations	20
1.4 Infinite presentations of groups	26
1.5 The Conjugacy Problem	30
1.6 Enumeration of relators	32
2 The sets C and L and the function A	36
2.1 Straight line algorithms	36
2.2 The set C and the function η	39
2.3 Properties of the corollas	43
2.4 The set L and the function A	52
2.5 Statement of the results	54
3 Preliminary results	59
3.1 2-cell complexes for straight line algorithms	59
3.2 Preliminary results I	65
3.3 Preliminary results II	70
4 The Main Theorem	78
4.1 The proof of the Main Theorem: a case by case analysis	78
4.1.1 Case I	82
4.1.2 Case II	84
4.1.3 Case III	86
4.1.4 Case IV	87

4.2	The proof of the Main Theorem: conclusion	91
5	Applications and complexity	94
5.1	Applications to the Word Problem	94
5.2	Straight line algorithms for reduced words	100
5.3	Comparison of the complexities	104
A		106
A.1	Computation of the complexity	106
A.2	Recursively defined sets and straight line algorithms	113
A.3	A long calculation	114
	Bibliography	130

Introduction

The starting point of this thesis is the following: we have a finite group presentation and we have not additional information about the group presented. This is a very natural point of view since one can give a finite presentation by simply listing a finite set of words on a given alphabet; the words and the alphabet represent respectively the defining relators and the generators of the presentation.

A question that naturally arises is: what can be said about the group defined by this presentation? It is easy to convince oneself that the latter is a very hard question to answer in general due to the arbitrariness of the defining relators. Therefore it does not come as a surprise the fact that all the important problems concerning finite presentations have resulted to be unsolvable.

The situation is much better if the presentation verifies some strong hypothesis, like for instance a *small cancellation* condition. When this is not the case one hope comes from the *Knuth-Bendix algorithm* (see [26] or [19]). But as it is known this algorithm does not work for every presentation, in particular it can fail or run forever.

Many decision problems for groups are based on the decidability of certain sets of relators. For instance the Word Problem is solvable if for every natural number n one can decide the set of relators of length n ; or the Conjugacy Problem is solvable if for every natural numbers n_1 and n_2 one can decide the set of relators of the form $u_1 a u_2 a^{-1}$ where u_1 and u_2 are words of length n_1 and n_2 respectively.

It must be observed that for a finite presentation the set of relators is always recursively enumerable.

If the presentation does not verify some special condition or if the Knuth-Bendix algorithm does not work, the only methods currently known in the literature to enumerate the relators are two methods based on *van Kampen diagrams*. Let us fix natural numbers k and n ; the first method consists in enumerating all the van Kampen diagrams of area and length up to k and n

respectively; the second uses the fact that a relator of area and length up to k and n is a product of conjugates of defining relators with the length of the conjugating elements bounded above by $mk + n$, where m is the maximal length of a defining relator.

Unfortunately both algorithms are quite bad and require a huge amount of calculations.

The main achievement of this thesis is an algorithm enumerating the relators of area and length up to k and n and whose complexity is less by a factor of at least $a^{k^2} a^{kn}$ than those of the classical methods using van Kampen diagrams (a is a constant).

This is obtained in the following way. First we define by a double recursion a certain set D of relators, whose elements can be enumerated by an algorithm whose complexity is the one shown above. Then we prove that every relator belongs in fact to this set, thus that algorithm enumerates in fact all the relators.

This result can be applied to every situation in which there is an enumeration of relators by means of the associated van Kampen diagrams, since the complexity of this method is better than the usual methods. In fact we show also how to associate with any element of D a van Kampen diagram with certain additional properties, thus proving that it is not necessary to consider all the van Kampen diagrams but only those verifying a special property (see Section 5.3).

Another possible direction of research can be that of implementing the algorithm presented in this thesis in the form of a computer program for treating group presentations for which the Knuth-Bendix algorithm does not work.

It would be also interesting to generalize these results to monoid and semigroup presentations and finding an algorithm for these kinds of presentations.

Overview of the results

Let $\langle X | R \rangle$ be a group presentation where the set of defining relators R is a set of cyclically reduced non-empty words such that $R^{-1} \subset R$.

Let us denote C_1 the set of the cyclic conjugates (Definition 1.1.4) of the defining relators. For $k > 1$ let us denote C_k the set of the cyclic conjugates of the cyclically reduced products (Definition 1.1.7) of words u and v such that the following three conditions are satisfied:

1. $u \in C_{k-1}$ and $v \in C_1$ or $u \in C_1$ and $v \in C_{k-1}$;

2. $u \neq v^{-1}$;
3. either u^{-1} is a prefix of v , or v^{-1} is a suffix of u or the last letter of u is the inverse of the first of v but the first letter of u is not the inverse of the last of v .

We call k -corollas the elements of C_k (Definitions 2.2.6 and 2.3.9, Remark 2.3.13). If R is finite then there is a finite algorithm which computes C_k (Remark 2.3.13). We denote C the union of all the C_k .

Let us consider for example the following presentation

$$\langle a, b \mid aba^{-1}b^{-1} \rangle$$

which is the standard presentation for \mathbb{Z}^2 , the free abelian group of rank 2. In fact, since we have assumed that the set of defining relators must contain the inverse of any of its elements, then we rewrite the above presentation in the following form

$$\langle a, b \mid aba^{-1}b^{-1}, bab^{-1}a^{-1} \rangle,$$

where the second defining relator is the inverse of the first. Let us compute the set of k -corollas for $k = 1, 2$. Let us denote \mathcal{A} the set of generators and inverses of them, that is

$$\mathcal{A} := \{a, b, a^{-1}, b^{-1}\}.$$

C_1 is the set of the cyclic conjugates of the defining relators, that is

$$C_1 := \{\mathbf{xyx}^{-1}\mathbf{y}^{-1} : \mathbf{x}, \mathbf{y} \in \mathcal{A}, \mathbf{x}^{\pm 1}, \mathbf{y}^{\pm 1} \text{ distinct}\}. \quad (1)$$

We express the relators as monomials in the unknowns \mathbf{x} and \mathbf{y} ; to obtain the actual relators one has just to replace the unknowns with the letters of \mathcal{A} . By the definition, the elements of C_2 are the cyclic conjugates of the cyclically reduced products of the pairs (u, v) of elements of C_1 satisfying conditions 1-3. Since no element of C_1 is a proper prefix or suffix of another element of C_1 , then the only product to consider is

$$(\mathbf{xyx}^{-1}\mathbf{y}^{-1})(\mathbf{yx}^{-1}\mathbf{y}^{-1}\mathbf{x}) = \mathbf{xyx}^{-2}\mathbf{y}^{-1}\mathbf{x};$$

the second member of the above product is obtained by replacing in the general monomial of (1) the letter \mathbf{x} with \mathbf{y} and \mathbf{y} with \mathbf{x}^{-1} , that is if $m(\mathbf{x}, \mathbf{y}) = \mathbf{xyx}^{-1}\mathbf{y}^{-1}$ then $\mathbf{yx}^{-1}\mathbf{y}^{-1}\mathbf{x} = m(\mathbf{y}, \mathbf{x}^{-1})$. Now we have to compute the cyclic conjugates of this monomial to obtain C_2 , that is

$$C_2 := \{\mathbf{xyx}^{-2}\mathbf{y}^{-1}\mathbf{x}, \mathbf{yx}^{-2}\mathbf{y}^{-1}\mathbf{x}^2, \mathbf{x}^{-2}\mathbf{y}^{-1}\mathbf{x}^2\mathbf{y}, \mathbf{x}^{-1}\mathbf{y}^{-1}\mathbf{x}^2\mathbf{yx}^{-1},$$

$$\mathbf{y}^{-1}\mathbf{x}^2\mathbf{y}\mathbf{x}^{-2}, \mathbf{x}^2\mathbf{y}\mathbf{x}^{-2}\mathbf{y}^{-1}, : \mathbf{x}, \mathbf{y} \in \mathcal{A}, \mathbf{x}^{\pm 1}, \mathbf{y}^{\pm 1} \text{ distinct}\}.$$

In fact the last three monomials are obtained from the first three by replacing each letter with its inverse, thus we can write C_2 in the following more compact form

$$C_2 := \{\mathbf{x}^{-1}\mathbf{y}^{-1}\mathbf{x}^2\mathbf{y}\mathbf{x}^{-1}, \mathbf{y}^{-1}\mathbf{x}^2\mathbf{y}\mathbf{x}^{-2}, \mathbf{x}^2\mathbf{y}\mathbf{x}^{-2}\mathbf{y}^{-1}, \mathbf{x}, \mathbf{y} \in \mathcal{A}, \mathbf{x}^{\pm 1}, \mathbf{y}^{\pm 1} \text{ distinct}\}.$$

As seen in Remark 2.3.3, with any k -corolla c can be associated in a standard way a product of conjugates of defining relators whose reduced form is c . Since as we have seen, any element of C_2 can be obtained in two ways, then we have that all the 2-corollas of this presentation can be expressed in two different ways as product of conjugates of defining relators.

Let us return to the general case. Given words $w := w_1w_2$ and u , we say that the word w_1uw_2 is *the insertion of u into w at w_1* (Definition 2.2.1).

We denote D_1 the set of words which are reduced and which are of the form uwu^{-1} where $w \in C_1$. Suppose by induction to have defined D_h for every $h < k$ and define D_k as the set of reduced words which are either of the form uwu^{-1} where $w \in C_k$ or are insertions of a word of D_m into one of D_n for $m + n = k$. We denote D the union of all the D_k .

In a way analogous to that of Remarks 2.3.3 and 2.3.4 for C_k , we can associate with any element w of D_k a product of k conjugates of defining relators whose reduced form is w and a van Kampen diagram labeled by w with k faces. In particular that any element of D is a relator.

The main result of the thesis is the following (Theorem 4.1.1 and Section 5.2): **Let w be a relator of $\langle X | R \rangle$; then w belongs to D . Moreover $\text{Area}(w) = \min\{k : w \in D_k\}$.**

To compute the relators of area and length up to k and n one can use the algorithm consisting in enumerating the elements of $D_1 \cup D_2 \cup \dots \cup D_k$ of length up to n . This algorithm is presented in Section A.1. There are currently two other methods in the literature for this kind of computation and our algorithm is much better than both of them.

These two methods, which are illustrated in Section 1.6, are the following. The first consists in enumerating all the van Kampen diagrams of area up to k and boundary of up to n edges. The second classical method uses the following fact (Remark 1.2.1), which is a consequence of the properties of van Kampen diagrams: a relator of area and length up to k and n is a product of conjugates of defining relators with the length of the conjugating elements bounded above by $mk + n$, where m is the maximal length of a defining relator. This implies that one can find all the relators of area and length up to k and n by computing a finite number of products of conjugates

of defining relators. The complexity of this method is $q^k a^{kn} s^{k^2}$, where q, a and s are constants depending on the presentation (see Section 1.6 for details). We have the following result (Theorem 5.3.1): **The complexity of the algorithm presented in this thesis is bounded above by $n^3 \beta^n \gamma^k$, where β and γ are constants, and is less than those of the classical methods described above by a factor of at least $a^{k(k-c_1)} a^{n(k-c_2)}$, with c_1 and c_2 constants.**

Let us make some observations about these complexities. The value $n^3 \beta^n \gamma^k$ given above is far from being an optimal bound for the complexity of our method; it is only a value obtained with not too complicated calculations. With non-trivial arguments this result could be probably much improved. Instead the value $q^k a^{kn} s^{k^2}$ is the real complexity of the classical method, that is it is the exact number of words to be considered with this method to find all the relators of length and area up to n up to k . The same is true also for the factor 2^k given as the improvement with respect to the first method and which could be probably much bigger.

Let us present other results; we say that a k -corolla c is a *proper k -corolla* if for $h < k$, c does not belong to D_h . In particular if c is a proper k -corolla then $\text{Area}(c) = k$. For every natural number n we set

$$\Delta_0(n) := \max\{\text{Area}(c) : c \text{ is a proper corolla and } |c| \leq n\}.$$

Obviously $\Delta_0(n) \leq \Delta(n)$ where $\Delta(n)$ is the Dehn function (Definition 1.2.2). We have (Theorem 5.1.1): **Let $\langle X | R \rangle$ be a finite presentation; then the Word Problem is solvable if and only if Δ_0 is bounded above by a computable function.**

This result improves a well known result (see Proposition 1.2.4) because Δ_0 is bounded above by the Dehn function. An analogous result can be stated for non-necessarily finite presentations. In fact R. I. Grigorchuk and S. V. Ivanov in a recent paper [16] have introduced a function f_1 which plays for finitely generated decidable presentations the same rôle of the Dehn function. They proved that for such presentations, the Word Problem is solvable if and only if f_1 is bounded above by a computable function (see Proposition 1.4.3 of this thesis).

As pointed out by Grigorchuk and Ivanov at the end of Sec. 2 of their paper [16], the function f_1 is equivalent (in the usual sense, see Definition 1.3.5) to the function *Work* introduced by J.-C. Birget in ([7], 1.4). We have proved in Section 1.5 this equivalence; moreover we have introduced in Definition 2.4.6 a function Ω_0 such that if Ω is the function *Work* then $\Omega_0 \leq \Omega$ and the Word Problem is solvable for a finitely generated decidable

presentation if and only if Ω_0 is bounded by a computable function. This improves the result of Grigorchuk and Ivanov.

The main problem with the function Ω is that, unlike the Dehn function which is invariant (up to equivalence) for finite presentations of the same group, there is not a similar situation for finitely generated decidable presentations. Anyway we have found conditions under which the function Ω is invariant. Let us give some details.

What is special about finite presentations for the same group is that given any two of them, one can be obtained from the other by applications of *elementary* Tietze transformations. Given two non-necessarily finite presentations for the same group this is not always the case. In fact we have generalized this situation by introducing the so-called *Tietze transformations of bounded area* (see Section 1.2) and we have proved that the Dehn function does not change if one applies to a (finite or infinite) presentation some Tietze transformations of bounded area (an elementary Tietze transformation is of bounded area).

In the same way we have introduced the so-called *Tietze transformations of bounded work* (see Definition 1.4.4) and we have proved that Ω does not change if one applies to a presentation Tietze transformations of this kind. This improves a result of Grigorchuk and Ivanov ([16], The. 1.6) which states that Ω is invariant under some transformations called *T-transformations* and *stabilizations* (they are special cases of Tietze transformations of bounded work).

We have also introduced a function, denoted Γ , which plays for the Conjugacy Problem the same rôle of the Dehn function for the Word Problem. We have proved (Proposition 1.5.1) that the Conjugacy Problem is solvable for a finitely generated presentation if and only if the Word Problem is solvable and Γ is bounded above by a computable function. It can be surprising that despite the fact that the Conjugacy Problem is harder to solve than the Word Problem, here the finite generation is sufficient to obtain the same results for the Word Problem. No hypothesis is needed for the set of defining relators, which can be infinite and also non-decidable (even non-enumerable). It is surprising too that the function Γ is invariant for any two finitely generated presentations of the same group (Proposition 1.5.2).

Other results are the following:

Corollary 4.1.3: If w is a relator of $\langle X \mid R \rangle$ then w has a contiguous subword equal to a proper corolla whose area is at most equal to the area of w .

Corollary 4.1.4: Let α be a positive constant; if $\Delta_0(n) \leq \alpha n$ then $\Delta(n) \leq \alpha n$ (and the presentation is hyperbolic, Definition 1.3.9). This

result is generalized in Propositions 5.1.10 and 5.1.12: **If Δ_0 is equivalent to a function f which is polynomial or exponential, then Δ too is equivalent to f** (see Definition 1.3.5 for equivalence of functions).

Structure of the thesis

The thesis is organized as follows: Chapter 1 is about group presentations and decision problems. In this chapter we do not simply list all the known results, instead we generalize some of them and we present some new notions. In Chapter 2 we introduce the main tool of the thesis, *straight line algorithms*, and the main objects, the sets C , L and the function A . In Chapter 3 we present results necessary for the proof of the Main Theorem, which occupies Chapter 4. In Chapter 5 we present some applications of the results proved and we compute the complexity of the algorithm presented in this thesis, which is shown to be better than the other methods currently known in the literature. Finally in the Appendix we prove some technical results.

Chapter 1

Finite and infinite presentations of groups

This chapter presents result about group presentations and decision problems for groups. Sections 1.1 and 1.2 introduce the elementary facts about words, van Kampen diagrams, the area of a relator and decision problems for group presentations. Section 1.3 is about Tietze transformations and the invariance of the Dehn function under a change of group presentation. To address the last question we introduce the original notion of *Tietze transformation of bounded area*. Sections 1.4 and 1.5 treat respectively the Word Problem for infinite presentations and the Conjugacy Problem. The approach is the same, we define functions analogous to the Dehn function and consider the classes of Tietze Transformations which preserve them. These two sections contain some original ideas and results. Finally Section 1.6 illustrates the two methods known in the literature for computing the relators of a group presentation.

1.1 Words and presentations

Let X be a set (finite or infinite), let X^{-1} be a set disjoint from X such that $|X| = |X^{-1}|$ and suppose given a bijection $X \rightarrow X^{-1}$. We denote x^{-1} the image by this bijection of an element $x \in X$ and we call it *the inverse of x* . If $y \in X^{-1}$ we denote y^{-1} the element of X such that $(y^{-1})^{-1} = y$. We call *letters* the elements of $X \cup X^{-1}$.

Let $\mathcal{M}(X \cup X^{-1})$ be the free monoid on $X \cup X^{-1}$ and $\mathcal{F}(X)$ the free group on X . The elements of $\mathcal{M}(X \cup X^{-1})$ are called *words*; the unity of $\mathcal{M}(X \cup X^{-1})$ is the word with zero letters, called the *the empty word* and

denoted 1. The elements of $\mathcal{F}(X)$ are called *reduced words*.

Let $w := x_1 \cdots x_m$ be a word; the x_i are called *the letters of w* . Given $1 \leq i_1 < \cdots < i_n \leq m$, the word $\prod_{\alpha=1}^m x_{i_\alpha}$ is called a (*non-necessarily contiguous*) *subword* of w . A *contiguous subword* of w is a subword in which the indices i_1, \dots, i_n are consecutive.

A *null-word* is a word of the form xx^{-1} where x is a letter. A word is (*freely*) *reduced* if it has no contiguous subword equal to a null word. Given a word w of the form $w'xx^{-1}w''$, the word $w'w''$ is a *one step (free) reduction* of w . A sequence of words $w = w_0, w_1, \dots, w_n$ is called a (*free*) *reduction of w* if w_i is a one step reduction of w_{i-1} and w_n is reduced. The word w_n is called a *reduced form of w* . By The. 1.2 of [22], two reduced forms of the same word are equal, then we can talk about *the* reduced form of w .

Definition 1.1.1 We let $\rho : \mathcal{M}(X \cup X^{-1}) \rightarrow \mathcal{F}(X)$ be the function sending a word to its unique *reduced form*.

Definition 1.1.2 Let w_1 and w_2 be words and let $w = w_1w_2$. The words w_1 and w_2 are called respectively a *prefix* and a *suffix* of w .

Definition 1.1.3 Given $u, v \in \mathcal{F}(X)$ there exist $u_1, v_1, a \in \mathcal{F}(X)$ such that $u = u_1a$, $v = a^{-1}v_1$ and $\rho(uv) = u_1v_1$. $\rho(uv)$ is called the *reduced product* of u by v and is the product in $\mathcal{F}(X)$, whereas uv denotes the product in $\mathcal{M}(X \cup X^{-1})$, which is the juxtaposition of words. Therefore $uv = u_1aa^{-1}v_1$. The word aa^{-1} is called *the cancelled part in the reduced product of u by v* .

Let $w := x_1 \cdots x_n$ be a word; the word $x_n^{-1} \cdots x_1^{-1}$ is *the inverse of w* and is denoted w^{-1} . The *length of w* is $|w| = n$. It is easy to see that $\rho(ww') = \rho(w)\rho(w')$ and that $\rho(w^{-1}) = \rho(w)^{-1}$.

Definition 1.1.4 Let w_1 and w_2 be words, let $w := w_1w_2$ and let $n = |w_1|$. The word w_2w_1 is called *the n -th cyclic conjugate of w* . If $n > |w|$ we define the n -th cyclic conjugate of w as w itself.

Definition 1.1.5 A reduced word is *cyclically reduced* if its last letter is not the inverse of the first one, that is if all its cyclic conjugates are reduced. We denote $\mathcal{F}(X)_c$ the set of cyclically reduced words.

Definition 1.1.6 Given a word u , either $\rho(u)$ is cyclically reduced or there exist (a unique) $t \in \mathcal{F}(X) \setminus \{1\}$ and $w \in \mathcal{F}(X)_c$ such that $\rho(u) = twt^{-1}$. The word w is called the *cyclically reduced form of u* .

If a word is cyclically reduced then it coincides with its own cyclically reduced form.

Definition 1.1.7 We let $\pi : \mathcal{M}(X \cup X^{-1}) \times \mathcal{M}(X \cup X^{-1}) \rightarrow \mathcal{F}(X)_c$ be the function sending two words to the cyclically reduced form of their product. Given two words u and v , the word $\pi(u, v)$ is called the *cyclically reduced product* of u by v .

The restriction of π to $\mathcal{F}(X)_c \times \mathcal{F}(X)_c$ is a non-associative product in $\mathcal{F}(X)_c$.

Let $\langle X | R \rangle$ be a group presentation where X is the set of generators and R that of defining relators. It is not restrictive to suppose that R is a set of cyclically reduced non-empty words such that $R^{-1} \subset R$.

Van Kampen diagrams. Let w be a non-necessarily reduced relator, that is the reduced form of w is a relator. This means that there exist defining relators r_1, \dots, r_k and words a_1, \dots, a_k such that the reduced form of w is equal to the reduced form of $a_1 r_1 a_1^{-1} \dots a_k r_k a_k^{-1}$. Then there exists a simply connected and planar 2-cell complex with the following properties:

1. the edges are labeled by elements of $X \cup X^{-1}$,
2. there are at most k faces and the set¹ of the labels of their boundaries is a subset of $\{r_1, \dots, r_k\}$,
3. there is a cycle, called a *boundary cycle*, labeled by w and containing all the exterior edges.

This complex is called a *van Kampen diagram for w* and the word w is called the *boundary label* for the diagram. The way to construct it is the following (see V.1 of [20]). One starts with k faces, k simple cycles (which we denote $\gamma_1, \dots, \gamma_k$) bounding each one a face and k simple non-closed paths (which we denote π_1, \dots, π_k). The initial vertices of all the π_i coincide and for every i , the final vertex of π_i coincides with the initial one of γ_i . All the other vertices are simple. π_i is labeled by a_i and γ_i by r_i .

Let us consider the cycle which traverses once the γ_i and which traverses twice the π_i in the two opposite directions (one giving a_i and the other a_i^{-1}). This cycle contains all the exterior edges of the complex (in fact there are no interior edges) and its label is $a_1 r_1 a_1^{-1} \dots a_k r_k a_k^{-1}$. The word w is obtained from $a_1 r_1 a_1^{-1} \dots a_k r_k a_k^{-1}$ by canceling or inserting words of the form xx^{-1} . The idea is that the cancelation of xx^{-1} “translates” into the folding of the

¹ $\{r_1, \dots, r_k\}$ is in fact a multiset since some of the r_i can be repeated

two edges labeled by x and x^{-1} , giving an interior edge; and the insertion of xx^{-1} translates into an insertion of an edge labeled by x (its opposite is labeled by x^{-1}).

When all these “foldings” and insertions are carried out, the resulting complex is labeled by w . In fact the situation is a bit more complicated because in this process some 2-sphere can be discarded (see 2.1 of [12]) and the final complex can have less than k faces.

Therefore a van Kampen diagram is determined by a product of conjugates of defining relators and a sequence of cancellations and insertions of null words.

Identities among the relations. Let r_1, \dots, r_m be defining relators, let a_1, \dots, a_m be words and suppose that the reduced form of

$$a_1 r_1 a_1^{-1} \cdots a_m r_m a_m^{-1}$$

is equal to 1. Then we say that the expression $E := ((a_1, r_1), \dots, (a_m, r_m))$ determines an identity among the relations. Identities among the relations exist in any presentation; for instance if r and s are defining relators then the reduced forms of $(r)(r^{-1})$ and $(rsr^{-1})(r)(s^{-1})(r^{-1})$ are equal to 1.

The group of the “non-trivial” of such identities is the quotient of the group of all the identities among the relations over the subgroup generated by the so-called *Peiffer relations* (see [10] or III.10 of [20]). This group is isomorphic to the second homotopy group of the presentation complex (see [10]; for the presentation complex see III.2 of [20]). We recall that the first homotopy group of the complex of a presentation of a group \mathcal{G} is isomorphic to \mathcal{G} itself (Prop. III.2.3 of [20]).

Let w be a relator and suppose that a single relator can be expressed in two ways as product of conjugates of defining relators, that is

$$w = \rho(a_1 r_1 a_1^{-1} \cdots a_m r_m a_m^{-1}) = \rho(b_1 s_1 b_1^{-1} \cdots b_n s_n b_n^{-1}).$$

It is obvious that this gives an identity among relations, namely

$$\rho(a_1 r_1 a_1^{-1} \cdots a_m r_m a_m^{-1} b_1 s_1^{-1} b_1^{-1} \cdots b_n s_n^{-1} b_n^{-1}) = 1. \quad (1.1)$$

Let us consider the van Kampen diagrams associated with some free reductions of $a_1 r_1 a_1^{-1} \cdots a_m r_m a_m^{-1}$ and $b_1 s_1 b_1^{-1} \cdots b_n s_n b_n^{-1}$. These two diagrams need not to be isomorphic. If they are, then the identity (1.1) is trivial (see [11]).

Area of a relator. For a group presentation $\langle X | R \rangle$ we denote \mathcal{N} the set of relators, that is the normal closure of R in $\mathcal{F}(X)$.

Definition 1.1.8 For every $w \in \mathcal{N}$ there exists a natural number k and there exist $r_1, \dots, r_k \in R$ and $a_1, \dots, a_k \in \mathcal{F}(X)$ such that w is the reduced form of $a_1 r_1 a_1^{-1} \dots a_k r_k a_k^{-1}$. We call *area of w* (denoted $\text{Area}(w)$) the least of such k , that is the least k such that w can be expressed in $\mathcal{F}(X)$ as product of k conjugates of defining relators.

The area of a relator was introduced by K. Madlener and F. Otto in ([21], Sec. 3) with the name of *derivational complexity* (in the more general context of monoid presentations) and later by M. Gromov independently in ([17], Sec. 2.3).

Definition 1.1.9 Let w and a be reduced words and let r be a defining relator. Set $w' := \rho(wara^{-1})$; we say that the pair (w, w') is a *derivation of length one (by means of r) from w to w'* . Since R contains the inverse of any of its elements and since $w = \rho(w'ar^{-1}a^{-1})$ then also (w', w) is a derivation of length one. A finite sequence (w_1, \dots, w_{k+1}) of $k+1$ reduced words is a *derivation of length k from w_1 to w_k* if (w_i, w_{i+1}) is a derivation of length one for $i = 1, \dots, k-1$. More specifically, if r_1, \dots, r_k are defining relators such that (w_i, w_{i+1}) is a derivation by means of r_i and if S is a subset of R containing r_1, \dots, r_k , then we say that (w_1, \dots, w_{k+1}) is an *S -derivation of length k (from w_1 to w_k)*.

Remark 1.1.10 Let w and w' be words; then there exists an S -derivation of length k from w to w' if and only if there exist words a_1, \dots, a_k and defining relators $s_1, \dots, s_k \in S$ such that $w = \rho(w'a_1 s_1 a_1^{-1} \dots a_k s_k a_k^{-1})$.

In particular if w is a relator then the area of w can be defined as the minimal length of a derivation from w to 1. We observe that the area of w can be also defined as the minimal number of faces of van Kampen diagrams with boundary label equal to w .

We now prove some properties of the Area. For every $w \in \mathcal{N}$ and for every $t \in \mathcal{F}(X)$ we have

$$\text{Area}(\rho(twt^{-1})) \leq \text{Area}(w)$$

because if

$$w = \rho(a_1 r_1 a_1^{-1} \dots a_k r_k a_k^{-1})$$

with $k = \text{Area}(w)$, then

$$\rho(twt^{-1}) = \rho(b_1 r_1 b_1^{-1} \dots b_k r_k b_k^{-1})$$

with $b_i = ta_i$. But conversely

$$\text{Area}(w) = \text{Area}(\rho(t^{-1}(tw t^{-1})t)) \leq \text{Area}(\rho(twt^{-1})),$$

that is

$$\text{Area}(\rho(twt^{-1})) = \text{Area}(w). \quad (1.2)$$

This implies that if $w \in \mathcal{N}$ and if w' is a cyclic conjugate of w (Definition 1.1.4), then $\text{Area}(w') = \text{Area}(w)$.

In the same way one proves that $\text{Area}(w^{-1}) \leq \text{Area}(w)$ and $\text{Area}(w) \leq \text{Area}(w^{-1})$, therefore

$$\text{Area}(w^{-1}) = \text{Area}(w). \quad (1.3)$$

Finally for every $v, w \in \mathcal{N}$ we have

$$\text{Area}(\rho(vw)) \leq \text{Area}(v) + \text{Area}(w), \quad (1.4)$$

because if v and w are respectively products of h and k conjugates of defining relators, then vw is product of $k + h$ of them. This implies that

$$\text{Area}(\pi(v, w)) \leq \text{Area}(v) + \text{Area}(w) \quad (1.5)$$

because vw is conjugate to $\pi(v, w)$ and thus has the same area of the latter by (1.2) (π is the cyclically reduced product, see Definition 1.1.7).

1.2 Decision problems for groups

For *computable functions* and *decidable sets* we follow [25]. Let S be a subset of \mathbb{N} and let f be a function from S to \mathbb{N} . The function f is said *computable* if there exists an algorithm which taken as input an $n \in \mathbb{N}$ then

- it halts and gives $f(n)$ as output if $n \in S$;
- it does not halt if $n \notin S$.

A computable function is also called *recursive*. The set $S \subset \mathbb{N}$ is said *decidable* if its characteristic function is computable, i.e., if there exists an algorithm which determines whether an arbitrary $n \in \mathbb{N}$ belongs to S . Any finite subset of \mathbb{N} is decidable (see 1.2 of [25]). The set S is said *enumerable* if there exists an algorithm which enumerates the elements of S . This means that there is an algorithm which for every n outputs a certain s_n and that $S = \{s_n : n \in \mathbb{N}\}$. We assume that for some n the

output of this algorithm can be empty, that is to be formal we must write $S = \{s_n : n \in \mathbb{N} \text{ and } s_n \text{ is not empty}\}$. We also assume that s_m can be equal to s_n for $m \neq n$, but that we are able to determine whether or not $s_m = s_n$.

A decidable set is enumerable. It is obvious that S is decidable if and only if S and $\mathbb{N} \setminus S$ are enumerable. Decidable and enumerable sets are also called *recursive* and *recursively enumerable* respectively.

Let U and V be enumerable sets, that is $U = \{u_n : n \in \mathbb{N}\}$ and $V = \{v_n : n \in \mathbb{N}\}$, where there are two algorithms whose n -th inputs are u_n and v_n respectively. Let V' be a subset of V and let f be a function from V' to U . Let \bar{f} be the following function: let n be a natural such that $v_n \in V'$ and let $f(v_n) = u_m$; then set $\bar{f}(n) = m$. Let $E = \{n \in \mathbb{N} : v_n \in V'\}$; then \bar{f} is a function from E to \mathbb{N} . We say that f is *computable* if \bar{f} is computable, that is if there exists an algorithm which taken v_n as input, it halts and gives $f(v_n)$ as output if $v_n \in V'$, otherwise it does not halt. In an analogous way one can define *decidable* and *enumerable* subsets of an enumerable set.

Let $\mathcal{P} = \langle X | R \rangle$ be a group presentation. The normal subgroup of $\mathcal{F}(X)$ normally generated by R is the set of relators of \mathcal{P} which we denote \mathcal{N} .

If X is enumerable then also $\mathcal{F}(X)$ is enumerable. Let R be enumerable too; then the set of products of the form

$$a_1 r_1 a_1^{-1} \cdots a_k r_k a_k^{-1}$$

is enumerable for $a_i \in \mathcal{F}(X)$, $r_i \in R$ and $k \in \mathbb{N}$, that is the set of relators is enumerable.

A group presentation $\mathcal{P} = \langle X | R \rangle$ is said *finitely generated* if X is finite; it is said *finitely related* if R is finite. A presentation is *finite* if it is finitely generated and related. A presentation which is infinitely generated but finitely related is a free product of a finite presentation with an infinite rank free group presentation.

A finitely generated presentation \mathcal{P} is said *decidable* or *enumerable* if R is respectively decidable or enumerable in $\mathcal{F}(X)$.

If a group admits an enumerable presentation then it admits also a decidable one. Indeed let \mathcal{G} be a group and let $\langle X | R \rangle$ be an enumerable presentation of \mathcal{G} . This means that there is an algorithm which enumerates R , that is there is an algorithm whose k -th output is a word w_k and $R = \{w_k : k \in \mathbb{N}\}$. Let y be an element not belonging to $\mathcal{F}(X)$ and let $R' = \{y^k w_k : k \in \mathbb{N}\}$. Then $\langle X \cup \{y\} | R' \cup \{y\} \rangle$ is a decidable presentation of \mathcal{G} .

A presentation *has a solvable Word Problem* if given any $w \in \mathcal{F}(X)$ there exists an algorithm which determines whether w is a relator; this is equivalent to say that the set of relators is decidable. A presentation *has a solvable Word Search Problem* if it has a solvable Word Problem and for any relator w there exists an algorithm which finds a product of conjugates of defining relators whose reduced form is w .

If X and R are enumerable then the solvability of the Word Problem is equivalent to that of the Word Search Problem. Indeed if w is a relator then we can execute the algorithm described above which computes the reduced form of the products of conjugates of defining relators; necessarily after a finite time this algorithm will give w as output.

The complexity of the Word Search Problem can be much greater than that of the simple Word Problem. Madlener and Otto showed in ([21], Cor. 6.14) group presentations with Word Problem solvable in polynomial time and with Word Search Problem² arbitrarily hard. Namely for every $m \geq 3$ they constructed a group $G(m)$ with these properties: the complexity of the Word Problem for $G(m)$ is at most polynomial, that of the Word Search Problem is bounded above by a function in the *Grzegorzcyk class* E_m (see Ch. 12 of [14]) but by no function in the Grzegorzcyk class E_{m-1} .

Remark 1.2.1 Let $\mathcal{P} := \langle X \mid R \rangle$ be a finite presentation, let m be the maximal length of elements of R , let w be a relator of \mathcal{P} and let r_1, \dots, r_k be defining relators and a_1, \dots, a_k be words such that w is the reduced form of

$$a_1 r_1 a_1^{-1} \cdots a_k r_k a_k^{-1}.$$

Let $|w| = n$; by using the properties of the associated van Kampen diagram one can prove that there exist words b_1, \dots, b_k such that $|b_i| \leq mk + n$ and w is the reduced form of

$$b_1 r_1 b_1^{-1} \cdots b_k r_k b_k^{-1},$$

that is we can choose the conjugating elements of length no more than $mk + n$. This implies that the sum of the lengths of the conjugating elements is bounded above by $mk^2 + kn$. See Prop. 2.2 of [15] or The. 1.1 and 2.2 of [24] for a proof of this fact³ (see also Lem. 7.1 of [23]).

²Madlener and Otto call *pseudo-natural algorithm* an algorithm for solving the Word Search Problem

³In ([20], Rem. after Lem. V.1.2) it is given kn as bound which is worse than $mk + n$ since m is a constant.

Definition 1.2.2 Let \mathcal{P} be a finitely generated presentation and let n be a natural number; the *Dehn function* at n of \mathcal{P} is

$$\Delta(n) := \max\{\text{Area}(w) : w \in \mathcal{N} \text{ and } |w| \leq n\}.$$

The Dehn function is a function from \mathbb{N} to \mathbb{N} . We have the following

Proposition 1.2.3 *Let \mathcal{P} be a presentation whose set of defining relators is enumerable and with solvable Word Problem and let Δ be the Dehn function of \mathcal{P} . If \mathcal{P} is finitely generated then Δ is bounded above by a computable function; if \mathcal{P} is finite then Δ is computable.*

Proof Since the set of generators and that of the defining relators are enumerable, the solution of the Word Problem implies that of the Word Search Problem. Let n be a natural number; since the presentation is finitely generated then the number of words of length bounded by n is finite. For any of these words we solve the Word Search Problem; this gives for any relator w of length less or equal to n an upper bound h_w for the area of w . We can compute in a finite time the maximum of these bounds and this is an upper bound for $\Delta(n)$.

Let \mathcal{P} be finite and let m be the maximal length of defining relators of \mathcal{P} . Let n be a natural number and let w be a relator such that $|w| = n' \leq n$. For any $k = 1, \dots, h_w$ let us compute the reduced forms of the products of conjugates of k defining relators with the length of conjugating elements bounded above by $mk + n'$. By virtue of Remark 1.2.1, at least one these reduced forms for some k is equal to w and a minimal k for which this happens is equal to the area of w . Therefore we can compute $\Delta(n)$ in a finite time and thus Δ is computable. \square

When \mathcal{P} is finite the converse of Proposition 1.2.3 is true:

Proposition 1.2.4 *A finite presentation has a solvable Word Problem if and only if its Dehn function is computable, if and only if its Dehn function is bounded above by a computable function.*

Proof Let Δ be the Dehn function of \mathcal{P} . By Proposition 1.2.3, if the Word Problem is solvable for \mathcal{P} then Δ is computable which implies trivially that Δ is bounded above by a computable function. We have to prove that if Δ is bounded above by a computable function then the Word Problem is solvable.

Let $\{h_n\}_{n \in \mathbb{N}}$ be a computable function such that $\Delta(n) \leq h_n$ and let w be a word of length less or equal to n . We have that w is a relator for \mathcal{P} if

and only if it is the reduced form of a product of at most h_n conjugates of defining relators with the length of the conjugating elements bounded above by $mh_n + n$ by Remark 1.2.1. Since these products can be computed in a finite time then we have a solution of the Word Problem. \square

Proposition 1.2.4 was first proved (in a less general form) by Madlener and Otto in ([21], Lem. 3.2).

Proposition 1.2.4 is no longer true if the number of relators is infinite even when it is decidable: see Example 2.4 of [16], where it is shown a decidable presentation with unsolvable Word Problem and Dehn function constantly equal to 2.

Let $\mathcal{P} = \langle X | R \rangle$ be a presentation for a group \mathcal{G} ; \mathcal{P} has *has a solvable Conjugacy Problem* if given $u, v \in \mathcal{F}(X)$ there exists an algorithm which determines whether the elements of \mathcal{G} represented by u and v are conjugated, that is whether there exists a word $t \in \mathcal{F}(X)$ such that $utv^{-1}t^{-1}$ is a relator. This is equivalent to say that the set

$$\{(u, v, t) : u = tvt^{-1} \text{ in } \mathcal{G}\} \quad (1.6)$$

is decidable. The solvability of the Conjugacy Problem implies that of the Word Problem if we take $v = 1$.

Let \mathcal{N} be the set of relators of \mathcal{P} . If $\mathcal{F}(X)$ and \mathcal{N} are enumerable, then the set (1.6) is enumerable. This is because in this case the set $\mathcal{F}(X)^3 \times \mathcal{N}$ is enumerable and thus is equal to a set of the form $\{\alpha_n = (u_n, v_n, t_n, w_n) : n \in \mathcal{N}\}$, where there is an algorithm whose n -th output is α_n . Consider the algorithm whose n -th output is (u_n, v_n, t_n) if $u_n t_n v_n^{-1} t_n^{-1} = w_n$, otherwise the output is empty; this algorithm enumerates (1.6).

We say that \mathcal{P} has *has a solvable Conjugacy Search Problem* if it has a solvable Conjugacy Problem and if there exists an algorithm which finds the conjugating word t . If $\mathcal{F}(X)$ is enumerable (in particular if X is enumerable) then the solvability of the Conjugacy Problem is equivalent to that of the Conjugacy Search Problem. Indeed $\mathcal{F}(X) = \{t_n : n \in \mathbb{N}\}$, where there is an algorithm whose n -th output is t_n . Let u and v be conjugated in \mathcal{G} ; for every n let us apply the algorithm solving the Word Problem to the word $s_n = t_n u t_n^{-1} v^{-1}$. For some n the word s_n will be equal to 1, thus t_n will be the conjugating word.

We observe that if u and v are words and if u' and v' are the cyclically reduced forms of u and v respectively (see Definition 1.1.6), then u and v are conjugated in \mathcal{G} if and only this is true for u' and v' . Therefore in studying the Conjugacy Problem it is not restrictive to consider only cyclically reduced words.

Let $\mathcal{P}_1 = \langle X_1 | R_1 \rangle$ and $\mathcal{P}_2 = \langle X_2 | R_2 \rangle$ be two group presentations, let \mathcal{N}_i be the normal subgroup of $\mathcal{F}(X_i)$ normally generated by R_i for $i = 1, 2$ and suppose that there exists a computable function f from $\mathcal{F}(X_1)$ to $\mathcal{F}(X_2)$ which is not necessarily an homomorphism and such that for $u \in \mathcal{F}(X_1)$ we have that u belongs to \mathcal{N}_1 if and only if $f(u)$ belongs to \mathcal{N}_2 . Then the Word Problem is solvable for \mathcal{P}_1 if and only if the same is true for \mathcal{P}_2 . We observe that it is not necessary that the groups presented by \mathcal{P}_1 and \mathcal{P}_2 are isomorphic.

1.3 Tietze transformations

Given two finite presentations for the same group, it is well known (see for instance Prop. 1.3.3 of [8]) that the Dehn functions relative to them are equivalent. This is a consequence of the fact that one of them can be obtained from the other by applications of elementary Tietze transformations. This result is no longer true if the presentations are not finite. In this section we define a kind of Tietze transformations, said *of bounded area*, that when applied to a presentation, finite or infinite, give a presentation with the same Dehn function (up to equivalence).

A group presentation is determined by two sets usually denoted X and R , where X is a set of letters and represents the generators of the group and R is a set of (cyclically) reduced words in $X \cup X^{-1}$ and represents the defining relators of the group. We denote $\langle\langle R \rangle\rangle$ the normal subgroup of the free group $\mathcal{F}(X)$ which is normally generated by R .

Definition 1.3.1 Let us consider the following transformations on a group presentation which consist in adding or deleting “superfluous” generators and defining relators. They are called *Tietze transformations* (see Sec. 1.5 of [22]):

1. Let $S \subset \langle\langle R \rangle\rangle$; then replace R with $R \cup S$, that is replace $\langle X | R \rangle$ with $\langle X | R \cup S \rangle$;
2. Let $S \subset R$ be such that $\langle\langle R \setminus S \rangle\rangle = \langle\langle R \rangle\rangle$; then replace R with $R \setminus S$, that is replace $\langle X | R \rangle$ with $\langle X | R \setminus S \rangle$;
3. Let $U \subset \mathcal{F}(X)$ and for every $u \in U$ let y_u be an element not belonging to $\mathcal{F}(X)$ and such that if u and u' are distinct elements of U we have $y_u \neq y_{u'}$. Set $Y := \{y_u : u \in U\}$ and $T := \{y_u u^{-1} : u \in U\}$; then replace X with $X \cup Y$ and R with $R \cup T$, that is replace $\langle X | R \rangle$ with $\langle X \cup Y | R \cup T \rangle$;

4. Let $Y \subset X$ and suppose that for every $y \in Y$ there exists a word u_y not containing neither z nor z^{-1} for every $z \in Y$ and such that $yu_y^{-1} \in R$. Let φ be the homomorphism from $\mathcal{F}(X)$ to $\mathcal{F}(X \setminus Y)$ which sends any $y \in Y$ to u_y and any $x \in X \setminus Y$ to itself. Then set $T := \{yu_y : y \in Y\}$, replace X with $X \setminus Y$ and R with $\varphi(R \setminus T)$, that is replace $\langle X \mid R \rangle$ with $\langle X \setminus Y \mid \varphi(R \setminus T) \rangle$.

The transformations 1 and 2 add or delete respectively superfluous defining relators; transformation 3 and 4 add or delete superfluous generators. Transformations of types 1 and 2 are inverse one of the other; the inverse of a transformations of type 3 is a transformation of type 4. The inverse of a transformations of type 4 is a transformation of type 3, followed by one of type 1 and by one of type 2; this is because first we have to add Y to the generators and T to the defining relators obtaining $\langle X \mid T \cup \varphi(R \setminus T) \rangle$, then add R and finally delete $\varphi(R \setminus T)$ from the defining relators.

It is obvious that applying such transformations to a presentation, we obtain a presentation for the same group. The converse is also true, that is if \mathcal{P} and \mathcal{P}' are presentations for the same group then there exists a finite sequence of Tietze transformations which applied to \mathcal{P} gives \mathcal{P}' (see Th. 1.5 of [22]). In fact by the proof of Th. 1.5 of [22] we have the following stronger result:

Proposition 1.3.2 *Two presentations of the same group can be obtained one from the other by applications of at most four Tietze transformations, namely a transformation of type 3 followed by one of type 1, then by one of type 2 and finally by one of type 4 (some of these transformations can be empty).*

A Tietze transformation is said *finite* if it adds or deletes only finitely many generators or defining relators, that is if the sets S , T and Y are finite⁴. In the same way a Tietze transformation is said *decidable* if the sets S , T and Y are decidable.

By Cor. 1.5 of [22] we have that two finite [respectively decidable] presentations define the same group if and only if one can be obtained from the other by repeated applications of finite [respectively decidable] Tietze transformations. Moreover Proposition 1.3.2 holds also in the special cases

⁴In the literature an *elementary Tietze transformation* is defined as a Tietze transformation which adds or deletes exactly one generator or defining relator. An elementary Tietze transformation is obviously finite and any finite Tietze transformation is obtained by repeated applications of elementary Tietze transformations.

of finite or decidable presentations, that is two finite or decidable presentations for the same group can be obtained one from the other by applications of at most four Tietze transformations of the types specified in Proposition 1.3.2.

We say that a Tietze transformation of type 1 or 2 is of *bounded area* if it adds or deletes a set of relators whose area is bounded, that is if $\sup\{\text{Area}(s) : s \in S\}$ is finite. We say that a Tietze transformation of type 3 or 4 is of *bounded length* if it adds or deletes a set of generators whose length is bounded, that is if $\sup\{|u| : u \in U\}$ or $\sup\{|u_y| : y \in Y\}$ (respectively for type 3 or 4) are finite.

A finite Tietze transformation is obviously of bounded area or length. If the presentation is finitely generated then any Tietze transformation of bounded length is necessarily finite. But if the presentation is finitely related then a Tietze transformation of bounded area can be finite or infinite.

Remark 1.3.3 Let \mathcal{P} be a presentation and let \mathcal{P}' be the presentation obtained from \mathcal{P} by application of a Tietze transformation of bounded area or length. We want to determine the relationship between the area of relators and the length of group elements between \mathcal{P} and \mathcal{P}' .

Suppose that \mathcal{P}' is obtained from \mathcal{P} by application of a Tietze transformation of type 1 of bounded area and let c be the maximal area of defining relators added. If Area and Area' are the functions area relative to \mathcal{P} and \mathcal{P}' respectively, then we have for a relator w that

$$\text{Area}'(w) \leq \text{Area}(w) \leq c\text{Area}'(w).$$

This implies that if Δ and Δ' are the Dehn functions relative to \mathcal{P} and \mathcal{P}' then

$$\Delta' \leq \Delta \leq c\Delta'. \quad (1.7)$$

Let us now suppose that \mathcal{P}' is obtained from \mathcal{P} by application of a Tietze transformation of type 3 of bounded length. By using the notation of 3 of Definition 1.3.1, we have that there exists a natural number c such that $|u| \leq c$ for every $u \in U$. Let φ be the function from $\mathcal{F}(X \cup Y)$ to $\mathcal{F}(X)$ sending any element of X to itself and any $y_u \in Y$ to u . We have that φ is the identity on $\mathcal{F}(X)$, in particular $\varphi(r) = r$ for every $r \in R$, and that $\varphi(t) = 1$ for every $t \in T$. Moreover for every $w \in \mathcal{F}(X \cup Y)$ we have that $|\varphi(w)| \leq c|w|$.

If we denote \mathcal{N} and \mathcal{N}' the normal subgroups of $\mathcal{F}(X)$ and $\mathcal{F}(X \cup Y)$ normally generated by R and $R \cup T$ respectively, then we have that $\mathcal{N} \subset \mathcal{N}'$ and $\varphi(\mathcal{N}') = \mathcal{N}$.

Let Area and Area' be the functions area relative to \mathcal{P} and \mathcal{P}' respectively. Let $w \in \mathcal{N}'$ and let

$$w = \rho(a_1 r_1 a_1^{-1} \cdots a_k r_k a_k^{-1})$$

where $r_i \in R \cup T$ and $k = \text{Area}'(w)$. Then

$$\rho(\varphi(w)) = \rho(b_1 s_1 b_1^{-1} \cdots b_k s_k b_k^{-1})$$

where $b_i = \varphi(a_i) \in \mathcal{F}(X)$ and s_i is equal to r_i if $r_i \in R$, s_i is equal to 1 if $r_i \in T$. This implies that

$$\text{Area}(\varphi(w)) \leq \text{Area}'(w).$$

If $w \in \mathcal{N}$ then since $\varphi(w) = w$ and since obviously $\text{Area}'(w) \leq \text{Area}(w)$, then $\text{Area}(w) = \text{Area}'(w)$. In particular if Δ and Δ' are the Dehn functions relative to \mathcal{P} and \mathcal{P}' respectively, we have that

$$\Delta \leq \Delta'.$$

Let $w \in \mathcal{N}'$; then there exists an $(R \cup T)$ -derivation from w to $\varphi(w)$ of length at most $|w|$. Since there exists an R -derivation from $\varphi(w)$ to 1 of length $\text{Area}(\varphi(w))$ then this gives an $(R \cup T)$ -derivation from w to 1 of length $\text{Area}(\varphi(w)) + |w|$, that is

$$\text{Area}'(w) \leq \text{Area}(\varphi(w)) + |w|$$

and then

$$\Delta'(n) \leq \Delta(cn) + n,$$

that is

$$\Delta(n) \leq \Delta'(n) \leq \Delta(cn) + n. \quad (1.8)$$

Let us now determine the relationship between the length of group elements between \mathcal{P} and \mathcal{P}' . If \mathcal{G} is the group presented and if g is any element of \mathcal{G} then

$$|g|' \leq |g| \leq c|g|' \quad (1.9)$$

where $|\cdot|$ and $|\cdot|'$ denote respectively the length with respect to the set of generators of \mathcal{P} and \mathcal{P}' respectively.

Remark 1.3.4 Let $\mathcal{P} := \langle X \mid R \rangle$ be a group presentation such that X and R are enumerable and let \mathcal{P}' be the presentation obtained from \mathcal{P} by adding to R all the relators of \mathcal{P} , that is if \mathcal{N} is the set of all relators of \mathcal{P} then $\mathcal{P}' = \langle X \mid \mathcal{N} \rangle$.

The set of defining relations of \mathcal{P}' is not finite, is enumerable and is decidable if and only if the Word Problem is solvable for \mathcal{P} . The Dehn function for \mathcal{P}' is eventually equal to 1.

Definition 1.3.5 Let $f, g : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ be two non-decreasing functions. We write $f \preceq g$ if there exists a positive constant α such that

$$f(n) \leq \alpha g(\alpha n) + \alpha n$$

for every $n \in \mathbb{N}^*$. We say that f and g are *equivalent* if $f \preceq g$ and $g \preceq f$ and in this case we write $f \simeq g$.

Let $f, g : \mathbb{R}_+^2 \rightarrow \mathbb{R}_+^2$ be two functions. We write $f \preceq_s g$ if there exists a positive constant α such that

$$f(n_1, n_2) \leq \alpha g(n_1, n_2)$$

for every $n_1, n_2 \in \mathbb{N}^*$. We say that f and g are *strongly equivalent* if $f \preceq_s g$ and $g \preceq_s f$ and in this case we write $f \simeq_s g$.

If $f \leq g$ then $f \preceq_s g$ and $f \preceq g$. We consider Δ as a function defined on \mathbb{R}_+ by assigning the value $\Delta(n)$ to every $x \in]n, n + 1[$.

Remark 1.3.6 Since $\alpha g(\alpha n) + \alpha n \leq \alpha' g(\alpha' n) + \alpha' n$ if $\alpha \leq \alpha'$, then $f \preceq g$ if and only if there exists $\alpha_0 > 0$ such that $f(n) \leq \alpha g(\alpha n) + \alpha n$ for every $\alpha \geq \alpha_0$.

Proposition 1.3.7 *Let \mathcal{P} and \mathcal{P}' be group presentations, let Δ and Δ' be the Dehn functions for \mathcal{P} and \mathcal{P}' respectively. Let \mathcal{P}' be obtained from \mathcal{P} by applications of Tietze transformations of bounded area or length (in particular, let \mathcal{P} and \mathcal{P}' be finite presentations for the same group); then Δ and Δ' are equivalent. In particular Δ' is computable (or bounded above by a computable function) if and only if the same is true for Δ .*

Proof By proposition 1.3.2, \mathcal{P}' can be obtained from \mathcal{P} by applications of finitely many Tietze transformations. By (1.7) and (1.8), we have that applying a Tietze transformation of type 1 or 3, the equivalence class of the Dehn function does not change. This is also true by applying a Tietze transformation of type 2 because its inverse is a transformation of type 1;

and is true also for a Tietze transformation of type 4 since its inverse is a transformation of type 3 followed by one of type 1 and by one of type 2. \square

The result of Proposition 1.3.7 is stated in the literature only in the case where \mathcal{P} and \mathcal{P}' are finite, that is when \mathcal{P} is finite and \mathcal{P}' is obtained from \mathcal{P} by applications of finite Tietze transformations. See for instance Prop. 1.3.3 of [8]; the first proof of this result was given (in a less strong form) by Madlener and Otto in ([21], Cor. 3.5).

Remark 1.3.8 If \mathcal{P}' is obtained from \mathcal{P} by applying non-bounded Tietze transformations then Δ and Δ' are in general non-equivalent. For instance if \mathcal{P}' and \mathcal{P} are as in Remark 1.3.4, then Δ and Δ' are equivalent if and only if Δ is equivalent to a constant function. In particular if \mathcal{P} is a finite presentation with unsolvable Word Problem then Δ is greater than any computable function while Δ' is constant. This shows that if in Proposition 1.3.7 we remove the hypothesis of boundedness for the Tietze transformations applied to a presentation, then the Dehn functions of two presentations for the same group can be not related at all.

This shows also that a decidable Tietze transformation needs not be of bounded area. Indeed let \mathcal{P} and \mathcal{P}' as in Remark 1.3.4, let \mathcal{P} be decidable, let Δ be not equivalent to a constant function and suppose that the Word Problem is solvable for \mathcal{P} . Then \mathcal{P}' is decidable, thus one can obtain \mathcal{P}' from \mathcal{P} by applications of decidable Tietze transformations; but since Δ and Δ' are not equivalent then \mathcal{P}' cannot be obtained from \mathcal{P} by applications of Tietze transformations of bounded area.

We have seen that two presentations define the same group if and only if they can be obtained one from the other by repeated applications of Tietze transformations. Let us consider a graph whose vertices are all the presentations of all the groups and with an edge joining two presentations if one can be obtained from the other by application of a Tietze transformation; any connected component of this graph corresponds to an isomorphism class of groups. Furthermore by Proposition 1.3.2, two vertices are either non-connected or they are connected by a path of length at most four.

Moreover let \mathcal{G} be a group, let \mathcal{P} and \mathcal{P}' be two finite [respectively decidable] presentations of \mathcal{G} . Then there is a path (of length at most four) from \mathcal{P} to \mathcal{P}' whose edges are finite [respectively decidable] Tietze transformations.

Suppose now that instead we join two presentations if one can be obtained from the other by application of a Tietze transformation of bounded

area or length. All the presentations belonging to a same connected component define the same group and moreover by Proposition 1.3.7 they have the same Dehn function up to equivalence. However in this case two different connected components can define the same group as we have seen in Remark 1.3.8.

Finally the Dehn function is related also to the *hyperbolicity* of a group.

Definition 1.3.9 Let $\langle X | R \rangle$ be a finite presentation of a group \mathcal{G} . The group \mathcal{G} is said *hyperbolic* if there exists a positive real constant α such that $\Delta(n) \leq \alpha n$ (see [13]).

By Proposition 1.3.7, if the inequality $\Delta(n) \leq \alpha n$ holds in a finite presentation of \mathcal{G} , then it holds in every finite presentations of \mathcal{G} .

1.4 Infinite presentations of groups

In this section we consider a function (called *work*) which plays for finitely generated decidable presentations the same rôle played by the Dehn function for finite presentations. This function has been introduced by J.-C. Birget in ([7], 1.4) in the more general context of semigroup presentations and was studied in a recent paper by R. I. Grigorchuk and S. V. Ivanov [16]. As done for the Dehn function, we define a kind of Tietze transformations, said *of bounded work*, that when applied to a presentation give a presentation with the same work function. This improves a result of [16].

We recall that ρ is the reduced form of a word and $\mathcal{F}(X)$ is the free group on X .

Definition 1.4.1 Let $\mathcal{P} := \langle X | R \rangle$ be a group presentation and let w be a relator. The *work of w* is defined as

$$\text{Work}(w) = \min\{|r_1| + \cdots + |r_n| : \rho(a_1 r_1 a_1^{-1} \cdots a_n r_n a_n^{-1}) = w, \\ r_1, \cdots, r_n \in R, a_1, \cdots, a_n \in \mathcal{F}(X)\}.$$

Let \mathcal{P} be finitely generated; then for a natural number n we define

$$\Omega(n) = \max\{\text{Work}(w) : w \text{ is a relator and } |w| \leq n\}.$$

The functions L_1 and f_1 of Definition 1.4.2 have been introduced by Grigorchuk and Ivanov in [16].

Definition 1.4.2 Let $\mathcal{P} := \langle X \mid R \rangle$ be a group presentation and let w be a relator. We set $L_1(w)$ as the minimal number of edges of van Kampen diagrams with boundary cycle equal to w . If n is a natural number we set

$$f_1(n) = \max\{L_1(w) : w \text{ is a relator and } |w| \leq n\}.$$

We prove that the functions Ω and f_1 are equivalent. Let $a_1, \dots, a_n \in \mathcal{F}(X)$ and $r_1, \dots, r_n \in R$ and let w be the reduced form of $a_1 r_1 a_1^{-1} \cdots a_n r_n a_n^{-1}$. We set $E := ((a_1, r_1), \dots, (a_n, r_n))$ and let $\mathcal{V}(E)$ be the van Kampen diagram relative to a freely reduction of $a_1 r_1 a_1^{-1} \cdots a_n r_n a_n^{-1}$ to w . We set

$$\text{Work}(E) := |r_1| + \cdots + |r_n|$$

and we define $L_1(E)$ as the number of edges of $\mathcal{V}(E)$. Obviously $\text{Work}(w)$ and $L_1(w)$ are equal to the the minimal $\text{Work}(E)$ and $L_1(E)$ respectively where E is an expression for w .

Let $l_1(E), l_2(E)$ and $l'_2(E)$ be the number of edges of $\mathcal{V}(E)$ belonging respectively to no faces, to a single face and to two faces of $\mathcal{V}(E)$. Then

$$L_1(E) = l_1(E) + l_2(E) + l'_2(E).$$

Since in computing the function Work we are interested in finding an expression for which $|r_1| + \cdots + |r_n|$ is minimal, then we can suppose that in constructing $\mathcal{V}(E)$ no 2-sphere has been discarded, that is we can suppose that

$$\text{Work}(E) = l_2(E) + 2l'_2(E).$$

This implies that

$$\text{Work}(E) \leq 2L_1(E)$$

and since $l_1(E) < 2|w|$ then

$$L_1(E) \leq \text{Work}(E) + 2|w|.$$

This means that

$$\text{Work}(w) \leq 2L_1(w), \quad L_1(w) \leq \text{Work}(w) + 2|w|$$

and then that

$$\Omega(n) \leq 2f_1(n), \quad f_1(n) \leq \Omega(n) + 2n,$$

that is the the functions Work and f_1 are equivalent.

We have seen that Proposition 1.2.4 is no longer true for a presentation whose set of defining relators is infinite. But if we replace the Dehn function by the function Ω then we have analogous results for decidable presentations.

- Proposition 1.4.3** 1. A finitely generated decidable presentation has a solvable Word Problem if and only if its function Ω is computable (Th. 1.2 of [16]);
2. For a finite presentation the function Ω is equivalent to the Dehn function (Th. 1.7 of [16]).

We have seen in Proposition 1.3.7 that the Dehn function is invariant under bounded Tietze transformations. The. 1.6 of [16] shows that Ω is invariant under *T-transformations* and *stabilizations*, which are special cases of finite Tietze transformations. We will show that indeed Ω is invariant under a more general class of transformations, the so-called Tietze transformations of *bounded work*, which are not necessarily finite. For that we introduce

Definition 1.4.4 A Tietze transformation of type 1 or 2 is said of *bounded work* if it adds or deletes a set S of defining relators whose work is bounded, that is if $\sup\{\text{Work}(s) : s \in S\}$ is finite.

A finite Tietze transformation of type 1 or 2 is of bounded work. Conversely if the presentation is finitely related then a Tietze transformation of bounded work is necessarily finite. If the presentation is finitely generated then a Tietze transformation of bounded work is also of bounded area; if the presentation is finitely related then a Tietze transformation of bounded area is also of bounded work. This implies in particular that for a finite presentation a Tietze transformation is of bounded work if and only if it is of bounded area.

Remark 1.4.5 Let \mathcal{P} be a presentation and let \mathcal{P}' be the presentation obtained from \mathcal{P} by application of a Tietze transformation of bounded work or length. We want to determine the relationship between the area of relators in \mathcal{P} and \mathcal{P}' .

Suppose that \mathcal{P}' is obtained from \mathcal{P} by application of a Tietze transformation of type 1 of bounded work and let c be the maximal area of defining relators added. If Work and Work' are the functions work relative to \mathcal{P} and \mathcal{P}' respectively, then we have for a relator w that

$$\text{Work}'(w) \leq \text{Work}(w) \leq c\text{Work}'(w).$$

This implies that if Ω and Ω' are the functions as defined in Definition 1.4.1 relative to \mathcal{P} and \mathcal{P}' then

$$\Omega' \leq \Omega \leq c\Omega'. \tag{1.10}$$

Let us now suppose that \mathcal{P}' is obtained from \mathcal{P} by application of a Tietze transformation of type 3 of bounded length. By using the notation of 3 of Definition 1.3.1, we have that there exists a natural number c such that $|u| \leq c$ for every $u \in U$. Let φ be the function from $\mathcal{F}(X \cup Y)$ to $\mathcal{F}(X)$ sending any element of X to itself and any $y_u \in Y$ to u . We have that φ is the identity on $\mathcal{F}(X)$, in particular $\varphi(r) = r$ for every $r \in R$, and that $\varphi(t) = 1$ for every $t \in T$. Moreover for every $w \in \mathcal{F}(X \cup Y)$ we have that $|\varphi(w)| \leq c|w|$.

If we denote \mathcal{N} and \mathcal{N}' the normal subgroups of $\mathcal{F}(X)$ and $\mathcal{F}(X \cup Y)$ normally generated by R and $R \cup T$ respectively, then we have that $\mathcal{N} \subset \mathcal{N}'$ and $\varphi(\mathcal{N}') = \mathcal{N}$.

Let Work and Work' be the functions work relative to \mathcal{P} and \mathcal{P}' respectively. Let $w \in \mathcal{N}'$ and let

$$w = \rho(a_1 r_1 a_1^{-1} \cdots a_k r_k a_k^{-1})$$

where $r_i \in R \cup T$ and $k = \text{Work}'(w)$. Then

$$\rho(\varphi(w)) = \rho(b_1 s_1 b_1^{-1} \cdots b_k s_k b_k^{-1})$$

where $b_i = \varphi(a_i) \in \mathcal{F}(X)$ and s_i is equal to r_i if $r_i \in R$, s_i is equal to 1 if $r_i \in T$. This implies that

$$\text{Work}(\varphi(w)) \leq \text{Work}'(w).$$

If $w \in \mathcal{N}$ then since $\varphi(w) = w$ and since obviously $\text{Work}'(w) \leq \text{Work}(w)$, then $\text{Work}(w) = \text{Work}'(w)$. In particular we have that

$$\Omega \leq \Omega'.$$

Let $w \in \mathcal{N}'$; since the length of any $t \in T$ is at most $c + 1$, then there exists an $(R \cup T)$ -derivation from w to $\varphi(w)$ of work at most $(c + 1)|w|$. Since there is an $(R \cup T)$ -derivation from $\varphi(w)$ to 1 of work $\text{Work}(\varphi(w))$, then we have

$$\text{Work}'(w) \leq \text{Work}(\varphi(w)) + (c + 1)|w|,$$

thus

$$\Omega(n) \leq \Omega'(n) \leq \Omega(cn) + (c + 1)n. \quad (1.11)$$

Proposition 1.4.6 *Let \mathcal{P} and \mathcal{P}' be group presentations and let Ω and Ω' be the functions as defined in Definition 1.4.1 relative to \mathcal{P} and \mathcal{P}' respectively. Let \mathcal{P}' be obtained from \mathcal{P} by applications of Tietze transformations of bounded work or length; then Ω and Ω' are equivalent.*

Proof By proposition 1.3.2, \mathcal{P}' can be obtained from \mathcal{P} by applications of finitely many Tietze transformations. By (1.10) and (1.11), we have that applying a Tietze transformation of type 1 or 3, the equivalence class of the function Ω does not change. This is also true by applying a Tietze transformation of type 2 because its inverse is a transformation of type 1; and is true also for a Tietze transformation of type 4 since its inverse is a transformation of type 3 followed by one of type 1 and by one of type 2. \square

1.5 The Conjugacy Problem

In this section we define a function, denoted Γ , which plays for the Conjugacy Problem the same rôle played by the Dehn function (or the function work) for the Word Problem. It is surprising that despite the fact that the Conjugacy Problem is harder to solve than the Word Problem, anyway to obtain results analogous to those valid for the Word Problem, the only hypotheses needed is the finite generation of the presentation.

No hypothesis is necessary on the set of defining relators, which can be even non-decidable or non-enumerable. It is also surprising that the function Γ is constant under a much larger class of Tietze transformations than for the Dehn (or work) function. The results of this section are apparently new.

We recall that $\mathcal{F}(X)_c$ denotes the set of cyclically reduced words on $X \cup X^{-1}$.

Let \mathcal{G} be a group, let X be a generating set for \mathcal{G} and let $w_1, w_2 \in \mathcal{F}(X)_c$ be conjugated in \mathcal{G} . We set

$$\gamma(w_1, w_2) := \min\{|t| : t \in \mathcal{F}(X) \text{ and } w_1 = tw_2t^{-1} \text{ in } \mathcal{G}\}. \quad (1.12)$$

Let X be finite and let n_1, n_2 be natural numbers: we set

$$\Gamma(n_1, n_2) := \max\{\gamma(w_1, w_2) : w_1 \text{ and } w_2 \text{ are conjugated in } \mathcal{G} \quad (1.13)$$

$$\text{and } |w_1| \leq n_1, |w_2| \leq n_2\}.$$

The functions γ and Γ depend on the generating set X . If \mathcal{P} is a presentation, the function Γ *relative to* \mathcal{P} is the function Γ for the group presented by \mathcal{P} with respect to the set of generators for \mathcal{P} .

Let \mathcal{G} be generated by a set X , let u be a word in $X \cup X^{-1}$ such that the element of \mathcal{G} represented by u is central; if v is another word then u and v are conjugated in \mathcal{G} if and only if they determine the same element of \mathcal{G} ; in this case $\gamma(u, v) = 0$. Thus if \mathcal{G} is an abelian group then Γ is equal to

the zero function. The converse is also true, that is a group is abelian if and only if $\Gamma(n_1, n_2) = 0$ for every n_1 and n_2 . This result holds with respect to every generating set of \mathcal{G} .

If \mathcal{G} is a finite group then Γ is bounded. Indeed if X is a generating set for \mathcal{G} and if k is the longest length of elements of \mathcal{G} then Γ is eventually equal to a constant less or equal to k .

On the other side, let \mathcal{G} be generated by a finite set X and let Γ be bounded; then this implies that there exists a finite subset $\{g_1, \dots, g_n\}$ of \mathcal{G} such that for every h and h' which are conjugated in \mathcal{G} and which are equal to cyclically reduced products of elements of $X \cup X^{-1}$, then there exists $i = 1, \dots, n$ such that $h' = g_i h g_i^{-1}$.

Problem. *Find a finitely generated infinite non-abelian group whose function Γ (with respect to a finite generating set) is bounded; or prove that if Γ is bounded then \mathcal{G} is finite or abelian.*

The next result is the analogous for the Conjugacy Problem of Proposition 1.2.4. It has to be noticed that unlike for the Word Problem, here we do not need that the number of defining relators be finite.

Proposition 1.5.1 *A finitely generated presentation has a solvable Conjugacy Problem if and only if it has a solvable Word Problem and Γ is bounded above by a computable function. In this case Γ is computable.*

Proof Let \mathcal{G} be the group presented by \mathcal{P} .

1. Let \mathcal{P} have a solvable Word Problem and let $\Gamma(n_1, n_2) \leq h(n_1, n_2)$ where $h(n_1, n_2)$ is computable. Since \mathcal{P} is finitely generated, then for any natural numbers n_1 and n_2 the number of pairs of words (w_1, w_2) such that $|w_1| \leq n_1$ and $|w_2| \leq n_2$ is finite. Let w_1, w_2 be words such that $|w_1| \leq n_1$ and $|w_2| \leq n_2$; w_1 and w_2 are conjugated in \mathcal{G} if and only there exists a word t of length no more than $h(n_1, n_2)$ such that $w_1 t w_2^{-1} t^{-1}$ is a relator.

Let us solve the Word Problem for all the words of the form $w_1 t w_2^{-1} t^{-1}$ where $|t| \leq h(n_1, n_2)$; this solves the Conjugacy Problem for the pair (w_1, w_2) . Moreover if w_1 and w_2 are conjugate in \mathcal{G} , then the minimal length of a conjugating word is equal to $\gamma(w_1, w_2)$ and thus $\Gamma(n_1, n_2)$ is computable since it is the maximum of the $\gamma(w_1, w_2)$.

2. Let \mathcal{P} be have a solvable Conjugacy Problem. Let n_1, n_2 be natural numbers; since \mathcal{P} is finitely generated, then the number of pairs of words (w_1, w_2) such that $|w_1| \leq n_1$ and $|w_2| \leq n_2$ is finite. Let us

solve the Conjugacy Problem for these pairs of words; this gives for any pair of conjugated words (w_1, w_2) an upper bound for $\gamma(w_1, w_2)$. The maximum of these bounds is an upper bound for $\Gamma(n_1, n_2)$ which is then bounded above by a computable function.

□

It would be interesting to compute the function Γ for presentations with a solvable Conjugacy Problem. For instance for a finite presentation \mathcal{P} satisfying the small cancellation condition $C'(1/8)$ then $\Gamma(n_1, n_2) \leq 6 \max(n_1, n_2)$. If \mathcal{P} satisfies $C'(1/6)$ then $\Gamma(n_1, n_2) \leq 12 \max(n_1, n_2)$ and if \mathcal{P} satisfies $C'(1/4)$ and $T(4)$ then $\Gamma(n_1, n_2) \leq 16 \max(n_1, n_2)$ (see The. V.5.4 of [20]). More generally, if \mathcal{P} is a finite presentation of an hyperbolic group, then there exists a constant K such that $\Gamma(n_1, n_2) \leq K \max(n_1, n_2)$ (see III-Γ-2.11 and 2.12 of [9]).

Proposition 1.5.2 *Let \mathcal{P} and \mathcal{P}' be group presentations and let Γ and Γ' be the functions as defined in (1.13) relative to \mathcal{P} and \mathcal{P}' respectively. Suppose that \mathcal{P}' is obtained from \mathcal{P} by applications of Tietze transformations of type 3 or 4 of bounded length and by any Tietze transformations of type 1 or 2 (in particular, let \mathcal{P} and \mathcal{P}' be finitely generated presentations for the same group). Then Γ and Γ' are strongly equivalent (Definition 1.3.5).*

Proof Let \mathcal{G} be the group presented by \mathcal{P} and \mathcal{P}' . Since Γ is independent from the defining relators of a presentation, then by applying Tietze transformations of type 1 or 2 the function Γ does not change. Let us apply a Tietze transformation of length bounded by a natural number m and let γ and γ' be the functions as defined in (1.12) relative to \mathcal{P} and \mathcal{P}' respectively. By (1.9) we have that

$$\gamma'(w_1, w_2) \leq \gamma(w_1, w_2) \leq m\gamma'(w_1, w_2)$$

for every $w_1, w_2 \in \mathcal{F}(X)_c$ conjugated in \mathcal{G} , thus

$$\Gamma' \leq \Gamma \leq m\Gamma'$$

and that proves the claim. □

1.6 Enumeration of relators

Let $\mathcal{P} := \langle X \mid R \rangle$ be a finite presentation and let k and n be natural numbers. Currently there are two known methods to compute all the relators

of \mathcal{P} of area and length at most k and n : the first consists in constructing all the van Kampen diagrams with at most k faces and with boundary of at most n edges; the second uses the result of Remark 1.2.1 which states that if m is the maximal length of elements of R and if w is a relator of area $k' \leq k$ and length $n' \leq n$, then w is a product of k' conjugates of defining relators, where the length of the conjugating elements is less or equal to $mk' + n'$.

Let us consider the first method. The way of proceeding is the following: one first constructs all the van Kampen diagrams with at most k faces and with boundary of at most n edges and which have no *spines*, i.e., in which every edge belongs to a face. Then one considers all the van Kampen diagrams with at most k faces and with boundary of at most n edges and which are obtained by *adjoining* (see [5]) one by one two or more of these *spineless* diagrams and some (even zero) labeled edges in such a way that any adjunction is made on a single vertex.

Spineless van Kampen diagrams are constructed in this way: one starts with a face and then adds one by one another face by identifying a vertex of the face with a vertex of the boundary of the diagram already constructed; or by identifying one or more consecutive edges of the face with one or more consecutive edges of the boundary of the diagram already constructed.

We recall that any face of a van Kampen diagram is labeled by a defining relator and that since the identification of two edges corresponds to a cancellation of two letters between the labels of the boundaries, then the edges to be identified must be labeled by opposite letters.

It must be observed that with this method we have to construct also diagrams whose boundary label is not reduced. This is because there can exist diagrams whose boundary label is reduced but which cannot be adjunctions of two diagrams with reduced boundary labels.

Let us compute the complexity of this method expressed as the number of diagrams to be constructed. We will count the number of diagrams without spines and which are obtained by adjunctions only along vertices. The number of such diagrams will result to be more than factorial in k .

Let q be the minimal length of a defining relator; suppose that we have a face F_1 and that we want to add a second face F_2 . We have at least q^2 ways to do it, any corresponding to the identification of a given vertex of F_1 with one of F_2 . These diagrams have boundary with length equal at least to $2q$ and there are at least $2q \cdot q = 2q^2$ ways to add a third face F_3 , therefore there are at least $2q^2 \cdot q^2 = 2q^4$ diagrams with three faces. These diagrams have length $3q$ and thus the diagrams with four faces are at least $2q^4 \times 3q = 3!q^5$. By continuing this way we see that for a natural number j ,

there are at least $(j-1)!q^{2(j-1)}$ spineless diagrams obtained by adjunctions along vertices.

Since we want to obtain diagrams with boundary of length at most n , then for $j = 1, \dots, k$ we are not interested in those diagrams with $k-j$ faces and whose boundary is longer than $n+jm$ (we recall that m is the maximal length of a defining relator). If j is such that $n+mj \leq (k-j)q$, anyway all the spineless diagrams obtained by adjunctions along vertices must be computed. This gives as condition that

$$j \leq \frac{q}{m+q}k - \frac{n}{m+q} = c_1k - c_2n,$$

with c_1 and c_2 positive constants less than 1. We recall that k is the number of faces of the diagrams, thus it is reasonable to take $k \geq \Delta(n)$, where $\Delta(n)$ is the Dehn function at n . If $\Delta(n)/n$ goes to infinity then we can assume that $c_1k - c_2n$ has the same asymptotic behavior of k and the number of these diagrams is asymptotically equal at least to

$$(k-1)!q^{2(k-1)}, \tag{1.14}$$

that is it is a product of a factorial and an exponential in k .

If $\Delta(n)/n$ does not go to infinity then the Dehn function is linear in n and the group is hyperbolic (Definition 1.3.9). These groups are already well studied in the literature.

We observe that (1.14) does not take into account spineless diagrams obtained by adjunctions along vertices and with a number of faces different than $c_1k - c_2n$; and does not take into account the diagrams obtained by adjoining along edges and also those containing spines. Thus the complexity of this method must be much bigger than (1.14).

Now let us consider the second method. We want to compute its complexity expressed as the number of words to be constructed to find the desired relators. Let N be this number. To determine N we have to compute the number of products of h conjugates of defining relators for $h = 1, \dots, k$ where each conjugating element has length bounded above by $mh + n$.

Let U be the set of reduced words of length bounded above by $mk + n$ and let $p := |R|$. Then we have

$$N := \sum_{h=1}^k (p|U|)^h = \frac{(p|U|)^{k+1} - p|U|}{p|U| - 1}.$$

Let us compute $|U|$. Let $a = 2|X| - 1$; then we have that

$$|U| = 1 + (a + 1) \sum_{i=0}^{mk+n-1} a^i.$$

If we set $M := mk + n$ then

$$\sum_{i=0}^{mk+n-1} a^i = \frac{a^M - 1}{a - 1}$$

and thus

$$|U| = 1 + (a + 1) \frac{a^M - 1}{a - 1}.$$

For simplicity we make the following approximation:

$$|U| \approx \frac{a + 1}{a - 1} a^M.$$

We have that $N \approx (p|U|)^k$ and since $M = mk + n$ then

$$N \approx \left(p \frac{a + 1}{a - 1} \right)^k a^{mk^2 + kn} = q^k a^{kn} s^{k^2}, \quad (1.15)$$

where $q = p(a + 1)/(a - 1)$ and $s = a^m$. We recall that $p = |R|$, $a = 2|X| - 1$ and m is the maximal length of the elements of R .

The complexity of this algorithm (expressed as the number of words among which looking for to find the desired relators) is the product of three exponentials: one in k , one in kn and one in k^2 . This complexity is less than (1.14), thus this algorithm is better than the first one.

Given natural numbers k , m and n , it can be quite difficult to find a finite presentation whose maximal length of defining relators is m and with a relator w of length n , of area k and which is the reduced form of a product of k conjugates of defining relators where the conjugating elements have length $mk + n$. Anyway the following method can go very near to such a situation.

Let $\mathcal{F}(X)$ be the free group on the set X , let r_1, \dots, r_{k-1} be cyclically reduced words in X (not necessarily distinct), let m be a natural number such that $m \geq |r_i|$ for $i = 1, \dots, k - 1$ and let a_1, \dots, a_{k-1} be reduced words of length $mk + n$. Let w be the reduced form of $a_1 r_1 a_1^{-1} \dots a_{k-1} r_{k-1} a_{k-1}^{-1}$, let v be a word of length n , set $r_k := w^{-1}v$ and set $R := \{r_1, \dots, r_k, r_1^{-1}, \dots, r_k^{-1}\}$. Then in the presentation $\langle X | R \rangle$, we have that v is a relator of length n and is the reduced form of $a_1 r_1 a_1^{-1} \dots a_k r_k a_k^{-1}$.

Chapter 2

The sets C and L and the function A

In this chapter we present the main tools and objects of the thesis. In Section 2.1 we introduce a class of algorithms called *straight line algorithms* by means of which we define and study in Sections 2.2 and 2.3 some special relators called *corollas* and in Section 2.4 the set L and the functions A (which will be shown in the Main Theorem 4.1.1 to coincide with the set of all relators and the function *area* respectively). Finally in Section 2.5 we state the main results of the thesis.

2.1 Straight line algorithms

In this section we introduce the main tool of which we make use in this thesis: *straight line algorithms*. They are algorithms which generate elements of a given set U starting from a set $B \subset U$ and applying some given operations. As observed in Remark 2.1.4, a straight line algorithm is an algorithm such that there is one and only one path from a given step to the final one; in particular there are no cycles. In Section A.2 it will be shown that they are a natural tool for describing recursively defined sets.

In the current literature the term “straight line algorithm” denotes a slightly different object (see for instance 3.1.3 of [19])

Definition 2.1.1 Let U be a set and let Φ be a family of functions $\varphi : U^{n_\varphi} \rightarrow U$ (where n_φ is a given non-zero natural number depending on φ) with codomain U and with domain some Cartesian power of U . A *straight line algorithm (or SLA) relative to (U, B, Φ)* is a finite algorithm in which a

step can be either an element b of B (in this case b is the output of the step and there is no input) or the application of a function $\varphi \in \Phi$ to n_φ outputs $t_1, \dots, t_{n_\varphi}$ of preceding steps ($t_1, \dots, t_{n_\varphi}$ are the inputs and $\varphi(t_1, \dots, t_{n_\varphi})$ is the output). We require also the conditions that $t_1, \dots, t_{n_\varphi}$ be outputs of distinct steps and that the output of any step, except the last, be an input of one and only one of the successive steps. U is called the *universe set*, B the *base set* and Φ is called *the set of operations*. The elements of B are called *base elements*, a step equal to an element of B is called a *base step*.

This notion of straight line algorithm is used very often in mathematics. For instance let U be a group, let B be a subset of U and let Φ be equal to the operations of product and inversion in U . Let a, b, c be elements of B (not necessarily distinct); the following is an SLA relative to (U, B, Φ) :

step 1 : a step 2 : b step 3 : ab step 4 : c step 5 : c^{-1} step 6 : abc^{-1} .

The steps 1, 2 and 4 are equal to elements of B , the 3 applies the product (which is an operation of Φ) to outputs of preceding steps (the 1 and 2), the 5 applies the inversion to the output of the step 4 and finally the 6 applies the product to the outputs 3 and 5. The output of any step (except the last) is input of one and only one of the successive steps. The result of any of these straight line algorithms is an element of the subgroup of U generated by B . If we add to Φ also the operation of conjugation with an element of U then the result is an element of the normal subgroup generated by B .

Definition 2.1.2 Let σ be a straight line algorithm and let s and s' be steps such that the output of s is one of the inputs of s' ; we say that s' *depends directly on* s or that s' *uses directly* s . The latter is a relation in the set of steps of σ . We call *relation of dependence* the transitive reflexive closure [1] of this relation; that is, given steps s and s' , we say that s' *depends on* s if $s = s'$ or if there exists a finite sequence of steps starting with s , ending with s' and such that every step in the sequence depends directly on the preceding. If s' depends on s we can say also that s' *uses* s .

The first step of a straight line algorithm is always a base step because it cannot use preceding steps. The final output of a straight line algorithm is its *result*. By abuse of notation we will sometimes identify a step with its output, but this will not cause ambiguity.

Proposition 2.1.3 *Let σ be an SLA. Then:*

1. *the steps using a given step of σ form a chain with respect to the relation of dependence;*

2. the final step of σ uses every step;
3. if a step s'' uses a step s , then there exists a step s' used by s'' and using directly s ;
4. let s and s' be steps such that s' uses s and let s'_1, \dots, s'_n be all the steps used directly by s' ; then one and only one of the s'_i uses s .

Proof

1. Take a step s of σ and let s' be a step using s . There exists a chain of steps $s_0 := s, s_1, s_2, \dots$ such that s_i uses directly s_{i-1} ; since s_i is the unique step using directly s_{i-1} , this chain is unique. Since s' uses s , then necessarily s' is one of the s_i .
2. Let s be a step of σ . Since the chain of steps of σ using s is finite (being σ a finite algorithm), this chain ends necessarily with the last step of σ , which therefore uses s .
3. By Part 1 there exists a chain of steps $s_1 := s, s_2, \dots, s_m := s''$ such that s_i uses directly s_{i-1} . Thus $s' := s_2$ uses directly s and is used by s'' .
4. There exist steps $s_0 := s, s_1, \dots, s_m := s'$ such that s_i uses directly s_{i-1} . Since s' uses directly s_{m-1} then s_{m-1} is one of the s'_i and uses $s_0 = s$.

Suppose that s'_j and s'_k are two different steps used directly by s' and using s . By Part 1 the steps using s' form a chain and therefore s'_j uses s'_k (or s'_k uses s'_j). By Part 3 there exists a step used by s'_j (therefore preceding it) and using directly s'_k . This step cannot be s' because s' uses s'_j and therefore follows it; this is impossible because s' is the only step using directly s'_k .

□

Remark 2.1.4 There is a natural way to associate a directed graph with an algorithm: the vertices of this graph are the steps of the algorithm and there is an edge directed from a step s_1 to a step s_2 if the output of s_1 is one of the inputs of s_2 .

The graph associated with a straight line algorithm is such that for every vertex there is one and only one path beginning at that vertex and ending

at the vertex corresponding to the final step¹. Furthermore this property characterizes straight line algorithms in the class of finite algorithms.

Remark 2.1.5 Let σ be an SLA and let s be one of its steps. It is easy to see that the steps used by s form a straight line algorithm. This SLA is called *the proper straight line subalgorithm (pSLsA) determined by s* . Every base element of a pSLsA of σ is also a base element of σ .

In Definition 3.3.6 we will generalize this notion of proper straight line subalgorithm; this explains the use here of the adjective “proper”.

Definition 2.1.6 A *multiset* is a set whose elements can be repeated; it is defined as a pair (S, λ) where S is a set and λ is a function from S to the natural numbers. The value of λ on an element of S is the *multiplicity* of that element.

Definition 2.1.7 Let σ be an SLA relative to (U, B, Φ) , let $\lambda : B \rightarrow \mathbb{N}$ be the function such that for $b \in B$, $\lambda(b)$ is the number of steps of σ equal to b . The multiset (B, λ) is called *the multiset of base elements of σ* .

Definition 2.1.8 Given two multisets $M_1 := (S, \lambda_1)$ and $M_2 := (S, \lambda_2)$ we define their union as $M_1 \cup M_2 := (S, \lambda_1 + \lambda_2)$, that is the multiplicity of an element of S in $M_1 \cup M_2$ is the sum of its multiplicities in M_1 and M_2 .

Remark 2.1.9 Let σ be an SLA and let s be one of its steps. Let $s_1 := s, s_2, \dots, s_m$ be the chain of steps of σ depending on s (see Part 1 of Proposition 2.1.3); in particular s_i depends directly on s_{i-1} and s_m is the last step of σ . We can reorder the steps of σ in such a way that s_1 depends on every step preceding it and that for $i = 2, \dots, m$, s_i depends on every step comprised between s_{i-1} and s_i . This reorder of the steps of σ does not change the relative order of s_1, \dots, s_m and obviously does not change the result and the multiset of base elements.

2.2 The set C and the function η

In this section we introduce a very important object for this thesis, the so-called *corollas*. Corollas together with *stems*, i.e., words of the form ww^{-1} are the “ingredients” to construct the set L defined in the next section and which will be shown in the Main Theorem 4.1.1 to coincide with the set of

¹In particular this graph has no cycles and then is a *tree*.

all relators. Thus corollas can be considered the “non-trivial” parts of the relators.

Definition 2.2.1 Let w_1, w_2 and u be words and let $w := w_1w_2$. The word w_1uw_2 is called *the insertion of u into w at w_1* . If $n = |w_1|$, the word w_1uw_2 is also called *the n -th insertion of u into w* or *the insertion of u into w at the n -th letter*. If $n \geq |w|$ we define the n -th insertion of u into w as the product wu .

The n -insertions are binary operations in $\mathcal{M}(X \cup X^{-1})$.

Definition 2.2.2 Let \mathcal{S} be the set of words of the form ww^{-1} where w is reduced and $w \neq 1$. We call *stems* the elements of \mathcal{S} .

By Definition 1.1.3, the product of two words u and v is an insertion of cancelled part (which is a stem) into $\rho(uv)$.

Remark 2.2.3 Let u and v be reduced words and let $w = \pi(u, v)$ be the cyclically reduced product of u by v . Let us study the relation between u, v and $\pi(u, v)$. As in Definition 1.1.3 let $u_1, v_1, a \in \mathcal{F}(X)$ be such that $u = u_1a$, $v = a^{-1}v_1$ and $\rho(uv) = u_1v_1$, that is $uv = u_1aa^{-1}v_1$. If $w = 1$ then $t = 1$ because the word u_1v_1 is reduced and in this case $u = v^{-1}$. Let $w \neq 1$; since $u_1v_1 = twt^{-1}$, three cases are possible:

1. u_1 is a prefix of t ;
2. u_1 is a prefix of tw but not of t ;
3. u_1 is not a prefix of tw .

Let us examine the three cases.

1. there exists a word t_1 such that $t = u_1t_1$. Therefore $v_1 = t_1wt^{-1} = t_1wt_1^{-1}u_1^{-1}$ and $u = u_1a$, $v = a^{-1}t_1wt_1^{-1}u_1^{-1}$, thus $uv = u_1aa^{-1}t_1wt_1^{-1}u_1^{-1}$. Moreover v^{-1} is a prefix of v .
2. since u_1 is not a prefix of t , t is a prefix of u_1 . Moreover v_1 is a suffix of wt^{-1} . This means that there exist words w_1 and w_2 such that $w = w_1w_2$ and $u_1 = tw_1$ and $v_1 = w_2t^{-1}$. Therefore $u = tw_1a$, $v = a^{-1}w_2t^{-1}$ and thus $uv = tw_1aa^{-1}w_2t^{-1}$.
3. since u_1 is not a prefix of tw , tw is a prefix of u_1 and thus there exists a word t_1 such that $u_1 = twt_1^{-1}$ and $t^{-1} = t_1^{-1}v_1$. Therefore $u_1 = v_1^{-1}t_1wt_1^{-1}$ and $u = v_1^{-1}t_1wt_1^{-1}a$, $v = a^{-1}v_1$ and thus $uv = v_1^{-1}t_1wt_1^{-1}aa^{-1}v_1$. Moreover v^{-1} is a suffix of u .

In Case 2 if $w_1 = 1$ then we obtain the Case 1, if $w_2 = 1$ the Case 3, therefore we can suppose that in Case 2, w_1 and w_2 are non-empty. In Case 1, u is completely cancelled in the reduced product by v , in Case 3 it is v to be completely cancelled. In Case 2 no one of them is completely cancelled. If a is empty there is no cancellation in the reduced product of u by v ; if also t is empty there is no cancellation also in their cyclically reduced product.

Remark 2.2.4 Let u and v be reduced words such that v^{-1} is not a suffix (Definition 1.1.2) of u and u^{-1} is not a prefix of v . Then there exist a cyclic conjugate u' of u and a cyclic conjugate v' of v such that $\rho(u'v') = \pi(u, v)$. To prove it let us consider the second case of Remark 2.2.3. We have that $u = tw_1a$, $v = a^{-1}w_2t^{-1}$ and $\pi(u, v) = w$. Set $u' := w_1at$ and $v' := t^{-1}a^{-1}w_2$; then $\rho(u'v') = \pi(u, v)$.

Proposition 2.2.5 *Let u and v be reduced words and let $w = \pi(u, v)$ be the cyclically reduced product of u by v ; then $\pi(v, u)$ is a cyclic conjugate of $\pi(u, v)$.*

Proof Let us prove the claim part by showing that it holds in the three cases of Remark 2.2.3.

1. we have that $v = a^{-1}t_1wt_1^{-1}u_1^{-1}$ and $u = u_1a$, therefore $\rho(vu) = a^{-1}t_1wt_1^{-1}a$ and $\pi(v, u) = w = \pi(u, v)$.
2. we have that $v = a^{-1}w_2t^{-1}$ and $u = tw_1a$, therefore $\rho(vu) = a^{-1}w_2w_1a$ and $\pi(v, u) = w_2w_1$ which is a cyclic of $\pi(u, v) = w_1w_2$.
3. we have that $v = a^{-1}v_1$ and $u = v_1^{-1}t_1wt_1^{-1}a$, therefore $\rho(vu) = a^{-1}t_1wt_1^{-1}a$ and $\pi(v, u) = w = \pi(u, v)$.

□

For every word w and for every natural number n , we let $\psi_n(w)$ denote the reduced form of the n -th cyclic conjugate of w and we set

$$\Psi := \{\psi_n : n \in \mathbb{N}^*\} \cup \{\pi\},$$

where π has been introduced in Definition 1.1.7.

Straight line algorithms have been defined in Section 2.1.

Definition 2.2.6 Let R be a subset of $\mathcal{F}(X)_c \setminus \{1\}$ containing the inverse of any of its elements and let Σ be the set of $(\mathcal{F}(X)_c, R, \Psi)$ -straight line

algorithms σ such that if $\pi(u, v)$ is a step of σ then $\pi(u, v) \neq 1$ and there is at least one cancellation in $\pi(u, v)$, that is $|\pi(u, v)| < |u| + |v|$. We denote \overline{R} the set of results of Σ and we call *generalized corollas* or *g. corollas* the elements of \overline{R} .

Let Σ_0 the subset of Σ consisting of straight line algorithms σ such that if $\pi(u, v)$ is a step of σ then either u or v or both are cyclic conjugates of elements of R . We denote C the set of results of Σ_0 and we call *corollas* the elements of C .

We will call *straight line algorithms in \overline{R}* or *\overline{R} -straight line algorithms* the elements of Σ . The elements of Σ_0 are called *straight line algorithms in C* or *C -straight line algorithms*

Proposition 2.2.7 *Let \mathcal{N} be the normal closure of R in $\mathcal{F}(X)$, i.e., the intersection of all normal subgroups of $\mathcal{F}(X)$ containing R . Then $\mathcal{N} \supset \overline{R}$.*

Proof Let σ be an SLA in \overline{R} , let c be the result of σ and let n be the number of steps of σ . We will prove the claim by induction on n , being trivial for $n = 1$.

Let the last step of σ be a cyclic conjugation of a word c' and let σ' be the proper straight line subalgorithm (Remark 2.1.5) computing c' . There exist words d and e such that $c' = de$ and $c = ed$. Then $c = \rho(d^{-1}c'd)$ and belongs to \mathcal{N} since $c' \in \mathcal{N}$.

Let the last step of σ be the cyclically reduced product of two words c_1 and c_2 and let σ_1 and σ_2 be the proper straight line subalgorithms computing c_1 and c_2 . Then c is the reduced form of a conjugate of the product of c_1 by c_2 and thus belongs to \mathcal{N} . \square

We recall that a base step (Definition 2.1.1) of a straight line algorithm is a step equal to a base element. A base step for a straight line algorithm in \overline{R} is a step equal to a defining relators (the other two kinds of steps are the cyclic conjugations and the cyclically reduced products)

Definition 2.2.8 Let τ be a straight line algorithm in \overline{R} . We set $\eta(\tau)$ as the number of steps of τ equal to base steps.

η is a function going from the set of SLA's in \overline{R} to the natural numbers. If τ is an SLA with only one step then this step is necessarily a base step and $\eta(\tau) = 1$. Suppose that τ has more than one step. Let the final step of τ be the cyclic conjugation of a preceding output c . If τ' is the pSLA of τ (Remark 2.1.5) computing c then τ' has the same number of base steps as τ and thus $\eta(\tau) = \eta(\tau')$. Let the final step of τ be the cyclically reduced

product of preceding outputs c_1 and c_2 and let τ_1 and τ_2 be the pSLsA's of τ computing c_1 and c_2 ; then the base steps of τ are those of τ_1 and of τ_2 and thus $\eta(\tau) = \eta(\tau_1) + \eta(\tau_2)$.

Definition 2.2.9 Let $c \in \overline{R}$; we set $\eta(c) := \min\{\eta(\tau) : \tau \text{ is an SLA in } \overline{R} \text{ computing } c\}$.

Proposition 2.2.10 Let τ be an SLA in \overline{R} and let c be its result. Then $\text{Area}(c) \leq \eta(\tau)$.

Proof We prove the claim by induction on the number of steps of τ . If τ has only one step then $\eta(\tau) = 1$ and c is a base element; this means that c belongs to R and therefore $\text{Area}(c) = 1$.

Let τ have more than one step and let the claim be true for every SLA with less steps than τ . Let the final step of τ be the cyclic conjugation of a preceding output c' and let c be the final output of τ ; if τ' is the pSLsA of τ computing c' we have $\eta(\tau) = \eta(\tau')$ by the construction of η and $\text{Area}(c) = \text{Area}(c')$ by (1.2). By induction hypothesis we have $\text{Area}(c') \leq \eta(\tau')$, therefore $\text{Area}(c) \leq \eta(\tau)$.

Let the final step of τ be the cyclically reduced product of preceding outputs c_1 and c_2 , that is $c = \pi(c_1, c_2)$. If τ_1 and τ_2 are the pSLsA's of τ computing c_1 and c_2 , we have $\eta(\tau) = \eta(\tau_1) + \eta(\tau_2)$ by the construction of η and $\text{Area}(c) \leq \text{Area}(c_1) + \text{Area}(c_2)$ by (1.5). By induction hypothesis we have $\text{Area}(c_1) \leq \eta(\tau_1)$ and $\text{Area}(c_2) \leq \eta(\tau_2)$, therefore $\text{Area}(c) \leq \eta(\tau)$. \square

Corollary 2.2.11 If $c \in \overline{R}$ then $\text{Area}(c) \leq \eta(c)$.

Proof Follows from Definition 2.2.9 and Proposition 2.2.10. \square

2.3 Properties of the corollas

In this section we prove some properties of the corollas. In Remarks 2.3.3 and 2.3.4 we show how to associate a product of conjugates of defining relators and a van Kampen diagram with a straight line algorithm computing a corolla. Remark 2.3.6 says that if the presentation is finite and m is the maximal length of a defining relator then a corolla of length n and area k can be expressed as product of conjugates of defining relators with the sum of the lengths of the conjugating elements bounded above by $(mk - 1)/2 + n - 1$, while for a general relator this sum is bounded above by $mk^2 + kn$, see Remark 1.2.1. Remark 2.3.13 gives an algorithm for computing the corollas when the presentation is finite.

Remark 2.3.1 Let c be a g. corolla and let c' be a cyclic conjugate of c ; then $\eta(c') = \eta(c)$. Indeed let τ be an SLA in \overline{R} computing c and such that $\eta(\tau) = \eta(c)$. Let τ' be the SLA in \overline{R} obtained by adding to τ a cyclic conjugation from c to c' ; τ' computes c' then $\eta(c') \leq \eta(\tau')$ and $\eta(\tau') = \eta(\tau)$. This implies that $\eta(c') \leq \eta(c)$. Since c is a cyclic conjugate of c' then in the same way we prove that $\eta(c) \leq \eta(c')$ and thus that $\eta(c') = \eta(c)$.

Remark 2.3.2 Let c and c' be g. corollas such that $|\pi(c, c')| < |c| + |c'|$, let τ and τ' be SLA's in \overline{R} computing c and c' respectively and such that $\eta(c) = \eta(\tau)$ and $\eta(c') = \eta(\tau')$. Let τ'' be the SLA obtained by adding to τ the steps of τ' and finally a step equal to $\pi(c, c')$; τ'' is an SLA in \overline{R} (see Definition 2.2.6). We have that $\eta(\tau'') = \eta(\tau) + \eta(\tau')$ and thus that $\eta(\tau'') = \eta(c) + \eta(c')$. Since $\eta(\pi(c, c')) \leq \eta(\tau'')$ then we have that $\eta(\pi(c, c')) \leq \eta(c) + \eta(c')$.

Remark 2.3.3 Let σ be a straight line algorithm in \overline{R} ; we show how to find a product of conjugates of $\eta(\sigma)$ defining relators whose reduced form is the result of σ .

Let σ have one step; then this step is a defining relator r and we associate r with σ . Let σ have more than one step and suppose to have proved the claim for every SLA with less steps than σ . Let the last step of σ be the cyclic conjugation of a word c' into a word c ; then there exist words d and e such that $c' = de$ and $c = ed$. Let σ' be the proper straight line subalgorithm (Remark 2.1.5) computing c' ; by induction hypothesis

$$c' = \rho(a_1 r_1 a_1^{-1} \cdots a_m r_m a_m^{-1})$$

where r_1, \dots, r_m are defining relators, a_1, \dots, a_m are words and $m = \eta(\sigma')$. Then $m = \eta(\sigma)$ and

$$c = \rho(b_1 r_1 b_1^{-1} \cdots b_m r_m b_m^{-1})$$

where $b_i = d^{-1} a_i$.

Let the last step of σ be the cyclically reduced product of two words c_1 and c_2 , that is the result of σ is $c = \pi(c_1, c_2)$ (Definition 1.1.7). Let σ_1 and σ_2 be the proper straight line subalgorithms computing c_1 and c_2 ; then by induction hypothesis

$$c_1 = \rho(a_1 r_1 a_1^{-1} \cdots a_k r_k a_k^{-1}), \quad c_2 = \rho(a_{k+1} r_{k+1} a_{k+1}^{-1} \cdots a_m r_m a_m^{-1})$$

where $k = \eta(\sigma_1)$ and $m - k = \eta(\sigma_2)$.

By Definition 1.1.6 there exist a word t such that

$$t c t^{-1} = \rho(a_1 r_1 a_1^{-1} \cdots a_m r_m a_m^{-1}).$$

and thus

$$c = \rho(b_1 r_1 b_1^{-1} \cdots b_m r_m b_m^{-1})$$

where $b_i = t^{-1} a_i$ and $m = \eta(\sigma)$.

Remark 2.3.4 Let σ be a straight line algorithm in \overline{R} , let $k = \eta(\sigma)$ and let c be its result. By Remark 2.3.3, c is the reduced form of a product of k conjugates of defining relators. Thus we can associate with c a van Kampen diagram with k faces as seen in Section 1.1 but we show a more direct way. The procedure is analogous to that of Remark 2.3.3. We will prove that the diagram associated with σ is planar, contractible and homeomorphic to a 2-disc. In particular, unlike the general situation described in Section 1.1, in the construction of this diagram no 2-sphere is discarded and the number of faces of the diagram is equal to the number of base steps of σ .

Let σ have one step; then this step is a defining relator $r = x_1 \cdots x_m$ and we associate with σ a complex with a single face whose boundary has m edges labeled consecutively by x_1, \dots, x_m . This diagram verifies trivially the desired properties.

Let σ have more than one step and suppose to have proved the claim for every SLA with less steps than σ . Let the last step of σ be the cyclic conjugation of a word c' into a word c ; then there exist words d and e such that $c' = de$ and $c = ed$. Let σ' be the proper straight line subalgorithm computing c' ; by induction hypothesis there exists a diagram verifying the three properties above. The boundary cycle of this diagram is of the form $\delta\epsilon$ where δ is labeled by d and ϵ by e . Then we associate with σ the same van Kampen diagram with boundary label $\epsilon\delta$.

Let the last step of σ be the cyclically reduced product of two words c_1 and c_2 , that is the result of σ is $c = \pi(c_1, c_2)$. Let σ_1 and σ_2 be the proper straight line subalgorithms computing c_1 and c_2 ; then by induction hypothesis we can suppose that we have associated van Kampen diagrams \mathcal{V}_1 and \mathcal{V}_2 with σ_1 and σ_2 . By Definition 1.1.6 there exists a word t such that $\rho(c_1 c_2) = t c t^{-1}$ where $\rho(c_1 c_2)$ is the reduced product of c_1 by c_2 . By Definition 1.1.3, there exist words a, c'_1, c'_2 such that $c_1 = c'_1 a$, $c_2 = a^{-1} c'_2$ and $\rho(c_1 c_2) = c'_1 c'_2$. First we associate a complex with $\rho(c_1 c_2)$ by folding the subpath of \mathcal{V}_1 labeled by a onto the subpath of \mathcal{V}_2 labeled by a^{-1} ; this complex is the *adjunction* (see [5]) of \mathcal{V}_1 to \mathcal{V}_2 along the subgraph of \mathcal{V}_1 labeled by a into the subgraph of \mathcal{V}_2 labeled by a^{-1} . Then we consider the quotient of the obtained complex given by identifying the edges in the path labeled by t with the opposite of the edges of the path labeled by t^{-1} . The complex obtained is planar and homeomorphic to a 2-disc because it

is the adjunction of two complexes with these properties. It is contractible by Ex. 23 in Chapter 0 of [18] because it is the union of two contractible 2-complexes whose intersection is the path labeled by t which is contractible.

Remark 2.3.5 Let σ be a straight line algorithm in \overline{R} ; in Remark 2.3.3 we have shown how to associate with σ a product of $\eta(\sigma)$ conjugates of defining relators whose reduced form is the result of σ . We show now another way to obtain the same product.

If σ has one step, then this step is a defining relator r and we associate r with σ . Let σ have more than one step and suppose that the last step of σ is a cyclic conjugation of a word c' into a word c ; then there exist words d and e such that $c' = de$ and $c = ed$ and thus c is the reduced form of $d^{-1}cd$.

Let the last step of σ be the cyclically reduced product of two words c_1 and c_2 , that is the result of σ is $c = \pi(c_1, c_2)$. By Definition 1.1.6 there exist a word t such that $tct^{-1} = \rho(c_1c_2)$, that is c is the reduced form of $t^{-1}c_1tt^{-1}c_2t$.

In both cases c is the reduced form of a product of conjugates of g. corollas of σ . Any of these g. corollas is a cyclic conjugate of another g. corolla of σ or the cyclically reduced product of two g. corollas of σ , then we can repeat the same procedure to these g. corollas. Continuing this way until all the g. corollas obtained are the base elements of σ , we obtain an expression of c as product of conjugates of defining relators. This product obviously coincides with that defined in Remark 2.3.3.

Remark 2.3.6 Let σ be a straight line algorithm in \overline{R} , let c be the result of σ and let

$$c = \rho(a_1r_1a_1^{-1} \cdots a_mr_ma_m^{-1})$$

where this expression is that obtained as in Remark 2.3.3. We show that there exists a sequence of cancellations reducing $a_1r_1a_1^{-1} \cdots a_mr_ma_m^{-1}$ to c such that for $i = 1, \dots, m$:

1. if l is a letter of a_i which cancels, then l cancels either with a letter of some of the r_j or with a letter of a_{i-1}^{-1} ;
2. if l is a letter of a_i^{-1} which cancels, then l cancels either with a letter of some of the r_j or with a letter of a_{i+1} .

In particular this implies that a letter of a_1 or one of a_m^{-1} can cancel only with letters of some of the r_j .

We use Remark 2.3.5. If σ has only one step then the claim is trivial. Let σ have more than one step; then by induction hypothesis c is the reduced

form of some product $b_1c_1b_1^{-1} \cdots b_nc_nb_n^{-1}$ where the c_i are g. corollas of σ and the b_i verify the two properties above. Let c_i for some i be the output of a step of σ consisting in a cyclic conjugation of a g. corolla c' . Then there exist words d and e such that $c' = de$ and $c = ed$, that is c is the reduced form of $a_1c'_1a_1^{-1} \cdots a_nc'_na_n^{-1}$, where $c'_i = c$, $a_i = b_id^{-1}$ and $a_j = b_j$, $c'_j = c_j$ for $j \neq i$. The a_i verify the two properties above because the suffix d^{-1} of a_i cancels with c'_i .

Let c_i for some i be the output of a step of σ consisting in a cyclically reduced product of two g. corollas d_1 and d_2 , that is $c_i = \pi(d_1, d_2)$. By Definition 1.1.6 there exists a word t such that $tc_it^{-1} = \rho(d_1d_2)$, that is c_i is the reduced form of $t^{-1}d_1tt^{-1}d_2t$. In this case c is the reduced form of $a_1c'_1a_1^{-1} \cdots a_{n+1}c'_{n+1}a_{n+1}^{-1}$, where $a_j = b_j$ and $c'_j = c_j$ for $j < i$, $a_i = a_{i+1} = b_it^{-1}$, $c'_i = d_1$, $c'_{i+1} = d_2$ and $a_j = b_{j-1}$ and $c'_j = c_{j-1}$ for $j > i$. The a_i verify the two properties above because the suffix t^{-1} of a_i cancels with c'_i , a_i^{-1} cancels with a_{i+1} and the prefix t of a_{i+1}^{-1} cancels with c'_{i+1} .

Remark 2.3.7 Let σ be a straight line algorithm in \overline{R} , let c be the result of σ and let

$$c = \rho(a_1r_1a_1^{-1} \cdots a_kr_ka_k^{-1})$$

where this expression is that obtained as in Remark 2.3.3. Let

$$\alpha = |a_1| + \cdots + |a_k|, \quad \beta = |r_1| + \cdots + |r_k|.$$

We show that either $\alpha < \beta$ or

$$\alpha \leq (\beta - 1)/2 + |c| - 1.$$

In particular let m be the maximal length of an element of R and let $|c| \leq n$; then if $\alpha \geq \beta$ this implies that

$$\alpha \leq (mk - 1)/2 + n - 1.$$

Let Λ be the set of letters of $a_1r_1a_1^{-1} \cdots a_kr_ka_k^{-1}$ which are cancelled in the free reduction to c and define a function

$$\varphi : \Lambda \rightarrow \Lambda$$

such that for every $l \in \Lambda$, the letter l cancels with $\varphi(l)$ and the cancellations verify the two properties of Remark 2.3.6. The function φ is a bijection and $\varphi^2 = id$.

Consider the set of sequences $(l_1, l_2, \dots, l_{2h})$ of elements of Λ such that:

1. $l_{2i} = \varphi(l_{2i-1})$ for $i = 1, \dots, h$;
2. l_i belongs to some of the $a_j^{\pm 1}$ for $i = 2, \dots, 2h - 1$;
3. $l_{2i+1} = l_{2i}^{-1}$ for $i = 1, \dots, h - 1$;
4. either l_1 is a letter of some of the r_j or it is a letter of some of the $a_j^{\pm 1}$ and l_1^{-1} does not belong to Λ (i.e., it is not cancelled).
5. either l_{2h} is a letter of some of the r_j or it is a letter of some of the $a_j^{\pm 1}$ and l_{2h}^{-1} does not belong to Λ (i.e., it is not cancelled).

By condition 2, the l_{2i} of condition 3 belong to some of the $a_j^{\pm 1}$, therefore condition 3 says that there exists $j := 1, \dots, k$ such that $a_j = bxc$ for words b and c and a letter x and $\{l_{2i}, l_{2i+1}\} = \{x, x^{-1}\}$.

If a sequence $(l_1, l_2, \dots, l_{2h})$ verifies the four properties above then also does the sequence $(l_{2h}, l_{2h-1}, \dots, l_1)$.

We observe that any sequence contains at most one letter of a given a_j or a_j^{-1} : indeed let l_i be a letter of a_j . If i is odd, then l_{i+1} is the letter cancelled with l_i . By Remark 2.3.6, either l_{i+1} belongs to some of the r_j and thus l_{i+1} is the last element of the sequence or l_{i+1} belongs to a_{j-1}^{-1} . This means that the indices of the a_j which have letters in the sequence are strictly decreasing and in particular there is at most one letter for any of the a_j . The same is true if l_i is a letter of a_j^{-1} , in which case the indices are strictly increasing. If i is even then l_{i+1} is a letter of a_j^{-1} , thus $i + 1$ is odd what said above applies.

Moreover if two sequences have an element in common then one is obtained from the other by reversing the order of its elements. Any letter cancelled uniquely determines the first and the last letters of the sequence to which it belongs. If a sequence contains the letter x of some $a_j = bxc$ and the letter x^{-1} of $a_j^{-1} = c^{-1}x^{-1}b^{-1}$ does not belong to the sequence, then x^{-1} is not cancelled. Otherwise, if x and x^{-1} are cancelled then they belong to the same sequence and that sequence is uniquely determined by its first and last element. Therefore corresponding to x and x^{-1} there are two letters which are a cancelled letter of some of the r_j and a non-cancelled one of some of the $a_j^{\pm 1}$ or there are two letters which are both of one of these two types.

This means that the sum of cancelled letters of the $a_j^{\pm 1}$ is no more than the sum of non-cancelled letters of the $a_j^{\pm 1}$ plus the cancelled letters of the r_j .

Let $\alpha = |a_1| + \cdots + |a_k|$ and $\beta = |r_1| + \cdots + |r_k|$. Then if $w = a_1 r_1 a_1^{-1} \cdots a_k r_k a_k^{-1}$, then $|w| = 2\alpha + \beta$. Let α_1 [respectively β_1] be the number of letters of the $a_j^{\pm 1}$ [respectively of the r_j] which are cancelled and α_2 [respectively β_2] that of the non-cancelled. Then by what seen above we have

$$\alpha_1 \leq \alpha_2 + \beta_1. \quad (2.1)$$

Let $\alpha \geq \beta$, that is $\alpha = \beta + \gamma$ where $\gamma \geq 0$. Since $2\alpha = \alpha_1 + \alpha_2$ then $\alpha_1 + \alpha_2 = 2\beta_1 + 2\beta_2 + 2\gamma$ and $\alpha_1 = -\alpha_2 + 2\beta_1 + 2\beta_2 + 2\gamma$, that is by (2.1) we have

$$-\alpha_2 + 2\beta_1 + 2\beta_2 + 2\gamma \leq \alpha_2 + \beta_1$$

and thus

$$\alpha_2 \geq \gamma + \beta_2 + \frac{\beta_1}{2} = \frac{\beta + \beta_2}{2} + \gamma$$

since $\beta = \beta_1 + \beta_2$. Then

$$|c| = \alpha_2 + \beta_2 \geq \frac{\beta + 3\beta_2}{2} + \gamma.$$

Let n be a natural number and let $|c| \leq n$; then

$$\frac{\beta + 3\beta_2}{2} + \gamma \leq n$$

that is

$$\gamma \leq n - \frac{\beta + 3\beta_2}{2}.$$

Since $\beta_2 \geq 1$ then

$$\gamma \leq n - \frac{\beta + 3}{2}.$$

Then

$$\alpha = \beta + \gamma \leq \beta + n - \frac{\beta + 3}{2} = \frac{\beta - 3}{2} + n.$$

Let m be the maximal length of elements of R ; then $\beta \leq mk$, that is

$$\alpha = \beta + \gamma \leq \frac{mk - 3}{2} + n = \frac{mk - 1}{2} + n - 1.$$

Lemma 2.3.8 *Let τ be an SLA in \overline{R} , let c be the result of τ and suppose that $\eta(\tau) = \eta(c)$. Then if τ' is a pSLsA of τ and if c' is the result of τ' then $\eta(\tau') = \eta(c')$.*

Proof Let n be the number of steps of τ ; we prove the claim by induction of n being evident for $n = 1$. Let $n > 2$ and the claim be true for all the SLA's in \overline{R} with less steps than τ . Let the last step of τ be the cyclic conjugation of a word c'' and let τ'' be the pSLsA of τ computing c'' . If τ' is a pSLsA of τ then either $\tau' = \tau$ and the claim is obvious or τ' is a pSLsA of τ'' , in which case the claim is true by induction hypothesis. Let the last step of τ be the cyclic reduced product of two words c_1 and c_2 and let τ_1 and τ_2 be the pSLsA's of τ computing c_1 and c_2 respectively. If $\tau' = \tau$ the claim is obvious, otherwise τ' is a pSLsA of either τ_1 or τ_2 and the claim is true by induction hypothesis. \square

Definition 2.3.9 Let σ be an SLA in \overline{R} such that $\eta(\sigma) = k$ and let c be the result of σ . Then we say that c is a k -g. corolla. We denote \overline{R}_k the set of k -g. corollas. If σ is an SLA in C then we call c a k -corolla. We denote C_k the set of k -corollas.

Let c be a k -g. corolla, that is there exists σ whose result is c and such that $\eta(\sigma) = k$. Let c' be a cyclic conjugate of c and let us call σ' the SLA obtained by adding to σ the cyclic conjugation from c to c' . Then $\eta(\sigma') = k$ and the result of σ' is c' , that is c' is a k -g. corolla and thus \overline{R}_k contains the cyclic conjugates of any of its elements.

We have the following result, which we prove in the appendix.

Proposition A.3.2 *Let σ be an \overline{R} -SLA; then there exists a C -SLA σ' with the same set of base elements and result of σ and such that $\eta(\sigma') = \eta(\sigma)$. In particular $\overline{R}_k = C_k$.*

Remark 2.3.10 We prove that \overline{R}_k and C_k contain the inverse of any of its elements, that is if σ computes c and $\eta(\sigma) = k$ then there exists τ which computes c^{-1} and $\eta(\tau) = k$. We give the proof for \overline{R}_k , that for C_k being analogous.

Let σ be a \overline{R} -straight line algorithm computing c and such that $\eta(\sigma) = k$ and let n be the number of steps of σ . If $n = 1$ then $c \in R$, thus $c^{-1} \in R$ and therefore there is an SLA with one step equal to c^{-1} .

Let $n > 1$ and the claim be true for every SLA with less steps than σ . Let the last step of σ be a cyclic conjugation of a word c_0 and let σ_0 be the straight line subalgorithm computing c_0 ; then $\eta(\sigma_0) = \eta(\sigma) = k$. By induction hypothesis $c_0^{-1} \in \overline{R}_k$ and this means that there exists an SLA τ_0 computing c_0^{-1} and such that $\eta(\tau_0) = k$. Since c^{-1} is a cyclic conjugate of c_0^{-1} then if we add to τ_0 the cyclic conjugation from c_0^{-1} to c^{-1} then we obtain an SLA which we denote τ that computes c^{-1} and such that $\eta(\tau) = k$.

Let the last step of σ be a cyclically reduced product of two words c_1 and c_2 and let σ_1 and σ_2 be the proper straight line subalgorithms computing c_1 and c_2 . We have that $k = \eta(\sigma) = \eta(\sigma_1) + \eta(\sigma_2)$. By induction hypothesis we have that there exist straight line algorithms τ_1 and τ_2 computing c_1^{-1} and c_2^{-1} and such that $\eta(\tau_1) + \eta(\tau_2) = k$. Let τ be the straight line algorithm obtained by adding to the steps of τ_1 and τ_2 the cyclically reduced product of c_2^{-1} by c_1^{-1} . Then τ computes c^{-1} and $\eta(\tau) = k$.

Lemma 2.3.11 \overline{R}_1 is the set of cyclic conjugates of elements of R and is equal to C_1 . Let $k > 1$; then \overline{R}_k is the set of the cyclic conjugates of the cyclically reduced products of an element of \overline{R}_m by one of \overline{R}_n , for m and n non-zero natural numbers such that $m + n = k$ and $m \leq n$; C_k is the set of the cyclic conjugates of the cyclically reduced products of an element of \overline{R}_{k-1} by one of C_1 .

Proof For $k = 1$ the claim is trivial. Let $k > 1$, let σ be an SLA in \overline{R} such that $\eta(\sigma) = k$ and let c be the result of σ . Let s be the last step of τ which is not a cyclic conjugation and let c' be the output of s . Let τ' be the pSLsA of τ computing c' . There exist preceding outputs c_1 and c_2 such that $c' = \pi(c_1, c_2)$. Let τ_1 and τ_2 be the pSLsA's of τ computing c_1 and c_2 respectively. Let $m = \eta(\tau_1)$ and $n = \eta(\tau_2)$, that is $c_1 \in \overline{R}_m$ and $c_2 \in \overline{R}_n$. This means that c is a cyclic conjugate of the cyclically reduced product of c_1 by c_2 and $m + n = k$. Finally by Proposition 2.2.5 we have that $\pi(c_2, c_1)$ is a cyclic conjugate of $\pi(c_1, c_2)$, therefore we can assume that $m \leq n$.

Analogously is for C_k . \square

Theorem 2.3.12 If R is finite (in particular $\langle X | R \rangle$ is a finite presentation) then \overline{R}_k is finite for every natural number k .

Proof We prove the claim by induction on k . Let $k = 1$; by Lemma 2.3.11, \overline{R}_1 is equal to the set of cyclic conjugates of the elements of R and is finite since R is finite. Let $k > 1$ and $\overline{R}_{k'}$ be finite for every $k' < k$; by Lemma 2.3.11, \overline{R}_k is contained in the set of cyclic conjugates of the cyclically reduced products of an element of \overline{R}_m by one of \overline{R}_n , for m and n non-zero natural numbers such that $m + n = k$. The claim follows from the fact that by induction hypothesis \overline{R}_m and \overline{R}_n are finite and that the number of cyclic conjugates of a given word is finite. \square

Remark 2.3.13 Let R be finite, let k be a natural number and let us use Lemma 2.3.11 and Remark 2.2.4 to find an algorithm computing the elements of C_k . If $k = 1$ then we compute the cyclic conjugates of the

elements of R . Let $k > 1$ and suppose to have computed C_1, \dots, C_{k-1} ; if $c \in C_k$ then there exist c_1, c_2 such that $c_1 \neq c_2^{-1}$ and $c_1 \in C_{k-1}, c_2 \in C_1$ or $c_1 \in C_1, c_2 \in C_{k-1}$ and c is a cyclic conjugate of $\pi(c_1, c_2)$. By Remark 2.2.4 we have that either c_1^{-1} is a prefix of c_2 or c_2^{-1} is a suffix of c_1 or there exist cyclic conjugates w_1 of c_1 and w_2 of c_2 such that $\pi(c_1, c_2) = \rho(w_1 w_2)$. Since any C_h is closed under cyclic conjugations, then to compute the elements of C_k it is not necessary to compute all the $\pi(c_1, c_2)$ with $c_1 \in C_{k-1}$ and $c_2 \in C_1$ or $c_1 \in C_1$ and $c_2 \in C_{k-1}$, but just those for which there is cancellation between a suffix of c_1 and a prefix of c_2 but not between a prefix of c_1 and a suffix of c_2 .

2.4 The set L and the function A

We recall that we have called *stem* (Definition 2.2.2) a word of the form ww^{-1} where w is reduced and $w \neq 1$, and that we have denoted \mathcal{S} the set of all stems. The set C has been introduced in Definition 2.2.6 (we recall that the elements of C are called *corollas*) and insertions of words in Definition 2.2.1.

Definition 2.4.1 We denote L the set of results of straight line algorithms (Definition 2.1.1) whose universe set is $\mathcal{M}(X \cup X^{-1})$, whose base set is $B = \mathcal{S} \cup C$ and whose operations are the insertions of words. We will call *L-straight line algorithms* or *straight line algorithms in L* these straight line algorithms.

We denote L_g the set of results of straight line algorithms whose universe set is $\mathcal{M}(X \cup X^{-1})$, whose base set is $B_g = \mathcal{S} \cup \overline{R}$ and whose operations are the insertions of words. We will call *L_g-straight line algorithms* or *straight line algorithms in L_g* these straight line algorithms.

We observe that $\overline{R} \cap \mathcal{S} = \emptyset$ because every element of \overline{R} is reduced and every one of \mathcal{S} is not. Obviously $L_g \supset L$ since $\overline{R} \supset C$. We recall from that an element of B_g is called a *base element*.

Conjugating a word v with a reduced word w is equivalent to inserting v into the stem ww^{-1} at w . By Definition 1.1.3, the product of two reduced words is equal to an insertion of the cancelled part (which is a stem) into their reduced product.

L_g is closed under product (which is a special case of insertion) and under conjugation with a reduced word, because if $l \in L_g$ and if w is reduced then ww^{-1} is a stem, therefore belongs to L_g and wlw^{-1} is an insertion of l

into $w w^{-1}$. This means that L_g contains any “non-cancelled” product of conjugates of elements of C . This implies

Proposition 2.4.2 *Let \mathcal{N} be the normal closure of R in $\mathcal{F}(X)$, i.e., the set of relators of the presentation $\langle X | R \rangle$. If $w \in \mathcal{N}$ then there exists an element of L_g whose reduced form is w .*

Proof Follows from what said above because every element of \mathcal{N} is the reduced form of a product of conjugates of elements of $R \subset C$. \square

The following result is a converse of Proposition 2.4.2.

Proposition 2.4.3 *The reduced form of any element of L_g is a relator, that is it belongs to \mathcal{N} .*

Proof We have to prove that $\rho(L) \subset \mathcal{N}$ (recall that ρ denotes the reduced form, Definition 1.1.1). Let σ be an SLA in L_g , let w be the result of σ and let n be the number of steps of σ ; we prove the claim by induction on n .

Let $n = 1$; then w belongs either to C (in which case $\rho(w) = w \in C \subset \mathcal{N}$) or $w \in \mathcal{S}$ (in which case $\rho(w) = 1 \in \mathcal{N}$).

Let $n > 1$ and the claim be true for every SLA with less steps than σ . Then w is of the form $uw'v$ and the last step is the insertion of w' into uv at u . By induction hypothesis, $\rho(uv)$ and $\rho(w')$ belong to \mathcal{N} ; since $\rho(w) = \rho(uw'u^{-1}uv)$ then $\rho(w)$ belongs to \mathcal{N} . \square

We recall that the *g. corollas* are the elements of C . The function $\eta(c)$ for a *g. corolla* c has been introduced in Definition 2.2.9.

Definition 2.4.4 Let σ be an SLA in L_g ; we set $A(\sigma) := \sum \eta(c)$ where c varies in the set of *g. corollas* of σ . Let $w \in L_g$; we set $A(w) := \min\{A(\sigma) : \sigma \text{ is an SLA in } L \text{ computing } w\}$.

Remark 2.4.5 Let c be a *g. corolla* and let σ be the SLA in L_g with a single step equal to c . Then σ computes c and $A(\sigma) = \eta(c)$, therefore $A(c) \leq \eta(c)$.

For the area and the work of a relator see Definitions 1.1.8 and 1.4.1 respectively.

Definition 2.4.6 We call *proper (g.) corolla* a (g.) corolla c such that $A(c) = \eta(c)$. For every natural number n set

$$\Delta_0(n) := \max\{\text{Area}(w) : w \text{ is a proper corolla and } |w| \leq n\},$$

$$\Omega_0(n) := \max\{\text{Work}(w) : w \text{ is a proper corolla and } |w| \leq n\}.$$

Obviously $\Delta_0 \leq \Delta$ and $\Omega_0 \leq \Omega$ where Δ is the Dehn function (Definition 1.2.2) and Ω has been introduced in Definition 1.4.1.

2.5 Statement of the results

Definition 2.5.1 Let σ be a straight line algorithm in L_g , let c_1, \dots, c_m be the corollas of σ (counted with their multiplicity) and let τ_1, \dots, τ_m be straight line algorithms in \overline{R} computing them and such that $\eta(\tau_i) = \eta(c_i)$ for $i = 1, \dots, m$. The union² of the multisets of base elements (Definition 2.1.7) of τ_1, \dots, τ_m is called a *complete multiset of defining relators* (abbreviated CMDR) for σ .

Remark 2.5.2 Let σ be a straight line algorithm in L_g and let M be a CMDR for σ . Then it is obvious that $A(\sigma) = |M|$.

Let σ, σ_1 and σ_2 be straight line algorithms in L_g such that the multiset of corollas of σ is the union of those of σ_1 and of σ_2 and let M_1 and M_2 be CMDR for σ_1 and σ_2 respectively. Then $A(\sigma) = A(\sigma_1) + A(\sigma_2)$ and $M_1 \cup M_2$ is a CMDR for σ .

In particular this is the case when the last step of an SLA σ is the insertion of a word w_2 into a word w_1 and σ_1 and σ_2 are the pSLsA's (Remark 2.1.5) of σ computing w_1 and w_2 .

Proposition 2.5.3 *Let σ be an SLA in L_g and let w be its result. Then $\text{Area}(\rho(w)) \leq A(\sigma)$; in particular $\text{Area}(\rho(w)) \leq A(w)$.*

Proof We prove the claim by induction on the number of steps of σ . If σ has only one step then w is a stem or a corolla. If w is a stem then $\rho(w) = 1$, $\text{Area}(\rho(w)) = 0$ and $A(\sigma) = 0$. If w is a corolla (in particular it is reduced, i.e., $\rho(w) = w$) then $A(\sigma) = \eta(w)$ and the claim follows from Corollary 2.2.11.

Let σ have more than one step and the claim be true for every SLA with less steps than σ . The last step of σ is the insertion of a word w_2 into a word w_1 , that is there exist words u, v such that $w_1 = uv$ and $w = uw_2v$. Let σ_1 and σ_2 be the pSLsA's computing w_1 and w_2 ; by induction hypothesis $\text{Area}(\rho(w_i)) \leq A(\sigma_i)$ for $i = 1, 2$. Since $A(\sigma) = A(\sigma_1) + A(\sigma_2)$ by Remark 2.5.2, then

$$\text{Area}(\rho(w_1)) + \text{Area}(\rho(w_2)) \leq A(\sigma). \quad (2.2)$$

²for union of multisets see Definition 2.1.8

Since $\rho(w) = \rho(uw_2u^{-1}uv)$ and $w_1 = uv$, then

$$\rho(w) = \rho(uw_2u^{-1})\rho(w_1);$$

by (1.4) we have that

$$\text{Area}(\rho(w)) \leq \text{Area}(\rho(uw_2u^{-1})) + \text{Area}(\rho(w_1)). \quad (2.3)$$

Finally the claim follows from (2.3) by virtue of (2.2) and of the fact that $\text{Area}(\rho(uw_2u^{-1})) = \text{Area}(\rho(w_2))$ by (1.2) of Section 1.1. \square

Lemma 2.5.4 *Let $w \in L_g$ and let σ be an SLA computing w and such that $\text{Area}(\rho(w)) = A(\sigma)$. Then any corolla of σ is a proper corolla (Definition 2.4.6).*

Proof We prove the claim by induction on the number of steps of σ . If σ has one step then w is the only corolla of σ . Moreover it is reduced, i.e., $\rho(w) = w$ and $A(\sigma) = \eta(w)$. By Definition 2.4.4, $A(w) \leq A(\sigma)$ and $A(\sigma) = \text{Area}(\rho(w))$ by hypothesis. Since $\text{Area}(\rho(w)) \leq A(w)$ by Proposition 2.5.3, then

$$A(w) \leq A(\sigma) = \eta(w) = \text{Area}(\rho(w)) \leq A(w),$$

therefore $A(w) = \eta(w)$ and w is a proper corolla.

Let σ have more than one step and the claim be true for every SLA with less steps than σ . The last step of σ is the insertion of a word w_2 into a word w_1 , that is there exist words u, v such that $w_1 = uv$ and $w = uw_2v$. As in the proof of Proposition 2.5.3, $\rho(w) = \rho(uw_2u^{-1}w_1)$ and

$$\text{Area}(\rho(w)) \leq \text{Area}(\rho(w_2)) + \text{Area}(\rho(w_1)). \quad (2.4)$$

Let σ_1 and σ_2 be the pSLA's computing w_1 and w_2 ; we have that $A(\sigma) = A(\sigma_1) + A(\sigma_2)$ by Remark 2.5.2. If $\text{Area}(\rho(w_1)) < A(\sigma_1)$ or $\text{Area}(\rho(w_2)) < A(\sigma_2)$, then by (2.4)

$$\text{Area}(\rho(w)) < A(\sigma_1) + A(\sigma_2) = A(\sigma)$$

which is contrary to the hypothesis. Thus $A(\sigma_1) = \text{Area}(\rho(w_1))$ and $A(\sigma_2) = \text{Area}(\rho(w_2))$, therefore by induction hypothesis for every corolla c of σ_1 or of σ_2 we have that $A(c) = \eta(c)$. The claim follows from the fact that every corolla of σ is a corolla of σ_1 or of σ_2 . \square

We can now state the Main Theorem of this thesis; we recall that \overline{R} (the set of corollas) has been introduced in Definition 2.2.6, L in Definition 2.4.1,

the function A in Definition 2.4.4 and complete multiset of defining relators in Definition 2.5.1.

Main Theorem 4.1.1 *Let $\langle X | R \rangle$ be a group presentation and let \mathcal{N} be the set of reduced relators. Then \mathcal{N} coincides with the subset of L consisting of reduced words. Let w be the reduced form of $f_1 r_1 f_1^{-1} \cdots f_n r_n f_n^{-1}$, where $r_i \in R$; then there exist a submultiset M of $\{r_1, \dots, r_n\}$ and a straight line algorithm σ computing w which has M as a complete multiset of defining relators (CMDR) and such that $A(\sigma) \leq n$. If $n = \text{Area}(w)$ then $A(\sigma) = n$, every corolla of σ is a proper corolla and $\{r_1, \dots, r_n\}$ is a CMDR for σ . Finally $A(w) = \text{Area}(w)$.*

The Main Theorem implies the following

Corollary 4.1.2 *Let $w \in \mathcal{N}$ and let σ be an SLA computing w and such that $A(\sigma) = A(w)$. Then the area of w is equal to the sum of the areas of the corollas of σ , that is if c_1, \dots, c_m are the corollas of σ then $\text{Area}(w) = \sum_{i=1}^m \text{Area}(c_i)$ and $|w| \geq \sum_{i=1}^m |c_i|$.*

Let $\langle X | R \rangle$ be a group presentation and suppose that there exists a positive real constant α such that $\text{Area}(c) \leq \alpha|c|$ for every proper corolla c . Let w be a relator; by virtue of Corollary 4.1.2 there exist proper corollas c_1, \dots, c_m such that $\text{Area}(w) = \sum_{i=1}^m \text{Area}(c_i)$ and $|w| \geq \sum_{i=1}^m |c_i|$. Therefore

$$\text{Area}(w) = \sum_{i=1}^m \text{Area}(c_i) \leq \sum_{i=1}^m \alpha|c_i| \leq \alpha|w|$$

and $\langle X | R \rangle$ is hyperbolic (Definition 1.3.9). Since the converse is obvious, this proves the following

Corollary 4.1.4 *The presentation $\langle X | R \rangle$ is hyperbolic if and only if there exists a positive real constant α such that $\text{Area}(c) \leq \alpha|c|$ for every proper corolla c .*

Proposition 5.1.10 is stronger than Corollary 4.1.4, anyway the proof of Corollary 4.1.4 is direct and does not use Proposition 5.1.10.

For every natural number n we have set $\Delta_0(n)$ as the maximal area of proper corollas of length at most n (Definition 2.4.6); obviously $\Delta_0(n) \leq \Delta(n)$. By the preceding calculation we have

Corollary 4.1.5 *Let α be a positive real number; then the Dehn function Δ is bounded by the linear function αn if and only if the Δ_0 is.*

To prove the Main Theorem it is sufficient to prove

Lemma 4.1.6 *Let $l := l_1 z z^{-1} l_2$ (where l_1 and l_2 are words and z a letter) be an element of L_g ; then $l_1 l_2 \in L_g$. In particular if σ is a straight line algorithm computing l and if M is a CMDR for σ (Definition 2.5.1), then there exists a straight line algorithm σ' computing $l_1 l_2$, such that $A(\sigma') \leq A(\sigma)$ and such that if M' is a CMDR for σ' then $M' \subset M$. Moreover if $A(\sigma) = \text{Area}(\rho(l))$ then $A(\sigma') = A(\sigma)$ and $M' = M$.*

Let Lemma 4.1.6 be true; take $w \in \mathcal{N}$ and let

$$w = \rho(f_1 r_1 f_1^{-1} \cdots f_n r_n f_n^{-1})$$

where $f_i \in \mathcal{F}(X)$ and $r_i \in R$ for $i = 1, \dots, n$. Since $R \subset \overline{R}$, then the r_i are corollas. Let σ be the SLA consisting in the insertions of r_i into the stem $f_i f_i^{-1}$ at f_i which give $g_i := f_i r_i f_i^{-1}$ and then in the products $g_1 g_2, g_1 g_2 g_3, \dots, g_1 g_2 \cdots g_n$. Its result is $f_1 r_1 f_1^{-1} \cdots f_n r_n f_n^{-1}$, $A(\sigma) = n$ and $\{r_1, \dots, r_n\}$ is a complete multiset of defining relators for σ . w is the reduced form of $f_1 r_1 f_1^{-1} \cdots f_n r_n f_n^{-1}$ and is obtained from the latter by performing all the possible cancellations. By applying repeatedly Lemma 4.1.6, we obtain an L_g -SLA σ' whose result is w , such that $A(\sigma') \leq A(\sigma)$ and such that if M' is a complete multiset of defining relators for σ' then M' is contained in $\{r_1, \dots, r_n\}$. By Proposition A.3.2 it follows that $L = L_g$.

Let $n = \text{Area}(w)$; then $n \leq A(\sigma')$ by Proposition 2.5.3 and since $A(\sigma') \leq A(\sigma) = n$ then $A(\sigma') = n$. Thus we have that $A(w) \leq A(\sigma') = \text{Area}(w)$ and since $\text{Area}(w) \leq A(w)$ by Proposition 2.5.3, this implies that $A(w) = \text{Area}(w)$. By Remark 2.5.2 we have that $|M'| = n$ therefore $M' = \{r_1, \dots, r_n\}$ and $\{r_1, \dots, r_n\}$ is a CMDR for σ' . Finally Lemma 2.5.4 implies that every corolla of σ' is a proper corolla.

Lemma 4.1.6 also implies

Lemma 4.1.7 1. *Let $l \in L$ and let $w \in \mathcal{M}(X \cup X^{-1})$ be such that $\rho(w) = \rho(l)$. Then $w \in L$.*

2. *L contains the cyclic conjugate of any of its elements.*

Proof

1. w is obtained from l by insertions and deletions of words of the form $z z^{-1}$ where $z \in X \cup X^{-1}$. Since $z z^{-1}$ is a stem, if we insert $z z^{-1}$ into an element of L we obtain an element of L ; Lemma 4.1.6 says that if we delete a subword of the form $z z^{-1}$ from an element of L we still have an element of L .

2. Let $l \in L$ and let l' be a cyclic conjugate of l ; then there exist words l_1 and l_2 such that $l = l_1l_2$ and $l' = l_2l_1$. The word $l_1^{-1}l_1l_2l_1$ belongs to L because it is an insertion of l into the stem $l_1^{-1}l_1$. By applying repeatedly Lemma 4.1.6 to $l_1^{-1}l_1l_2l_1$ we have that l_2l_1 belongs to L .

□

Lemma 4.1.7 implies the following interesting result,

Theorem 4.1.8 *L is the subset of $\mathcal{M}(X \cup X^{-1})$ of words whose reduced form belongs to \mathcal{N} , i.e., if $\rho : \mathcal{M}(X \cup X^{-1}) \rightarrow \mathcal{F}(X)$ is the function “reduced form” (Definition 1.1.1) then $L = \rho^{-1}(\mathcal{N})$.*

Proof By Proposition 2.4.3 we have that $L \subset \rho^{-1}(\mathcal{N})$; to prove Theorem 4.1.8 it is sufficient to prove the reverse inclusion. Let $w \in \mathcal{M}(X \cup X^{-1})$ be such that $\rho(w) \in \mathcal{N}$; by Proposition 2.4.2 there exists $l \in L$ such that $\rho(l) = \rho(w)$ and by Part 1 of Lemma 4.1.7, $w \in L$. □

Chapter 3

Preliminary results

In Section 3.1 we show how to associate a 2-cell complex with a straight line algorithm in L . Sections 3.2 and 3.3 introduce useful tools like *stem elements*, *flowers*, *flower elements*, *straight line subalgorithms*, *ramifications* and *surrounds*. These notions, although being technical, have a clear and intuitive interpretation as their names suggest.

3.1 2-cell complexes for straight line algorithms

In this section we show how to associate a 2-cell complex with any L_g -straight line algorithm. For definitions and properties of 2-cell complexes see III of [20]. In this thesis we will consider only 2-complexes equipped with a cycle γ such that for every edge e of the complex either e or e^{-1} are contained in γ . We call γ and its initial vertex respectively *the boundary cycle* and *the initial vertex* of the 2-complex. We will suppose also that these complexes are connected and that every edge is labeled by an element of $X \cup X^{-1}$.

Definition 3.1.1 We say that the *orientation* of a 2-complex is *compatible* with the *orientation* of a face it contains if the boundary cycle of the face is a (non-necessarily contiguous) subpath of the boundary cycle of the 2-complex.

This means in particular that the edges of the boundary of the face are in the same order in the boundary of the 2-complex.

Definition 3.1.2 Given two faces F and F' of a complex, we say that F is *comprised* in F' if all the edges of the boundary cycle of F are comprised

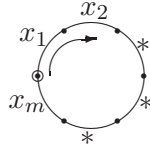
between two consecutive edges of the boundary cycle of F' . The latter is a transitive and antisymmetric relation in the set of faces of a given complex. Consider the reflexive closure [1] of this relation; since it is a finite partial order, by Zorn's lemma [6] there are minimal elements. We call such minimal elements *extremal faces*.

From now on, unless otherwise specified, with the term *straight line algorithm* (or SLA) without other specifications we mean *straight line algorithm* in L_g .

Let σ be an SLA and let s be one of its steps; three cases are possible:

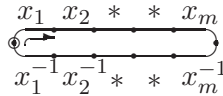
1. s is a corolla; **2.** s is a stem; **3.** there exist two steps s_1 and s_2 preceding s such that s is an insertion of s_2 into s_1 (we recall that we identify a step with its output).

First case: We say that s is a corolla of σ . If s is the empty word then we associate with s a graph consisting of a single vertex. If $s = x_1 \cdots x_m$ then we associate with s the following contractible 2-cell complex



whose edges are labeled consecutively by x_1, x_2, \dots, x_m . The vertex with a circle surrounding it, is the initial vertex. The boundary, whose orientation is determined by the arrow inside it, is a simple cycle.

Second case: We say that s is a stem of σ . If $s = x_1 \cdots x_m x_m^{-1} \cdots x_1^{-1}$ then we associate with s the following contractible 2-cell complex



whose edges are labeled consecutively by $x_1, \dots, x_m, x_m^{-1}, \dots, x_1^{-1}$. The boundary is a simple cycle. The second vertex of the edge labeled by x_m (which coincides with the first vertex of that labeled by x_m^{-1}) is called *vertex in the middle* or *mid-vertex* of the stem.

We use the terms *corolla* and *stem* also for the associated complexes, that is we call *corolla* (or *stem*) a 2-cell whose boundary is a simple cycle labeled by a word of \overline{R} (or of S). This will not cause ambiguity.

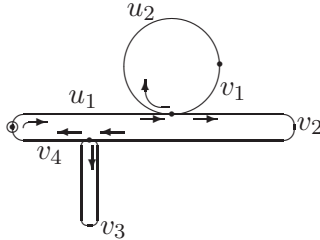
Third case: Let $s_1 := x_1 \cdots x_m$, $s_2 := y_1 \cdots y_p$. Then there exists $n : 1 \leq n \leq m$ such that

$$s = x_1 \cdots x_n y_1 \cdots y_p x_{n+1} \cdots x_m.$$

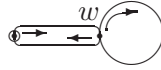
We say that s is the insertion of s_2 into s_1 at the n -th letter or at x_n or at the subword $x_1 \cdots x_n$. Let $i : 1 \leq i \leq n$; we say that the i -th letter of s comes directly from (the i -th letter of) s_1 . Let $i : n + 1 \leq i \leq n + p$; we say that the i -th letter of s comes directly from (the $(i - n)$ -th letter of) s_2 . Let $i : p + n + 1 \leq i \leq p + m$; we say that the i -th letter of s comes directly from (the $(i - p)$ -th letter of) s_1 .

Let \mathcal{C}_1 and \mathcal{C}_2 be the complexes associated with s_1 and s_2 respectively and let v_2 be the initial vertex of \mathcal{C}_2 . Let v_1 be the final vertex of the edge of \mathcal{C}_1 labeled by x_n ; we associate with s the complex obtained by grafting \mathcal{C}_2 into \mathcal{C}_1 at v_2 and v_1 (see [5]), that is the complex $\mathcal{C}_1 \cup_f \mathcal{C}_2$ where f is the function from $\{v_2\}$ to \mathcal{C}_1 such that $f(v_2) = v_1$. This complex is obtained by joining \mathcal{C}_1 to \mathcal{C}_2 in such a way that v_2 coincides with v_1 . The intersection of \mathcal{C}_1 and \mathcal{C}_2 is a single vertex and $\mathcal{C}_1 \cup_f \mathcal{C}_2$ is their union. The initial vertex of $\mathcal{C}_1 \cup_f \mathcal{C}_2$ is the initial vertex of \mathcal{C}_1 , its boundary cycle is the cycle obtained by inserting the boundary cycle of \mathcal{C}_2 into that of \mathcal{C}_1 between the edges labeled by x_n and x_{n+1} .

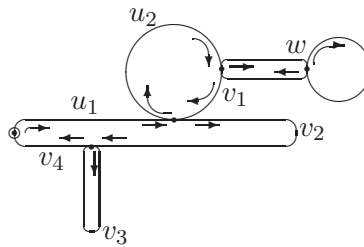
Suppose for instance that we have associated the following labeled complex with s_1



where $u_1, u_2, v_1, \dots, v_4$ are words such that $x_1 \cdots x_n = u_1 u_2$ and $x_{n+1} \cdots x_m = v_1 v_2 v_3 v_4$; and the following one to s_2



where $w = y_1 \cdots y_p$; then we associate with s the following complex



whose label is $u_1 u_2 w v_1 v_2 v_3 v_4 = x_1 \cdots x_n s_2 x_{n+1} \cdots x_m$. We say that the complex of s_2 has been *grafted into the complex of s_1 at the n -th vertex*.

We associate with a straight line algorithm σ the complex that has been associated with its last step.

If a step s depends directly on a step s' , then the output of s' is a subword of the output of s . More generally this is true also if s depends on s' .

Definition 3.1.3 We have defined in the Third case when a letter of a step comes directly from one of another step. We now define in the set of the letters of (the outputs of) the steps of σ , the reflexive transitive closure [1] of the relation “coming directly from” and we call it *relation of coming from*. If a letter x is in that relation with another one x' , then we say that x *comes from x'* . Then x comes from x' if either they are the same letter of the same step or if there is a finite sequence of letters starting with x , ending with x' and such that every letter of the sequence comes directly from the previous one.

If a letter x of a step s comes from a letter x' of s' , then we can say improperly that s *contains s'* .

Remark 3.1.4 If a step s contains a letter of a step s' , then this means that s depends on s' ; therefore s' is a subword of s , that is s contains all the letters of s' .

Definition 3.1.5 We call \mathcal{L} the set of 2-complexes associated with straight line algorithms in the way shown in the three cases above.

Let \mathcal{M} be the set of connected 2-cell complexes whose edges are labeled by elements of $X \cup X^{-1}$ and let \mathcal{B} be the set of stems and corollas. \mathcal{L} is the set of results of SLA's whose universe set is \mathcal{M} , whose base set is \mathcal{B} and whose operation is the *grafting* of complexes as seen in the Third Case. We call SLA's in \mathcal{L} these SLA's.

We have the following result.

Theorem 3.1.6 \mathcal{L} is the set of labeled connected 2-cell complexes

- whose faces are stems or corollas,
- whose orientation is compatible with the orientation of its faces (see Definition 3.1.1),
- in which given an edge e , either e or e^{-1} belong to the boundary of some face.

Proof Let σ be an SLA in \mathcal{L} , let \mathcal{C} be the result of σ and let n be the number of steps of σ . We prove by induction on n that \mathcal{C} has the three properties stated in the thesis of the proposition, being this evident for $n = 1$.

Let $n > 1$ and the claim be true for all the SLA's in \mathcal{L} with less steps than σ . The last step of σ is a grafting of a complex \mathcal{C}_1 into a complex \mathcal{C}_2 at vertices v_1 and v_2 of \mathcal{C}_1 and \mathcal{C}_2 respectively. By induction hypothesis \mathcal{C}_1 and \mathcal{C}_2 verify the properties of the claim. \mathcal{C} is connected because it is the non-disjoint union of two connected complexes; its faces are the faces of \mathcal{C}_1 and those of \mathcal{C}_2 , therefore they are stems and corollas. Let γ'_1 and γ''_1 be paths such that $\gamma_1 = \gamma'_1\gamma''_1$ and the final vertex of γ'_1 is v_1 and let $\gamma = \gamma'_1\gamma_2\gamma''_1$; γ_1 and γ_2 are subpaths of γ . A face of \mathcal{C} is a face of \mathcal{C}_1 or of \mathcal{C}_2 , thus its boundary cycle is a subpath of γ_1 or γ_2 and therefore of γ , thus the orientation of \mathcal{C} is compatible with that of its faces. Finally every edge e of \mathcal{C} is an edge of \mathcal{C}_1 or of \mathcal{C}_2 , therefore either e or e^{-1} are contained in the boundary of a face of \mathcal{C}_1 or \mathcal{C}_2 and thus in the boundary of a face of \mathcal{C} .

We now prove by induction on the number of faces that any complex \mathcal{C} verifying the three properties of the theorem belongs to \mathcal{L} . If \mathcal{C} has only one face then it is a stem or a corolla and thus belongs to \mathcal{L} . Suppose to have proved the claim for any complex with less faces than \mathcal{C} . Remove from \mathcal{C} an extremal face (see Definition 3.1.2) and any edge and vertex belonging to its boundary and not belonging to the boundary of another face. We

obtain a 2-cell complex with less faces than \mathcal{C} , which is still connected, whose faces are also faces of \mathcal{C} (therefore they are stems or corollas) and whose edges are also edges of \mathcal{C} (therefore given an edge e either e or e^{-1} are contained in the boundary of some face). Moreover the boundary cycle of this complex is a subpath of that of \mathcal{C} , therefore its orientation is compatible with the orientation of its faces. Since \mathcal{C}' has less faces than \mathcal{C} , by induction hypothesis \mathcal{C}' belongs to \mathcal{L} . \mathcal{C} is obtained from \mathcal{C}' by adding to it the face, the edges and vertices removed; \mathcal{C} is thus equal to the grafting of an element of \mathcal{L} (with only one face) into \mathcal{C}' and therefore belongs to \mathcal{L} . \square

Proposition 3.1.7 *Let \mathcal{C} be an element of \mathcal{L} . Then*

1. \mathcal{C} is planar and contractible;
2. the boundary cycle of \mathcal{C} has no repeated edges and its only non-simple vertices are the initial vertices of its stems and corollas (except at most the initial vertex of \mathcal{C}).

Proof Let σ be an SLA in \mathcal{L} , let \mathcal{C} be the result of σ and let n be the number of steps of σ . We prove by induction on n that \mathcal{C} being this evident for $n = 1$.

Let $n > 1$ and the claim be true for all the SLA's in \mathcal{L} with less steps than σ . The last step of σ is a grafting of a complex \mathcal{C}_1 into a complex \mathcal{C}_2 at vertices v_1 and v_2 of \mathcal{C}_1 and \mathcal{C}_2 respectively. By induction hypothesis \mathcal{C}_1 and \mathcal{C}_2 verify the properties of the claim.

By 1 of Theorem 3.1.6 the faces of \mathcal{C} are its stems and corollas and they are planar by the First and Second case. Theor. 27 of [27] says that a graph is planar if its unseparable components are; therefore \mathcal{C} is planar since its unseparable components are its stems and corollas. Ex. 23 in Chapter 0 of [18] says that the union of two contractible 2-complexes is contractible if their intersection is contractible, which is the case for \mathcal{C} being equal to the union of \mathcal{C}_1 and \mathcal{C}_2 and being the intersection of the latter equal to a single vertex.

The boundary cycle of \mathcal{C} has no repeated edges because it is the insertion of that of \mathcal{C}_2 into that \mathcal{C}_1 and both have no repeated edges by induction hypothesis.

All the vertices that are non-simple in \mathcal{C}_1 and \mathcal{C}_2 are also non-simple in \mathcal{C} . This means that the initial vertices of the stems and corollas of \mathcal{C} are non-simple, except at most the initial vertices of \mathcal{C}_1 and \mathcal{C}_2 . Since the intersection of \mathcal{C}_1 and \mathcal{C}_2 consists only in the initial vertex of \mathcal{C}_2 , the latter is non-simple and furthermore all the vertices that are simple in \mathcal{C}_1 and \mathcal{C}_2

are still simple in \mathcal{C} . Finally the initial vertex of \mathcal{C}_1 coincides with the initial vertex of \mathcal{C} . \square

Theorem 4.1.8 says that L_g is the set of all relators, reduced and non-reduced. This implies the following

Corollary 4.1.9 *The set of relators (reduced and non) of the presentation $\langle X \mid R \rangle$ coincides with set of labels of elements of \mathcal{L} .*

3.2 Preliminary results I

We recall that *corollas* have been introduced in Definition 2.2.6; the set L_g has been introduced in Definition 2.4.1. The words of the form ww^{-1} (where w is a reduced word) are called *stems* (Definition 2.2.2).

The term SLA without other specifications means SLA *relative to L*. We also recall that a stem or a corolla of an SLA is called a *base element* of that SLA (Definition 2.1.7). The relation of “coming from” for components of outputs was introduced in Definition 3.1.3

Theorem 3.2.1 *Let $l \in L_g$ be computed by σ . Then every component of l comes from a base element of σ .*

Proof Let n be the number of steps of σ ; we prove the claim by induction on n . If $n = 1$ then l is a base element and the claim is evident. Let $n > 1$ and the claim be true for every $n' < n$; l is the insertion of a preceding output l_1 into another one l_2 . Let σ_1 and σ_2 be the pSLsA’s (Definition 2.1.5) computing l_1 and l_2 ; then every component of l comes from l_1 or l_2 and every base element of σ is a base element of σ_1 or of σ_2 . The claim follows from induction hypothesis because σ_1 and σ_2 have less steps than σ . \square

Definition 3.2.2 The result of an SLA whose base elements are all stems is called a *stem element*. The insertion (Definition 2.2.1) of a corolla into a stem ww^{-1} at w is called a *flower*. An insertion of a corolla into a stem element is called a *flower element*.

A stem is a stem element and a flower is a flower element. The function A has been introduced in Definition 2.4.4.

Remark 3.2.3 If s is a stem element then $A(s) = 0$.

The reduced form of a stem element is 1. The converse is proved in the following

Proposition 3.2.4 *Let w be a word whose reduced form is 1. Then w is a stem element.*

Proof Let $w := x_1 \cdots x_m$ where the x_i are letters; we prove the claim by induction on m , being trivial for $m = 2$. Let $m > 2$ and the claim be true for every $m' < m$. Since $x_1 \cdots x_m = 1$ in $\mathcal{F}(X)$, then there exists $i : 1 \leq i \leq m - 1$ such that $x_{i+1} = x_i^{-1}$ (otherwise w would be reduced and different from 1). This implies that $w' := x_1 \cdots x_{i-1} x_{i+2} \cdots x_m$ is equal to 1 in $\mathcal{F}(X)$. By induction hypothesis w' is a stem element and thus there exists a straight line algorithm σ whose base elements are all stems and whose result is w' . If we add to σ a base step equal to the stem $x_i x_{i+1}$ and a step equal to the insertion of $x_i x_{i+1}$ into w' at x_{i-1} , then we have obtained an SLA whose base elements are all stems and whose result is w . \square

We recall that $\rho(w)$ (Definition 1.1.1) denotes the reduced form of w .

Proposition 3.2.5 1. *An insertion of a stem element into another one is still a stem element;*

2. *a cyclic conjugate of a stem element is a stem element;*

3. *the inverse of a stem element is a stem element;*

4. *a cyclic conjugate of a g . corolla is a g . corolla.*

Proof

1. Trivial by virtue of Proposition 3.2.4.

2. Let w be a stem element and let w' be a cyclic conjugate of w . There exist words u and v such that $w = uv$ and $w' = vu$. Since $\rho(w) = 1$ then $\rho(u)\rho(v) = 1$, $\rho(u) = \rho(v)^{-1}$, $\rho(v)\rho(u) = 1$ and finally $\rho(vu) = 1$. Proposition 3.2.4 implies that vu is a stem element.

3. Trivial by Proposition 3.2.4.

4. Trivial because \overline{R} is closed with respect to cyclic conjugation.

\square

Proposition 3.2.6 *Let $w, u, v_1, \dots, v_{m-1} \in L_g$ and let $w := x_1 \cdots x_m, u := u'u''$. Then*

$$w' := u'x_1v_1 \cdots x_{m-1}v_{m-1}x_mu'' \in L.$$

Let $\sigma, \tau, \tau_1, \dots, \tau_{m-1}$ be SLA's computing respectively $w, u, v_1, \dots, v_{m-1}$; then there exists an SLA σ' computing w' such that

$$A(\sigma') = A(\sigma) + A(\tau) + A(\tau_1) + \dots + A(\tau_{m-1}). \quad (3.1)$$

In particular

$$A(w') \leq A(w) + A(u) + A(v_1) + \dots + A(v_{m-1}). \quad (3.2)$$

Finally, if $M, N, N_1, \dots, N_{m-1}$ are CMDR for $\sigma, \tau, \tau_1, \dots, \tau_{m-1}$ respectively (Definition 2.5.1), then $M \cup N \cup N_1 \cup \dots \cup N_{m-1}$ is a CMDR for σ' .

Proof Let $\sigma, \tau, \tau_1, \dots, \tau_{m-1}$ be SLA's computing $w, u, v_1, \dots, v_{m-1}$ respectively. We define σ' as the SLA whose steps are all the steps of $\sigma, \tau, \tau_1, \dots, \tau_{m-1}$, plus the insertions of v_i at x_i for every i and finally the insertion of $x_1 v_1 \dots x_{m-1} v_{m-1} x_m$ into u at u' . σ' computes w' and verifies (3.1). Since $A(w') \leq A(\sigma')$ by Proposition 2.4.4, to prove (3.2) it is sufficient to take $\sigma, \tau, \tau_1, \dots, \tau_{m-1}$ such that $A(\sigma) = A(w), A(\tau) = A(u), A(\tau_1) = A(v_1), \dots, A(\tau_{m-1}) = A(v_{m-1})$. Finally by Remark 2.5.2, the union of $M, N, N_1, \dots, N_{m-1}$ is a CMDR for σ' if the latter are CMDR for $\sigma, \tau, \tau_1, \dots, \tau_{m-1}$ respectively. \square

Corollary 3.2.7 1. Let σ and σ' be SLA's with results w and w' and let v be an insertion of w into w' . Then there exists an SLA σ'' computing v such that $A(\sigma'') = A(\sigma) + A(\sigma')$; in particular $A(v) \leq A(w) + A(w')$. Moreover the union of a CMDR for σ and of one for σ' is a CMDR for σ'' .

2. Let σ be an SLA with result w and let x be a letter. There exists an SLA σ' computing xwx^{-1} and such that $A(\sigma') = A(\sigma)$; in particular $A(xwx^{-1}) \leq A(w)$. Moreover a CMDR for σ is a CMDR for σ' .

Proof Follows from Proposition 3.2.6. \square

Remark 3.2.8 Let f be a flower element which is the insertion of a g . corolla c into a stem element s . By Proposition 3.2.6 we have that $A(f) \leq A(c) + A(s)$ and since $A(s) = 0$ by Remark 3.2.3, then $A(f) \leq A(c)$.

Proposition 3.2.9 Let c and c' be g . corollas and let $cc' = f_1 z z^{-1} f_2$ (where f_1 and f_2 are words and z a letter). Then $f_1 f_2$ belongs to L_g , in particular it is a stem if $c' = c^{-1}$ or it is an insertion of a stem into a reduced flower (i.e., a reduced word which is a flower) whose g . corolla is $\pi(c, c')$. If moreover c and c' are proper g . corollas (Definition 2.4.6) then $A(f_1 f_2) \leq A(c) + A(c')$.

Proof If $c' = c^{-1}$ then cc' is a stem and z is the last letter of c and z^{-1} the first of c' since c and c' are reduced. In this case $c = f_1z$, $c' = z^{-1}f_2$ and f_1f_2 is a stem. Therefore $A(f_1f_2) = 0 \leq A(c) + A(c')$.

Let $c' \neq c^{-1}$; then the reduced product of c by c' is of the form udu^{-1} (which is a reduced flower) where $d := \pi(c, c')$ is their cyclically reduced product; d is a g. corolla because there is cancellation in $\pi(c, c')$. By Definitions 1.1.3 and 1.1.6, cc' is an insertion of the cancelled part aa^{-1} , which is a stem, into udu^{-1} . Since udu^{-1} is reduced, zz^{-1} is a subword of aa^{-1} . In particular since a is reduced then z is the last letter of a and consequently is z^{-1} the first one of a^{-1} . Therefore $a = bz$ for some reduced word b and thus f_1f_2 is the insertion of the stem bb^{-1} into udu^{-1} at the same letter as aa^{-1} is inserted into udu^{-1} to give cc' .

By Proposition 3.2.6 we have that $A(f_1f_2) \leq A(uu^{-1}) + A(bb^{-1}) + A(d)$. Since uu^{-1} and bb^{-1} are stems then $A(uu^{-1}) = A(bb^{-1}) = 0$ by Remark 3.2.3 and $A(f_1f_2) \leq A(d)$. Since $d = \pi(c, c')$, then $A(d) \leq \eta(\pi(c, c'))$ by Remark 2.4.5 and $\eta(\pi(c, c')) \leq \eta(c) + \eta(c')$ by Remark 2.3.2. Thus the inequality $A(f_1f_2) \leq A(c) + A(c')$ follows from the fact that if c and c' are proper g. corollas then $A(c) = \eta(c)$ and $A(c') = \eta(c')$. \square

Lemma 3.2.10 *Let f be an insertion of a stem element into a flower element with g. corolla c and let f' be a cyclic conjugate of f . f' is an insertion of two stem elements (possibly empty) into a flower element with g. corolla a cyclic conjugate of c .*

Proof f is an insertion of a stem element u into a flower element s_1cs_2 , where s_1s_2 is a stem element. Therefore f is

1. either of the form $s'_1us''_1cs_2$, where $s'_1s''_1 = s_1$,
2. or of the form $s_1c_1uc_2s_2$, where $c_1c_2 = c$,
3. or of the form $s_1cs'_2us''_2$, where $s'_2s''_2 = s_2$.

We can suppose that f is of the form $t_1c_1vc_2t_2$ where $c_1c_2 = c$ and t_1t_2 and v are stem elements such that

1. $t_1 = s'_1us''_1$, $t_2 = s_2$ and $v = 1$ in case 1,
2. $t_1 = s_1$, $t_2 = s_2$ and $v = u$ in case 2,
3. $t_1 = s_1$, $t_2 = s'_2us''_2$ and $v = 1$ in case 3.

Since f' is a cyclic conjugate of $f = t_1c_1vc_2t_2$ then f' is

- either of the form $t_1''c_1vc_2t_2t_1'$, where $t_1't_1'' = t_1$,
- or of the form $c_1''vc_2t_2t_1c_1'$, where $c_1'c_1'' = c_1$,
- or of the form $v_2c_2t_2t_1c_1v_1$, where $v_1v_2 = v$,
- or of the form $c_2''t_2t_1c_1vc_2'$, where $c_2'c_2'' = c_2$
- or of the form $t_2''t_1c_1vc_2t_2'$, where $t_2't_2'' = t_2$.

The following are cyclic conjugates of c : c_1c_2 , $c_1''c_2c_1'$, c_2c_1 , $c_2''c_1c_2'$. By Parts 1 and 2 of Proposition 3.2.5, the following are stem elements: $t_1''t_2t_1'$, t_2t_1 , v_2v_1 , $t_2''t_1t_2'$.

Therefore in all the cases f' is either a flower element or an insertion of one or two stem elements into a flower element (a g. corolla is a flower element). The g. corollas of those flower elements are cyclic conjugates of c . \square

Proposition 3.2.11 *Let c and c' be g. corollas, let f be an insertion of c' into c and let $f = f_1zz^{-1}f_2$ (where f_1 and f_2 are words and z a letter). Then f_1f_2 belongs to L_g , in particular it is a stem element if $c' = c^{-1}$ or it is an insertion of a stem element into a flower element with g. corolla a cyclic conjugate of $\pi(d, c')$, where d is a cyclic conjugate of c . If moreover c and c' are proper g. corollas then $A(f_1f_2) \leq A(c) + A(c')$.*

Proof There exist words c_1 and c_2 such that $c = c_1c_2$ and $f = c_1c'c_2$. Let $d = c_2c_1$; then f is a cyclic conjugate of dc' , which is the product of two g. corollas (d is a g. corolla by Part 4 of Proposition 3.2.5). By Definitions 1.1.3 and 1.1.6, dc' is an insertion of the cancelled part aa^{-1} , which is a stem, into the reduced flower $ud'u^{-1}$, where $d' = \pi(d, c')$. By Lemma 3.2.10, f is an insertion of two stem elements into a flower element with g. corolla a cyclic conjugate of d' .

Since $ud'u^{-1}$ is the reduced form of dc' , then either zz^{-1} is a subword of the cancelled part aa^{-1} , or z is the first letter of u and consequently z^{-1} is the last one of u^{-1} . In both cases f_1f_2 is a cyclic conjugate of an insertion of a stem into a flower with g. corolla d' . Therefore by Lemma 3.2.10 it is an insertion of two stem elements into a flower element with g. corolla a cyclic conjugate of d' . Let d'' be that cyclic conjugate. Thus $A(f_1f_2) \leq A(d'')$ by Proposition 3.2.6 and by Remark 3.2.3; $A(d'') \leq \eta(d'')$ by Remark 2.4.5; $\eta(d'') = \eta(d')$ by Remark 2.3.1; $\eta(d') \leq \eta(d) + \eta(c')$ by Remark 2.3.2 and $\eta(d) = \eta(c)$ by Remark 2.3.1. The final inequality follows from the fact that if c and c' are proper g. corollas then $A(c) = \eta(c)$ and $A(c') = \eta(c')$. \square

Remark 3.2.12 Let c and c' be g. corollas and let $c = c_1c_2$ where c_1 and c_2 are words. By virtue of Propositions 3.2.9 and 3.2.11, if f is a word such that $\rho(f) = \rho(cc')$ or $\rho(f) = \rho(c_1c'c_2)$ then either $c' = c^{-1}$ or there exists an SLA computing f and that has only one g. corolla, which we call d , such that $\eta(d) \leq \eta(c) + \eta(c')$. The word d is equal to $\pi(c, c')$ if $\rho(f) = \rho(cc')$ or equal to a cyclic conjugate of $\pi(c_2c_1, c')$ if $\rho(f) = \rho(c_1c'c_2)$.

Let σ_1 be an SLA, let M_1 be its multiset of g. corollas and let c and c' be elements of M . Suppose that $c' = c^{-1}$ and that σ_2 is an SLA such that $M \setminus \{c, c'\}$ is the multiset of g. corollas of σ_2 ¹. Then it is obvious that $A(\sigma_2) < A(\sigma_1)$.

Now suppose that $c' \neq c^{-1}$ and let d as above. Let σ_1 and σ_2 be SLA's, let M_1 and M_2 be respectively their multisets of g. corollas and let c and c' be elements of M_1 . Suppose also that M_1 and M_2 coincide except that in M_2 , c and c' are replaced by d , that is $M_1 \setminus \{c, c'\} = M_2 \setminus \{d\}$. Since $\eta(d) \leq \eta(c) + \eta(c')$, then $A(\sigma_2) \leq A(\sigma_1)$.

We have that $A(\sigma_2) = A(\sigma_1)$ if and only if $\eta(d) = \eta(c) + \eta(c')$. Let τ and τ' be SLA's in \overline{R} computing c and c' respectively and such that $\eta(\tau) = \eta(c)$ and $\eta(\tau') = \eta(c')$. We suppose that $\eta(d) = \eta(c) + \eta(c')$; this implies that there exists an SLA in \overline{R} , which we call τ'' , which computes d and such that $\eta(\tau'') = \eta(d)$. τ'' is constructed in the following way. If d is the g. corolla of cc' then τ'' is as constructed in Remark 2.3.2. If d is the g. corolla of $c_1c'c_2$ then we take all the steps of τ and τ' and we add: the cyclic conjugation from c to c_2c_1 ; the cyclically reduced product of c_2c_1 by c' which we denote d' ; and finally the cyclic conjugation from d' to d . We have that $\eta(\tau'') = \eta(\tau) + \eta(\tau') = \eta(d)$ because a cyclic conjugation does not change the value of η and with a cyclically reduced product the value of η is the sum.

Finally the equality $\eta(d) = \eta(c) + \eta(c')$ implies that a CMDR for σ_1 is a CMDR also for σ_2 , because M_1 and M_2 coincide except that d replaces c and c' in M_2 and because the multiset of base elements of τ'' is the union of those of τ and τ' .

3.3 Preliminary results II

In this section we continue proving results necessary for the proof of the Lemma 4.1.6. We define *straight line subalgorithms*, we introduce the intuitive notions of *ramifications* and *surround* and we prove some technical

¹If $M_1 := (S, \lambda_1)$ then the multiset difference $M \setminus \{c, c'\}$ is the multiset $M_2 := (S, \lambda_2)$ where $\lambda_2(c) = \lambda_1(c) - 1$, $\lambda_2(c') = \lambda_1(c') - 1$ and λ_2 coincides with λ_1 in $S \setminus \{c, c'\}$

lemmas.

Definition 3.3.1 Let σ be an SLA with result w and let s_1 and s_2 be two steps of σ ; since we identify a step with its output, we consider s_1 and s_2 as subwords of w . We say that s_1 *comprises* s_2 if in w all the letters of s_2 are comprised between two consecutive letters of s_1 . We say that s_1 *precedes* s_2 if in w any letter of s_1 precedes any letter of s_2 .

Remark 3.3.2 If s_2 is inserted into s_1 at a letter which is not the last then s_1 comprises s_2 . Consider the reflexive closure of the relation “being comprised in”; it is a partial order equal to that of Definition 3.1.2. Since the set of steps of σ is finite, then by Zorn’s Lemma [6] any step of σ either is minimal or comprises a minimal step. This minimal step is thus a contiguous subword of the given step.

Proposition 3.3.3 *Given two steps of an SLA such that none of them depends on the other, then one of them comprises or precedes the other.*

Proof Let s_1 and s_2 be two steps of an SLA and let t be the first step containing both of them, that is t is the first step such that s_1 and s_2 are subwords of t . We have that t is different from s_1 and s_2 because by hypothesis none of them depends on the other. This means that t is the insertion of a preceding step t_2 into another t_1 with t_2 depending on s_2 and t_1 on s_1 .

If t is the product of t_1 by t_2 , then every letter of t_1 precedes every letter of t_2 , therefore s_1 precedes s_2 . Suppose on the contrary that t is the insertion of t_2 into t_1 at a letter x that is not the last one. Let x' be the last letter of t_1 coming from s_1 and preceding or equal to x . If x' is the last letter of s_1 then it precedes the first one of t_2 and therefore s_1 precedes s_2 . Suppose that x' is not the last letter of s_1 . Let x'' be the first letter of t_1 following x and coming from s_1 ; then all the letters of t_2 (and thus of s_2) are comprised between x' and x'' , that is between two consecutive letters of s_1 and s_1 comprises s_2 . Since the steps following t do not change the relative order of the letters of s_1 and s_2 , we have proved the claim. \square

Remark 3.3.4 We prove that every step of an SLA contains as a contiguous subword a base element which is minimal with respect to the order defined in Remark 3.3.2.

Let σ be an SLA and let s be a step of σ ; s is or comprises a minimal step s' and therefore contains it as a contiguous subword. If this step is a base step the claim is proved; if it is not then any base step used by s' is minimal

because otherwise s' would not be minimal and therefore this minimal base step is a contiguous subword of s' (and therefore of s).

This means that if w is the result of σ and if s is a step of σ , then s is a contiguous subword of w if and only if s is minimal. If w is reduced then no stem of σ is minimal because a stem is not reduced and w cannot have contiguous subwords which are non-reduced. Therefore if w is reduced then there is at least a g. corolla of σ which is a contiguous subword of w .

Let σ be an SLA and let $M := (B, \lambda)$ be its multiset of base elements (Definition 2.1.7). We represent M as the set of pairs (b, k) where $b \in B$ and k is a non-zero natural number less or equal to the multiplicity of b . For instance, if the multiplicity of an element b is 3, then M contains $(b, 1)$, $(b, 2)$, $(b, 3)$ and does not contain (b, k) for $k > 3$. b is called *the underlying element of (b, k)* . Sometimes we will identify the pair (b, k) with b . There is a natural bijection between the base steps of σ and M , given by sending a base step s to (b, k) if s is the k -th step of σ equal to b .

Let σ_1 and σ_2 be two SLA's with multisets of base elements M_1 and M_2 respectively. An *homomorphism of multisets* is an application $\omega : M_1 \rightarrow M_2$ that sends an element of M_1 to an element of M_2 with the same underlying element, for instance sends $(b, 3)$ to $(b, 1)$. Since a base element cannot be at the same time a stem and a g. corolla, an homomorphism sends stems to stems and g. corollas to g. corollas. If ω is injective then for every $b \in B$ the multiplicity of b in σ_1 is less or equal to the multiplicity in σ_2 ; this means in particular that $A(\sigma_1) \leq A(\sigma_2)$ because to every g. corolla of σ_1 corresponds the same g. corolla in σ_2 . If there is an element of B with non-zero multiplicity in σ_1 and zero multiplicity in σ_2 , then no homomorphism can be defined from M_1 to M_2 .

Definition 3.3.5 Let σ_1 and σ_2 be SLA's with results w_1 and w_2 , with multisets of base elements M_1 and M_2 respectively and let $\omega : M_1 \rightarrow M_2$ be an homomorphism. One letter of w_1 and one of w_2 are said to *correspond by ω* if there exists $\mu \in M_1$ such that the two letters come (Definition 3.1.3) from the same letter of μ and $\omega(\mu)$ respectively (we recall that μ and $\omega(\mu)$ have the same underlying element).

We now define a notion of straight line subalgorithm which generalizes that of Remark 2.1.5.

Definition 3.3.6 Let σ_1 and σ_2 be SLA's with results w_1 and w_2 and with multisets of base elements M_1 and M_2 respectively. σ_1 is a *straight line subalgorithm (SLsA)* of σ_2 if w_1 is a (not necessarily contiguous) subword of

w_2 and if there exists an injective homomorphism from M_1 to M_2 such that every letter of w_1 corresponds by ω to the same letter in w_2 (since w_1 is a subword of w_2 , every letter of w_1 is also a letter of w_2). In this case we say that w_1 is a part of w_2 .

A proper straight line subalgorithm (Remark 2.1.5) is a straight line subalgorithm.

Remark 3.3.7 Let σ be an SLA with result w and with multiset of base elements M and let N be a *sub-multiset* of M (denoted $N \subset M$), that is if $M = (B, \lambda)$ then $N = (B, \lambda_0)$ where $\lambda_0(b) \leq \lambda(b)$ for every $b \in B$. There is an SLsA of σ whose result is the subword of w whose letters come from the elements of N ; its multiset of base elements is N . This SLsA and its result are called *the SLsA and the part determined by N* . It is constructed in the following way. If N has only one element, take the SLsA with a single step equal to this element. Let $|N| > 1$ and let the construction be done for every N' with less elements than N . Let ν be an element minimal in N with respect to the order of Definition 3.3.1 and let $N' = N \setminus \{\nu\}$, that is $N' = (B, \lambda')$ where $\lambda'(\nu) = \lambda_0(\nu) - 1$ and λ' coincide with λ_0 on $B \setminus \{\nu\}$. Let τ' be the SLsA of σ defined by N' and let f' be its result. Let f be the subword of w whose letters come from elements of N . Since ν is minimal, there exist words f'_1 and f'_2 such that $f = f'_1 \nu f'_2$ and $f' = f'_1 f'_2$. If we add to τ' a base step equal to ν and another one equal to the insertion of ν into f' at f'_1 , then we have constructed an SLsA with result f and with multiset of base elements equal to N .

Definition 3.3.8 Let σ_1 and σ_2 be SLA's with results w_1 and w_2 and with multisets of base elements M_1 and M_2 respectively and suppose given an homomorphism ω from M_1 to M_2 . Let $N_1 \subset M_1$ and let f_1 be the part of w_1 determined by N_1 (Remark 3.3.7). Let $N_2 := \omega(N_1)$ and let f_2 be the part of w_2 determined by N_2 . We say that f_1 *corresponds to f_2 by ω* .

Definition 3.3.9 Let σ be an SLA with result $w := x_1 \cdots x_m$, let s be a step² of σ and let x_i and x_k (with $i < k$) be letters of w coming from two consecutive letters of s . The subword $x_{i+1} \cdots x_{k-1}$ is called *a ramification from s* . Let x_f and x_l be letters of w coming respectively from the first and the last letters of s ; the subword $x_1 \cdots x_{f-1} x_{l+1} \cdots x_m$ is called *the surround of s* . $x_1 \cdots x_{f-1}$ is called *the preceding of s* and $x_{l+1} \cdots x_m$ *the following of s* .

²in particular, since we identify a step with its output, s is a not necessarily contiguous subword of w .

Remark 3.3.10 Given two steps s and s' of an SLA, we have that s comprises s' (Remark 3.3.2) if and only if s' is contained in a ramification from s , if and only if the surround of s' contains s ; s precedes s' if and only if the following of s contains s' , if and only if the preceding of s' contains s .

Proposition 3.3.11 *Let σ be an SLA and let s and s' be steps of σ such that none of them depends on the other. Then*

1. *if a ramification from s contains a letter of s' then it contains all the letters of s' ;*
2. *if the surround of s contains a letter of s' then it contains all the letters of s' .*

Proof It is a consequence of Proposition 3.3.3 in view of Remark 3.3.10. If a ramification from s contains a letter of s' then it is not possible that s precedes s' , nor that s' precedes s , nor that s' comprises s . Thus s comprises s' , that is all the letters of s' are contained in the given ramification from s . Since two different ramifications have no letters in common then Part 1 is proved.

If the surround of s contains a letter of s' then it is not possible that s comprises s' , nor that s precedes s' . If s' comprises s then by Remark 3.3.10 the surround of s contains s' ; if s' precedes s then the preceding of s (and therefore its surround) contains s' . \square

Proposition 3.3.12 *Let σ be an SLA whose result is w and let s be a step of σ . The surround of s and any ramification from s are parts of w .*

Proof Let q be the surround of s ; we have to prove that there exists an SLsA of σ computing q . Let M be the multiset of base elements of σ and let N be the sub-multiset of M of the elements which have at least one letter contained in q ; let f be the result of the SLsA defined by N (Remark 3.3.7). f is a part of w and contains q as a subword. Vice versa we prove that q contains f as a subword. Let s' be a base step which has at least one letter in common with q . s' does not use s because a base step does not any step; s does not use s' because otherwise s' must be a subword of s and instead at least one letter of s' is contained in q (which has no letters in common with s). Therefore by Proposition 3.3.11 q contains every base element with which it has at least a letter in common; thus $q = f$.

Analogously we do for a ramification. \square

Definition 3.3.13 Let $\tau, \tau_0, \tau_1, \dots, \tau_{m-1}$ be SLA's with results respectively the words $w, q, r_1, \dots, r_{m-1}$. Let $w := x_1 \cdots x_m$ and $q := q_0 q_1$ (with the x_i letters and q_0 and q_1 words) and let ι_0 be the insertion of w into q at q_0 ; its result is $w_0 := q_0 w q_1$. Let ι_1 be the insertion of r_1 into w_0 at x_1 ; its result is $w_1 := q_0 x_1 r_1 x_2 \cdots x_m q_1$. \dots Let ι_{m-1} be the insertion of r_{m-1} into w_{m-2} at x_{m-1} ; its result is $q_0 x_1 r_1 \cdots x_{m-1} r_{m-1} x_m q_1$.

Then $\sigma := (\tau, \tau_0, \iota_0, \tau_1, \iota_1, \dots, \tau_{m-1}, \iota_{m-1})$ is an SLA, τ is a pSLsA computing w , q is the surround of w and r_1, \dots, r_{m-1} are the ramifications from w .

We say that σ defines consecutively the insertions into w and that $\tau_0, \tau_1, \dots, \tau_{m-1}$ are the pSLsA's of σ which compute respectively the surround and the ramifications from w .

Given an SLA σ and given a step s , we want to prove that there exists an SLA "equivalent" to σ (in a sense that we are going to specify) which defines consecutively the insertions into s .

Definition 3.3.14 If σ and σ' are SLA's such that any of the two is an SLsA of the other (Definition 3.3.6), then we say that σ and σ' are equivalent.

Remark 3.3.15 Let σ_1 and σ_2 be SLA's with multisets of base elements M_1 and M_2 respectively. Then σ_1 and σ_2 are equivalent if and only if their results are equal (let w be their result) and there exists an isomorphism $\omega : M_1 \rightarrow M_2$ such that any letter of w corresponds (Definition 3.3.5) to itself by ω . If σ and σ' are equivalent then $A(\sigma) = A(\sigma')$.

Proposition 3.3.16 Let σ be an SLA and let s be one of its steps. Then there exists an SLA σ' equivalent to σ and defining consecutively the insertions into the step of σ' corresponding to s (Definition 3.3.8).

Proof Let $s := x_1 \cdots x_m$. By Proposition 3.3.12 there exist SLsA's $\tau_0, \tau_1, \dots, \tau_{m-1}$ computing respectively the surround q and the ramifications r_1, \dots, r_{m-1} from s .

We define the insertions $\iota_0, \iota_1, \dots, \iota_{m-1}$ in the following way. ι_0 is the insertion of s into q at q_0 , where q_0 is the preceding of s ; call w_0 its result. We have that $w_0 = q_0 s q_1$ where q_1 is the following of s . We define recursively ι_j for $j = 1, \dots, m-1$ as the insertion of r_j into w_{j-1} at x_j .

Let τ be an SLA computing s . Then $\sigma' := (\tau, \tau_0, \iota_0, \tau_1, \iota_1, \dots, \tau_{m-1}, \iota_{m-1})$ is an SLA, its result is the same of σ and there is an evident isomorphism between its multiset of base elements and that of σ . Moreover σ' defines consecutively the insertions into s . \square

Lemma 3.3.17 *Let σ be an SLA whose result is $w := x_1 \cdots x_m$, let $s := y_1 \cdots y_p y_p^{-1} \cdots y_1^{-1}$ be a stem of σ , let h and h' be indices such that $x_h = y_n$ and $x_{h'} = y_n^{-1}$ for some $n : 1 \leq n \leq p$. Then there exist two SLA's σ_1 and σ_2 computing respectively*

$$x_1 \cdots x_{h-1} x_{h'+1} \cdots x_m \quad \text{and} \quad x_{h+1} \cdots x_{h'-1}$$

and such that $A(\sigma_1) + A(\sigma_2) = A(\sigma)$. Moreover the union of a CMDR for σ_1 and of one for σ_2 is a CMDR for σ .

Proof By Proposition 3.3.16 we can suppose that σ defines consecutively the insertions into s . Let q_0 and q_1 be the preceding and the following of s and let τ be the SLsA computing the surround $q := q_0 q_1$. Let r_1, \dots, r_p be the ramifications from s at y_1, \dots, y_p respectively and r'_2, \dots, r'_p the ones at $y_2^{-1}, \dots, y_p^{-1}$. Let τ_1, \dots, τ_p and τ'_2, \dots, τ'_p be the SLsA's computing them. This means that

$$w = q_0 \mathbf{y}_1 r_1 \mathbf{y}_2 \cdots \mathbf{y}_p r_p \mathbf{y}_p^{-1} r'_p \cdots \mathbf{y}_2^{-1} r'_2 \mathbf{y}_1^{-1} q_1.$$

(we write in bold the letters y_i). Set

$$s_1 := y_1 \cdots y_{n-1} y_{n-1}^{-1} \cdots y_1^{-1} \quad \text{and} \quad s_2 := y_{n+1} \cdots y_p y_p^{-1} \cdots y_{n+1}^{-1}.$$

s_1 and s_2 are stems. Set

$$\sigma_1 := (s_1, \tau, \tau_1, \dots, \tau_{n-1}, \tau'_2, \dots, \tau'_n, \iota_0, \iota_1, \dots, \iota_{n-1}, \iota'_2, \dots, \iota'_n)$$

and

$$\sigma_2 := (s_2, \tau_n, \dots, \tau_p, \tau'_{n+1}, \dots, \tau'_p, \iota_n, \dots, \iota_p, \iota'_{n+1}, \dots, \iota'_p),$$

where ι_0 is the insertion of s_1 into q at q_0 and for $j \neq 1$, ι_j and ι'_j are the insertions of r_j and of r'_j at y_j and y_j^{-1} respectively. The results of σ_1 and σ_2 are

$$w_1 := q_0 \mathbf{y}_1 r_1 \cdots \mathbf{y}_{n-1} r_{n-1} r'_n \mathbf{y}_{n-1}^{-1} r'_{n-1} \cdots \mathbf{y}_2^{-1} r'_2 \mathbf{y}_1^{-1} q_1$$

and

$$w_2 := r_n \mathbf{y}_{n+1} r_{n+1} \cdots \mathbf{y}_p r_p \mathbf{y}_p^{-1} r'_p \cdots \mathbf{y}_{n+1}^{-1} r'_{n+1}$$

respectively and $w_1 = x_1 \cdots x_{h-1} x_{h'+1} \cdots x_m$, $w_2 = x_{h+1} \cdots x_{h'-1}$. Finally, the equality $A(\sigma_1) + A(\sigma_2) = A(\sigma)$ and the last claim follow from Remark 2.5.2. \square

Lemma 3.3.18 *Let σ be an SLA and let $w := x_1 \cdots x_m$ be its result. If the first [respectively the last] letter of w comes (Definition 3.1.3) from a g. corolla of σ , then there exists an SLA σ' whose result is $x_2 \cdots x_m x_1$ [respectively $x_m x_1 \cdots x_{m-1}$], such that $A(\sigma') = A(\sigma)$ and such that a CMDR for σ is a CMDR also for σ' .*

Proof Let $c := y_1 \cdots y_p$ be the g. corolla from which comes x_1 [respectively x_m]. By Proposition 3.3.16 we can suppose that σ defines consecutively the insertions into c . Since $x_1 = y_1$ [respectively $x_m = y_p$] then the preceding [respectively the following] of c is empty, therefore w is equal to $\mathbf{y}_1 r_1 \cdots r_{p-1} \mathbf{y}_p q$ [respectively to $q \mathbf{y}_1 r_1 \cdots r_{p-1} \mathbf{y}_p$] where q is the surround and the r_j are the ramifications from c . This means that σ is of the form

$$(c, \tau, \iota, \tau_1, \iota_1, \cdots, \tau_{p-1}, \iota_{p-1})$$

where τ computes q , τ_j computes r_j , ι is the product cq [respectively the product qc] and ι_j is the insertion of r_j at y_j .

Set $d := y_2 \cdots y_p y_1$ [respectively $d := y_p y_1 \cdots y_{p-1}$] and

$$\sigma' := (d, \tau, \tau_1, \iota', \iota'_1, \tau_2, \iota_2, \cdots, \tau_{p-1}, \iota_{p-1})$$

where ι' is the product $r_1 d$ [respectively $\iota' = \iota_1$] and ι'_1 is the insertion of q at y_p . σ' is an SLA whose result is $x_2 \cdots x_m x_1$ [respectively $x_m x_1 \cdots x_{m-1}$].

The g. corollas of σ and those of σ' coincide except that d takes the place of c in σ' ; that is, the multiplicity of d in the multiset of g. corollas of σ' is greater by one than that in σ (consequently the multiplicity of c is less by one in σ' than in σ). This implies that $A(\sigma') = A(\sigma)$ because $\eta(c) = \eta(d)$ by Remark 2.3.1. Moreover if τ is an SLA in \overline{R} computing c and such that $\eta(\tau) = \eta(c)$ then if we add to τ a step equal to the cyclic conjugation of c (which gives d), we obtain an SLA (which we call τ') computing d , such that $\eta(d) = \eta(\tau')$ and such that the multiset of base elements of τ coincides with that of τ' . This implies that a CMDR for σ is a CMDR also for σ' . \square

Chapter 4

The Main Theorem

In this chapter we prove the Main Theorem of the thesis. The proof is split in two parts, the first part in Section 4.1 in a specific case and the second part in Section 4.2 in the general case.

4.1 The proof of the Main Theorem: a case by case analysis

Let X be a set of letters, let X^{-1} be the set of inverses of elements of X and let R be a set of cyclically reduced non-empty words in $X \cup X^{-1}$ such that $R^{-1} \subset R$. Let $\mathcal{M}(X \cup X^{-1})$ be the free monoid on $X \cup X^{-1}$ and let L_g (Definition 2.4.1) be the subset of $\mathcal{M}(X \cup X^{-1})$ recursively defined by g. corollas and stems and by the operation of insertion. Let $\mathcal{F}(X)$ be the free group on X and let \mathcal{N} be the normal closure of R in $\mathcal{F}(X)$; in particular \mathcal{N} is the set of (reduced) relators of the group presentation $\langle X \mid R \rangle$. Let the functions Area and A as in Definitions 1.1.8 and 2.4.4. Complete multisets of defining relators have been introduced in Definition 2.5.1.

In this section and in the next we will show that the following result holds

Theorem 4.1.1 *Let $\langle X \mid R \rangle$ be a group presentation and let \mathcal{N} be the set of reduced relators. Then \mathcal{N} coincides with the subset of L consisting of reduced words. Let w be the reduced form of $f_1 r_1 f_1^{-1} \cdots f_n r_n f_n^{-1}$, where $r_i \in R$; then there exist a submultiset M of $\{r_1, \dots, r_n\}$ and a straight line algorithm σ computing w which has M as a complete multiset of defining relators (CMDR) and such that $A(\sigma) \leq n$. If $n = \text{Area}(w)$ then $A(\sigma) = n$,*

every corolla of σ is a proper corolla and $\{r_1, \dots, r_n\}$ is a CMDR for σ . Finally $A(w) = \text{Area}(w)$.

The equality $\text{Area}(w) = A(w)$ is very interesting because it gives an alternative way to define the area of a relator and therefore the Dehn function of a presentation.

Theorem 4.1.1 implies the following

Corollary 4.1.2 *Let $w \in \mathcal{N}$ and let σ be an SLA computing w and such that $A(\sigma) = A(w)$. Then the area of w is equal to the sum of the areas of the g . corollas of σ , that is if c_1, \dots, c_m are the g . corollas of σ then $\text{Area}(w) = \sum_{i=1}^m \text{Area}(c_i)$ and $|w| \geq \sum_{i=1}^m |c_i|$.*

We have seen in Remark 3.3.4 that any reduced element of L_g has a contiguous subword equal to a proper g . corolla. By Definition 2.4.6 and Theorem 4.1.1 we have that if c is a proper g . corolla then $\eta(c) = \text{Area}(c)$. If $m = \text{Area}(c)$ then $c \in \overline{R}_m$; if R is finite then \overline{R}_m is finite by Theorem 2.3.12. Thus we have

Corollary 4.1.3 *A relator of area m has a contiguous subword equal to a proper g . corolla whose area is less or equal to m . If the presentation is finite then there are finitely many of such proper g . corollas.*

In Section 2.5 we have given the proof of

Corollary 4.1.4 *The presentation $\langle X | R \rangle$ is hyperbolic (Definition 1.3.9) if and only if there exists a positive real constant α such that $\text{Area}(c) \leq \alpha|c|$ for every proper g . corolla c .*

Corollary 4.1.4 says that to verify if a group is hyperbolic it is sufficient to verify the inequality $\text{Area}(w) \leq \alpha|w|$ only on proper g . corollas instead of all relators. This is a very interesting result because the set of g . corollas is a proper subset of the set of all relators, in particular it contains only cyclically reduced words.

For every n let $\Delta_0(n)$ be the maximal area of proper g . corollas of length at most n ; obviously $\Delta_0(n) \leq \Delta(n)$. In Section 2.5 we have proved

Corollary 4.1.5 *Let α be a positive real number; the Dehn function Δ is bounded by the linear function αn if and only if the Δ_0 is.*

As we have seen in Section 2.5, to prove the Main Theorem 4.1.1 it is sufficient proving the following

Lemma 4.1.6 *Let $l := l_1 z z^{-1} l_2$ (where l_1 and l_2 are words and z a letter) be an element of L_g ; then $l_1 l_2 \in L_g$. In particular if σ is a straight line algorithm computing l and if M is a CMDR for σ (Definition 2.5.1), then there exists a straight line algorithm σ' computing $l_1 l_2$, such that $A(\sigma') \leq A(\sigma)$ and such that if M' is a CMDR for σ' then $M' \subset M$. Moreover if $A(\sigma) = \text{Area}(\rho(l))$ then $A(\sigma') = A(\sigma)$ and $M' = M$.*

Lemma 4.1.6 is proved in this and in the following sections. Lemma 4.1.6 implies

Lemma 4.1.7 *1. Let $l \in L$ and let $w \in \mathcal{M}(X \cup X^{-1})$ be such that $\rho(w) = \rho(l)$. Then $w \in L$.*

2. L contains the cyclic conjugate of any of its elements.

Finally Lemma 4.1.7 implies the following interesting result

Theorem 4.1.8 *L is the subset of $\mathcal{M}(X \cup X^{-1})$ of words whose reduced form belongs to \mathcal{N} , i.e., if $\rho : \mathcal{M}(X \cup X^{-1}) \rightarrow \mathcal{F}(X)$ is the function “reduced form” (Definition 1.1.1) then $L = \rho^{-1}(\mathcal{N})$.*

Lemma 4.1.7 and Theorem 4.1.8 have been proved in Section 2.5 having assumed that Lemma 4.1.6 is true. Theorem 4.1.8 says in particular that L_g is the set of all relators (reduced and non). In Section 2.5 we have proved the following

Corollary 4.1.9 *The set of relators (reduced and non) of the presentation $\langle X | R \rangle$ coincides with the set of labels of the elements of \mathcal{L} (Definition 3.1.5).*

In this section we will prove Lemma 4.1.6 under the following hypothesis: **the only output of σ containing the subword $z z^{-1}$ of $l_1 z z^{-1} l_2$ is the last one.** We fix the notation until the end of Subsection 4.1.3: l will denote the result of σ ; $t := x_1 \cdots x_m$ and $t' := y_1 \cdots y_p$ will denote the steps of σ such that l is the insertion of t' into t ; τ and τ' will denote the pSLsA's of σ computing t and t' respectively. By Remark 2.5.2 we have that $A(\sigma) = A(\tau) + A(\tau')$.

By the hypothesis assumed for this section, the letters z and z^{-1} of $z z^{-1}$ do not come both from t or t' ; therefore since l contains $z z^{-1}$ and since l is the insertion of t' into t , then z comes from t and z^{-1} from t' or vice versa z comes from t' and z^{-1} from t . Furthermore the insertion of t' into t makes z and z^{-1} consecutive. This means that there exists $n : 1 \leq n \leq m$ such that $l = x_1 \cdots x_n y_1 \cdots y_p x_{n+1} \cdots x_m$ and:

- either $x_n = z$ and $y_1 = z^{-1}$ (we call it *subcase* α);
- or $y_p = z$ and $x_{n+1} = z^{-1}$ (we call it *subcase* β).

Until the end of the Subsection 4.1.3 we also denote s and s' the base steps of σ such that one of them contains the letter z of zz^{-1} and the other one contains z^{-1} and such that t depends on s , t' depends on s' . In the subcase α , s contains z and s' contains z^{-1} ; in the subcase β , s' contains z and s contains z^{-1} . We can assume that $s \neq s'$ because $s = s'$ implies that s contains zz^{-1} , therefore s is the last step of σ in view of our hypothesis. Since s is a base step, it cannot use preceding steps and this means that s is the only step of σ . s cannot be a g. corolla because it contains zz^{-1} as a subword and g. corollas are reduced. Indeed s would be a stem and z would be the last letter of its first half (z^{-1} would be the first letter of the second half.) For this situation Lemma 4.1.6 is trivially true.

Four cases are then possible: I) s and s' are stems; II) s is a stem and s' a g. corolla; III) s is a g. corolla and s' a stem; IV) s and s' are g. corollas.

Let s be a stem (Cases I and II); since s is the product of a word by its inverse and since s contains either the letter z or the letter z^{-1} of zz^{-1} , then two of its opposite letters (and therefore two letters of t) are equal to z and z^{-1} , one (and only one) of which is of the subword zz^{-1} of $l_1zz^{-1}l_2$. We let $h, h' : 1 \leq h < h' \leq m$ be such that x_h and $x_{h'}$ are those letters of t , that is $\{x_h, x_{h'}\} = \{z, z^{-1}\}$. We call *subcase* 1 when $x_h = z$ and $x_{h'} = z^{-1}$, we call *subcase* 2 when $x_h = z^{-1}$ and $x_{h'} = z$. Therefore in the subcase 1 α we have $n = h$ and $x_{h'} = y_1 = z^{-1}$; in the subcase 1 β we have $n + 1 = h'$ and $x_h = y_p = z$; in the subcase 2 α we have $n = h'$ and $x_h = y_1 = z^{-1}$; in the subcase 2 β we have $n + 1 = h$ and $x_{h'} = y_p = z$.

Finally we let $j, j' : 1 \leq j < j' \leq p$ be such that the letters y_j and $y_{j'}$ of t' are equal respectively to the first and the last letter of s' . In the subcase α we have $j = 1$ and therefore $y_1 = z^{-1}$; in the subcase β we have $j' = p$ and $y_p = z$. If s' is a stem (Cases I and III) then in the subcase α we have $y_{j'} = z$, in the subcase β we have $y_j = z^{-1}$.

We recall that we have denoted τ the proper straight line subalgorithm of σ computing t .

Lemma 4.1.10 *Let s be a stem (Cases I and II) and let v_1, v_2 and v be the following subwords of t :*

$$v_1 = x_1 \cdots x_{h-1}, \quad v_2 = x_{h'+1} \cdots x_m, \quad v = x_{h+1} \cdots x_{h'-1}.$$

There exist two SLA's of σ , denoted σ_1 and σ_2 , which compute v_1v_2 and v

respectively and such that $A(\sigma_1) + A(\sigma_2) = A(\tau)$. Moreover the union of a CMDR for σ_1 and of one of σ_2 is a CMDR for τ .

Proof Follows from Lemma 3.3.17. \square

We recall that we have denoted τ' the proper straight line subalgorithm of σ computing t' .

Lemma 4.1.11 *Let s' be a stem (Cases I and III) and let w_1, w_2, w'_1 and w'_2 be the following subwords of t' :*

$$w_1 = y_1 \cdots y_{j-1}, \quad w_2 = y_{j+1} \cdots y_{p-1}, \quad w'_1 = y_2 \cdots y_{j'-1}, \quad w'_2 = y_{j'+1} \cdots y_p.$$

There exist two SLA's of σ , denoted τ_1 and τ_2 , such that:

1. *in the subcase α , τ_1 and τ_2 compute w'_1 and w'_2 respectively and $A(\tau_1) + A(\tau_2) = A(\tau')$;*
2. *in the subcase β , τ_1 and τ_2 compute w_1 and w_2 respectively and $A(\tau_1) + A(\tau_2) = A(\tau')$.*

Finally the union of a CMDR for τ_1 and of one for τ_2 is a CMDR for τ .

Proof

1. Follows from Lemma 3.3.17 because in the subcase α , $y_1 = z^{-1}$ and $y_{j'} = z$.
2. Follows from Lemma 3.3.17 because in the subcase β , $y_j = z^{-1}$ and $y_p = z$.

\square

Remark 4.1.12 Let σ' be an SLA computing $l_1 l_2$ and such that $A(\sigma') \leq A(\sigma)$ and let $A(\sigma) = \text{Area}(\rho(l))$. We have that $\text{Area}(\rho(l)) = \text{Area}(\rho(l_1 l_2))$ since $\rho(l) = \rho(l_1 l_2)$ and $\text{Area}(\rho(l_1 l_2)) \leq A(\sigma')$ by Proposition 2.5.3. These inequalities imply that $A(\sigma') = A(\sigma)$.

4.1.1 Case I

s and s' are stems. As in Lemmas 4.1.10 and 4.1.11 we let $v_1 = x_1 \cdots x_{h-1}$, $v_2 = x_{h'+1} \cdots x_m$, $v = x_{h+1} \cdots x_{h'-1}$, $w_1 = y_1 \cdots y_{j-1}$, $w_2 = y_{j+1} \cdots y_{p-1}$, $w'_1 = y_2 \cdots y_{j'-1}$ and $w'_2 = y_{j'+1} \cdots y_p$.

Remark 4.1.13 By Lemmas 4.1.10 and 4.1.11 there exist SLA's σ_1 and σ_2 computing $v_1 v_2$ and v and SLA's τ_1 and τ_2 computing w'_1 and w'_2 in the subcase α , w_1 and w_2 in the subcase β , such that $A(\tau) = A(\sigma_1) + A(\sigma_2)$ and $A(\tau') = A(\tau_1) + A(\tau_2)$. Furthermore, since $A(\tau) + A(\tau') = A(\sigma)$ by Remark 2.5.2, then

$$A(\sigma_1) + A(\sigma_2) + A(\tau_1) + A(\tau_2) = A(\sigma).$$

Finally the union of CMDR's for $\sigma_1, \sigma_2, \tau_1$ and τ_2 is a CMDR for σ .

Subcase 1 α . We have $n = h$, $x_h = y_{j'} = z$ and $x_{h'} = y_1 = z^{-1}$. Therefore

$$l = x_1 \cdots x_{h-1} z (z^{-1} y_2 \cdots y_{j'-1} z y_{j'+1} \cdots y_p) x_{h+1} \cdots x_{h'-1} z^{-1} x_{h'+1} \cdots x_m = \\ v_1 z (z^{-1} w'_1 z w'_2) v z^{-1} v_2$$

and $l_1 = v_1$, $l_2 = w'_1 z w'_2 v z^{-1} v_2$. By Remark 4.1.13, Proposition 3.2.6 and Part 2 of Corollary 3.2.7 there exists an SLA σ' computing

$$v_1 w'_1 z w'_2 v z^{-1} v_2 = l_1 l_2$$

such that $A(\sigma') = A(\sigma_1) + A(\sigma_2) + A(\tau_1) + A(\tau_2) = A(\sigma)$ and such that a CMDR for σ is a CMDR also for σ' .

Subcase 1 β . We have that $n + 1 = h'$, that $x_h = y_p = z$ and that $x_{h'} = y_j = z^{-1}$. Therefore

$$l = x_1 \cdots x_{h-1} z x_{h+1} \cdots x_{h'-1} (y_1 \cdots y_{j-1} z^{-1} y_{j+1} \cdots y_{p-1} z) z^{-1} x_{h'+1} \cdots x_m = \\ v_1 z v (w_1 z^{-1} w_2 z) z^{-1} v_2$$

and $l_1 = v_1 z v w_1 z^{-1} w_2$, $l_2 = v_2$. By Remark 4.1.13, Proposition 3.2.6 and Part 2 of Corollary 3.2.7 there exists an SLA σ' computing

$$v_1 z v w_1 z^{-1} w_2 v_2 = l_1 l_2$$

such that $A(\sigma') = A(\sigma_1) + A(\sigma_2) + A(\tau_1) + A(\tau_2) = A(\sigma)$ and such that a CMDR for σ is a CMDR also for σ' .

Subcase 2 α . We have that $n = h'$, that $x_{h'} = y_{j'} = z$ and that $x_h = y_1 = z^{-1}$. Therefore

$$l = x_1 \cdots x_{h-1} z^{-1} x_{h+1} \cdots x_{h'-1} z (z^{-1} y_2 \cdots y_{j'-1} z y_{j'+1} \cdots y_p) x_{h'+1} \cdots x_m =$$

$$v_1 z^{-1} v z (z^{-1} w'_1 z w'_2) v_2$$

and $l_1 = v_1 z^{-1} v$, $l_2 = w'_1 z w'_2 v_2$. By Remark 4.1.13, Proposition 3.2.6 and Part 2 of Corollary 3.2.7 there exists an SLA σ' computing

$$v_1 z^{-1} v w'_1 z w'_2 v_2 = l_1 l_2$$

such that $A(\sigma') = A(\sigma_1) + A(\sigma_2) + A(\tau_1) + A(\tau_2) = A(\sigma)$ and such that a CMDR for σ is a CMDR also for σ' .

Subcase 2 β . We have that $n + 1 = h$, that $x_{h'} = y_p = z$ and that $x_h = y_j = z^{-1}$. Therefore

$$l = x_1 \cdots x_{h-1} (y_1 \cdots y_{j-1} z^{-1} y_{j+1} \cdots y_{p-1} z) z^{-1} x_{h+1} \cdots x_{h'-1} z x_{h'+1} \cdots x_m = \\ v_1 w_1 z^{-1} w_2 z z^{-1} v z v_2$$

and $l_1 = v_1 w_1 z^{-1} w_2$, $l_2 = v z v_2$. By Remark 4.1.13, Proposition 3.2.6 and Part 2 of Corollary 3.2.7 there exists an SLA σ' computing

$$v_1 w_1 z^{-1} w_2 v z v_2 = l_1 l_2$$

such that $A(\sigma') = A(\sigma_1) + A(\sigma_2) + A(\tau_1) + A(\tau_2) = A(\sigma)$ and such that a CMDR for σ is a CMDR also for σ' .

4.1.2 Case II

s is a stem and s' a g. corolla. As in Lemmas 4.1.10 and 4.1.11 we let $v_1 = x_1 \cdots x_{h-1}$, $v_2 = x_{h'+1} \cdots x_m$, $v = x_{h+1} \cdots x_{h'-1}$, $w_1 = y_1 \cdots y_{j-1}$, $w_2 = y_{j+1} \cdots y_{p-1}$, $w'_1 = y_2 \cdots y_{j'-1}$ and $w'_2 = y_{j'+1} \cdots y_p$.

Remark 4.1.14 Set $u := y_1 \cdots y_{p-1}$ and $u' := y_2 \cdots y_p$. In the subcase α we have $t' = z^{-1} u'$ and the first letter of t' comes from s' ; in the subcase β we have $t' = u z$ and the last letter of t' comes from s' . By Lemma 3.3.18 there exists an SLA τ'_1 computing $u' z^{-1}$ in the subcase α , computing $z u$ in the subcase β such that $A(\tau'_1) = A(\tau')$ and a CMDR for τ' is a CMDR also for τ'_1 .

By Lemma 4.1.10 there exist SLA's σ_1 and σ_2 computing $v_1 v_2$ and v and such that $A(\sigma_1) + A(\sigma_2) = A(\tau)$. Furthermore, since $A(\tau) + A(\tau') = A(\sigma)$ by Remark 2.5.2, then

$$A(\sigma_1) + A(\sigma_2) + A(\tau'_1) = A(\sigma).$$

Finally the union of CMDR's for σ_1, σ_2 and τ'_1 is a CMDR for σ .

Subcase 1 α . We have that $n = h$, that $x_h = z$ and that $x_{h'} = y_1 = z^{-1}$. Therefore

$$l = x_1 \cdots x_{h-1} z (z^{-1} y_2 \cdots y_p) x_{h+1} \cdots x_{h'-1} z^{-1} x_{h'+1} \cdots x_m = \\ v_1 z (z^{-1} u') v z^{-1} v_2$$

and $l_1 = v_1$, $l_2 = u' v z^{-1} v_2$.

By Remark 4.1.14 and Proposition 3.2.6 there exists an SLA σ' computing

$$v_1 u' v z^{-1} v_2 = l_1 l_2$$

such that $A(\sigma') = A(\sigma_1) + A(\sigma_2) + A(\tau'_1) = A(\sigma)$ and a CMDR for σ is a CMDR also for σ' .

Subcase 1 β . We have that $n + 1 = h'$, that $x_h = y_p = z$ and that $x_{h'} = z^{-1}$. Therefore

$$l = x_1 \cdots x_{h-1} z x_{h+1} \cdots x_{h'-1} (y_1 \cdots y_{p-1} z) z^{-1} x_{h'+1} \cdots x_m = \\ v_1 z v (u z) z^{-1} v_2$$

and $l_1 = v_1 z v u$, $l_2 = v_2$.

By Remark 4.1.14 and Proposition 3.2.6 there exists an SLA σ' computing

$$v_1 z v u v_2 = l_1 l_2$$

such that $A(\sigma') = A(\sigma_1) + A(\sigma_2) + A(\tau'_1) = A(\sigma)$ and a CMDR for σ is a CMDR also for σ' .

Subcase 2 α . We have that $n = h'$, that $x_{h'} = z$ and that $x_h = y_1 = z^{-1}$. Therefore

$$l = x_1 \cdots x_{h-1} z^{-1} x_{h+1} \cdots x_{h'-1} z (z^{-1} y_2 \cdots y_p) x_{h'+1} \cdots x_m = \\ v_1 z^{-1} v z (z^{-1} u') v_2$$

and $l_1 = v_1 z^{-1} v$, $l_2 = u' v_2$. By Remark 4.1.14 and Proposition 3.2.6 there exists an SLA σ' computing

$$v_1 z^{-1} v u' v_2 = l_1 l_2$$

such that $A(\sigma') = A(\sigma_1) + A(\sigma_2) + A(\tau'_1) = A(\sigma)$ and a CMDR for σ is a CMDR also for σ' .

Subcase 2 β . We have that $n + 1 = h$, that $x_{h'} = y_p = z$ and that $x_h = z^{-1}$. Therefore

$$l = x_1 \cdots x_{h-1} (y_1 \cdots y_{p-1} z) z^{-1} x_{h+1} \cdots x_{h'-1} z x_{h'+1} \cdots x_m = \\ v_1 (u z) z^{-1} v z v_2$$

and $l_1 = v_1 u$, $l_2 = v z v_2$.

By Remark 4.1.14 and Proposition 3.2.6 there exists an SLA σ' computing

$$v_1 u v z v_2 = l_1 l_2$$

such that $A(\sigma') = A(\sigma_1) + A(\sigma_2) + A(\tau'_1) = A(\sigma)$ and a CMDR for σ is a CMDR also for σ' .

4.1.3 Case III

s is a g. corolla and s' a stem.

Subcase α . We have that $y_1 = z^{-1}$ and that $x_n = y_{j'} = z$. Set $u_1 := x_1 \cdots x_{n-1}$ and $u_2 := x_{n+1} \cdots x_m$; thus $t = u_1 z u_2$ and as said at the beginning of the section, t is computed by the pSLsA τ . As in Lemma 4.1.11, let $w'_1 = y_2 \cdots y_{j'-1}$ and $w'_2 = y_{j'+1} \cdots y_p$. Therefore

$$l = x_1 \cdots x_{n-1} z (z^{-1} y_2 \cdots y_{j'-1} z y_{j'+1} \cdots y_p) x_{n+1} \cdots x_m = \\ u_1 z (z^{-1} w'_1 z w'_2) u_2$$

and $l_1 = u_1$, $l_2 = w'_1 z w'_2 u_2$. By Lemma 4.1.11 and by Proposition 3.2.6 there exists an SLA σ' computing

$$u_1 w'_1 z w'_2 u_2 = l_1 l_2$$

and such that $A(\sigma') = A(\tau) + A(\tau')$. By Remark 2.5.2, $A(\tau) + A(\tau') = A(\sigma)$, thus $A(\sigma') = A(\sigma)$, and a CMDR for σ is a CMDR also for σ' .

Subcase β . We have that $x_{n+1} = y_j = z^{-1}$ and that $y_p = z$. Set $u_1 := x_1 \cdots x_n$ and $u_2 := x_{n+2} \cdots x_m$; thus $t = u_1 z^{-1} u_2$ and as said at the beginning of the section, t is computed by the pSLsA τ . As in Lemma 4.1.11, let $w_1 = y_1 \cdots y_{j-1}$ and $w_2 = y_{j+1} \cdots y_{p-1}$. Therefore

$$l = x_1 \cdots x_n (y_1 \cdots y_{j-1} z^{-1} y_{j+1} \cdots y_{p-1} z) z^{-1} x_{n+2} \cdots x_m = \\ u_1 (w_1 z^{-1} w_2 z) z^{-1} u_2$$

and $l_1 = u_1 w_1 z^{-1} w_2$, $l_2 = u_2$. By Lemma 4.1.11 and by Proposition 3.2.6 there exists an SLA σ' computing

$$u_1 w_1 z^{-1} w_2 u_2 = l_1 l_2$$

and such that $A(\sigma') = A(\tau) + A(\tau')$. By Remark 2.5.2, $A(\tau) + A(\tau') = A(\sigma)$, thus $A(\sigma') = A(\sigma)$, and a CMDR for σ is a CMDR also for σ' .

4.1.4 Case IV

There exist two g. corollas c and c' such that one of them contains the letter z of zz^{-1} and the other one contains z^{-1} . Let $l := z_1 \cdots z_e$ be the result of σ , let $c := x_1 \cdots x_m$, $c' := y_1 \cdots y_p$ and let $h_1, \dots, h_m, i_1, \dots, i_p$ be indices such that

$$z_{h_1} = x_1, \dots, z_{h_m} = x_m, z_{i_1} = y_1, \dots, z_{i_p} = y_p.$$

There are two possibilities: either there exists $k : 1 \leq k \leq m$ such that $x_k = z$, $y_1 = z^{-1}$ and $h_k + 1 = i_1$ (we call it *subcase α*) or there exists $k : 1 < k \leq m$ such that $y_p = z$, $x_k = z^{-1}$ and $i_p + 1 = h_k$ (we call it *subcase β*)¹. We call *subcase α_1* the subcase α with $1 \leq k < m$, *subcase α_2* the subcase α with $k = m$.

Let r_1, \dots, r_{m-1} be the ramifications (Definition 3.3.9) from c at x_1, \dots, x_{m-1} respectively; let r'_1, \dots, r'_{p-1} be the ones from c' at y_1, \dots, y_{p-1} . Let q_0 be the preceding of c and q_1 its following (Definition 3.3.9), that is $q_0 q_1$ is the surround of c .

Subcase α_1 . We have that $x_k = z$ and $y_1 = z^{-1}$. Since $h_k + 1 = i_1$ then

$$h_1 < \cdots < h_k < i_1 < \cdots < i_p < h_{k+1} < \cdots < h_m$$

and

$$l = z_1 \cdots z_{h_1} \cdots z_{h_k} (z_{i_1} \cdots z_{i_p}) z_{i_p+1} \cdots z_{h_{k+1}-1} z_{h_{k+1}} \cdots z_{h_m} \cdots z_e.$$

By Proposition 3.3.16 we can suppose that σ defines consecutively the insertions into c' . Since $z_{i_1} = y_1$ and $z_{i_p} = y_p$, then the surround of c' is

$$l' := z_1 \cdots z_{h_k} z_{i_p+1} \cdots z_{h_{k+1}-1} z_{h_{k+1}} \cdots z_e.$$

By Proposition 3.3.12 there exists an SLsA of σ , denoted τ , which computes l' and c is one of its g. corollas. By Proposition 3.3.16 we can suppose that τ

¹the case $y_p = z$ and $x_1 = z^{-1}$ is analogous to the case $x_m = z$ and $y_1 = z^{-1}$.

defines consecutively the insertions into c . Since $z_{h_k} = x_k$ and $z_{h_{k+1}} = x_{k+1}$, then the ramification of l' from c at x_k is $v := z_{i_p+1} \cdots z_{h_{k+1}-1}$ and by Proposition 3.3.12 there exists an SLsA of τ (and therefore of σ) which computes it.

We have that:

$$z_1 \cdots z_{h_k-1} = u, \text{ where } u = q_0 \mathbf{x}_1 r_1 \cdots \mathbf{x}_{k-1} r_{k-1}; \quad z_{h_k} = \mathbf{z};$$

$$z_{i_1} = \mathbf{z}^{-1}; \quad z_{i_1+1} \cdots z_{i_p} = u', \text{ where } u' = r'_1 \mathbf{y}_2 \cdots r'_{p-1} \mathbf{y}_p;$$

$$z_{h_{k+1}} \cdots z_e = u'', \text{ where } u'' = \mathbf{x}_{k+1} r'_{k+1} \cdots r'_{m-1} \mathbf{x}_m q_1$$

(we write in bold the letters coming from c and c').

Thus

$$l = u z (z^{-1} u') v u'' =$$

$$q_0 \mathbf{x}_1 r_1 \cdots \mathbf{x}_{k-1} r_{k-1} \mathbf{z} (\mathbf{z}^{-1} r'_1 \mathbf{y}_2 \cdots r'_{p-1} \mathbf{y}_p) v \mathbf{x}_{k+1} r'_{k+1} \cdots r'_{m-1} \mathbf{x}_m q_1$$

and $l_1 = u$, $l_2 = u' v u''$.

We have that $c = x_1 \cdots x_{k-1} z x_{k+1} \cdots x_m$ and $c' = z^{-1} y_2 \cdots y_p$.

As in the proof of Proposition 3.2.11 we set

$$c_1 := x_1 \cdots x_{k-1}, \quad c_2 := x_{k+1} \cdots x_m, \quad d' := \pi(c_2 c_1, c')$$

$$f_1 := x_1 \cdots x_{k-1}, \quad f_2 := y_2 \cdots y_p x_{k+1} \cdots x_m.$$

By Proposition 3.2.11, either $f_1 f_2$ is a stem element or an insertion of two stem elements (possibly empty) into a flower element with g. corolla a cyclic conjugate of d' , which we denote d'' ; in this case $\eta(d'') \leq \eta(c) + \eta(c')$.

We modify σ by replacing c and c' with an SLsA τ' defined in the following way: if $f_1 f_2$ is a stem element then τ' has only one step which is equal to $f_1 f_2$; otherwise τ' is an SLsA computing $f_1 f_2$ and having only one g. corolla, equal to d'' , therefore $A(\tau') = \eta(d'')$. We consider the insertions at a letter of c or c' as insertions at the same letter of $f_1 f_2$. An insertion at z^{-1} is replaced by an insertion at the last letter that in the output of the same step of σ was preceding z . With this modification we obtain an SLsA σ' computing $u u' v u'' = l_1 l_2$.

Let N and N' be the multisets of base elements of σ and σ' respectively. For any g. corolla of σ let us fix an SLsA in \overline{R} computing that g. corolla and let M be the union of the multisets of the base elements of the SLsA's in \overline{R} for the elements of N . M is a CMDR for σ . If $f_1 f_2$ is a stem then $N' = N \setminus \{c, c'\}$ and thus $A(\sigma') < A(\sigma)$. Then M minus the base elements of the chosen SLsA's in \overline{R} for c and c' is a CMDR for σ' . Let $f_1 f_2$ be not

a stem; then $N' \setminus \{d'\} = N \setminus \{c, c'\}$, which means that the g. corollas of σ and σ' coincide except that c and c' are replaced in σ' by d'' ; therefore the inequality $\eta(d'') \leq \eta(c) + \eta(c')$ implies that $A(\sigma') \leq A(\sigma)$. Moreover M is a CMDR for σ' .

If $A(\sigma) = \text{Area}(\rho(l))$ then $A(\sigma') = A(\sigma)$ by Remark 4.1.12, which implies by Remark 3.2.12 that a CMDR for σ is a CMDR also for σ' .

Subcase β . We have that $y_p = z$ and $x_k = z^{-1}$. Since $i_p + 1 = h_k$, then

$$h_1 < \cdots < h_{k-1} < i_1 < \cdots < i_p < h_k < \cdots < h_m$$

and

$$l = z_1 \cdots z_{h_1} \cdots z_{h_{k-1}} \cdots z_{i_1-1} (z_{i_1} \cdots z_{i_p}) z_{h_k} \cdots z_{h_m} \cdots z_e.$$

By Proposition 3.3.16 we can suppose that σ defines consecutively the insertions into c' . Since $z_{i_1} = y_1$ and $z_{i_p} = y_p$, then the surround of c' is

$$l' = z_1 \cdots z_{h_1} \cdots z_{h_{k-1}} \cdots z_{i_1-1} z_{h_k} \cdots z_{h_m} \cdots z_e.$$

By Proposition 3.3.12 there exists an SLsA of σ , denoted τ , which computes l' and c is one of its g. corollas. By Proposition 3.3.16 we can suppose that τ defines consecutively the insertions into c . Since $z_{h_{k-1}} = x_{k-1}$ and $z_{h_k} = x_k$, then the ramification of l' from c at x_{k-1} is $v := z_{h_{k-1}+1} \cdots z_{i_1-1}$ and by Proposition 3.3.12 there exists an SLsA of τ (and therefore of σ) which computes it.

We have that

$$z_1 \cdots z_{i_1-1} = u, \text{ where } u = q_0 \mathbf{x}_1 r_1 \cdots \mathbf{x}_{\mathbf{k}-1} v;$$

$$z_{i_1} \cdots z_{i_p-1} = u', \text{ where } u' = \mathbf{y}_1 r'_1 \cdots \mathbf{y}_{\mathbf{p}-1} r'_{\mathbf{p}-1}; \quad z_{i_p} = \mathbf{z}; \quad z_{h_k} = \mathbf{z}^{-1};$$

$$z_{h_{k+1}} \cdots z_e = u'', \text{ where } u'' = \mathbf{x}_{\mathbf{k}+1} r'_{\mathbf{k}+1} \cdots r'_{\mathbf{m}-1} \mathbf{x}_{\mathbf{m}} q_1.$$

Thus

$$l = u v (u' z) z^{-1} u'' =$$

$$q_0 \mathbf{x}_1 r_1 \cdots \mathbf{x}_{\mathbf{k}-1} v (\mathbf{y}_1 r'_1 \cdots \mathbf{y}_{\mathbf{p}-1} r'_{\mathbf{p}-1} \mathbf{z}) \mathbf{z}^{-1} \mathbf{x}_{\mathbf{k}+1} r'_{\mathbf{k}+1} \cdots r'_{\mathbf{m}-1} \mathbf{x}_{\mathbf{m}} q_1$$

and $l_1 = uvu'$, $l_2 = u''$.

We have that $c = x_1 \cdots x_{k-1} z^{-1} x_{k+1} \cdots x_m$ and $c' = y_1 \cdots y_{p-1} z$. As in the proof of Proposition 3.2.11 we set

$$c_1 := x_1 \cdots x_{k-1}, \quad c_2 := x_{k+1} \cdots x_m, \quad d' := \pi(c_2 c_1, c')$$

$$f_1 := x_1 \cdots x_{k-1} y_1 \cdots y_{p-1}, \quad f_2 := x_{k+1} \cdots x_m.$$

By Proposition 3.2.11, either $f_1 f_2$ is a stem element or an insertion of two stem elements (possibly empty) into a flower element with g. corolla a cyclic conjugate of d' , which we denote d'' ; in this case $\eta(d'') \leq \eta(c) + \eta(c')$.

We modify σ by replacing c and c' with an SLA τ' defined in the following way: if $f_1 f_2$ is a stem element then τ' has only one step which is equal to $f_1 f_2$; otherwise τ' is an SLA computing $f_1 f_2$ and having only one g. corolla, equal to d'' , therefore $A(\tau') = \eta(d'')$. We consider the insertions at a letter of c or c' as insertions at the same letter of $f_1 f_2$. An insertion at z^{-1} is replaced by an insertion at the last letter that in the output of the same step of σ was preceding z . With this modification we obtain an SLA σ' computing $uvu'u'' = l_1 l_2$.

Let N and N' be the multisets of base elements of σ and σ' respectively. For any g. corolla of σ let us fix an SLA in \overline{R} computing that g. corolla and let M be the union of the multisets of the base elements of the SLA's in \overline{R} for the elements of N . M is a CMDR for σ . If $f_1 f_2$ is a stem then $N' = N \setminus \{c, c'\}$ and thus $A(\sigma') < A(\sigma)$. Then M minus the base elements of the chosen SLA's in \overline{R} for c and c' is a CMDR for σ' . Let $f_1 f_2$ be not a stem; then $N' \setminus \{d''\} = N \setminus \{c, c'\}$, which means that the g. corollas of σ and σ' coincide except that c and c' are replaced in σ' by d'' ; therefore the inequality $\eta(d'') \leq \eta(c) + \eta(c')$ implies that $A(\sigma') \leq A(\sigma)$. Moreover M is a CMDR for σ' .

If $A(\sigma) = \text{Area}(\rho(l))$ then $A(\sigma') = A(\sigma)$ by Remark 4.1.12, which implies by Remark 3.2.12 that a CMDR for σ is a CMDR also for σ' .

Subcase α_2 . We have that $x_m = z$ and $y_1 = z^{-1}$. Since $h_m + 1 = i_1$, then

$$h_1 < \cdots < h_m < i_1 < \cdots < i_p$$

and

$$l = z_1 \cdots z_{h_1} \cdots z_{h_m} (z_{i_1} \cdots z_{i_p}) z_{i_p+1} \cdots z_e.$$

By Proposition 3.3.16 we can suppose that σ defines consecutively the insertions into c' . Since $z_{h_1} = x_1$ and $z_{h_m} = x_m$, then the surround of s is

$$l' = z_1 \cdots z_{h_1-1} z_{i_1} \cdots z_{i_p} z_{i_p+1} \cdots z_e.$$

By Proposition 3.3.12 there exists an SLA of σ , denoted τ , which computes l' and c is one of its g. corollas. By Proposition 3.3.16 we can suppose that τ defines consecutively the insertions into c .

We have that

$$z_1 \cdots z_{h_m-1} = u, \text{ where } u = q_0 \mathbf{x}_1 r_1 \cdots \mathbf{x}_{\mathbf{m}-1} r_{\mathbf{m}-1}; \quad z_{h_m} = \mathbf{z}; \quad z_{i_1} = \mathbf{z}^{-1};$$

$$z_{i_1+1} \cdots z_{i_p} = u', \text{ where } u' = r'_1 \mathbf{y}_2 \cdots r'_{p-1} \mathbf{y}_p.$$

Thus

$$l = u z (z^{-1} u') q_1 = q_0 \mathbf{x}_1 r_1 \cdots \mathbf{x}_{m-1} r_{m-1} z (z^{-1} r'_1 \mathbf{y}_2 \cdots r'_{p-1} \mathbf{y}_p) q_1$$

and $l_1 = u$, $l_2 = u' q_1$.

We have that $c = x_1 \cdots x_{m-1} z$ and $c' = z^{-1} y_2 \cdots y_p$. As in the proof of Proposition 3.2.9 we set

$$d := \pi(c, c'), \quad f_1 := x_1 \cdots x_{m-1}, \quad f_2 := y_2 \cdots y_p.$$

By Proposition 3.2.11, either $f_1 f_2$ is a stem or an insertion of a stem into a flower element with g. corolla d and $\eta(d) \leq \eta(c) + \eta(c')$.

We modify σ by replacing c and c' with an SLA τ' defined in the following way: if $f_1 f_2$ is a stem then τ' has only one step which is equal to $f_1 f_2$; otherwise τ' is an SLA computing $f_1 f_2$ and having only one g. corolla, equal to d , therefore $A(\tau') = \eta(d)$. We consider the insertions at a letter of c or c' as insertions at the same letter of $f_1 f_2$. An insertion at z^{-1} is replaced by an insertion at the last letter that in the output of the same step of σ was preceding z . With this modification we obtain an SLA σ' computing $uu'q_1 = l_1 l_2$.

Let N and N' be the multisets of base elements of σ and σ' respectively. For any g. corolla of σ let us fix an SLA in \overline{R} computing that g. corolla and let M be the union of the multisets of the base elements of the SLA's in \overline{R} for the elements of N . M is a CMDR for σ . If $f_1 f_2$ is a stem then $N' = N \setminus \{c, c'\}$ and thus $A(\sigma') < A(\sigma)$. Then M minus the base elements of the chosen SLA's in \overline{R} for c and c' is a CMDR for σ' . Let $f_1 f_2$ be not a stem; then $N' \setminus \{d\} = N \setminus \{c, c'\}$, which means that the g. corollas of σ and σ' coincide except that c and c' are replaced in σ' by d ; therefore the inequality $\eta(d) \leq \eta(c) + \eta(c')$ implies that $A(\sigma') \leq A(\sigma)$. Moreover M is a CMDR for σ' .

If $A(\sigma) = \text{Area}(\rho(l))$ then $A(\sigma') = A(\sigma)$ by Remark 4.1.12, which implies by Remark 3.2.12 that a CMDR for σ is a CMDR also for σ' .

4.2 The proof of the Main Theorem: conclusion

In this section we prove Lemma 4.1.6 in the general case. Let $l := l_1 z z^{-1} l_2$ be an element of L_g computed by a straight line algorithm σ ; we construct an SLA σ' computing $l_1 l_2$ and such that $A(\sigma') \leq A(\sigma)$. Moreover if $A(\sigma) = \text{Area}(\rho(l))$ then $A(\sigma') = A(\sigma)$ and a CMDR for σ is a CMDR also for σ' .

Lemma 4.2.1 *Let σ be an SLA, let l be its result and let $A(\sigma) = \text{Area}(\rho(l))$. If τ is a pSLsA of σ with result w then $A(\tau) = \text{Area}(\rho(w))$.*

Proof We prove the claim by induction of the number of steps of σ . If σ has only one step the claim is obvious because the only pSLsA is σ itself. Let the number of steps of σ be greater than one and the claim be true for every SLA with less steps than σ ; let τ be a pSLsA of σ and let w be its result. The last step of σ is the insertion of a word l_2 into a word l_1 . By Part 2 of Proposition 2.1.3, l uses w and since l uses directly l_1 and l_2 , then by Part 4 of the same proposition either l_1 or l_2 uses w . This implies that if σ_1 and σ_2 are the pSLsA's of σ computing l_1 and l_2 , then τ is a pSLsA of σ_1 or σ_2 . The claim follows thus by induction hypothesis because σ_1 and σ_2 have less steps than σ . \square

Let s be the first step of σ whose output contains as subword the subword zz^{-1} of $l_1zz^{-1}l_2$. Let $w := x_1 \cdots x_m$ be the output of s and let $k : 1 \leq k < m$ be such that $x_k x_{k+1} = zz^{-1}$. By Remark 2.1.9 we can reorder the steps of σ in such a way that s depends on every step preceding it. By Remark 2.1.5 these steps form a pSLsA τ whose result is w . By the results of the preceding section we have that $w' := x_1 \cdots x_{k-1} x_{k+2} \cdots x_m$ belongs to L_g and that there exists an SLA τ' computing w' and such that $A(\tau') \leq A(\tau)$. Furthermore, by Lemma 4.2.1, if $A(\sigma) = \text{Area}(\rho(l))$ then $A(\tau) = \text{Area}(\rho(w))$ and thus by the results of the preceding section, $A(\tau') = A(\tau)$ and a CMDR for τ is a CMDR also for τ' .

If s is the last step of σ , then we are in the situation of the preceding section. Suppose that s is not the last step; for every step t in σ that follows s we define a new step t' in the following way. Let t be the first step that follows s ; t cannot be an insertion because it can use directly only s (the steps preceding s are already used by s by the observation made earlier), therefore t is a base step. We set $t' := t$. Let $n > 1$ and let t be the n -th step that follows s . If t does not use s then we set $t' := t$. If t does, t is an insertion of a step t_2 into a step t_1 and by Part 4 of Proposition 2.1.3, one and only one between t_1 and t_2 uses s . We can assume by induction hypothesis that we have already defined t'_1 and t'_2 . We let t' be the insertion of t'_2 into t'_1 at the same letter as t_2 is inserted into t_1 . This letter cannot be equal to x_k , because either t_1 does not contain it or does contain both x_k and x_{k+1} consecutively. If t is the insertion of t_2 into t_1 at x_{k+1} , then we let t' be the insertion of t'_2 into t'_1 at the letter of t_1 that precedes x_k .

For every step t , the output of t' is equal to the output of t if t does not use s ; if t uses s then the output of t' is the word obtained by cancelling zz^{-1} from the output of t . If t is the last step, then the output is $l_1 l_2$. Replacing

τ with τ' and every step t that follows s with the corresponding step t' we obtain an SLA σ' computing $l_1 l_2$.

The base steps of σ following s coincide with those of σ' following s' . This implies that since $A(\tau') \leq A(\tau)$ then $A(\sigma') \leq A(\sigma)$. Moreover we have seen that if $A(\sigma) = \text{Area}(\rho(l))$ then $A(\tau') = A(\tau)$ and a CMDR for τ is a CMDR also for τ' ; this implies that $A(\sigma') = A(\sigma)$ and a CMDR for σ is a CMDR also for σ' .

Chapter 5

Applications and complexity

In Section 5.1 we illustrate some applications to the Word Problem of the results of this thesis. In Section 5.2 we show how, given an SLA in L whose result is a reduced word, one can find an SLA with the same result and whose intermediate outputs are reduced words. Finally in Section 5.3 we show that the algorithm presented in this thesis to compute the relators has a better complexity than the other methods currently known in the literature.

5.1 Applications to the Word Problem

Let $\langle X | R \rangle$ be a group presentation and let R be finite. Consider the following functions introduced in Definition 2.4.6:

$$\Delta_0(n) := \max\{\text{Area}(w) : w \text{ is a proper corolla and } |w| \leq n\},$$

$$\Omega_0(n) := \max\{\text{Work}(w) : w \text{ is a proper corolla and } |w| \leq n\}.$$

It is obvious that $\Delta_0 \leq \Delta$ and $\Omega_0 \leq \Omega$ where Δ is the Dehn function (Definition 1.2.2) and Ω has been introduced in Definition 1.4.1.

By Proposition 1.2.4 a finite presentation has a solvable Word Problem if and only if its Dehn function is bounded above by a computable function if and only if its Dehn function is computable. Let us improve this result.

Let n be a natural number and let w be a relator of length at most n . By Corollary 4.1.2 there exist proper corollas c_1, \dots, c_m such that $\text{Area}(w) = \sum_{i=1}^m \text{Area}(c_i)$ and $|w| \geq |c_i|$ for every i . Thus

$$\text{Area}(w) \leq \Delta_0(|c_1|) + \dots + \Delta_0(|c_m|),$$

that is

$$\Delta(n) \leq \max\{\Delta_0(k_1) + \cdots + \Delta_0(k_m) : k_1 + \cdots + k_m \leq n\} \leq n\Delta_0(n)$$

and then we have the following inequality:

$$\Delta_0(n) \leq \Delta(n) \leq n\Delta_0(n). \quad (5.1)$$

This means that if Δ_0 is bounded by a sequence $\{k_n\}_{n \in \mathbb{N}^*}$ then Δ is bounded by $\{nk_n\}_{n \in \mathbb{N}^*}$. As we have said, this bound can be improved if k_n is linear in n in which case Δ is bounded by k_n (see Corollary 4.1.5).

If $\{k_n\}_{n \in \mathbb{N}^*}$ is computable then also $\{nk_n\}_{n \in \mathbb{N}^*}$ is computable. Thus if Δ_0 is bounded above by a computable function then so is Δ and the Word Problem is solvable.

We prove that in this case Δ_0 is computable. Since the presentation is finite we can compute the results of all the $L-SLA$'s τ such that $A(\tau) \leq k_n$ and which compute a word of length at most n . In this way we determine all the proper corollas of length at most n and their area, thus we compute Δ_0 . Thus

Theorem 5.1.1 *A finite presentation has a solvable Word Problem if and only if the function Δ_0 is bounded by a computable function if and only if the function Δ_0 is computable. Moreover Δ is computable or bounded by a computable function if and only if the same is true for Δ_0 .*

In the same way one sees that

$$\Omega_0(n) \leq \Omega(n) \leq n\Omega_0(n)$$

and thus we improve part 1 of Proposition 1.4.3 with the following

Theorem 5.1.2 *A finitely generated decidable presentation has a solvable Word Problem if and only if the function Ω_0 is bounded by a computable function if and only if the function Ω_0 is computable.*

We now exhibit an explicit algorithm for solving the Word Problem for a finite presentation for which Δ_0 is bounded by a computable function. This gives a direct proof of Theorem 5.1.1, i.e., a proof not relying on Proposition 1.2.4.

The algorithm is the following. Let $\langle X | R \rangle$ be a finite presentation and for every k let C_k (Definition 2.3.9) be the set of k -corollas. As we have seen in Remark 2.3.13, there is an explicit algorithm for computing C_k . Suppose

that Δ_0 is bounded by a computable function, that is $\Delta_0(n) \leq k_n$ for every n where k_n is computable by a finite algorithm and let w be a reduced word in the alphabet $X \cup X^{-1}$.

By Corollary 4.1.3, if w is a relator of $\langle X | R \rangle$ then w has a contiguous subword equal to a proper corolla whose area is at most equal to the area of w . Let n be the length of w ; if no element of C_h for $h \leq k_n$ is a contiguous subword of w , then w is not a relator. Suppose on the contrary that there exists an element c of C_h for some $h \leq k_n$ which is a contiguous subword of w ; this means that there exist reduced words w' and w'' such that $w = w'cw''$. Let w_1 be the reduced form of $w'w''$; if $w_1 = 1$ then w is a relator. Let $w_1 \neq 1$; w is a relator if and only if w_1 is a relator. Moreover the length of w_1 is less than that of w .

If w_1 is a relator, its area is equal at most to the minimum between $k_n - h$ and $k_{|w_1|}$. Let m_1 be that minimum; if no element of C_h for $h \leq m_1$ is a contiguous subword of w_1 then w_1 is not a relator and neither w ; if yes, we repeat for w_1 the same procedure done for w and we find a word w_2 of length less than that of w_1 . This algorithm stops after at most n steps: if for some $i = 1, 2, \dots$, we have that $w_i = 1$, then w is a relator; if no contiguous subword of w_i is equal to an element of C_h for $h \leq m_i$ then w is not a relator. This concludes the algorithm.

For every h set $P_h := C_h \setminus \{C_1 \cup \dots \cup C_{h-1}\}$ and let m_h be the minimal length of words of P_h . If X is finite and if $m_h \neq 0$ for infinitely many h then the sequence $\{m_h\}_{h \in \mathbb{N}^*}$ diverges to infinity. Indeed suppose that $\{m_h\}_{h \in \mathbb{N}^*}$ does not diverge to infinity. Then there would exist a natural number n and an infinite number of indices h such that $m_h \leq n$. Since the P_h are disjoint two by two, there would be infinitely many words of length not greater than n and this is impossible because their number is bounded by $(2|X|)^n$.

Lemma 5.1.3 *For any n let $f(n)$ be the least natural number such that $m_h > n$ for every $h > f(n)$. Then $\Delta_0(n) \leq f(n)$.*

Proof Let $h > f(n)$; since $m_h > n$ then if $w \in P_h$ we have that $|w| > n$. Let w be a proper corolla of length not greater than n ; then w does not belong to P_h for every $h > f(n)$, that is it belongs to $P_1 \cup \dots \cup P_{f(n)}$. By Definition 2.4.6 and the Main Theorem 4.1.1, $\text{Area}(w) = \eta(w)$ and thus the area of w cannot be greater than $f(n)$, which implies that $\Delta_0(n) \leq f(n)$. \square

Lemma 5.1.3 implies:

Theorem 5.1.4 *The Word Problem is solvable for the finite presentation $\langle X | R \rangle$ if and only if the function f defined in Lemma 5.1.3 is bounded above by a computable function.*

Proof If f is bounded above by a computable function then by Lemma 5.1.3 also $\Delta_0(n)$ is bounded above by the same computable function and the Word Problem for $\langle X | R \rangle$ is solvable by Theorem 5.1.1.

Let the Word Problem for $\langle X | R \rangle$ be solvable; by Theorem 5.1.1 there exist computable k_n for every n such that $\Delta_0(n) \leq k_n$. That is, if w is a proper corolla and $|w| \leq n$ then $\text{Area}(w) \leq k_n$. This means that if w is a proper corolla and $\text{Area}(w) > k_n$ then $|w| > n$. Then $m_h > n$ for every $h > k_n$, thus $k_n \geq f(n)$ and f is bounded above by a computable function. \square

Theorem 5.1.4 says that the Word Problem is solvable for $\langle X | R \rangle$ if and only if for every n we can compute a k_n such that every proper corolla of area greater than k_n has length greater than n .

Corollary 5.1.5 *Let $\{a_h\}_{h \in \mathbb{N}^*}$ be a computable non-decreasing and divergent sequence. If $m_h \geq a_h$ for every h then the Word Problem for $\langle X | R \rangle$ is solvable.*

Proof Let n be a natural number; then there exists a natural number k_n such that $a_h > n$ for every $h > k_n$. We have that $f(n) \leq k_n$ where f is the function defined in Lemma 5.1.3. Let us compute a_1, a_2, \dots until we find an a_i greater than n . Then k_n is equal to this i and there exists a finite algorithm computing k_n . The Word Problem for $\langle X | R \rangle$ is solvable by Theorem 5.1.4. \square

Corollary 4.1.4 says that if $\Delta_0(n)$ is bounded by a linear function in n then also Δ is bounded by the same linear function and the presentation is hyperbolic. We now generalize this fact.

We recall (Definition 1.3.5) that we write $f \preceq g$ if there exists a positive constant α such that $f(n) \leq \alpha g(\alpha n) + \alpha n$ for every $n \in \mathbb{N}^*$. Obviously we have that $\Delta \preceq g$ [respectively $\Delta_0 \preceq g$] if and only if there exists a positive constant α such that

$$\text{Area}(w) \leq \alpha g(\alpha |w|) + \alpha |w| \tag{5.2}$$

for every relator w [respectively for every proper corolla w].

Lemma 5.1.6 *Let $g : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ be a non-decreasing function and suppose that there exists $\alpha_0 > 0$ such that for every $\alpha \geq \alpha_0$ there exists $\beta \in \mathbb{R}_+$ such that for every $y_1, \dots, y_m, z \in \mathbb{N}^*$ such that $y_1 + \dots + y_m \leq z$ we have*

$$\sum_{j=1}^m g(\alpha y_j) \leq g(\beta z). \quad (5.3)$$

If $\Delta_0 \preceq g$ then $\Delta \preceq g$.

Proof If $\Delta_0 \preceq g$ then there exists $\alpha \in \mathbb{R}_+$ such that for every proper corolla c we have that $\text{Area}(c) \leq \alpha g(\alpha|c|) + \alpha|c|$. By Remark 1.3.6 we can suppose that $\alpha \geq \alpha_0$.

Let n be a natural number and let w be a relator of length at most n . By Corollary 4.1.2 there exist proper corollas c_1, \dots, c_m such that $\text{Area}(w) = \sum_{j=1}^m \text{Area}(c_j)$ and $\sum_{j=1}^m |c_j| \leq |w|$. Then

$$\text{Area}(w) \leq \alpha \sum_{j=1}^m [g(\alpha|c_j|) + |c_j|]$$

and by (5.3) there exists β such that

$$\text{Area}(w) \leq \alpha[g(\beta|w|) + |w|].$$

Since g is non-decreasing, if we set $\beta' := \max\{\alpha, \beta\}$, then

$$\text{Area}(w) \leq \alpha[g(\beta|w|) + |w|] \leq \beta'[g(\beta'|w|) + |w|]$$

and the claim follows from (5.2). \square

We recall (Definition 1.3.5) that we write $f \simeq g$ if $f \preceq g$ and $g \preceq f$.

Theorem 5.1.7 *Let $g : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ be a non-decreasing function satisfying (5.3) and let $\Delta_0 \simeq g$; then $\Delta \simeq g$ and thus $\Delta_0 \simeq \Delta$.*

Proof We have that $\Delta_0 \preceq g$ and $g \preceq \Delta_0$. By Lemma 5.1.6 we have that $\Delta \preceq g$. Conversely we have that $g \preceq \Delta$ because $g \preceq \Delta_0$ and $\Delta_0 \leq \Delta$. \square

We now show that polynomial and exponential functions satisfy (5.3).

Lemma 5.1.8 1. *Let $r > 1$ and let $h(x) = (x + 1)^r - x^r - 1$. Then $h(x) > 0$ for every $x > 0$.*

2. *Let $r > 1$ and let $y_1, \dots, y_m > 0$. Then $(y_1 + \dots + y_m)^r > y_1^r + \dots + y_m^r$.*

Proof

1. We have that $h(0) = 0$ and that the derivative of h is

$$h'(x) = r(x+1)^{r-1} - rx^{r-1} = r[(x+1)^{r-1} - x^{r-1}]$$

which is positive for every $x \geq 0$.

2. It is enough to prove the claim for $m = 2$. Since $y_1, y_2 > 0$ then there exists $c > 0$ such that $y_2 = cy_1$, therefore the inequality is equivalent to $y^r + c^r y^r > (c+1)^r y^r$ for every $y, c > 0$ and the latter is equivalent to $(1+c)^r > 1+c^r$ for every $c > 0$. By Part 1, $(1+c)^r - c^r - 1 > 0$ for every $c > 0$ and thus we have the claim.

□

Remark 5.1.9 For $r = 1$ we have that $(y_1 + \cdots + y_m)^r = y_1^r + \cdots + y_m^r$; then by Part 2 of Lemma 5.1.8 we have that if $r \geq 1$ then $(y_1 + \cdots + y_m)^r \geq y_1^r + \cdots + y_m^r$.

Proposition 5.1.10 *If r is a real number and $r \geq 1$ then the polynomial functions x^r satisfy (5.3).*

Proof We will prove that for any $y_1, \dots, y_m, z \in \mathbb{N}^*$ such that $y_1 + \dots + y_m \leq z$ we have

$$\sum_{j=1}^m (\alpha y_j)^r \leq (\alpha z)^r.$$

We have that

$$\sum_{j=1}^m (\alpha y_j)^r \leq \left(\sum_{j=1}^m \alpha y_j \right)^r \leq (\alpha z)^r$$

when the first inequality follows from Remark 5.1.9. □

Remark 5.1.11 Let $r_1, \dots, r_n \geq 1$ be real numbers; we show that there exists $1 < a_0 \leq 2$ such that $x^{r_1 + \dots + r_n} \geq x^{r_1} + \dots + x^{r_n}$ for every $x \geq a_0$. It is sufficient to show the claim for $n = 2$. Let $\varphi(x) = x^{r_1 + r_2} - x^{r_1} - x^{r_2}$ and suppose that $r_1 \geq r_2$. Let us show that $\varphi(2) \geq 0$; we have that

$$\varphi(2) = 2^{r_1 + r_2} - 2^{r_1} - 2^{r_2} = 2^{r_1}(2^{r_2} - 1 - 2^{r_2 - r_1})$$

and $2^{r_2} - 1 - 2^{r_2-r_1} \geq 0$ because $2^{r_2} \geq 2$ (being $r_2 \geq 1$) and $2^{r_2-r_1} \leq 1$ (being $r_2 - r_1 \leq 0$). Let us show that $\varphi'(x) \geq 0$; we have that

$$\begin{aligned}\varphi'(x) &= (r_1 + r_2)x^{r_1+r_2-1} - r_1x^{r_1-1} - r_2x^{r_2-1} \\ &= r_1(x^{r_1+r_2-1} - x^{r_1-1}) + r_2(x^{r_1+r_2-1} - x^{r_2-1}) \geq 0.\end{aligned}$$

Proposition 5.1.12 *Let a_0 as in Remark 5.1.11. Then for every $a \geq a_0$ the functions a^x satisfy (5.3).*

Proof Let $y_1, \dots, y_m, z \in \mathbb{N}^*$ be such that $y_1 + \dots + y_m \leq z$ and let $\alpha \geq 1$. Since $\alpha y_j \geq 1$ for $j = 1, \dots, m$ then by Remark 5.1.11 we have that

$$\sum_{j=1}^m a^{\alpha y_j} \leq a^{\alpha z}.$$

□

We now show that for every $b > 1$ the function $\log_b x$ does not satisfy (5.3). Let $\alpha, \beta > 0$ and let x, y be non-zero natural numbers. Then there exists a rational number c such that $y = cx$. We have that

$$\log_b(\alpha x) + \log_b(\alpha y) \leq \log_b(\beta(x + y))$$

if and only if

$$\log_b(\alpha x) + \log_b(\alpha cx) \leq \log_b(\beta(c + 1)x)$$

which is equivalent to

$$\log_b(\alpha^2 c) + 2 \log_b(x) \leq \log_b(\beta(c + 1)) + \log_b(x)$$

and thus to

$$\log_b(x) + \log_b(\gamma) \leq 0$$

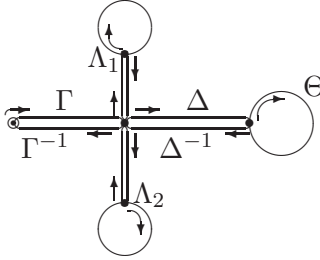
where $\gamma = \frac{\alpha^2 c}{\beta(c+1)}$. But this is false because $\log_b(\gamma)$ is constant and $\log_b(x)$ goes to infinity.

5.2 Straight line algorithms for reduced words

Let σ be an SLA whose result is a reduced word; in this section we will show how to find an SLA equivalent in the sense of Definition 3.3.14 to σ and such that the output of every step is a reduced word.

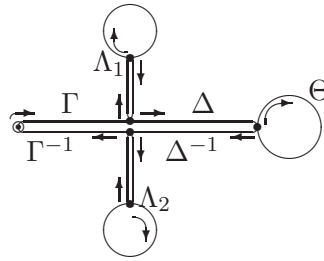
First we show that any SLA is equivalent to one in which the mid-vertex of a stem does not coincide with the initial vertex of another stem.

Consider the complex



Its label is $\Gamma \Lambda_1 \Delta \Theta \Delta^{-1} \Lambda_2 \Gamma^{-1}$, where: Γ is the label of the first half of the stem on the left and Δ the label of that on the right; Θ is the label of the corolla on the right; Λ_1 and Λ_2 the labels of the upper and lower flowers respectively. The mid-vertex of the stem on the left coincides with the initial vertex of the stem on the right.

The next complex has the same label as the preceding one and the latter situation does not happen.



The two stems labeled by $\Gamma\Gamma^{-1}$ and $\Delta\Delta^{-1}$ have been replaced by one labeled by $\Gamma\Delta\Delta^{-1}\Gamma^{-1}$.

Let us formalize this situation. Let σ be an SLA, let $w := x_1 \cdots x_m$ be its result and let $b_1 := y_1 \cdots y_p$ and b_2 be two stems such that the mid-vertex of b_1 coincides with the initial vertex of b_2 . We formalize the notion of “sharing a vertex” and then show how to modify σ in order to avoid it.

Let b_1 comprise b_2 . By Proposition 3.3.16 we can suppose that σ defines

consecutively the insertions into b_1 . Since b_2 is comprised in b_1 then all the letters of b_2 are comprised between two consecutive letters $y_h = x_{i_1}$ and $y_{h+1} = x_{j_1}$ of b_1 , where $1 \leq h < p$ and $1 \leq i_1 < j_1 \leq m$. Therefore by Definition 3.3.13, b_2 belongs to the pSLsA of σ which computes the ramification (Definition 3.3.9) from b_1 at y_h . Call τ_h and r_h this pSLsA and this ramification respectively. By Proposition 3.3.16 we can suppose that τ_h defines consecutively the insertions into b_2 .

Let x_{i_2} and x_{j_2} (for some indices i_2 and j_2) be respectively the first and the last letters of b_2 ; then we have that $1 \leq i_1 < i_2 < j_2 < j_1 \leq m$. Set $v_1 := x_{i_1+1} \cdots x_{i_2-1}$ and $v_2 := x_{j_2+1} \cdots x_{j_1-1}$. We call v_1 and v_2 *the subwords comprised between b_1 and b_2* .

Suppose that y_h is the last letter of the first half of b_1 ; we say that *the mid-vertex of b_1 coincides with the initial vertex of b_2* if the subwords comprised between b_1 and b_2 are parts of w (Definition 3.3.6).

$v_1 v_2$ is the surround of b_2 in the ramification r_h and by Definition 3.3.13 we can suppose that $v_1 v_2$ is the result of a pSLsA of τ_h ; call τ'_0 this pSLsA. In particular v_1 and v_2 are respectively the preceding and the following of b_2 in r_h and if we have supposed that they are parts of w , we can assume that τ'_0 is formed by two pSLsA's computing v_1 and v_2 respectively, followed by the product of v_1 by v_2 . We call t the step of the product of v_1 by v_2 .

We modify σ by replacing b_1 and b_2 with $s := y_1 \cdots y_h b_2 y_{h+1} \cdots y_p$ which is a stem because y_h is the last letter of the first half of b_1 . Furthermore we replace the step t by the insertions of v_1 at y_h and of v_2 at the last letter of b_2 and we consider the insertions at a letter of b_1 or b_2 as insertions at the corresponding letters of f or s respectively.

We obtain an SLA σ' with result w (the same of σ). σ and σ' have the same corollas, therefore $A(\sigma') = A(\sigma)$ and a CMDR for σ is a CMDR also for σ' .

With the notion of “equivalence” of SLA's of Definition 3.3.14, σ and σ' cannot be equivalent but it is intuitive that σ and σ' are equivalent in a more general sense. Let us modify this notion of equivalence.

Let τ_1 and τ_2 be SLA's with the same result (let w be their result), with multisets of base elements M_1 and M_2 and let $\omega : M_1 \rightarrow M_2$ be an application such that:

1. the restriction of ω to the corollas of M_1 is an isomorphism onto the corollas of M_2 ;
2. the restriction of ω to the stems of M_1 is surjective onto the stems of M_2 ;

3. let vv^{-1} be a stem of τ_2 and let $u_1u_1^{-1}, \dots, u_nu_n^{-1}$ be the stems of τ_2 whose image by ω is vv^{-1} and let the first letter of $u_iu_i^{-1}$ precedes the first of $u_{i+1}u_{i+1}^{-1}$ for $i = 1, \dots, n-1$. Then $vv^{-1} = u_1 \cdots u_nu_n^{-1} \cdots u_1^{-1}$;
4. any letter of w comes (Definition 3.1.3) from the same letter of μ and $\omega(\mu)$ respectively (we recall that μ is a subword of $\omega(\mu)$).

We say that τ_2 is a *refinement* of τ_1 .

Let σ be an SLA, let w be its result and let $A(\sigma) = A(w)$. If we apply repeatedly this procedure, we obtain an SLA σ'' with the same result of σ , such that $A(\sigma'') = A(w)$, such that a CMDR for σ is a CMDR also for σ'' and in which the mid-vertex of any stem does not coincide with the initial vertex of another stem. Moreover σ'' is a refinement of σ .

Any element w of L_g (and thus any relator of $\langle X|R \rangle$ by Theorem 4.1.1) is the result of an SLA σ , that is it is obtained by means of the operation of grafting starting with base elements (stems and corollas). By what said above, we can suppose that the mid-vertex of any stem of σ does not coincide with the initial vertex of another stem.

Suppose that w is reduced and suppose that one of the steps of σ is a stem uu^{-1} . We can suppose that σ defines consecutively the insertion in uu^{-1} . Since uu^{-1} is non-reduced and since the result of σ is a reduced word then the ramification r from the last letter of u is non-empty. Since the mid-vertex of uu^{-1} does not coincide with the initial vertex of another stem, then the first and the last letter of this ramification come from corollas. Let x be the last letter of u , that is x^{-1} is the first letter of u^{-1} , and let c be the corolla from which comes the first letter of r . The first letter of c is different from x^{-1} . If the last letter of c is different from x then the flower ucu^{-1} is reduced; otherwise, the subword comprised between c and u^{-1} is non-empty, the first letter is different from x^{-1} and comes from a corolla. By repeating the same procedure, we find that there exists a corolla c' such that $uc'u^{-1}$ is reduced and the subwords comprised between u and c' and between c' and u^{-1} are parts of w . That is in the multiset of base elements of σ we can replace uu^{-1} and c' with $uc'u^{-1}$ and then we can assume that the base elements are not stems and corollas but reduced flowers and corollas. Since a corolla can be considered a flower with trivial stem, then if w is reduced then we assume that the base elements are the reduced flowers.

We now prove that if w is reduced then σ is equivalent to an SLA the outputs of whose steps are all reduced. Suppose that σ has only one step; then this step is reduced since it is a reduced flower. Let the claim be true for every SLA with less steps than σ . Let f be the flower from which comes the first letter of w . The ramifications from f are reduced words since

they are contiguous subwords of a reduced word; the surround of f coincides with its following, therefore it is reduced since it is a contiguous subword of w . By induction hypothesis they are defined by SLA's whose outputs are all reduced and finally inserting the ramifications and the surround into f give also reduced outputs.

We denote D_1 the set of words which are reduced and which are of the form uwu^{-1} where $w \in C_1$. Suppose by induction to have defined D_{k-1} and define D_k as the set of reduced words which are either of the form uwu^{-1} where $w \in C_k$ or are insertions of a word of D_m into one of D_n for $m+n=k$. We denote D the union of all the D_k . Then by what said above, given an L_g -straight line algorithm σ there exists a straight line algorithm σ' whose base elements are reduced flowers, whose operations are insertions of words, such that the output of any step of σ' is reduced and such that σ' is a refinement of σ .

5.3 Comparison of the complexities

Let $\mathcal{P} := \langle X | R \rangle$ be a finite group presentation, let k and n be natural numbers and suppose that we want to find all the relators of \mathcal{P} of length at most n and which are products of at most k conjugates of defining relators. In Section 1.6 we have illustrated the two methods currently known in the literature; both use the van Kampen diagrams associated with relators. We have also computed (1.14) and (1.15), the complexities of these methods and shown that the better is (1.15), which is a product of three exponentials, one in k , one in kn and one in k^2 . Namely this complexity is equal to $q^k a^{kn} s^{k^2}$ where $q = p(a+1)/(a-1)$, $p = |R|$, $a = 2|X| - 1$, $s = a^m$ and m is the maximal length of an element of R . We have the following result

Theorem 5.3.1 *The complexity of the method illustrated in this thesis is bounded above by $n^3 \beta^n \gamma^k$ if $a > 4$, where $\beta = 2\sqrt{a}$ and $\gamma = 4p\sqrt{2}^m$; it is bounded above by $n^3 4^n \gamma^k$ if $a < 4$. This complexity is less than those of the two classical methods (illustrated in Section 1.6) by a factor of at least $a^{k(k-c_1)} a^{n(k-c_2)}$, with $c_1 = m/2 + 2$ and $c_2 = 2$.*

Obviously a cannot be equal to 4 since it is odd. The proof of Theorem 5.3.1 is given in Section A.1.

Theorem 5.3.1 proves that an upper bound for the complexity of our method is a product of a cubic polynomial times an exponential in n and one in k . This is much better than the complexities with the methods currently known in the literature. Moreover the value given in Theorem 5.3.1 is far

from being an optimal bound for the complexity of our method, but only a value obtained with not too complicated calculations. With non-trivial arguments this result could be probably much improved. Instead (1.15) is the real complexity of the classical method, that is it is the exact number of words to be considered with this method to find all the relators of length up to n and area up to k .

Finally let us say some words about the comparison of the method of this thesis with the first classical method illustrated in Section 1.6, i.e., the method consisting in enumerating the van Kampen diagrams with up to k faces and boundary of up to n edges. As shown in Section 3.1, with every SLA we can associate a van Kampen diagram.

In the diagrams associated with an SLA, the biconnected components correspond to the corollas. Thus the diagrams constructed with our method verify the following property: if \mathcal{B} is a biconnected component of the diagram then one can name the faces of \mathcal{B} as F_1, \dots, F_n in such a way that two F_i are distinct and $F_1 \cup F_2 \cup \dots \cup F_i$ is biconnected and has a cyclically reduced boundary label for every $i = 1, \dots, n$.

In the classical method one has to construct all the diagrams and there are diagrams not verifying the property above, in particular those whose boundary label is not cyclically reduced.

The central result of this thesis is that for finding all the relators one does not need to construct all the van Kampen diagrams, but only those associated with SLA's. The set of diagrams associated with SLA's is a proper subset of the set of all the diagrams, anyway it contains all the "important information" about the set of relators.

Let us explain the last sentence. Let a_1, \dots, a_m be words and r_1, \dots, r_m be defining relators, let $w := a_1 r_1 a_1^{-1} \dots a_m r_m a_m^{-1}$ and let v be the reduced form of w . There is a van Kampen diagram with boundary label equal to v for every sequence of cancellations from w to v ; and two of these diagrams are not necessarily equal. In Chapter 4 we have proved that there is a diagram for an SLA for at least one of these sequences of cancellations, thus by considering the set of SLA diagrams instead of that of all van Kampen diagrams no information about the relators is lost.

Appendix A

In Section A.1 we compute the complexity of the algorithm presented in this thesis for computing the relators. In Section A.2 we prove a result which is not needed in this thesis; in particular we prove that a recursively defined set can be defined as the set of results of a family of straight line algorithms. Finally in Section A.3 we show a result necessary for the proof of the equality between the set of corollas with that of the generalized corollas.

A.1 Computation of the complexity

Suppose given a finite presentation, let n and k be natural numbers and let us compute all the relators of length up to n and area up to k . In this section we show that an upper bound for the complexity of the method presented in this thesis is a product of a cubic polynomial times an exponential in n and one in k . This is much better than (1.15), the complexity with the method currently known in the literature, which is a product of three exponentials, one in k , one in kn and one in k^2 .

Let $\mathcal{P} := \langle X \mid R \rangle$ be a finite group presentation. Let m be the maximal length of elements of R , let $p := |R|$ and let $a := 2|X| - 1$.

Let n and k be natural numbers and let w be a relator of length at most n and which is product of at most k conjugates of defining relators. By Theorem 4.1.1 and Section 5.2, w is obtained by insertions of at most n flowers. That is there exist $h \leq k$ flowers f_1, \dots, f_h such that $|f_1| + \dots + |f_h| \leq n$ and w is the result of an SLA in D whose base elements are f_1, \dots, f_h . This means that f_2 is inserted into f_1 giving a word f'_2 , then f_3 is inserted into f'_2 giving a word f'_3 and so on until we have $f'_h = w$.

Let $u := u_1 u_2$ and v be words; the insertion $u_1 v u_2$ of v into u is the reduced form of $u u_2^{-1} v u_2$, therefore the number of possible insertions of v into u is equal to $|u|$. Let $n_i = |f_i|$; since $|f'_i| = |f_1| + \dots + |f_i|$, then the

number of possible insertions of words f_1, \dots, f_h is

$$n_1 + (n_1 + n_2) + (n_1 + n_2 + n_3) + \dots + (n_1 + n_2 + n_{h-1}) = \sum_{i=1}^{h-1} (h-i)n_i.$$

A flower of length n_i is obtained by the insertion of a corolla c_i of length n'_i into a stem of length $n_i - n'_i$ for some $n'_i = 1, \dots, n_i$. Moreover $n_i - n'_i$ must be even. The number of stems of length $n_i - n'_i$ is equal to the number of reduced words of length $(n_i - n'_i)/2$, which is 1 if $n_i - n'_i = 0$, is $a + 1$ if $n_i - n'_i = 2$ (we recall that $a = 2|X| - 1$) and is equal to $(a + 1)a^{(n_i - n'_i)/2 - 1}$ otherwise.

Let $k_i = \eta(c_i)$; then $k_1 + \dots + k_h \leq k$. A corolla is determined by a sequence of cyclically reduced products of 1-corollas, each cyclically reduced product followed by a cyclic conjugation.

A cyclic conjugation of a word w by i letters is equivalent to conjugate w by the prefix of w of length i and then taking the reduced form. We have seen in Remark 2.3.7 that the total length of the conjugating elements for a corolla c of length at most n'_i and such that $\eta(c) = k_i$ is no more than $(mk_i - 1)/2 + n'_i - 1$ (m is the maximal length of elements of R). This means that in constructing such a corolla the sum of the lengths of cyclic conjugations has been at most $(mk_i - 1)/2 + n'_i - 1$.

Let $q \leq (mk_i - 1)/2 + n'_i - 1$; suppose that we make k_i cyclically reduced products of defining relators, each followed by a cyclic conjugation of q_i letters for $i = 1, \dots, k_i$ and let $q = q_1 + \dots + q_{k_i}$. Then (q_1, \dots, q_{k_i}) is a *weak composition* of q in k_i parts (see [3]). The number of weak compositions of q in k_i parts is equal to

$$\binom{q + k_i - 1}{k_i - 1}.$$

Finally if $p = |R|$, then there are obviously p^{k_i} products of k_i defining relators.

Therefore if we want to find with the method presented in this thesis all the relators of length at most n and which are products of at most k conjugates of defining relators, then an upper bound for the number of relators which we compute is

$$\sum_{h=1}^{\min(k,n)} \sum_{n_1 + \dots + n_h \leq n} \sum_{j=1}^{h-1} (h-j)n_j \sum_{k_1 + \dots + k_h \leq k} \quad (\text{A.1})$$

$$\prod_{i=1}^h p^{k_i} \left(\sum_{n'_i=1}^{n_i} (a+1)a^{(n_i-n'_i)/2-1} \sum_{q=1}^{(mk_i-1)/2+n'_i-1} \binom{q+k_i-1}{k_i-1} \right).$$

Let us make some observations about this bound. The term p^{k_i} is unrealistically too big because it means that in finding all the corollas c such that $\eta(c) = k_i$ we make all possible cyclically reduced products, whereas by Section it is enough to take much less (in particular we need to make a product if there is a cancellation).

The term $\sum_{j=1}^{h-1} (h-j)n_j$ too is unrealistically too big because it considers that we make all possible insertions of the words f_1, \dots, f_h whereas by the result of Section 5.2, the insertions to be considered are only those such that the resulting word is reduced.

Let us find an upper bound for (A.1). Since $\binom{q+k_i-1}{k_i-1} < 2^{q+k_i-1}$ then

$$\begin{aligned} \sum_{q=1}^{(mk_i-1)/2+n'_i} \binom{q+k_i-1}{k_i-1} &< \sum_{q=1}^{(mk_i-1)/2+n'_i-1} 2^{q+k_i-1} = 2^{k_i-1} \sum_{q=1}^{(mk_i-1)/2+n'_i-1} 2^q = \\ &= 2^{k_i-1} (2^{\frac{mk_i-1}{2}+n'_i} - 2) < 2^{k_i-1} (2^{\frac{mk_i-1}{2}+n'_i}) = \frac{\sqrt{2}^{(m+2)k_i} 2^{n'_i}}{2\sqrt{2}} \end{aligned}$$

since we have the equality $\sum_{i=1}^n s^i = (s^{n+1} - s)/(s - 1)$ for $s > 1$. Thus

$$\begin{aligned} \sum_{n'_i=1}^{n_i} (a+1) a^{(n_i-n'_i)/2-1} \sum_{q=1}^{(mk_i-1)/2+n'_i-1} \binom{q+k_i-1}{k_i-1} &< \\ \sum_{n'_i=1}^{n_i} (a+1) a^{(n_i-n'_i)/2-1} \frac{\sqrt{2}^{(m+2)k_i} 2^{n'_i}}{2\sqrt{2}} &= \frac{(a+1) \sqrt{2}^{(m+2)k_i}}{2\sqrt{2} a} \sum_{n'_i=1}^{n_i} a^{(n_i-n'_i)/2} 2^{n'_i} = \\ &= \frac{(a+1) \sqrt{2}^{(m+2)k_i} \sqrt{a}^{n_i}}{2\sqrt{2} a} \sum_{n'_i=1}^{n_i} \left(\frac{2}{\sqrt{a}}\right)^{n'_i} \end{aligned} \quad (\text{A.2})$$

If s is a number greater than 1, we know that

$$\sum_{i=1}^n (1/s)^i = (s^n - 1)/s^n(s - 1).$$

If $s = s_1/s_2$ with $s_1 > s_2$ then

$$\sum_{i=1}^n (1/s)^i = (s_1^n - s_2^n) s_2 / s_1^n (s_1 - s_2).$$

Let $a > 4$; thus (A.2) is equal to

$$\frac{(a+1) \sqrt{2}^{(m+2)k_i} \sqrt{a}^{n_i}}{\sqrt{2} a} \frac{\sqrt{a}^{n_i} - 2^{n_i}}{\sqrt{a}^{n_i} (\sqrt{a} - 2)} = \frac{(a+1)}{\sqrt{2} a (\sqrt{a} - 2)} (\sqrt{a}^{n_i} - 2^{n_i}) \sqrt{2}^{(m+2)k_i}.$$

Let us compute now the term

$$\prod_{i=1}^h p^{k_i} \left(\sum_{n'_i=1}^{n_i} (a+1) a^{(n_i-n'_i)/2-1} \sum_{q=1}^{(mk_i-1)/2+n'_i-1} \binom{q+k_i-1}{k_i-1} \right). \quad (\text{A.3})$$

We have that (A.3) is less than

$$\begin{aligned} & \frac{(a+1)}{\sqrt{2} a (\sqrt{a} - 2)} \prod_{i=1}^h (\sqrt{a}^{n_i} - 2^{n_i}) p^{k_i} \sqrt{2}^{(m+2)k_i} = \\ & \frac{(a+1)}{\sqrt{2} a (\sqrt{a} - 2)} (\sqrt{a}^{n_1} - 2^{n_1}) \cdots (\sqrt{a}^{n_h} - 2^{n_h}) (p\sqrt{2}^{m+2})^{k_1+\cdots+k_h} = \\ & \frac{(a+1)}{\sqrt{2} a (\sqrt{a} - 2)} (\sqrt{a}^{n_1} - 2^{n_1}) \cdots (\sqrt{a}^{n_h} - 2^{n_h}) c^{k_1+\cdots+k_h}, \end{aligned}$$

where $c = p\sqrt{2}^{m+2} = 4p\sqrt{2}^m$.

Let us compute the term

$$\begin{aligned} & \sum_{k_1+\cdots+k_h \leq k} \prod_{i=1}^h p^{k_i} \\ & \left(\sum_{n'_i=1}^{n_i} (a+1) a^{(n_i-n'_i)/2-1} \sum_{q=1}^{(mk_i-1)/2+n'_i-1} \binom{q+k_i-1}{k_i-1} \right). \quad (\text{A.4}) \end{aligned}$$

We have that (A.4) is less than

$$\sum_{k_1+\dots+k_h \leq k} \frac{(a+1)}{\sqrt{2}a(\sqrt{a}-2)} (\sqrt{a}^{n_1} - 2^{n_1}) \dots (\sqrt{a}^{n_h} - 2^{n_h}) c^{k_1+\dots+k_h} =$$

$$\frac{(a+1)}{\sqrt{2}a(\sqrt{a}-2)} (\sqrt{a}^{n_1} - 2^{n_1}) \dots (\sqrt{a}^{n_h} - 2^{n_h}) \sum_{k_1+\dots+k_h \leq k} c^{k_1+\dots+k_h}.$$

We have that

$$\sum_{k_1+\dots+k_h \leq k} c^{k_1+\dots+k_h} = \sum_{\alpha=1}^k \sum_{k_1+\dots+k_h=\alpha} c^{k_1+\dots+k_h} =$$

$$= \sum_{\alpha=h}^k \binom{\alpha-1}{h-1} c^\alpha < \binom{k-1}{h-1} \sum_{\alpha=h}^k c^\alpha =$$

$$= \binom{k-1}{h-1} \frac{c^{k+1} - c^h}{c-1}.$$

Thus (A.4) is less than

$$\frac{(a+1)}{\sqrt{2}a(\sqrt{a}-2)} (\sqrt{a}^{n_1} - 2^{n_1}) \dots (\sqrt{a}^{n_h} - 2^{n_h}) \binom{k-1}{h-1} \frac{c^{k+1} - c^h}{c-1}.$$

We have that

$$\sum_{j=1}^{h-1} (h-j)n_j < (h-1)^2(n-h+1)$$

since every n_j is less or equal to $n-h+1$ because $n_1 + \dots + n_h \leq n$.

We have also that

$$\sum_{n_1+\dots+n_h \leq n} (\sqrt{a}^{n_1} - 2^{n_1}) \dots (\sqrt{a}^{n_h} - 2^{n_h}) < \sum_{n_1+\dots+n_h \leq n} \sqrt{a}^{n_1} \dots \sqrt{a}^{n_h} =$$

$$\sum_{l=1}^n \sum_{n_1+\dots+n_h=l} \sqrt{a}^{n_1+\dots+n_h} = \sum_{l=h}^n \binom{l-1}{h-1} \sqrt{a}^l < \binom{n-1}{h-1} \frac{\sqrt{a}^n - \sqrt{a}^h}{\sqrt{a}-1}.$$

Now we compute

$$\sum_{n_1+\dots+n_h \leq n} \sum_{j=1}^{h-1} (h-j)n_j \sum_{k_1+\dots+k_h \leq k} \quad (\text{A.5})$$

$$\prod_{i=1}^h p^{k_i} \left(\sum_{n'_i=1}^{n_i} (a+1)a^{(n_i-n'_i)/2-1} \sum_{q=1}^{(mk_i-1)/2+n'_i-1} \binom{q+k_i-1}{k_i-1} \right).$$

We have that (A.5) is less than

$$d(h-1)^2(n-h+1) \binom{n-1}{h-1} \binom{k-1}{h-1} (\sqrt{a}^n - \sqrt{a}^h) (c^k - c^{h-1}),$$

where

$$d = \frac{(a+1)c}{\sqrt{2}a(\sqrt{a}-2)(\sqrt{a}-1)(c-1)}.$$

This implies that (A.1) is bounded above by

$$d\sqrt{a}^n c^k \sum_{h=2}^{\min(k,n)} (h-1)^2(n-h+1) \binom{n-1}{h-1} \binom{k-1}{h-1}.$$

Using the equality

$$\sum_{h=2}^n (h-1)^2 \binom{n-1}{h-1} = (n-1 + (n-1)^2)2^{n-3} = n(n-1)2^{n-3}$$

(see [2], 6b), we have that (A.5) is less than

$$d\sqrt{a}^n c^k n \sum_{h=2}^n (h-1)^2 \binom{n-1}{h-1} \sum_{h=2}^k \binom{k-1}{h-1} <$$

$$d\sqrt{a}^n c^k n^2 (n-1)2^{n-3} 2^{k-1} =$$

$$\frac{d}{16} n^2 (n-1) \sqrt{a}^n c^k 2^{n+k} = d' n^2 (n-1) \beta^n \gamma^k, \quad (\text{A.6})$$

where $\beta = 2\sqrt{a} = 2\sqrt{2|X|-1}$, $\gamma = 2c = 4p\sqrt{2}^m = 4\sqrt{2}^m |R|$ (we recall that m is the maximal length of the elements of R) and

$$d' = \frac{d}{16} = \frac{(a+1)c}{16\sqrt{2}a(\sqrt{a}-2)(\sqrt{a}-1)(c-1)} \approx \frac{1}{16\sqrt{2}a}.$$

For $a < 4$ with analogous calculations we prove that (A.5) is less than

$$bn^2(n-1)4^n\gamma^k,$$

where

$$b \approx \frac{1}{16\sqrt{2}(2-\sqrt{a})}.$$

We recall that since $a = 2|X| - 1$, then a cannot be equal to 4 since it is odd.

We have thus proved that an upper bound for the complexity of our method is a product of a cubic polynomial times an exponential in n and one in k . This is much better than (1.15), the complexity with the method currently known in the literature, which is a product of three exponentials, one in k , one in kn and one in k^2 .

Let us compute the ratio of the complexity of the classical method over that of ours; for $a > 4$ it is

$$\frac{\left(\frac{a+1}{a-1}\right)^k p^k a^{mk^2+kn}}{n^2(n-1)p^k a^{n/2} 4^k 2^{mk/2}}. \quad (\text{A.7})$$

We can assume that $\left(\frac{a+1}{a-1}\right)^k > n^2(n-1)$ and since $a > 4$ then (A.7) is greater than

$$\frac{a^{mk^2+kn}}{a^{n/2+k+mk/2}} = a^{k(mk-m/2-1)+n(k-1/2)} > a^{k(k-c_1)+n(k-c_2)},$$

where $c_1 = m/2 + 1$ and $c_2 = 1/2$. For $a < 4$ we obtain the same result but with $c_1 = m/2 + 2$ and $c_2 = 2$.

Moreover (A.6) is far from being an optimal bound for the complexity of our method, but only a value which is obtainable with not too complicated calculations. Instead (1.15) is the real complexity of the classical method, that is it is the exact number of words to be considered with this method to find all the relators of length up to n and area up to k .

A.2 Recursively defined sets and straight line algorithms

Let U be a set and let Φ be a family of functions $\varphi : U^{n_\varphi} \rightarrow U$ (where n_φ is a given non-zero natural number depending on φ) with codomain U and with domain some Cartesian power of U . Let $T \subset U$; we say that T is Φ -closed if for every $\varphi \in \Phi$ and for every $t_1, \dots, t_{n_\varphi} \in T$ we have that $\varphi(t_1, \dots, t_{n_\varphi}) \in T$.

Definition A.2.1 Let $B \subset U$; the intersection of all Φ -closed subsets of U containing B is called *the subset of U recursively defined by B and Φ* .

B is called the *base set* and Φ *the set of operations*. Since an intersection of Φ -closed sets is still Φ -closed, *the subset of U recursively defined by B and Φ is the least Φ -closed subset of U containing B* .

Let C be the set of the results of the straight line algorithms (Definition 2.1.1) relative to (U, B, Φ) . We will now show that C coincides with the subset of U recursively defined by B and Φ .

Proposition A.2.2 C is Φ -closed.

Proof Let $\varphi \in \Phi$ and let $c_1, \dots, c_{n_\varphi} \in C$; we have to prove that

$$\varphi(c_1, \dots, c_{n_\varphi}) \in C.$$

Let $\sigma_1, \dots, \sigma_{n_\varphi}$ be *SLA*'s computing respectively $c_1, \dots, c_{n_\varphi}$. The algorithm whose steps are the steps of all the σ_i plus a last step equal to the application of φ to $c_1, \dots, c_{n_\varphi}$ is an *SLA* and its result is $\varphi(c_1, \dots, c_{n_\varphi})$. \square

Let $b \in B$; b is the result of the *SLA* with a single step equal to b , that is $b \in C$ and therefore $B \subset C$. Since C is Φ -closed and contains B , then by Definition A.2.1, C contains the subset of U recursively defined by B and Φ . The following theorem implies the opposite inclusion.

Proposition A.2.3 C is contained in any Φ -closed subset of U containing B .

Proof Let T be a Φ -closed subset of U containing B . If $c \in C$ then there exists an *SLA* σ whose result is c . We prove that the output of every step of σ (and in particular c) belongs to T .

Since the first step of σ is a base step, the first output is an element of B , which is contained in T . Suppose that the first $k - 1$ outputs of σ

belong to T . If the k -th is a base step, then its output is an element of B and therefore of T ; if not, there exist $\varphi \in \Phi$ and $c_1, \dots, c_{n_\varphi}$ outputs of preceding steps such that the output of the k -th step is $\varphi(c_1, \dots, c_{n_\varphi})$. Since $c_1, \dots, c_{n_\varphi}$ belong to T by induction hypothesis and since T is Φ -closed, then $\varphi(c_1, \dots, c_{n_\varphi}) \in T$. \square

We have thus proved the following result

Theorem A.2.4 *Let C be the set of the results of the straight line algorithms relative to (U, B, Φ) . Then C coincides with the subset of U recursively defined by B and Φ .*

Remark A.2.5 Proposition A.2.3 is a generalization of the *Principle of mathematical induction* (see [4]); it can be stated in the following way:

Let U be a set and let Φ be a family of functions $\varphi : U^{n_\varphi} \rightarrow U$ (where n_φ is a given non-zero natural number depending on φ) with codomain U and with domain some Cartesian power of U . Let \mathcal{P} be a proposition defined on a set U , let B be a subset of U and let \mathcal{P} be such that:

- \mathcal{P} is true for every element of B ;
- if $\varphi \in \Phi$ and if \mathcal{P} is true for $c_1, \dots, c_{n_\varphi}$ then \mathcal{P} is true also for $\varphi(c_1, \dots, c_{n_\varphi})$.

Then \mathcal{P} is true for every element of the subset of U recursively defined by B and Φ .

A.3 A long calculation

Remark A.3.1 Let x and w be cyclically reduced words and let w be a cyclic conjugate of $\pi(u, v)$, where u and v are cyclically reduced words. Let $y := \pi(x, w)$; we show that there exist words x', u', v' and y' which are cyclic conjugates of x, u, v and y respectively such that

- either $y' = \pi(p, u')$ where p is a cyclic conjugate of $\pi(x', v')$
- or $y' = \pi(p, v')$ where p is a cyclic conjugate of $\pi(x', u')$.

Proof There exist words w_1 and w_2 such that $w = w_1 w_2$ and $\pi(u, v) = w_2 w_1$. Thus by Remark 2.2.3, four cases are possible:

1. $u = u_1 a, \quad v = a^{-1} t w_2 w_1 t^{-1} u_1^{-1}$.

2. $u = tw_2w_4a$, $v = a^{-1}w_3t^{-1}$ and $w_4w_3 = w_1$.
3. $u = tw_3a$, $v = a^{-1}w_4w_1t^{-1}$ and $w_3w_4 = w_2$.
4. $u = v_1^{-1}tw_2w_1t^{-1}a$, $v = a^{-1}v_1$.

Again by Remark 2.2.3, three cases are possible:

- (a) $x = x_1b$, $w = b^{-1}sys^{-1}x_1^{-1}$.
- (b) $x = sy_1b$, $w = b^{-1}y_2s^{-1}$.
- (c) $x = w_5^{-1}sys^{-1}b$, $w = b^{-1}w_5$.

Cases (a), (b) and (c) split again. (a) splits in five cases:

- I There exist words b_1 and b_2 such that $b^{-1} = b_2^{-1}b_1^{-1}$ and $w_1 = b_2^{-1}$, $w_2 = b_1^{-1}sys^{-1}x_1^{-1}$.
- II There exist words s_1 and s_2 such that $s = s_1s_2$ and $w_1 = b^{-1}s_1$, $w_2 = s_2ys_2^{-1}s_1^{-1}x_1^{-1}$.
- III There exist words y_1 and y_2 such that $y = y_1y_2$ and $w_1 = b^{-1}sy_1$, $w_2 = y_2s^{-1}x_1^{-1}$.
- IV There exist words s_1 and s_2 such that $s = s_1s_2$ and $w_1 = b^{-1}s_1s_2ys_2^{-1}$, $w_2 = s_1^{-1}x_1^{-1}$.
- V There exist words x_2 and x_3 such that $x_1^{-1} = x_3^{-1}x_2^{-1}$ and $w_1 = b^{-1}sys^{-1}x_3^{-1}$, $w_2 = x_2^{-1}$.

(b) splits in three cases:

- I There exist words b_1 and b_2 such that $b^{-1} = b_2^{-1}b_1^{-1}$ and $w_1 = b_2^{-1}$, $w_2 = b_1^{-1}y_2s^{-1}$.
- II There exist words y_3 and y_4 such that $y_2 = y_3y_4$ and $w_1 = b^{-1}y_3$, $w_2 = y_4s^{-1}$.
- III There exist words s_1 and s_2 such that $s = s_1s_2$ and $w_1 = b^{-1}y_2s_2^{-1}$, $w_2 = s_1^{-1}$.

(c) splits in two cases:

I There exist words b_1 and b_2 such that $b^{-1} = b_2^{-1}b_1^{-1}$ and $w_1 = b_2^{-1}$,
 $w_2 = b_1^{-1}w_5$.

II There exists a word w_6 such that $w_5 = w_6w_2$ and $w_1 = b^{-1}w_6$.

Let us examine them all.

1 a I.

$$\begin{aligned} x &= x_1b_1b_2, \quad u = u_1a, \quad v = a^{-1}tb_1^{-1}sys^{-1}x_1^{-1}b_2^{-1}t^{-1}u_1^{-1}, \\ w &= w_1w_2 = b_2^{-1}b_1^{-1}sys^{-1}x_1^{-1}. \end{aligned}$$

$$y = \pi(x, w) = \pi(x_1b_1b_2, b_2^{-1}b_1^{-1}sys^{-1}x_1^{-1}).$$

$$x = x_1b_1b_2 \rightarrow b_1b_2x_1,$$

$$v = a^{-1}tb_1^{-1}sys^{-1}x_1^{-1}b_2^{-1}t^{-1}u_1^{-1} \rightarrow x_1^{-1}b_2^{-1}t^{-1}u_1^{-1}a^{-1}tb_1^{-1}sys^{-1}$$

$$\pi(b_1b_2x_1, x_1^{-1}b_2^{-1}t^{-1}u_1^{-1}a^{-1}tb_1^{-1}sys^{-1}) = b_1t^{-1}u_1^{-1}a^{-1}tb_1^{-1}sys^{-1}$$

because b_1t^{-1} and $s^{-1}b_1$ are subwords of v^{-1} .

$$b_1t^{-1}u_1^{-1}a^{-1}tb_1^{-1}sys^{-1} \rightarrow tb_1^{-1}sys^{-1}b_1t^{-1}u_1^{-1}a^{-1},$$

$$u = u_1a \rightarrow au_1$$

and

$$\pi(tb_1^{-1}sys^{-1}b_1t^{-1}u_1^{-1}a^{-1}, au_1) = y.$$

1 a II.

$$\begin{aligned} x &= x_1b, \quad u = u_1a, \quad v = a^{-1}ts_2ys_2^{-1}s_1^{-1}x_1^{-1}b^{-1}s_1t^{-1}u_1^{-1}, \\ w &= w_1w_2 = b^{-1}s_1s_2ys_2^{-1}s_1^{-1}x_1^{-1} \end{aligned}$$

$$y = \pi(x, w) = \pi(x_1b, b^{-1}s_1s_2ys_2^{-1}s_1^{-1}x_1^{-1}).$$

$$x = x_1b \rightarrow bx_1,$$

$$v = a^{-1}ts_2y s_2^{-1}s_1^{-1}x_1^{-1}b^{-1}s_1t^{-1}u_1^{-1} \rightarrow x_1^{-1}b^{-1}s_1t^{-1}u_1^{-1}a^{-1}ts_2y s_2^{-1}s_1^{-1}$$

$$\pi(bx_1, x_1^{-1}b^{-1}s_1t^{-1}u_1^{-1}a^{-1}ts_2y s_2^{-1}s_1^{-1}) = t^{-1}u_1^{-1}a^{-1}ts_2y s_2^{-1}$$

because $s_2^{-1}t^{-1}$ is a subword of v^{-1} .

$$t^{-1}u_1^{-1}a^{-1}ts_2y s_2^{-1} \rightarrow ts_2y s_2^{-1}t^{-1}u_1^{-1}a^{-1},$$

$$u = u_1a \rightarrow au_1$$

and

$$\pi(ts_2y s_2^{-1}t^{-1}u_1^{-1}a^{-1}, au_1) = y.$$

1 a III.

$$x = x_1b, \quad u = u_1a, \quad v = a^{-1}ty_2s^{-1}x_1^{-1}b^{-1}sy_1t^{-1}u_1^{-1},$$

$$w = w_1w_2 = b^{-1}sy_1y_2s^{-1}x_1^{-1}.$$

$$y = \pi(x, w) = \pi(x_1b, b^{-1}sy_1y_2s^{-1}x_1^{-1}).$$

$$x = x_1b \rightarrow bx_1,$$

$$v = a^{-1}ty_2s^{-1}x_1^{-1}b^{-1}sy_1t^{-1}u_1^{-1} \rightarrow x_1^{-1}b^{-1}sy_1t^{-1}u_1^{-1}a^{-1}ty_2s^{-1}$$

and

$$\pi(bx_1, x_1^{-1}b^{-1}sy_1t^{-1}u_1^{-1}a^{-1}ty_2s^{-1}) = y_1t^{-1}u_1^{-1}a^{-1}ty_2$$

because y_2y_1 is a cyclic conjugation of y which is cyclically reduced.

$$y_1t^{-1}u_1^{-1}a^{-1}ty_2 \rightarrow ty_2y_1t^{-1}u_1^{-1}a^{-1},$$

$$u = u_1a \rightarrow au_1$$

and

$$\pi(ty_2y_1t^{-1}u_1^{-1}a^{-1}, au_1) = y_2y_1$$

and finally

$$y_2y_1 \rightarrow y.$$

1 a IV.

$$x = x_1b, \quad u = u_1a, \quad v = a^{-1}ts_1^{-1}x_1^{-1}b^{-1}s_1s_2ys_2^{-1}t^{-1}u_1^{-1},$$

$$w = w_1w_2 = b^{-1}s_1s_2ys_2^{-1}s_1^{-1}x_1^{-1}.$$

$$y = \pi(x, w) = \pi(x_1b, b^{-1}s_1s_2ys_2^{-1}s_1^{-1}x_1^{-1}).$$

$$x = x_1b \rightarrow bx_1,$$

$$v = a^{-1}ts_1^{-1}x_1^{-1}b^{-1}s_1s_2ys_2^{-1}t^{-1}u_1^{-1} \rightarrow x_1^{-1}b^{-1}s_1s_2ys_2^{-1}t^{-1}u_1^{-1}a^{-1}ts_1^{-1}$$

and

$$\pi(bx_1, x_1^{-1}b^{-1}s_1s_2ys_2^{-1}t^{-1}u_1^{-1}a^{-1}ts_1^{-1}) = s_2ys_2^{-1}t^{-1}u_1^{-1}a^{-1}t$$

because ts_2 is a subword of v^{-1} .

$$s_2ys_2^{-1}t^{-1}u_1^{-1}a^{-1}t \rightarrow ts_2ys_2^{-1}t^{-1}u_1^{-1}a^{-1},$$

$$u = u_1a \rightarrow au_1$$

and

$$\pi(ts_2ys_2^{-1}t^{-1}u_1^{-1}a^{-1}, au_1) = y.$$

1 a V.

$$x = x_2x_3b, \quad u = u_1a, \quad v = a^{-1}tx_2^{-1}b^{-1}sys^{-1}x_3^{-1}t^{-1}u_1^{-1},$$

$$w = w_1w_2 = b^{-1}sys^{-1}x_3^{-1}x_2^{-1}.$$

$$y = \pi(x, w) = \pi(x_2x_3b, b^{-1}sys^{-1}x_3^{-1}x_2^{-1}).$$

$$x = x_2x_3b \rightarrow x_3bx_2,$$

$$v = a^{-1}tx_2^{-1}b^{-1}sy s^{-1}x_3^{-1}t^{-1}u_1^{-1} \rightarrow x_2^{-1}b^{-1}sy s^{-1}x_3^{-1}t^{-1}u_1^{-1}a^{-1}t$$

$$\pi(x_3bx_2, x_2^{-1}b^{-1}sy s^{-1}x_3^{-1}t^{-1}u_1^{-1}a^{-1}t) = x_3sy s^{-1}x_3^{-1}t^{-1}u_1^{-1}a^{-1}t$$

because x_3s and tx_3 are subwords of v^{-1} .

$$x_3sy s^{-1}x_3^{-1}t^{-1}u_1^{-1}a^{-1}t \rightarrow tx_3sy s^{-1}x_3^{-1}t^{-1}u_1^{-1}a^{-1},$$

$$u = u_1a \rightarrow au_1$$

and

$$\pi(tx_3sy s^{-1}x_3^{-1}t^{-1}u_1^{-1}a^{-1}, au_1) = y.$$

1 b I.

$$x = sy_1b_1b_2, \quad u = u_1a, \quad v = a^{-1}tb_1^{-1}y_2s^{-1}b_2^{-1}t^{-1}u_1^{-1},$$

$$w = w_1w_2 = b_2^{-1}b_1^{-1}y_2s^{-1}.$$

$$y = \pi(x, w) = \pi(sy_1b_1b_2, b_2^{-1}b_1^{-1}y_2s^{-1}).$$

$$x = sy_1b_1b_2 \rightarrow y_1b_1b_2s,$$

$$v = a^{-1}tb_1^{-1}y_2s^{-1}b_2^{-1}t^{-1}u_1^{-1} \rightarrow s^{-1}b_2^{-1}t^{-1}u_1^{-1}a^{-1}tb_1^{-1}y_2$$

$$\pi(y_1b_1b_2s, s^{-1}b_2^{-1}t^{-1}u_1^{-1}a^{-1}tb_1^{-1}y_2) = y_1b_1t^{-1}u_1^{-1}a^{-1}tb_1^{-1}y_2$$

because b_1t^{-1} is a subword of v^{-1} and y_2y_1 is a cyclic conjugation of y which is cyclically reduced.

$$y_1b_1t^{-1}u_1^{-1}a^{-1}tb_1^{-1}y_2 \rightarrow tb_1^{-1}y_2y_1b_1t^{-1}u_1^{-1}a^{-1},$$

$$u = u_1a \rightarrow au_1$$

and

$$\pi(tb_1^{-1}y_2y_1b_1t^{-1}u_1^{-1}a^{-1}, au_1) = y_2y_1$$

and finally

$$y_2y_1 \rightarrow y.$$

1 b II.

$$x = sy_1b, \quad u = u_1a, \quad v = a^{-1}ty_4s^{-1}b^{-1}y_3t^{-1}u_1^{-1},$$

$$w = w_1w_2 = b^{-1}y_3y_4s^{-1}.$$

$$y = \pi(x, w) = \pi(sy_1b, b^{-1}y_3y_4s^{-1}).$$

$$x = sy_1b \rightarrow y_1bs,$$

$$v = a^{-1}ty_4s^{-1}b^{-1}y_3t^{-1}u_1^{-1} \rightarrow s^{-1}b^{-1}y_3t^{-1}u_1^{-1}a^{-1}ty_4$$

$$\pi(y_1bs, s^{-1}b^{-1}y_3t^{-1}u_1^{-1}a^{-1}ty_4) = y_1y_3t^{-1}u_1^{-1}a^{-1}ty_4$$

because y_1y_3 and y_4y_1 are subwords of y and of a cyclic conjugate of y .

$$y_1y_3t^{-1}u_1^{-1}a^{-1}ty_4 \rightarrow ty_4y_1y_3t^{-1}u_1^{-1}a^{-1},$$

$$u = u_1a \rightarrow au_1$$

and

$$\pi(ty_4y_1y_3t^{-1}u_1^{-1}a^{-1}, au_1) = y_4y_1y_3$$

and finally

$$y_4y_1y_3 \rightarrow y.$$

1 b III.

$$x = s_1s_2y_1b, \quad u = u_1a, \quad v = a^{-1}ts_1^{-1}b^{-1}y_2s_2^{-1}t^{-1}u_1^{-1},$$

$$w = w_1w_2 = b^{-1}y_2s_2^{-1}s_1^{-1}.$$

$$y = \pi(x, w) = \pi(s_1s_2y_1b, b^{-1}y_2s_2^{-1}s_1^{-1}).$$

$$x = s_1 s_2 y_1 b \rightarrow s_2 y_1 b s_1,$$

$$v = a^{-1} t s_1^{-1} b^{-1} y_2 s_2^{-1} t^{-1} u_1^{-1} \rightarrow s_1^{-1} b^{-1} y_2 s_2^{-1} t^{-1} u_1^{-1} a^{-1} t$$

$$\pi(s_2 y_1 b s_1, s_1^{-1} b^{-1} y_2 s_2^{-1} t^{-1} u_1^{-1} a^{-1} t) = s_2 y_1 y_2 s_2^{-1} t^{-1} u_1^{-1} a^{-1} t$$

because $y_1 y_2 = y$ is reduced and $t s_2$ is a subword of v^{-1} .

$$s_2 y s_2^{-1} t^{-1} u_1^{-1} a^{-1} t \rightarrow t s_2 y s_2^{-1} t^{-1} u_1^{-1} a^{-1},$$

$$u = u_1 a \rightarrow a u_1$$

and

$$\pi(t s_2 y s_2^{-1} t^{-1} u_1^{-1} a^{-1}, a u_1) = y.$$

1 c I.

$$x = w_5^{-1} s y s^{-1} b_1 b_2, \quad u = u_1 a, \quad v = a^{-1} t b_1^{-1} w_5 b_2^{-1} t^{-1} u_1^{-1},$$

$$w = w_1 w_2 = b_2^{-1} b_1^{-1} w_1.$$

$$y = \pi(x, w) = \pi(w_5^{-1} s y s^{-1} b_1 b_2, b_2^{-1} b_1^{-1} w_1).$$

$$x = w_5^{-1} s y s^{-1} b_1 b_2 \rightarrow s y s^{-1} b_1 b_2 w_1^{-1},$$

$$v = a^{-1} t b_1^{-1} w_5 b_2^{-1} t^{-1} u_1^{-1} \rightarrow w_1 b_2^{-1} t^{-1} u_1^{-1} a^{-1} t b_1^{-1}$$

and

$$\pi(s y s^{-1} b_1 b_2 w_5^{-1}, w_5 b_2^{-1} t^{-1} u_1^{-1} a^{-1} t b_1^{-1}) = s y s^{-1} b_1 t^{-1} u_1^{-1} a^{-1} t b_1^{-1}$$

because $b_1 t^{-1}$ and $b_1 s$ are subwords of v^{-1} and x^{-1} respectively.

$$s y s^{-1} b_1 t^{-1} u_1^{-1} a^{-1} t b_1^{-1} \rightarrow t b_1^{-1} s y s^{-1} b_1 t^{-1} u_1^{-1} a^{-1},$$

$$u = u_1 a \rightarrow a u_1$$

and

$$\pi(tb_1^{-1}sys^{-1}b_1t^{-1}u_1^{-1}a^{-1}, au_1) = y.$$

1 c II.

$$x = w_2^{-1}w_6^{-1}sys^{-1}b, \quad u = u_1a, \quad v = a^{-1}tw_2b^{-1}w_6t^{-1}u_1^{-1}, \\ w = w_1w_2 = b^{-1}w_6w_2.$$

$$y = \pi(x, w) = \pi(w_2^{-1}w_6^{-1}sys^{-1}b, b^{-1}w_6w_2).$$

$$x = w_2^{-1}w_6^{-1}sys^{-1}b \rightarrow w_6^{-1}sys^{-1}bw_2^{-1},$$

$$v = a^{-1}tw_2b^{-1}w_6t^{-1}u_1^{-1} \rightarrow w_2b^{-1}w_6t^{-1}u_1^{-1}a^{-1}t$$

and

$$\pi(w_6^{-1}sys^{-1}bw_2^{-1}, w_2b^{-1}w_6t^{-1}u_1^{-1}a^{-1}t) = w_6^{-1}sys^{-1}w_6t^{-1}u_1^{-1}a^{-1}t$$

because $s^{-1}w_6$ and tw_6^{-1} are subwords of x^{-1} and v^{-1} respectively.

$$w_6^{-1}sys^{-1}w_6t^{-1}u_1^{-1}a^{-1}t \rightarrow tw_6^{-1}sys^{-1}w_6t^{-1}u_1^{-1}a^{-1},$$

$$u = u_1a \rightarrow au_1$$

and

$$\pi(tw_6^{-1}sys^{-1}w_6t^{-1}u_1^{-1}a^{-1}, au_1) = y.$$

2 a I.

$$x = x_1b_1w_3^{-1}w_4^{-1}, \quad u = tb_1^{-1}sys^{-1}x_1^{-1}w_4a, \quad v = a^{-1}w_3t^{-1}, \\ w_4w_3 = b_2^{-1}, \quad w = w_1w_2 = w_4w_3b_1^{-1}sys^{-1}x_1^{-1}.$$

$$y = \pi(x, w) = \pi(x_1b_1b_2, b_2^{-1}b_1^{-1}sys^{-1}x_1^{-1}).$$

$$x = x_1b_1w_3^{-1}w_4^{-1} \rightarrow b_1w_3^{-1}w_4^{-1}x_1,$$

$$u = tb_1^{-1}sys^{-1}x_1^{-1}w_4a \rightarrow x_1^{-1}w_4atb_1^{-1}sys^{-1}$$

and

$$\pi(b_1 w_3^{-1} w_4^{-1} x_1, x_1^{-1} w_4 a t b_1^{-1} s y s^{-1}) = b_1 w_3^{-1} a t b_1^{-1} s y s^{-1}$$

because $w_3^{-1} a$ and $s^{-1} b_1$ are subwords of v^{-1} and w^{-1} respectively.

$$b_1 w_3^{-1} a t b_1^{-1} s y s^{-1} \rightarrow b_1^{-1} s y s^{-1} b_1 w_3^{-1} a t,$$

$$v = a^{-1} w_3 t^{-1} \rightarrow t^{-1} a^{-1} w_3,$$

and

$$\pi(b_1^{-1} s y s^{-1} b_1 w_3^{-1} a t, t^{-1} a^{-1} w_3) = y.$$

2 a II.

$$x = x_1 b, \quad u = t s_2 y s_2^{-1} s_1^{-1} x_1^{-1} w_4 a, \quad v = a^{-1} w_3 t^{-1} \\ w_4 w_3 = b^{-1} s_1, \quad w = w_4 w_3 w_2 = b^{-1} s_1 s_2 y s_2^{-1} s_1^{-1} x_1^{-1}.$$

$$y = \pi(x, w) = \pi(x_1 b, b^{-1} s_1 s_2 y s_2^{-1} s_1^{-1} x_1^{-1}).$$

$$x = x_1 b \rightarrow b x_1,$$

$$u = t s_2 y s_2^{-1} s_1^{-1} x_1^{-1} w_4 a \rightarrow x_1^{-1} w_4 a t s_2 y s_2^{-1} s_1^{-1} \equiv x_1^{-1} b^{-1} s_1 w_3^{-1} a t s_2 y s_2^{-1} s_1^{-1}$$

since $w_4 \equiv b^{-1} s_1 w_3^{-1}$. We observe that the last word of the preceding line is not necessarily reduced.

$$\pi(b x_1, x_1^{-1} b^{-1} s_1 w_3^{-1} a t s_2 y s_2^{-1} s_1^{-1}) = w_3^{-1} a t s_2 y s_2^{-1}$$

because $w_3^{-1} a$ is a subword of v^{-1} ; moreover $w_3 s_2$ is reduced because the last letter of w_3 is equal to the last of s_1 which is not opposite to the first of s_2 .

$$w_3^{-1} a t s_2 y s_2^{-1} \rightarrow s_2 y s_2^{-1} w_3^{-1} a t,$$

$$v = a^{-1} w_3 t^{-1} \rightarrow t^{-1} a^{-1} w_3$$

and

$$\pi(s_2 y s_2^{-1} w_3^{-1} a t, t^{-1} a^{-1} w_3) = y.$$

2 a III.

$$x = x_1b, \quad u = ty_2s^{-1}x_1^{-1}w_4a, \quad v = a^{-1}w_3t^{-1} \text{ and } w_4w_3 = b^{-1}sy_1$$

$$w = w_4w_3w_2 = b^{-1}sys^{-1}x_1^{-1}$$

$$y = \pi(x, w) = \pi(x_1b, b^{-1}sys^{-1}x_1^{-1}).$$

$$x = x_1b \rightarrow bx_1,$$

$$u = ty_2s^{-1}x_1^{-1}w_4a \rightarrow x_1^{-1}w_4aty_2s^{-1} \equiv x_1^{-1}b^{-1}sy_1w_3^{-1}aty_2s^{-1}$$

since $w_4 \equiv b^{-1}sy_1w_3^{-1}$. The last word of the preceding line is not necessarily reduced.

$$\pi(bx_1, x_1^{-1}b^{-1}sy_1w_3^{-1}aty_2s^{-1}) = y_1w_3^{-1}aty_2$$

because y_2y_1 is reduced being a cyclic conjugate of y .

$$y_1w_3^{-1}aty_2 \rightarrow y_2y_1w_3^{-1}at,$$

$$v = a^{-1}w_3t^{-1} \rightarrow t^{-1}a^{-1}w_3$$

and

$$\pi(y_2y_1w_3^{-1}at, t^{-1}a^{-1}w_3) = y_2y_1.$$

Finally

$$y_2y_1 \rightarrow y.$$

2 a IV.

$$x = x_1b, \quad u = ts_1^{-1}x_1^{-1}w_4a, \quad v = a^{-1}w_3t^{-1},$$

$$w_4w_3 = b^{-1}s_1s_2ys_2^{-1}, \quad w = w_4w_3w_2 = b^{-1}s_1s_2ys_2^{-1}s_1^{-1}x_1^{-1}.$$

$$y = \pi(x, w) = \pi(x_1b, b^{-1}s_1s_2ys_2^{-1}s_1^{-1}x_1^{-1}).$$

$$x = x_1b \rightarrow bx_1,$$

$$u = ts_1^{-1}x_1^{-1}w_4a \rightarrow x_1^{-1}w_4ats_1^{-1} \equiv x_1^{-1}b^{-1}s_1s_2ys_2^{-1}w_3^{-1}ats_1^{-1}$$

since $w_4 \equiv b^{-1}s_1s_2ys_2^{-1}w_3^{-1}$. The last word of the preceding line is not necessarily reduced.

$$\pi(bx_1, x_1^{-1}b^{-1}s_1s_2ys_2^{-1}w_3^{-1}ats_1^{-1}) = s_2ys_2^{-1}w_3^{-1}at$$

since tw_3^{-1} is reduced being a subword of v^{-1} , thus ts_2 is reduced because the first letter of w_3^{-1} is equal to the first of s_2 .

$$v = a^{-1}w_3t^{-1} \rightarrow t^{-1}a^{-1}w_3$$

and

$$\pi(s_2ys_2^{-1}w_3^{-1}at, t^{-1}a^{-1}w_3) = y.$$

2 a V.

$$\begin{aligned} x &= w_2^{-1}x_3b, & u &= tw_2w_4a, & v &= a^{-1}w_3t^{-1}, \\ w_4w_3 &= b^{-1}sys^{-1}x_3^{-1}, & w &= w_4w_3w_2 = b^{-1}sys^{-1}x_3^{-1}x_2^{-1}. \end{aligned}$$

$$y = \pi(x, w) = \pi(w_2^{-1}x_3b, b^{-1}sys^{-1}x_3^{-1}x_2^{-1}).$$

$$x = w_2^{-1}x_3b \rightarrow x_3bw_2^{-1},$$

$$u = tw_2w_4a \rightarrow w_2w_4at \equiv w_2b^{-1}sys^{-1}x_3^{-1}w_3^{-1}at$$

since $w_4 \equiv b^{-1}sys^{-1}x_3^{-1}w_3^{-1}$. The last word of the preceding line is not necessarily reduced.

$$\pi(x_3bw_2^{-1}, w_2b^{-1}sys^{-1}x_3^{-1}w_3^{-1}at) = x_3sys^{-1}x_3^{-1}w_3^{-1}at$$

because x_3s is reduced being a subword of w^{-1} ; moreover tw_3 is reduced being a subword of v^{-1} , thus tx_3 is reduced because the first letter of x_3 is equal to the first of v .

$$v = a^{-1}w_3t^{-1} \rightarrow t^{-1}a^{-1}w_3$$

and

$$\pi(x_3sys^{-1}x_3^{-1}w_3^{-1}at, t^{-1}a^{-1}w_3) = y.$$

2 b I.

$$x = sy_1b_1b_2, \quad u = tb_1^{-1}y_2s^{-1}w_4a, \quad v = a^{-1}w_3t^{-1}.$$

$$w_4w_3 = w_1 = b_2^{-1}, \quad w = b_2^{-1}b_1^{-1}y_2s^{-1}.$$

$$y = \pi(x, w) = \pi(sy_1b_1b_2, b_2^{-1}b_1^{-1}y_2s^{-1}).$$

$$x = sy_1b_1b_2 \rightarrow b_2sy_1b_1,$$

$$u = tb_1^{-1}y_2s^{-1}w_4a \rightarrow b_1^{-1}y_2s^{-1}w_4at.$$

$$\pi(b_2sy_1b_1, b_1^{-1}y_2s^{-1}w_4at) = b_2sy_1y_2s^{-1}w_4at = b_2sys^{-1}w_4at$$

since tb_2 is reduced because tw_3^{-1} is reduced (being a subword of v^{-1}) and the first letter of w_3^{-1} is equal to the first of b_2 .

$$v = a^{-1}w_3t^{-1} \rightarrow t^{-1}a^{-1}w_3$$

and

$$\pi(b_2sys^{-1}w_4at, t^{-1}a^{-1}w_3) = b_2sys^{-1}w_4w_3 = y$$

since

$$w_4w_3 = b_2^{-1}.$$

2 b II.

$$x = sy_1b, \quad u = ty_4s^{-1}w_4a, \quad v = a^{-1}w_3t^{-1},$$

$$w_4w_3 = b^{-1}y_3, \quad w = b^{-1}y_3y_4s^{-1}$$

$$y = \pi(x, w) = \pi(sy_1b, b^{-1}y_3y_4s^{-1}).$$

$$x = sy_1b \rightarrow y_1bs,$$

$$u = ty_4s^{-1}w_4a \rightarrow s^{-1}w_4aty_4 \equiv s^{-1}b^{-1}y_3w_3^{-1}aty_4$$

since $w_4 \equiv b^{-1}y_3w_3^{-1}$. The last word of the preceding line is not necessarily reduced.

$$\pi(y_1bs, s^{-1}b^{-1}y_3w_3^{-1}aty_4) \equiv y_1y_3w_3^{-1}aty_4.$$

$$y_1y_3w_3^{-1}aty_4 \rightarrow y_4y_1y_3w_3^{-1}at$$

$$v = a^{-1}w_3t^{-1} \rightarrow t^{-1}a^{-1}w_3$$

and

$$\pi(y_4y_1y_3w_3^{-1}at, t^{-1}a^{-1}w_3) = y_4y_1y_3.$$

Finally

$$y_4y_1y_3 \rightarrow y.$$

2 b III.

$$x = s_1s_2y_1b, \quad u = ts_1^{-1}w_4a, \quad v = a^{-1}w_3t^{-1}, \\ w_4w_3 = b^{-1}y_2s_2^{-1}, \quad w = b^{-1}y_2s^{-1}.$$

$$y = \pi(x, w) = \pi(s_1s_2y_1b, b^{-1}y_2s^{-1}).$$

$$x = s_1s_2y_1b \rightarrow s_2y_1bs_1,$$

$$u = ts_1^{-1}w_4a \rightarrow s_1^{-1}w_4at \equiv s_1^{-1}b^{-1}y_2s_2^{-1}w_3^{-1}at$$

since $w_4 \equiv b^{-1}y_2s_2^{-1}w_3^{-1}$. The last word of the preceding line is not necessarily reduced.

$$\pi(s_2y_1bs_1, s_1^{-1}b^{-1}y_2s_2^{-1}w_3^{-1}at) = s_2y_1y_2s_2^{-1}w_3^{-1}at = s_2y s_2^{-1}w_3^{-1}at$$

because tw_3^{-1} is reduced being a subword of v^{-1} , thus ts_2 is reduced since the first letter of s_2 is equal to the first of w_3^{-1} .

$$v = a^{-1}w_3t^{-1} \rightarrow t^{-1}a^{-1}w_3$$

and

$$\pi(s_2y s_2^{-1}w_3^{-1}at, t^{-1}a^{-1}w_3) = y.$$

2 c I.

$$x = w_5^{-1}sys^{-1}b_1b_2, \quad u = tb_1^{-1}w_5w_4a, \quad v = a^{-1}w_3t^{-1}, \\ w_4w_3 = b_2^{-1}, \quad w = b_2^{-1}b_1^{-1}w_5$$

$$y = \pi(x, w) = \pi(w_5^{-1}sys^{-1}b_1b_2, b_2^{-1}b_1^{-1}w_5).$$

$$x = w_5^{-1}sys^{-1}b_1b_2 \rightarrow sys^{-1}b_1b_2w_5^{-1},$$

$$u = tb_1^{-1}w_5w_4a \rightarrow w_5w_4atb_1^{-1} \equiv w_5b_2^{-1}w_3^{-1}atb_1^{-1}$$

since $w_4 \equiv b_2^{-1}w_3^{-1}$. The last word of the preceding line is not necessarily reduced.

$$\pi(sys^{-1}b_1b_2w_5^{-1}, w_5b_2^{-1}w_3^{-1}atb_1^{-1}) = sys^{-1}b_1w_3^{-1}atb_1^{-1}$$

because b_1s is reduced being a subword of w^{-1} ; moreover $w_3^{-1}w_4^{-1} = b_2$, thus $b_1w_3^{-1}$ is reduced.

$$sys^{-1}b_1w_3^{-1}atb_1^{-1} \rightarrow b_1^{-1}sys^{-1}b_1w_3^{-1}at$$

$$v = a^{-1}w_3t^{-1} \rightarrow t^{-1}a^{-1}w_3$$

and

$$\pi(b_1^{-1}sys^{-1}b_1w_3^{-1}at, t^{-1}a^{-1}w_3) = y.$$

2 c II.

$$x = w_2^{-1}w_6^{-1}sys^{-1}b, \quad u = tw_2w_4a, \quad v = a^{-1}w_3t^{-1},$$

$$w_4w_3 = b^{-1}w_6, \quad w = b^{-1}w_6w_2.$$

There exists a word w_6 such that $w_5 = w_6w_2$ and $w_1 = b^{-1}w_6$.

$$y = \pi(x, w) = \pi(w_2^{-1}w_6^{-1}sys^{-1}b, b^{-1}w_6w_2).$$

$$x = w_2^{-1}w_6^{-1}sys^{-1}b \rightarrow w_6^{-1}sys^{-1}bw_2^{-1},$$

$$u = tw_2w_4a \rightarrow w_2w_4at \equiv w_2b^{-1}w_6w_3^{-1}at$$

since $w_4 \equiv b^{-1}w_6w_3^{-1}$. The last word of the preceding line is not necessarily reduced.

$$\pi(w_6^{-1}sys^{-1}bw_2^{-1}, w_2b^{-1}w_6w_3^{-1}at) \equiv w_6^{-1}sys^{-1}w_6w_3^{-1}at.$$

$$v = a^{-1}w_3t^{-1} \rightarrow t^{-1}a^{-1}w_3$$

and

$$\pi(w_6^{-1}sys^{-1}w_6w_3^{-1}at, t^{-1}a^{-1}w_3) = y.$$

Finally for case 3 the calculations are analogous to case 2 and for case 4 to case 1. \square

Proposition A.3.2 *Let σ be an \overline{R} -SLA; then there exists a C -SLA σ' with the same set of base elements and result of σ and such that $\eta(\sigma') = \eta(\sigma)$. In particular $\overline{R}_k = C_k$.*

Proof Let n be the number of steps of σ which cannot be steps of a C -SLA, that is steps of the form $\pi(x, w)$ where x and w are not 1-corollas. We prove the claim by induction on n .

Let $n = 1$ and let $\pi(x, w)$ be the step such that x and w are not 1-corollas. Let σ_1 and σ_2 be the pSLA's computing x and w . Since $n = 1$ then σ_1 and σ_2 are SLA's in C . This means in particular that w is a cyclic conjugate of $\pi(u, v)$ where either u or v or both are 1-corollas. Let $\eta(\sigma_2) = k$; by Remark A.3.1, $\pi(x, w)$ is equal to $\pi(p, u')$ or $\pi(p, v')$ where p is a cyclic conjugate of $\pi(x', v')$ or of $\pi(x', u')$ respectively and v' or respectively u' is a 1-corolla. Thus if σ_2 is the SLA of σ_2 computing u or v respectively, then $\eta(\sigma'_2) = k - 1$. By iterating a finite number of times we have the claim.

If $n > 1$ then we repeat the proceeding finitely many times and we obtain the claim. \square

Bibliography

- [1] http://en.wikipedia.org/wiki/Binary_relation
- [2] http://en.wikipedia.org/wiki/Binomial_coefficient
- [3] [http://en.wikipedia.org/wiki/Composition_\(number_theory\)](http://en.wikipedia.org/wiki/Composition_(number_theory))
- [4] http://en.wikipedia.org/wiki/Principle_of_mathematical_induction
- [5] <http://planetmath.org/encyclopedia/AdjunctionSpace.html>
- [6] <http://planetmath.org/encyclopedia/ZornsLemma.html>
- [7] J.-C. Birget, Infinite string rewrite systems and complexity, *J. Symbolic Comput.* **25**, (1998), no. 6, 759–793.
- [8] M. R. Bridson, The geometry of the Word Problem, in M. R. Bridson and S. M. Salamon, eds., *Invitations to Geometry and Topology*, Oxford Univ. Press, 2002, pp. 33–94.
- [9] M. R. Bridson, A. Haefliger, *Metric Spaces of Non-Positive Curvature*, Springer-Verlag, 1999.
- [10] R. Brown, J. Huebschmann, Identities among relations in *Low-dimensional topology (Bangor, 1979)*, London Math. Soc. Lecture Note Ser., vol. 48, Cambridge Univ. Press, 1982, pp. 153–202.
- [11] D. J. Collins, J. Huebschmann, Spherical Diagrams and Identities Among Relations, *Math. Ann.* **261**, (1982), no. 2, 155–183.
- [12] A. Carbone, Group cancellation and resolution, *Studia Logica* **82**, (2006), no. 1, 75–95.
- [13] M. Coornaert, T. Delzant, A. Papadopoulos, *Géométrie et théorie des groupes : les groupes hyperboliques de Gromov*, Springer-Verlag, 1990.

- [14] R. L. Epstein, W. A. Carnielli, *Computability. Computable Functions, Logic, and the Foundations of Mathematics*, Wadsworth Publishing, 1999.
- [15] S. M. Gersten, Dehn functions and l_1 -norms of finite presentations, in *Algorithms and classification in combinatorial group theory (Berkeley, CA, 1989)*, Math. Sci. Res. Inst. Publ., 23, Springer, 1992, pp. 195–224.
- [16] R. I. Grigorchuk, S. V. Ivanov, On Dehn functions of infinite presentations of groups, *Geom. Funct. Anal.* **18**, (2009), no. 6, 1841–1874.
- [17] M. Gromov, Hyperbolic groups, in *Essays in group theory*, Springer, 1987, pp. 75–263.
- [18] A. Hatcher, *Algebraic Topology*, Cambridge University Press, 2002 or <http://www.math.cornell.edu/~hatcher/AT/ATpage.html>
- [19] D. F. Holt, B. Eick, E. O’Brien, *A Handbook of computational group theory*, Chapman & Hall/CRC, 2005.
- [20] R. C. Lyndon, P. E. Schupp, *Combinatorial Group Theory*, Springer-Verlag, 1977.
- [21] K. Madlener, F. Otto, Pseudonatural algorithms for the word problem for finitely presented monoids and groups, *J. Symbolic Comput.* **1**, (1985), no. 4, 383–418.
- [22] W. Magnus, A. Karrass, D. Solitar, *Combinatorial Group Theory*, Dover Publications, 1976.
- [23] C. F. Miller III, Decision problems for groups - survey and reflections, in *Algorithms and classification in combinatorial group theory (Berkeley, CA, 1989)*, 1–59, Math. Sci. Res. Inst. Publ., 23, Springer, 1992.
- [24] H. Short, Diagrams and groups, in *The Geometry of the Word Problem for Finitely Generated Groups*, Birkhäuser, 2007.
- [25] A. Shen, N. K. Vereshchagin, *Computable functions*, American Mathematical Society, 2003.
- [26] C. C. Sims, *Computation with finitely presented groups*, Cambridge University Press, 1994.
- [27] H. Whitney, Non-separable and planar graphs, *Trans. Amer. Math. Soc.* **34**, (1932), no. 2, 339–362.

Addresses:

Institut de Mathématiques de Jussieu
175, rue du Chevaleret
75013 Paris - France

e-mail: vaccaro@math.jussieu.fr

and

Dipartimento di Matematica dell'Università di Palermo
Via Archirafi 34
90123 Palermo - Italy

e-mail: cvaccaro@math.unipa.it