AN EFFECTIVE VERSION OF STALLINGS' THEOREM IN THE CASE OF CONTEXT-FREE GROUPS

Géraud Sénizergues

LaBri
Université de Bordeaux I
351, Cours de la Libération 33405 Talence, France ** ***

Abstract. We give an algorithm producing from every p.d.a. $\mathcal{M}$ recognizing the word-problem for an infinite group G, a decomposition of G as an amalgamated product (with finite amalgamated subgroups) or as an HNN-extension (with finite associated subgroups).This algorithm has an elementary time-complexity.This result allows us to show that the isomorphism-problem for finitely generated virtually-free groups is primitive recursive,thus improving the decidability result of [Krstic,1989].

keywords: context-free groups, pushdown automata, Cayley graph, Thue-systems, complexity, graph of groups.

1 INTRODUCTION

1.1 Presentation of the result

Stallings theorem is a combinatorial group-theoretic theorem stating that every finitely generated group having at least two ends can be decomposed either as a non-trivial amalgamated product (with finite amalgamated subgroups) or as an HNN-extension (with finite associated subgroups) ([14], [5],[7]).

A context-free group is a group G defined by a presentation $< X; R >$ over a finite set X of generators, such that the word-problem for G on X can be solved by some pushdown automaton $\mathcal{M}$ (equivalently : such that the set of words $\{w \in (X \cup \overline{X})^* \mid w \xleftrightarrow{*}_R \epsilon\}$ is a context-free language)[1]. This class of groups is exactly the class of virtually-free groups ([10]) and is a strict sub-class of the class of automatic groups ([8]). It is known that every infinite c.f. group G has at least two ends ([10]), so that Stallings theorem applies on G.

In this paper we show that, given an effective description of G (i.e. a pushdown automaton $\mathcal{M}$ recognising the word-problem on a finite alphabet of generators X) we can perform in five-fold exponential time the following task:

- compute the number of ends N_e of G (which may be $0, 2$ or ∞)
- in the case where $N_e \in \{2, \infty\}$, effectively decompose G as an amalgamated product (case 1) or as an HNN-extension (case 2) ;
- in case 1 compute finite sets of generators X_i for G_i (where $i \in \{1, 2\}$), pushdown automata $\mathcal{M}_i$ recognising the word-problem for G_i on X_i and finite subgroups K_i of G_i such that $G =< G_1 * G_2; K_1 = K_2 >$
- in case 2 compute a finite set of generators X_1 of a subgroup G_1, a p.d.a. $\mathcal{M}_1$ recognising the word-problem of G_1 on X_1, finite subgroups K_1, K_2 of G_1 and an element $t \in G - G_1$ such that $G =< G_1, t; t^{-1}K_1t = K_2 >$.

** mailing adress:LaBri and UER Math-info, Université Bordeaux1
351 Cours de la libération -33405- Talence Cedex.
email:ges@geocub.greco-prog.fr
fax: 56-84-66-69

*** This work has been supported by the ESPRIT Basic Research Working Group "COMPUGRAPH II" and by the PRC MathInfo

The overall strategy for doing these computations is to follow the proof of Stallings theorem given in ([5], p41-56) and to make it constructive by using the p.d.a. $\mathcal{M}$. We use two kinds of arguments :

- "geometrical" arguments about the Cayley-graph of G (which strongly lean on the κ-triangulation property stated in [10] ;
- "language-theoretic" arguments about almost-invariant subsets of G or about left-stabilisers of almost-invariant subsets of G (they lean on a theorem of [3] concerning the right-linear rewriting systems defined in [4]).

1.2 Motivations

This algorithm is the first step of a work which aims to give an effective way to solve the following problems:

(P1) given a context-free group G, build a graph of groups (with finite vertex groups) admitting G as fundamental group (see definition p. 12 of [7])
(P2) given a context-free grammar which generates a group-language L defining a group G, build an equivalent NTS grammar G' generating L
(P3) given two c.f. groups G_1, G_2 (given by c.f. grammars) decide whether they are isomorphic.

The second step is done in [13] where we give an upper bound on the size of any minimal graph of groups admitting a given c.f. group G as its fundamental group; this bound is exponential with respect to the triangulation constant of the Cayley-graph of G.The present work shows that a solution to P1 can be computed in primitive recursive time from a description of G by an outer action of a finite group on a finitely generated free group (see the proof of theorem 17).Together with the second step it will show that P1 can be solved in primitive recursive time from a description of G by a pushdown automaton recognising its word-problem on some set of generators. Let us recall that P2 is solved in [2] by a construction which starts from a graph of groups with finite vertex groups, admitting G as its fundamental group. Problem P3 is solved in [9] by an algorithm working in exponential time from any "Culler's realizations" of G_1, G_2 (which can easily be deduced from their associated graphs of groups, see [9] p.123).

1.3 Organisation of the paper :

- in part 2 we recall some definitions and present our terminology concerning semi-Thue systems, automata, groups and graphs ;
- in part 3 we give the geometrical results concerning finite cocycles of the Cayley-graph of G and some consequences;
- in part 4 we give the language-theoretic results concerning right-linear rewriting systems and their consequences about almost-invariant subsets ;
- in part 5 we describe the whole decomposition algorithm, analyse its complexity and state the main results.

2 TERMINOLOGY and RECALLS

2.1 Semi-Thue systems

Let X be an alphabet. X^* is the free monoïd generated by X. ϵ denotes the empty string. A *semi-Thue system* S on X is a subset $S \subset X^* \times X^*$. The *one-step derivation* $\longrightarrow_S$ is defined for all strings $f, g \in X^*$ by : $f \longrightarrow_S g$ iff there exists $\alpha, \beta \in X^*$ and $(u, v) \in S$ such that $f = \alpha u \beta$ and $g = \alpha v \beta$. The *derivation-relation* $\xrightarrow{*}_S$ is then the reflexive and transitive closure of $\longrightarrow_S$. $\longleftrightarrow_S$ denotes the symmetric closure of $\longrightarrow_S$ and $\overset{*}{\longleftrightarrow}_S$ is the reflexive and transitive closure of $\longleftrightarrow_S$. $\overset{*}{\longleftrightarrow}_S$ is the *congruence generated* by S. For every $w \in X^*$, by $[w]_{\overset{*}{\longleftrightarrow}_S}$ we denote the set $\{f \in X^* \mid w \overset{*}{\longleftrightarrow}_S f\}$. Similarly, the *one-step right-linear derivation* $\longrightarrow_{r,S}$ is defined for all strings $f, g \in X^*$ by: $f \longrightarrow_{r,S} g$ iff there exists $\alpha \in X^*$ and $(u, v) \in S$ such that $f = \alpha u$ and $g = \alpha v$. The *right-linear derivation* $\xrightarrow{*}_{r,S}$ is then the reflexive and transitive closure of $\longrightarrow_{r,S}$ (this type of relation was originally defined in [4]).

2.2 Automata

A *finite automaton* on the alphabet X is a 5-tuple $\mathcal{B} = < X, Q, \delta, q_0, Q_+ >$ where Q is the finite set of states, $q_0 \in Q$ is the initial state, $Q_+ \subset Q$ is the set of terminal states and δ, the transition function, is a mapping : $\delta : Q \times X \to P(Q)$. By $q \xrightarrow{f}_{\mathcal{B}} q'$ we denote the fact that there exists some calculus of $\mathcal{B}$, starting with state q, reading f and reaching state q'.

A *pushdown automaton* on the alphabet X is a 6-tuple $\mathcal{A} = < X, Y, Q, \delta, q_0, y_0 >$ where Y is the finite stack-alphabet, Q is the finite set of states, $q_0 \in Q$ is the initial state, y_0 is the initial stack-symbol and δ, the transition function, is a mapping $\delta : YQ \times (X \cup \{\epsilon\}) \to \mathcal{P}(Y^*Q)$. Let $q, q' \in Q, \omega, \omega' \in Y^*, y \in Y, f \in X^*$ and $a \in X \cup \{\epsilon\}$; we note $(\omega y q, af) \longmapsto_{\mathcal{A}} (\omega\omega' q', f)$ if $\omega' q' \in \delta(yq, a)$. $\overset{*}{\longmapsto}_{\mathcal{A}}$ is the reflexive and transitive closure of $\longmapsto_{\mathcal{A}}$.

For every $\omega q, \omega' q' \in Y^*Q$ and $f \in X^*$,we note $\omega q \xrightarrow{f}_{\mathcal{A}} \omega' q'$ iff $(\omega q, f) \overset{*}{\longmapsto}_{\mathcal{A}} (\omega' q', \epsilon)$.

$\mathcal{A}$ is said *deterministic* iff, for every $yq \in YQ$:

1. either Card$(\delta(yq, \epsilon)) = 1$ and for every $a \in X$, Card $(\delta(yq, a)) = 0$
2. or Card$(\delta(yq, \epsilon)) = 0$ and for every $a \in X$, Card $(\delta(yq, a)) \leq 1$.

$\mathcal{A}$ is said *real-time* iff, for every $yq \in YQ$, Card$(\delta(yq, \epsilon)) = 0$. Given some finite set $F \subseteq Y^*Q$ of configurations, the *language recognized by $\mathcal{A}$ with final configurations* F is

$$L(\mathcal{A}, F) = \{w \in X^* \mid \exists c \in F, y_0 q_0 \xrightarrow{f}_{\mathcal{A}} c\}$$

.

2.3 Groups

Presentations Let S be a semi-Thue system on X. $X^*/\xleftrightarrow{*}_S$, is the set $\{[w]_{\xleftrightarrow{*}_S} \mid w \in X^*\}$. $X^*/\xleftrightarrow{*}_S$ is naturally equipped with the associative composition law : $[w_1]_{\xleftrightarrow{*}_S}.[w_2]_{\xleftrightarrow{*}_S} = [w_1w_2]_{\xleftrightarrow{*}_S}$, and admits the neutral element $[\epsilon]_{\xleftrightarrow{*}_S}$. Given a group G we say the pair $< X; S >$ (where S is a semi-Thue system on the alphabet X) is a *presentation of* G iff $G \approx X^*/\xleftrightarrow{*}_S$ (i.e. G is isomorphic to $X^*/\xleftrightarrow{*}_S$). A group G is said *context-free* iff there exists some finite alphabet Y and some semi-Thue system $S \subset Y^* \times Y^*$ such that $G \approx Y^*/\xleftrightarrow{*}_S$ and $[\epsilon]_{\xleftrightarrow{*}_S}$ is a context-free language ([1]). Given such a presentation it is easy to modify it such that it takes the form : $Y = X \cup \overline{X}$ where $\overline{X}$ is an alphabet in one-to-one correspondance with X and for every $x \in X, (x\overline{x}, \epsilon) \in S$ and $(\overline{x}x, \epsilon) \in S$ (where $\overline{x}$ is the letter associated to x in the above one-to-one correspondance).

We then say that $< X \cup \overline{X}; S >$ is a *symmetric presentation.* Let us suppose that $G \approx (X \cup \overline{X})^*/\xleftrightarrow{*}_S$ and

$$[\epsilon]_{\xleftrightarrow{*}_S} = L(\mathcal{M}, F)$$

(where $\mathcal{M}$ is a p.d.a. and F a finite set of configurations).
One can check that G is fully determined by $\mathcal{M}$ and F because $f \xleftrightarrow{*}_S g$ iff $f\tilde{\overline{g}} \in L(\mathcal{M}, F)$ (where $\overline{g}$ is the copy of g on $\overline{X}$ and $\tilde{\overline{g}}$ is the mirror image of $\overline{g}$).

Free product with amalgamation Let G_1, G_2 be groups admitting respectively the presentation $< X_1; R_1 >, < X_2; R_2 >$.Let $K_1 \subset G_1, K_2 \subset G_2$ be subgroups and $\varphi : K_1 \longrightarrow K_2$ an isomorphism. Then the free product of G_1, G_2 amalgamating the subgroups K_1, K_2 by φ is defined by the presentation

$$< X_1 \cup X_2; R_1 \cup R_2; k = \varphi(k), k \in K_1 >$$

it will be noted

$$< G_1 * G_2; k = \varphi(k), k \in K_1 >$$

HNN-extensions (HNN stands for **H**ighman-**N**eumann- **N**eumann)

Let G be a group and K_1, K_2 be subgroups of G with $\varphi : K_1 \longrightarrow K_2$ an isomorphism. If G admits the presentation $< X; R >$ then the HNN-extension of G, relative to K_1, K_2 and φ is the group $G_1 =< X \cup \{t, \overline{t}\}; R_1 >$ where $t, \overline{t}$ are new letters and R_1 is the semi-Thue system :

$$R_1 = R \cup \{(t\overline{t}, \epsilon), (\overline{t}t, \epsilon)\} \cup \{(\overline{t}k_1t, \varphi(k_1)) \mid k_1 \in K_1\}$$

(in fact, in the above system R_1, k_1 denotes any word in X^* representing the element $k_1 \in K_1$)). For short we use the notation

$$G_1 =< G, t; t^{-1}k_1t = \varphi(k_1), k_1 \in K_1 >$$

.

Almost-invariant subsets We define the relations $\subset_a$ (*almost-inclusion*), $=_a$ (*almost-equality*) between subsets of G by :

$$E \subset_a E' \quad \text{means that} \quad E \cap (G - E') \text{ is finite}$$

$$E =_a E' \quad \text{means that} \quad E \subset_a E' \text{ and } E' \subset_a E$$

A subset $E \in \mathcal{P}(G)$ is *almost-invariant* iff

$$\forall g \in G, Eg =_a E$$

The powerset $\mathcal{P}(G)$, equipped with the symmetric difference $\triangle$ is a vector-space over $\mathbb{Z}/2\mathbb{Z}$ and admits the subspaces :

$$\mathrm{INV}(G) = \{E \in \mathcal{P}(G) \mid E \text{ is almost-invariant } \}$$
$$\mathrm{FIN}(G) = \{E \in \mathcal{P}(G) \mid E \text{ is finite } \}$$

The *number-of-ends* of G is the dimension of the quotient-space $\mathrm{INV}(G)/\mathrm{FIN}(G)$. Hence G "has at least 2 ends" iff there exists some almost invariant subset E which is infinite and has infinite complement $G - E$. The number-of-ends of an arbitrary finitely generated group can be $0, 1, 2$ or ∞ ([5]).In the case of a context-free group it can only take values $0, 2$ or ∞ (1 is impossible, as shown in [10]).

2.4 Cayley graphs

Given a finitely generated group G and a finite set X_G of generators of G, the Cayley-graph of G over X_G is the following oriented, labeled graph $\Gamma = (V_\Gamma, E_\Gamma)$:
let X be an alphabet in one-to-one correspondance with X_G, $\overline{X}$ a disjoint alphabet in one-to-one correspondance with X_G^{-1}, such that for every $x_G \in X_G$, if $x \in X$ denotes $x_G, \overline{x} \in \overline{X}$ denotes x_G^{-1} ;

- V_Γ, the set of vertices, is equal to G
- $E_\Gamma = \{(g, x, g') \mid g, g' \in G, x \in X, g.x_G = g'\} \cup \{(g, \overline{x}, g') \mid g, g' \in G, x \in X, g.x_G^{-1} = g'\}$.

Given a subset $E \subset V_\Gamma$, we define the *frontier* $\triangle E$ of E by :

$$\triangle E = \{v \in E \mid \exists v' \in V_\Gamma - E, \exists x \in X \cup \overline{X}, (v', x, v) \in E_\Gamma\}$$

The *cofrontier* $\boldsymbol{\partial} E$ of E is defined by :

$$\boldsymbol{\partial} E = \{(v', x, v) \in E_\Gamma \mid v' \in V_\Gamma - E, x \in X \cup \overline{X}, v \in E\}$$

A *cocycle* $\boldsymbol{\partial}$ of G is any subset $\boldsymbol{\partial}$ of E_Γ such that there exists some subset E of V_Γ fulfilling $\boldsymbol{\partial} = \boldsymbol{\partial} E$. When $\boldsymbol{\partial} \subset E_\Gamma$, by $\boldsymbol{\partial}^{-1}$ we denote the set

$$\boldsymbol{\partial}^{-1} = \{(v, \overline{x}, v') \mid (v', x, v) \in \boldsymbol{\partial}\}$$

(here we extend the notation $\overline{x}$ to every $x \in X \cup \overline{X}$ by setting $\overline{\overline{x}} = x$).

By $\mathrm{d}(v, v')$ we denote the *distance* between two vertices v, v' in G : it is the minimal length of a path from v to v' in G.

We call *diameter of a cocycle* $\boldsymbol{\partial}$ the number

$$\mathrm{diam}(\boldsymbol{\partial}) = \max\{d(v_1, v_2) \mid \exists x_1, x_2 \in X \cup \overline{X}, \exists v_1', v_2' \in V_\Gamma, (v_1, x_1, v_1') \in \boldsymbol{\partial} \cup \boldsymbol{\partial}^{-1} \text{ and } (v_2, x_2, v_2') \in \boldsymbol{\partial} \cup \boldsymbol{\partial}^{-1}\}$$

The cocycle ∂E is said *elementary* iff E and $V_\Gamma - E$ are both connected (i.e. the subgraphs generated by the sets of vertices $E, V_\Gamma - E$ are both connected). Here we call *end* of Γ any subset $E \subset V_G$ such that

$$\mathrm{Card}(\boldsymbol{\partial} E) < \infty \text{ and } \mathrm{Card}(E) = \infty$$

One must notice that E is an end of Γ iff, E, considered as a subset of G, is an infinite almost-invariant subset.

By $\mathrm{B}(v, R)$ we denote the ball $\{v' \in V_\Gamma \mid d(v, v') < R\}$. Here we call *spherical end* of Γ any subset $E \subset V_\Gamma$ which is an infinite connected component of $\Gamma - \mathrm{B}(1, R)$ for some radius R. It is simply called "end" in [10] but it is convenient here to consider a slightly more general notion of end ; (the reader should be aware that the notion of end defined in [5] is a third different notion which is not used here).

3 GEOMETRICAL PROPERTIES

Let us fix (from now and up to the end of this paper) some context-free group G given by an alphabet X, a p.d.a. $\mathcal{M} = < X \cup \overline{X}, P, Y, \delta, y_0, q_0 >$ a finite set $F \subset Y^*P$ such that G admits some presentation $< X \cup \overline{X}; R >$ and $[\epsilon]_{\overset{*}{\longleftrightarrow}_S} = L(\mathcal{M}, F)$. As noticed in 2.3, G is fully determined by $\mathcal{M}$ and F.

It is known that we can compute an integer $\kappa > 0$ such that the Cayley-graph Γ of G on the set of generators $\{[x]_{\overset{*}{\longleftrightarrow}_S} \mid x \in X\}$ is κ-triangulable ([10], theorem I p. 302)

Lemma 1. *Given an integer $R > 0$, we can compute the finite graph* $\mathrm{B}(1, R)$.

Proof. Let us denote by T_R the tree whose vertices set V_R and edges set E_R are

$$V_R = \{w \in (X \cup \overline{X})^* \mid \quad |w| < R\}$$

$$E_R = \{(w, x, wx) \mid w \in V_R, x \in X \text{ and } wx \in V_R\} \cup \{(wx, \bar{x}, w) \mid w \in V_R, x \in X \text{ and } wx \in V_R\}$$

B(1, R) is the quotient of the graph T_R by the bisimulation $\sim$: $w \sim w'$ iff $w\widetilde{w'} \in L(\mathcal{M}, \mathcal{F})$.As $\sim$ is computable, $B(1, R)$ is computable too.

Lemma 2. *Let $\boldsymbol{\partial} \subset V_\Gamma \times (X \cup \overline{X}) \times V_\Gamma$ be a finite set of edges of Γ, whose initial and terminal vertices are all lying in* $\mathrm{B}(1, R)$*. Let A, A' be two vertices belonging to some edges of $\boldsymbol{\partial}$. There exists some path from A to A', which does not use any edge of $\boldsymbol{\partial} \cup \boldsymbol{\partial}^{-1}$, iff there exists some path from A to A', lying in* $\mathrm{B}(1, R + 2\kappa)$*, which does not use any edge of $\boldsymbol{\partial} \cup \boldsymbol{\partial}^{-1}$.*

The proof is technical and is omitted here.

Lemma 3. *Let $\partial \subset V_\Gamma \times (X \cup \overline{X}) \times V_\Gamma$ be a finite set of edges.*

1. *We can decide whether ∂ is a cocycle*
2. *We can decide whether ∂ is an elementary cocycle.*

Proof. Let R = diam $(\partial) + 1$. As properties (1), (2) are invariant by left-translation, we can suppose that all the vertices of ∂ lie in B(1,R). ∂ is a cocycle iff, for every $(C, x, A), (C', x', A') \in \partial$, there is no path from A to A', which does not use any edge of $\partial \cup \partial^{-1}$. By lemma 2 this property reduces to the same property in the graph $B(1, R + 2\kappa)$ which can be computed by lemma 1. A cocycle ∂ is elementary iff, for every (C, x, A), (C', x', A') which are both in ∂ or both in ∂^{-1} , there exists some path from A to A' which does not use any edge in $\partial \cup \partial^{-1}$. This can be tested by the same argument as above.

Lemma 4 ([11]). *If ∂ is a spherical cocycle, then diam$(\partial) \leq 3\kappa + 2$.*
(by "spherical"cocycle we mean the cofrontier of some spherical end).

This lemma is proved in [11], p 65.

In [11] the authors associate to every context-free graph some special deterministic p.d.a. $\mathcal{A}$ called *the canonical d.p.d.a* of Γ. The complete definition of $\mathcal{A}$ is technical, let us mention that if $\mathcal{A} = < X \cup \overline{X}, Z, Q, \delta_A, q_0, y_0 >$,then

(1) L$(\mathcal{A}, \{y_0 q_0\})$ = L$(\mathcal{M}, F) = [e]_{\overset{*}{\longleftrightarrow}_R}$
(i.e. $\mathcal{A}$ recognises the word-problem of G)

(2) the mapping $\overline{\tau} : G \rightarrow$ Config $(\mathcal{A})$, $[w]_{\overset{*}{\longleftrightarrow}_R} \mapsto \alpha q \in Z^* Q \mid y_0 q_0 \xrightarrow{w}_{\mathcal{A}} \alpha q$
is well-defined and bijective (Config $(\mathcal{A})$ is the set of accessible configurations of $\mathcal{A}$).

(3) $\forall g \in G, d(1_G, g) = \mid \overline{\tau}(g) \mid -1$
(i.e. the distance from the neutral element to g is equal to the stack-height of the configuration representing g minus 1).

Theorem 5. *We can compute from the p.d.a. $\mathcal{M}$ defining the group G the canonical d.p.d.a. $\mathcal{A}$ of the Cayley-graph Γ of G.*

Sketch of proof. The stack-alphabet Z corresponds to the classes of spherical ends (under end-isomorphism), Q correspond to the maximum number of frontier points on any spherical end and $\delta_{\mathcal{A}}$ encodes the edges of the spherical cocycles (see [11]). Hence $\mathcal{A}$ depends upon the spherical cocycles only and these cocycles can be computed by lemma 1 ,3 and 4.

Lemma 6. *Let ∂ be a finite elementary cocycle of Γ.*
Then diam$(\partial) \leq \frac{1}{2}(3\kappa + 2)($Card$(\partial) - 1)$.

The proof is technical and is omitted here.

4 LANGUAGE-THEORETIC PROPERTIES

The main mathematical object which leads to a decomposition of G is an almost-invariant set $E \subset G$, which is infinite, has infinite complement and such that every $g \in G$ is in one of the four sets :

$$\begin{aligned}
E_{+,+} &= \{g \in G \mid gE \subset E\} \\
E_{+,-} &= \{g \in G \mid gE \subset G - E\} \\
E_{-,+} &= \{g \in G \mid g(G - E) \subset E\} \\
E_{-,-} &= \{g \in G \mid g(G - E) \subset G - E\}
\end{aligned}$$

In order to compute such sets we define two ways for describing the elements of G by words (4.1), we then prove some properties of right-linear rewriting systems (4.2) and derive some consequences about the languages representing the sets $E_{\epsilon,\epsilon'}(\epsilon, \epsilon' \in \{+,-\})$ or other analogous sets (4.3).

4.1 Words representing the elements of G

There are two kinds of words representing an element $g \in G$:

1. the words $w \in (X \cup \overline{X})^*$ of minimal length such that $g = [w]_{\overset{*}{\longleftrightarrow}_R}$
2. the configuration $\omega q \in Z^* Q$ of the canonical automaton $\mathcal{A}$ which corresponds to the vertex g of Γ (noted $\overline{\tau}(g)$).

(We identify here the group G with the quotient-monoïd $(X \cup \overline{X})^* / \overset{*}{\longleftrightarrow}_R$).
Let us define some more notations and vocabulary.
A word $w \in (X \cup \overline{X})^*$ is said minimal iff, for every $w' \in (X \cup \overline{X})^*$, $w \overset{*}{\longleftrightarrow}_R w' \Rightarrow |w| \leq |w'|$. We denote by M the set of all minimal words.
$\Pi : (X \cup \overline{X})^* \to (X \cup \overline{X})^* / \overset{*}{\longleftrightarrow}_R = G$ is the canonical projection.
$\tau : (X \cup \overline{X})^* \to \mathrm{Config}(\mathcal{A})$ is the mapping "computed" by $\mathcal{A}$ in the following sense :

$$\forall w \in (X \cup \overline{X})^*, y_0 q_0 \xrightarrow{w}_{\mathcal{A}} \tau(w)$$

($\tau(w)$ is uniquely defined by the above condition because $\mathcal{A}$ is deterministic, real-time and complete).
Π_M (resp. τ_M) is the mapping Π (resp.τ) restricted to M. i is the embedding of M into $(X \cup \overline{X})^*$. $\overline{\tau}$ is the unique map such that $\tau = \overline{\tau} \circ \Pi$ (this fact was recalled in section 3). $\overline{\tau}$ is a bijection.
The situation is summarised in the commutative diagram 1.

Lemma 7. *τ_M is a rational transduction.*

Sketch of proof. It suffices to notice that a computation of $\mathcal{A}$ on a minimal word w must be increasing (i.e. each transition used must strictly increase the stack-height).

Let us notice that $M = \mathrm{domain}(\tau_M)$, hence M is rational.

4.2 Right-linear rewriting systems

Let $S \subset X^* \times X^*$ be a semi-Thue system.

Theorem 8 ([3]). *If S is finite,then $\xrightarrow{*}_{r,S}$ is a rational transduction.*

This theorem is proved in [3] even in the more general case where S is a recognisable subset of $X^* \times X^*$.

Let $K \subset X^*$. We define the language $\mathrm{H}(S, K)$ (the "heart" of S relative to K) as :

$$\mathrm{H}(S,K) = \{f \in X^* \mid \forall n \geq 0, \exists m \geq n, \exists k \in K, f \xrightarrow{m}_{r,S} k\}$$

Theorem 9. *If S is finite and K is rational, then $\mathrm{H}(S, K)$ is rational.*

The proof is technical and is omitted here.

It is a refinement of theorem 5 of [3] which asserts that $\mathrm{H}(S, X^*)$ is rational.

Let us consider some real-time p.d.a. $\mathcal{A} =< Y, Z, Q, \delta_A, q_0, y_0 >$ (for example,$\mathcal{A}$ could be the canonical automaton of Γ).

Let $R \subset Y^*, K \subset Z^*Q$ be two rational languages.

Lemma 10. *The two following languages are rational*

1. $\mathrm{Config}(R, K) = \{\omega q \in Z^*Q \mid \exists f \in R, \omega q \xrightarrow{f}_{\mathcal{A}} K\}$
2. $\mathrm{Config}_\infty(R, K) = \{\omega q \in Z^*Q \mid$ there exist infinitely many words$f \in R$ such that $\omega q \xrightarrow{f}_{\mathcal{A}} K\}$

(the notation $\omega q \xrightarrow{f}_{\mathcal{A}} K$ means : $\exists k \in K, \omega q \xrightarrow{f}_{\mathcal{A}} k$))

Proof. Let $\mathcal{B} = < Y, Q', \delta, q'_0, Q'_+) >$ be a f.a. recognising R. Let $\widehat{Z} = Z \cup \{[q, q'] \mid q \in Q, q' \in Q'\}$ be a new alphabet. We consider the semi-Thue sytem S constitued by all the rules

$$\omega_1[q_1, q'_1)] \rightarrow \omega_2[q_2, q'_2)]$$

such that

$$\begin{array}{lll} \omega_1, \omega_2 \in Z^*,\ q_1, q_2 \in Q, q'_1, q'_2 \in Q', & & \\ \exists y \in Y, & \omega_1 q_1 \xrightarrow{y}_{\mathcal{A}} \omega_2 q_2 & \text{is a transition of } \mathcal{A} \\ \text{and} & q'_1 \xrightarrow{y}_{\mathcal{B}} q'_2 & \text{is a transition of } \mathcal{B} \end{array}$$

We then have :

$$\omega q \in Config(R, K) \Longleftrightarrow \omega[q, q_0] \xrightarrow{*}_{r,S} K' \tag{1}$$

$$\omega q \in Config_\infty(R, K) \Longleftrightarrow \omega[q, q_0] \in H(S, K') \tag{2}$$

where

$$K' = \{\omega'[q', q"] \mid \omega' q' \in K, q" \in Q'_+\} \tag{3}$$

By (1) and theorem 9, Config (R, K) is rational. By (2) and theorem 9, $\mathrm{Config}_\infty(R, K)$ is rational.

4.3 Almost-invariant subsets as formal languages

The notion of rational language makes sense in any monoïd $(A, ., 1)$: the set of rational languages is the smallest subset of $\mathcal{P}(\mathrm{A})$ containing the finite subsets of A and closed by the operations:.(product of 2 subsets), $\cup$ (finite union) and $*$ (operation star). In the case of the monoïd G, rational subsets of G are related to rational languages of words by the following

Theorem 11. *Let $E \subset G$. The following properties are equivalent*

(1) *E is a rational subset of G*
(2) *$\overline{\tau}(E)$ is a rational subset of $(Z \cup Q)^*$*
(3) *$\Pi_M^{-1}(E)$ is a rational subset of $(X \cup \overline{X})^*$*

Sketch of proof. **(1) $\Longrightarrow$ (2):** there exists some rational subset R of $(X \cup \overline{X})^*$ such that $E = \Pi(R)$.Hence $\overline{\tau}(E) = \tau(R)$. But τ preserves rationality.
(2) $\Longrightarrow$ (3): $\Pi_M^{-1}(E) = \tau_M^{-1}(\overline{\tau}(E))$ and τ_M is a rational transduction (lemma 7).
(3) $\Longrightarrow$ (1): $E = \Pi(\Pi_M^{-1}(E))$ and every homomorphic image of a rational set is rational

Lemma 12. *The set Rat(G) of all rational subsets of G is closed under the operations $\cap$ (intersection of two subsets) and C (complement).*

Proof. As Rat(G) is closed under $\cup$, it is sufficient to prove that it is closed under complement. Let $R \in$ Rat(G). $\Pi_M^{-1}(G - R) = M - \Pi_M^{-1}(R)$ and Rat $((X \cup \overline{X})^*)$ is closed under complement. As $M, \Pi_M^{-1}(R)$ are rational, $\Pi_M^{-1}(G - R)$ is rational too, hence $G - R$ is rational.

The idea of lemma 12 is borrowed to [12] where it is proved undermore general hypothesis.

Lemma 13. *Let $E \subset G$ be an almost-invariant subset. Then*

(1) *E is rational*
(2) *given ∂E, we can compute a finite automaton recognising $\overline{\tau}(E)$.*

Sketch of proof.

(1)

case 1: E is a spherical end. Then its frontier $\triangle E$ is such that $\overline{\tau}(\triangle E) = \{\omega q_i \mid 1 \leq i \leq p\}$ where $\omega \in Z^*$ is a fixed word and $p =$Card$(\triangle E)$. Then $\overline{\tau}(E) = \omega Z^* Q \cap$ Config $(\mathcal{A})$, hence $\overline{\tau}(E)$ is rational.

case 2: E is a general almost-invariant subset. Let $R = \max\{d(1_G, c) \mid c \in \triangle E\}$. E is the finite union of a (finite) subset of B$(1, R)$ and some spherical ends associated to B$(1, R)$. Hence, by case 1, E is rational.

(2) The computation of the number R is straightforward. Let E_R be the unique subset of B$(1_G, R+1)$ such that $\partial E = \partial_B E_R$ (where B denotes B$(1, R+1)$ and $\partial_B E_R$ the cofrontier of E_R in the subgraph B). E is the union of E_R and the spherical ends whose frontier lies in E_R.

Lemma 14. *Let E, E' be two rational languages of G. Then the following languages are rational :*

(1) $L(E, E') = \{g \in G \mid gE \cap E' \neq \emptyset\}$

(2) $L_\infty(E, E') = \{g \in G \mid gE \cap E' \text{ is infinite}\}$

Proof.

$$L(E, E') = \Pi({\tau_M}^{-1}(\mathrm{Config}(R, K)))$$

$$L_\infty(E, E') = \Pi({\tau_M}^{-1}(\mathrm{Config}_\infty(R, K)))$$

where $R = \Pi_M^{-1}(E), K = \overline{\tau}(E')$.
Hence by lemma 10 and theorem 11, these languages are rational.

Lemma 15. *Let E be an almost-invariant subset of G (given by the cocycle ∂E). Then all the following sets are rational and finite automata recognising their inverse image by Π_M can be computed :*

(1) $E_{+,+}, E_{+,-}, E_{-,+}, E_{-,-}$
(2) $K = \{g \in G \mid gE =_a E\}$
(3) $H = \{g \in G \mid gE =_a E \text{ or } gE =_a G - E\}$
(4) $N = \{g \in K \mid \mathrm{Card}(gE \cap (G - E)) = \mathrm{Card}(g(G - E) \cap E)\}$
(5) $E' = \{g \in G \mid gE \subset_a E \text{ or } g(G - E) \subset_a E\}$
(6) $G_1 = \{g \in G \mid (E' - K)g = E' - K\}$
(7) $G_2 = \{g \in G \mid (E' - (H - K))g = E' - (H - K)\}$
(8) $P = \{g \in G \mid (E' - (H - K))g = E' - K\}$

Sketch of proof. We first remark that given rational subsets E_1, E_2 of G,

$$\alpha(E_1, E_2) = \{g \in G \mid gE_1 \subset E_2\}, \beta(E_1, E_2) = \{g \in G \mid gE_1 \subset_a E_2\}$$

are both rational languages by lemma 12, 14 and the following formula :

$$\alpha(E_1, E_2) = G - L(E_1, G - E_2); \beta(E_1, E_2) = G - L_\infty(E_1, G - E_2)$$

Hence points (1), (2), (3), (5) are proved.
By same means we can prove that $G_1^{-1}, G_2^{-1}, P^{-1}$ are rational. As the mapping $g \mapsto g^{-1}$ preserves rationality, points (6), (7), (8) are proved.
It remains to prove (4): if $\mathrm{Card}(K) < \infty$ then $K = N$, hence N is rational ;
if $\mathrm{Card}(K) = \infty$, then N is a finite subgroup of K which is included in $\mathrm{B}(1, \mathrm{diam}\ (\partial) + 3\ )$

5 EFFECTIVE DECOMPOSITION of G

We describe first the sequence of operations to be performed (we follow the proof given in p. 41-56 of [5](5.1), we explain then how every operation can be carried effectively (5.2), we evaluate the complexity of the algorithm (5.3) and then state the main result (5.4).

5.1 Sequence of operations

begin

(1) **If** $Card(G) < \infty$ **then begin** Num-ends :=0 ; Stop **end** ;

(2) Find an almost-invariant set E such that

$$\mathrm{Card}(E) = \infty \text{ and } \mathrm{Card}(G - E) = \infty \text{ and } G = E_{+,+} \cup E_{+,-} \cup E_{-,+} \cup E_{-,-}$$

(3) $K := \{g \in G \mid gE =_a E\}$

(4) **If** $\mathrm{Card}(K) = \infty$ **then** Num-ends := 2 **else** Num-ends := ∞

(5) **If** Num-ends = 2 **then begin**

> **(6)** $N := \{g \in K \mid \mathrm{Card}(gE \cap (G - E)) = \mathrm{Card}(g(G - E) - E)\}$;
> $\{Card(N) < \infty; N \lhd K \lhd G; K/N \approx \mathbb{Z}\text{and}[G : K] \leq 2\}$
>
> **(7)** **if** $K = G$ **then** "$G =< N, t; t^{-1}ut = \varphi(u), u \in N >$"
>
> **(8)** **if** $K \neq G$ **then begin** $\{G/K \approx \mathbb{Z}/2\mathbb{Z}\}$
>
> > **(9)** let $a \in G - K, t \in K - N$ such that tN generates K/N
> >
> > **(10)** let k, l be integers such that
> > $a^2 \equiv t^k \pmod N$ and $tat^{-1} \equiv at^l \pmod N$
> > $\{l = -2 \text{ or } l = 0\}$
> >
> > **(11)** **if** l =-2 **then** "$G =< G_3 * G_4; N = N >$"
> > $\{G_3 =< N, a >; G_4 =< N, ta >; [G3 : N] = [G4 : N] = 2\}$
> >
> > **(12)** **if** ($l = 0$ and $k = 2p$) **then**
> > "$G =< G_5, t; ta't^{-1} = a'', tut^{-1} = \varphi(u), u \in N >$"
> > $\{G_5 =< N, a' >, a' = at^{-p}\}$
> >
> > **(13)** **if** ($l = 0$ and $k = 2p + 1$) **then**
> > "$G =< N, t'; t'ut'^{-1} = \varphi(u), u \in N >$"
> > $\{t' = at^{-p}\}$
> >
> > **end** $\{8\}$
>
> **end** {of the case where Num-ends = 2 (line 5)}

(14) **if** Num-ends = ∞ **then begin**

> **(15)** $E' := \{g \in G \mid gE \subset_a E \text{ or } g(G - E) \subset_a E\}$
>
> **(16)** $H := \{g \in G \mid gE =_a E \text{ or } gE =_a G - E\}$
> $G_1 := \{g \in G \mid (E' - K)g = E' - K\}$
> $G_2 := \{g \in G \mid (E' - (H - K))g = E' - (H - K)\}$
> $P := \{g \in G \mid (E' - (H - K))g = E' - K\}$
>
> **(17)** **if** $P = \emptyset$ **then** "$G =< G_1 * G_2; K = K >$" ;
>
> **(18)** **if** ($P \neq \emptyset$ and $H \neq K$) **then** "$G =< G_1 * H; K = K >$" ;
>
> **(19)** **if** ($P \neq \emptyset$ and $H = K$) **then**
> "$G =< G_1, t; t^{-1}kt = \varphi(k), k \in K >$"; {where $t \in P$}
> **end** $\{14\}$

end

5.2 Effectiveness of the operations

(1) M is a rational language (lemma). For every $g \in G$, $\Pi_M^{-1}(g)$ is finite. Hence $\mathrm{Card}(G) < \infty$ iff $\mathrm{Card}(M) < \infty$.This last property can be tested.
(2) There exists some almost-invariant subset E, infinite and having an infinite complement, such that $\boldsymbol{\partial} E$ has minimal cardinality (among all a.invariant subsets which are infinite and co-infinite), and such that

$$G = \bigcup_{(\epsilon,\epsilon')\in\{+,-\}} E_{\epsilon,\epsilon'} \quad ([5], \text{lemma 3.2 p 44}).$$

There exists also some spherical end E_1 which is infinite and co-infinite. By minimality of E :

$$\mathrm{Card}(\boldsymbol{\partial} E) \leq \mathrm{Card}(\boldsymbol{\partial} E_1) \leq 2.\mathrm{Card}(Q).\mathrm{Card}(X)$$

$\boldsymbol{\partial}$ E must contain some elementary cocycle $\boldsymbol{\partial} E_2$ such that E_2 is infinite and co-infinite, and so, by minimality of $\boldsymbol{\partial} E$, $\boldsymbol{\partial} E$ is elementary.
Let us set $D = (3\kappa + 2)$. Card(Q). Card(X).
By lemma 6, diam $(\boldsymbol{\partial} E) \leq D$, hence some translate of E lies in $\mathrm{B}(1, D+1)$. We can compute the ball $\mathrm{B}(1, D+1)$ (lemma 1), enumerate all the elementary cocycles of that ball (lemma 3) and test each of them for the property :

$$G = \bigcup_{(\epsilon,\epsilon')\in\{+,-\}} E_{\epsilon,\epsilon'}$$

(this can be done by lemma 15, point 1).

The sets given in **(3)**, **(6)**, **(15)**, **(16)** can be computed (i.e. finite automata recognising their inverse image by Π_M can be computed) by lemma 15.
The tests instructions **(4)**, **(7)**, **(8)**, **(17)**, **(18)**, **(19)** amount to test the equivalence of some finite automata.

(9) amounts to choose some words w_a, w_t such that

(9.1) $w_a \in \Pi_M^{-1}(G) - \Pi_M^{-1}(K)$
(9.2) $\Pi(w_t)N$ is a generator of K/N

(9.1) is straightforward:it suffices to find some letter $a \in X$ such that $\Pi(a) \notin K$.

In order to find some w_t fulfilling **(9.2)** we compute a finite $Y \subset (X \cup \overline{X})^*$ such that $\Pi(Y)$ generates K :

$$Y = \{ax\overline{a} \mid \Pi(x) \in K\} \cup \{ax \mid \Pi(x) \notin K\}$$

($\Pi(Y)$ is the set of Schreier generators associated to the transversal $\{\Pi(\epsilon), \Pi(a)\}$)
The map $\varphi : K \to \mathbb{Z}$ defined by

$$\forall g \in K, \varphi(g) = Card(gE \cap (G - E)) - Card(g(G - E) \cap E)$$

is an homomorphism ([5], p31) such that Ker$\varphi = N$.
Let n = pgcd$\{\varphi(\Pi(y)) \mid y \in Y\}$. n can be computed. Every word w_t in $\Pi_M^{-1}(\varphi^{-1}(n))$ fulfills **(9.2)**.

(10) amounts to pick some words $(w_t)^k, (w_t)\ell$ respectively in the rational sets of words

- $(w_t)^* \cap \tau_M^{-1}(\Pi_M{}^{-1}(w_a^2\Pi(N)))$
- $(w_t)^* \cap \tau_M^{-1}(\Pi_M{}^{-1}(w_t w_a \tilde{w}_t \tilde{w}_a)\Pi_M^{-1}(N)))$

It remains to compute finite sets of generators for the two factor-subgroups of decompositions **(17)**,**(18)** and for the base-subgroup of decomposition **(19)**.
Let us treate decomposition **(17)**:
given decompositions of each "old" generator $\Pi(x)(x \in X)$ over the subgroups G_1, G_2 :

$$(D_x) : \Pi(x) = g_{x,1}g_{x,2}...g_{x,l(x)} \quad (\text{where } \ g_{x,j} \in G_1, G_2)$$

we can choose the following sets of "new" generators for G_i (where $i \in \{1, 2\}$:

$$Y_i = \{g_{x,j} \mid x \in X, 1 \leq j \leq l(x) \text{ and } \ g_{x,j} \in G_i\}$$

For every $x \in X$, we can build a decomposition of type (D_x) by determining some word in

$$\left(\Pi_M^{-1}(G_1) \cup \Pi_M^{-1}(G_2)\right)^* \cap (\mathrm{L}(\mathcal{M}, F)\overline{x}^{-1})$$

Let X_i be a new alphabet and $\alpha_i : X_i \to Y_i$ a bijection.α_i entends to an homomorphism $\varphi_i : (X_i \cup \overline{X_i})^* \to (X \cup \overline{X})^*$ by setting :

$$\forall a \in X_i, \varphi_i(a) = \alpha_i(a), \varphi_i(\overline{a}) = \overline{\alpha_i(a)}$$

$\varphi_i^{-1}(\mathrm{L}(\mathcal{A},\ y_0q_0))$ is exactly the word-problem for G_i on the generating set Y_i. From $\mathcal{A}, \varphi_)$ we can compute a d.p.d.a. $\mathcal{A}_i$ and a finite set of configurations F_i such that $L_i = \mathrm{L}(\mathcal{A}_i, F_i)$.The cases of decompositions **(18)**,**(19)** can be treated similarly.

5.3 Complexity

In the following we denote by $T(h, n)$ a tower of h exponentials i.e.

$$T(0, n) = n \ \text{ and } \ T(h + 1, n) = n^{T(h,n)}$$

complexity of the operations $\tau_M, \Pi_M^{-1}, \alpha, \beta$:

($\tau_M, \Pi_M^{-1}$are defined in section 4.1 and α, β are defined in the proof of lemma 15;we use below some g.s.m. $\mathcal{A}_M$ which computes τ_M)

Π_M^{-1} : $\quad \overline{\tau}(E) \to \Pi_M^{-1}(E)$
time $\mathrm{O}(||\mathcal{A}_M||.||\overline{\tau}(E)||)$

produces a d.f.a from a d.f.a

τ_M : $\Pi_M^{-1}(E) \to \overline{\tau}(E)$

time $O(||\mathcal{A}_M||.||\overline{\tau}(E)||)$

produces a n.f.a from a n.f.a

α : $(\Pi_M^{-1}(E_1), \overline{\tau}(E_2)) \to \overline{\tau}(\alpha(E_1, E_2))$

time $2^{O(||\Pi_M^{-1}(E_1)||^6 . ||\overline{\tau}(E_2)||^3 . ||\mathcal{A}||^3)}$

produces a deterministic f.a from two n.f.a's

β : $\Pi_M^{-1}(E_1), \overline{\tau}(E_2) \to \overline{\tau}(\beta(E_1, E_2))$

time $2^{O(||\Pi_M^{-1}(E_1)||^6 . (||\overline{\tau}(E_2)|| + ||\mathcal{A}||)^3 . ||\mathcal{A}||^3)}$

produces a d.f.a from a n.f.a recognizing $\Pi_M^{-1}(E_1)$ and a d.f.a recognizing $\overline{\tau}(E_2)$

complexity of the algorithm :

let $n = ||(\mathcal{M}, F)||$ where

$$||(\mathcal{M}, F)|| = \sum_{\omega q' \in \delta(yq,a)} |\omega q'| + |yqa| + \sum_{f \in F} |f|$$

triangulation constant: $\kappa \leq n^n$

canonical d.p.d.a $\mathcal{A}$: $||\mathcal{A}|| = O(T(3, n))$

we deduce from $\mathcal{A}$ a d.f.a $\mathcal{AC}$ recognizing Config($\mathcal{A}$), a g.s.m. $\mathcal{A}_M$ computing τ_M (see the proof of lemma 7), and a d.f.a $\mathcal{D}_M$ recognizing M, with the following sizes $||\mathcal{AC}|| = O(T(3, n))$, $||\mathcal{A}_M|| = O(T(3, n))$, $||\mathcal{D}_M|| = O(T(3, n))$.

instruction (1): time(1) $= O(T(3, n))$.

instruction (2): time(2) $= T(4, O(n))$.

instruction (3): time(3) $= T(4, O(n))$.

instruction (4): time(4) $= T(4, O(n))$.

instruction (6-9): time(6-9) $= T(3, O(n))$.

instruction (10): time(10) $= T(2, O(n))$.

instruction (15): time(15) $= T(4, O(n))$.

instruction (16): time(16) $= T(5, O(n))$.

instruction (17-19): time(17-19) $= T(5, O(n))$.

computation of generators for the factor-subgroups (or the base subgroup) done in time $T(5, O(n))$.

5.4 The main results

The above (rough) analysis proves the following

Theorem 16.

(1) *The algorithm defined in IV-1 produces from every p.d.a $\mathcal{M}$ (with set of final configurations F) of size n, recognizing a language of the form $[\epsilon]_\equiv$, where $X^* / \equiv = G$ is a group,*

- *the number of ends of* G, $N_e(G)$
- *when* $N_e(G) \in \{2, \infty\}$, *it produces a decomposition of* G *either as a non-trivial amalgamated product (with finite amalgamated subgroups) or as an HNN-extension (with finite associated subgroups).*

(2) *the time complexity of this algorithm is* $T(5, 0(n))$.

It is proved in [9] that the isomorphism problem is decidable for f.g. virtually-free groups. Using theorem 16 we can sharpen this theorem as

Theorem 17. *The isomorphism problem for finitely generated virtually free groups is primitive recursive.*

Sketch of proof. Let G, G' be finitely generated virtually free groups given by outer actions of finite groups A, A' respectively on finitely generated free groups F, F'.

From these actions we deduce for G, G' presentations of the form described in [10] p. 299, which in turn allow to build d.p.d.a's $\mathcal{M}, \mathcal{M}'$ recognizing the word problem for G (resp. G'). The sizes of $\mathcal{M}, \mathcal{M}'$ are equal to those of the outer actions.

The accessibility-length of G (resp. G') is $\leq \text{rank}(F) + \text{Card}(A)$ (resp. rank $(F') + \text{Card}(A')$).

A graph of groups $\mathcal{G}$ with only finite vertex-groups and with G as fundamental group can be obtained by iterating algorithm 5.1 at most $(\text{rank}(F) + \text{Card}(A))$ times. As the size of each p.d.a. obtained for a factor (or the base) at each step of decomposition is $T(5, \mathrm{O}(n))$ where n is the size of the previous p.d.a, the whole computation will take a time which is $\mathrm{O}(T(5.(\text{rank}(F)+\text{Card}(A))+1, n))$.

Some realization of G (resp. G') of the type described in the "Culler's realization theorem" can be computed in polynomial time from $\mathcal{G}$ (resp. $\mathcal{G}'$) by the method given in [9] p. 123. The final isomorphism test described in [9] p.137 can be done in time exponential with respect to the size of the realizations, hence neglectable with respect to the above tower of exponentials.

Remark. 1-We could give another proof of lemma 15 leaning on the fact that all the languages described in (1)...(9) can be defined by means of a logical formula with one free set-variable, in the language of monadic second order logic ; by an adaptation of Rabin's theory for S2S on the infinite tree to the case of an infinite context-free graph (see [11], [6]), we could conclude that the unique model of such a formula "corresponds" to a rational tree and is hence rational. The drawback of such a proof is that the complexity analysis of the corresponding algorithm would be more difficult and the complexity itself would be presumably higher.

2-We believe it would be possible to modify the algorithm of section 5.1 in such a way that its time-complexity becomes $T(3, \mathrm{O}(n))$.The main modifications would consist in replacing some applications of lemma 14, by the construction of some "ad-hoc" d.f.a. based on geometric considerations.These modifications would result in an increasing complexity of our paper and a decreasing complexity of the algorithm. We plan to carry out these modifications in a further version of this work.

Aknowledgments
I thank P.Schupp for advising me to read the proof of [5] and D.Holt for making me aware of [9].

References

1. A.V. Anisimov. Group languages. *Kibernetica 4*, pages 18–24, 1971.
2. J.M. Autebert, L. Boasson, and G. Sénizergues. Groups and nts languages. *JCSS vol.35, no2*, pages 243–267, 1987.
3. L. Boasson and M. Nivat. Centers of context-free languages. *LITP technical report no84-44*, 1984.
4. J.R. Buchi. Regular canonical systems. *the collected works of J.R. Buchi*, 1990.
5. D.E. Cohen. *Groups of cohomological dimension one.* Lectures Notes in math.,Springer vol.245, 1972.
6. B. Courcelle. The monadic second-order logic of graphs ii: infinite graphs of bounded width. *Math. Systems Theory 21*, pages 187–221, 1990.
7. W. Dicks and M.J. Dunwoody. *Groups acting on graphs.* Cambridge University Press, 1990.
8. D.B.A. Epstein, J.W. Cannon, D.F. Holt, S.V.F. Levy, M.S. Paterson, and W.P. Thurston. *Word processing in groups.* Jones and Bartlett, 1992.
9. S. Krstic. Actions of finite groups on graphs and related automorphisms of free groups. *Journal of algebra 124*, pages 119–138, 1989.
10. D.E. Muller and P.E. Schupp. Groups, the theory of ends and context-free languages. *JCSS vol 26, no 3*, pages 295–310, 1983.
11. D.E. Muller and P.E. Schupp. The theory of ends, pushdown automata and second-order logic. *TCS 37*, pages 51–75, 1985.
12. J. Sakarovitch. Description des monodes de type fini. *Elektronische Informationsverarbeitung und Kybernetic 17*, pages 417–434, 1981.
13. G. Sénizergues. On the finite subgroups of a context-free group. *in preparation*, 199?
14. Stallings. On torsion-free groups with infinitely many ends. *Ann. of Math. 88*, pages 312–334, 1968.