

# Equations in HNN-extensions.

M. Lohrey and Géraud Sénizergues

<sup>1</sup> Inst. für Informatik, Universität Leipzig, Germany

<sup>2</sup> LABRI, Université Bordeaux I, France

lohrey@informatik.uni-leipzig.de, ges@labri.fr

**Abstract.** Let  $\mathbb{H}$  be a cancellative monoid and let  $\mathbb{G}$  be an HNN-extension of  $\mathbb{H}$  with finite associated subgroups  $A, B \leq \mathbb{H}$ . We show that, if equations are algorithmically solvable in  $\mathbb{H}$ , then they are also algorithmically solvable in  $\mathbb{G}$ . The result also holds for equations with rational constraints and for the existential first order theory. Analogous results are derived for amalgamated product with finite amalgamated subgroups. Finally, a transfer theorem is shown for the fundamental group of a finite graph of groups with finite edge groups and vertex groups where the existential first-order theory is decidable.

**Keywords:**

Equations; groups and monoids; HNN-extensions; amalgamated product.

**Date:**

June 20, 2008

## 1 Introduction

*General context* Theories of equations over groups are a classical research topic at the borderline between algebra, mathematical logic, and theoretical computer science. This line of research was initiated by the work of Lyndon, Tarski, and others in the first half of the 20th century. A major driving force for the development of this field was a question that was posed by Tarski around 1945: Is the first-order theory of a free group  $F$  of rank two, i.e., the set of all statements of first-order logic with equations as atomic propositions that are true in  $F$ , decidable. Decidability results for fragments of this theory were obtained by Makanin (for the existential theory of a free group) [Mak83] and Merzlyakov and Makanin (for the positive theory of a free group) [Mak84, Mer66]. A complete (positive) solution of Tarski's problem was finally announced in [KM98]; the complete solution is spread over a series of papers. The complexity of Makanin's algorithm for deciding the existential theory of a free group was shown to be not primitive recursive in [KP98]. Based on [Pla99], a new PSPACE algorithm for the existential theory of a free group, which also allows to include rational constraints for variables, was presented in [DHG05]. Beside these results for free groups, also extensions to larger classes of groups were obtained in the past: [DL04, DM06, KMS05, RS95]. In [DL03], a general transfer theorem for existential theories was shown: the decidability of the existential theory is preserved by graph products over groups — a construction that generalizes both free and direct products, see e.g. [Gre90]. Moreover, it is shown in [DL03] that for a large class of graph products, the positive theory can be reduced to the existential theory.

The aim of this paper is to prove similar transfer theorems for HNN-extensions (this kind of extension was introduced in [HNN49], its definition is recalled by eq. (1) of section 2) and amalgamated free products (which is a classical tool in algebraic topology, its definition is recalled by eq. (10) of section 2). These two operations are of fundamental importance in combinatorial group theory [LS77]. One of the first important applications of HNN-extensions was a more transparent proof of the celebrated result of Novikov and Boone on the existence of a finitely presented group with an undecidable word problem, see e.g. [LS77]. Such a group can be constructed by a series of HNN-extensions starting from a free group. This shows that there is no hope to prove a transfer theorem for HNN-extensions, similar to the one for graph products from [DL03]. Therefore we mainly consider HNN-extensions and amalgamated free products, where the subgroup  $A$  in (1) and (10), respectively, is finite. These restrictions appear also in other contexts in combinatorial group theory: A seminal result of Stallings [Sta71] states that every group  $G$  with more than one end can be either written in the form (10) with  $A$  finite or in the form (1) with  $A$  finite. Those groups which can be built up from finite groups using the operations of amalgamated free products and HNN-extensions, both subject to the finiteness restrictions above, are precisely the virtually-free groups [DD90] (i.e., those groups with a free subgroup of finite index). Virtually-free groups also have strong connections to formal language theory and infinite graph theory [MS83].

*Main results of the paper* This paper is part of a sequence of three articles dealing with transfer theorems for HNN-extensions and free products with amalgamation where the associated subgroups are finite (see in [LS06] a survey of the full sequence). In [LS08] we studied the membership problem and other related algorithmic problems about rational subsets of monoids and subgroups of groups. Here we study the satisfiability problem for systems of equations (possibly together with disequations and rational constraints) in monoids. In a forthcoming paper ([LS05]) we study the validity of positive first-order formulas in groups.

The main result of this paper is Theorem 2: it states that the satisfiability problem for equations with rational constraints in a monoid  $\mathbb{G}$ , which is an HNN-extension of a cancellative monoid  $\mathbb{H}$ , with finite associated subgroups, is Turing-reducible to the same problem over the base monoid  $\mathbb{H}$ .

Several variations and corollaries of this result are also derived:

- the same transfer property is shown for systems of equations with constants (Theorem 5) and for systems of equations and disequations with rational constraints (Theorem 6);
- a similar theorem is proved for systems of equations and disequations with rational constraints in an amalgamated product (Theorem 10).

As a corollary, the satisfiability problem for equations and disequations with rational constraints in the fundamental group of a finite graph of groups with finite edge groups is Turing-reducible to the join of the same problems in the vertex groups (Theorem 11).

### *Contents*

Section 2 consists of recalls and notation on the subject of monoids and groups, rational subsets of monoids, equations in monoids and algorithmic problems in general. In section 3 we introduce the main technical tool allowing us to deal with equations in HNN-extensions: the notion of AB-algebra. This notion is defined in general. We then study two particular AB-algebras, denoted by  $\mathbb{H}_t$  and  $\mathbb{W}$ , which are crucial in our reductions. The domain of the AB-algebra  $\mathbb{H}_t$  is essentially the set of reduced sequences of the HNN-extension; the domain of  $\mathbb{W}$  is a free product of the finite associated subgroups  $A, B$  with a free monoid generated by all the possible “types” of sequences that might occur in  $\mathbb{H}_t$ , quotiented by relations expressing the pseudo-commutations between each type of sequence and the elements of  $A \cup B$ . In section 4 we make precise our notion of system of equations with rational constraints in a monoid and give normal forms for such systems. In section 5 we provide a reduction of equations over an HNN-extension  $\mathbb{G}$  of a monoid  $\mathbb{H}$  to equations over the AB-algebra  $\mathbb{H}_t$  and equations over the base monoid  $\mathbb{H}$ . In section 6 we reduce equations over the AB-algebra  $\mathbb{H}_t$  to equations over the AB-algebra  $\mathbb{W}$ . In section 7 we reduce equations over the AB-algebra  $\mathbb{W}$  to equations over some finitely generated group  $\mathbb{U}$  which turns out to be virtually-free. In section 8 we show, by induction over the size of the associated subgroups  $A, B$ , that equations in  $\mathbb{U}$  are algorithmically solvable. We then prove a transfer theorem concerning groups only and prove finally our main Theorem 2 concerning cancellative monoids. In section 9 we adapt the proof-techniques developed in the previous sections in

order to prove some variants of Theorem 2 where the constraints can be positive only, in particular to the case of equations with constants. In section 10 we extend to equations and disequations the reduction exposed in section 5. We thus prove some transfer theorems for systems of equations and disequations in HNN-extensions of cancellative monoids. In section 11 we deduce from our previous results on HNN-extensions a transfer theorem for systems of equations and disequations with rational constraints in free products with amalgamation of cancellative monoids (with finite amalgamated subgroups). In section 12 we synthesize two transfer theorems obtained previously, one for HNN-extensions and the other for free products with amalgamation, into a single theorem about finite graphs of groups.

## Table of Contents

Equations in HNN-extensions. . . . .	1
1 Introduction. . . . .	2
2 Preliminaries . . . . .	7
2.1 Partial semi-groups . . . . .	7
2.2 Monoids and groups . . . . .	7
Monoids . . . . .	7
HNN-extensions . . . . .	8
Amalgamated products . . . . .	9
2.3 Rational subsets of a monoid . . . . .	10
2.4 Equations and disequations over a monoid . . . . .	10
Equations . . . . .	10
Disequations . . . . .	11
Special constraints . . . . .	11
Definable subsets . . . . .	11
2.5 Reductions among decision problems . . . . .	12
3 AB-algebras . . . . .	13
3.1 Types . . . . .	13
3.2 AB-algebra axioms . . . . .	14
3.3 AB-homomorphisms . . . . .	16
3.4 Finite $t$ -automata . . . . .	16
3.5 The AB-algebra $\mathbb{H}_t$ . . . . .	21
$\mathbb{H} * \{t, \bar{t}\}^*$ . . . . .	21
$\mathbb{H}_t$ . . . . .	22
Algebraic properties . . . . .	23
3.6 The AB-algebra $\mathbb{W}$ . . . . .	26
$\mathcal{W}^* * A * B$ . . . . .	26
$\mathbb{W}$ . . . . .	28
$\mathbb{W}_t, \mathbb{W}_{\mathbb{H}}, \hat{\mathbb{W}}$ . . . . .	28
Involutions . . . . .	29
Homomorphisms . . . . .	31
4 Equations with rational constraints over $\mathbb{G}$ . . . . .	40
4.1 Equations with rational constraints . . . . .	40
Quadratic normal form . . . . .	40
Rational constraints . . . . .	41
4.2 Equations and disequations with rational constraints . . . . .	42
5 Equations over $\mathbb{H}_t$ . . . . .	44
5.1 $t$ -equations . . . . .	44
5.2 From $\mathbb{G}$ -equations to $t$ -equations . . . . .	44
From $\mathbb{G}$ -solutions to $t$ -solutions . . . . .	47
From $t$ -solutions to $\mathbb{G}$ -solutions . . . . .	51
6 Equations over $\mathbb{W}$ . . . . .	53
6.1 $\mathbb{W}$ -equations . . . . .	53
6.2 From $t$ -equations to $\mathbb{W}$ -equations . . . . .	53
From $t$ -solutions to $\mathbb{W}$ -solutions . . . . .	53

	From $\mathbb{W}$ -solutions to $\mathbf{t}$ -solutions .....	63
7	Equations over $\mathbb{U}$ .....	65
7.1	The group $\mathbb{U}$ .....	65
7.2	From $\mathbb{W}$ -equations to $\mathbb{U}$ -equations .....	65
	From $\mathbb{W}$ -solutions to $\mathbb{U}$ -solutions .....	66
	From $\mathbb{U}$ -solutions to $\mathbb{W}$ -solutions .....	67
	Bijection $\Phi$ .....	69
8	Transfer of solvability .....	70
8.1	The structure of $\mathbb{U}$ .....	70
8.2	Transfer results .....	71
	Transfer for groups .....	71
	Transfer for cancellative monoids .....	75
9	Equations with positive rational constraints over $\mathbb{G}$ .....	81
9.1	Positive rational constraints .....	81
9.2	Positive subgroup constraints .....	81
9.3	Constants .....	83
10	Equations and disequations with rational constraints over $\mathbb{G}$ .....	84
10.1	Rational constraints .....	84
	From $\mathbb{G}$ -solutions to $\mathbf{t}$ -solutions .....	86
	From $\mathbf{t}$ -solutions to $\mathbb{G}$ -solutions .....	89
10.2	Positive rational constraints .....	91
10.3	Constants .....	92
11	Equations and disequations over an amalgamated product .....	93
11.1	Free product .....	93
11.2	Free product with amalgamation .....	93
11.3	Equations over an amalgamated product .....	94
12	Equations and disequations over a graph of groups .....	95

## 2 Preliminaries

We recall in this section all the needed definitions and classical results concerning partial semi-groups, semi-groups, monoids and groups.

### 2.1 Partial semi-groups

Let  $(P, \cdot)$  be a set endowed with a function  $\cdot : P \times P \rightarrow P$ . By  $D(\cdot) \subseteq P \times P$  we denote the domain of the law  $\cdot$ . The structure

$$\langle P, \cdot \rangle$$

is a *partial semi-group* iff, for every  $p, q, r \in P$ ,

$$(p, q) \in D(\cdot) \wedge ((p \cdot q), r) \in D(\cdot) \Leftrightarrow (q, r) \in D(\cdot) \wedge (p, (q \cdot r)) \in D(\cdot)$$

and, in the case where  $((p \cdot q), r) \in D(\cdot)$

$$(p \cdot q) \cdot r = p \cdot (q \cdot r).$$

Let us notice that, when  $P$  is a partial semi-group, the following structure is a semi-group:

$$\langle \mathcal{P}(P), \cdot \rangle$$

where the product is defined by  $\cdot$ , for every  $R, S \in \mathcal{P}(P)$

$$R \cdot S = \{r \cdot s \mid (r, s) \in R \times S \cap D(\cdot)\}.$$

Let  $A, B$  be two groups. For every  $K, K' \in \{A, B\}$ , we denote by  $\text{PIs}(K, K')$  the set of all group isomorphisms  $\varphi$  with  $\text{dom}(\varphi) \subseteq K, \text{im}(\varphi) \subseteq K'$ . We then define

$$\text{PGI}(A, B) := \text{PIs}(A, A) \cup \text{PIs}(A, B) \cup \text{PIs}(B, A) \cup \text{PIs}(B, B).$$

The pair  $\langle \text{PGI}(A, B), \circ \rangle$  is a partial semi-group.

### 2.2 Monoids and groups

**Monoids** A semi-group is a pair  $(M, \cdot)$  such that  $\cdot$  is a total mapping  $M \times M \rightarrow M$  which is associative i.e.  $\forall x, y, z \in M, ((x \cdot y) \cdot z) = (x \cdot (y \cdot z))$ . A monoid is a triple  $(M, \cdot, e)$  such that  $(M, \cdot)$  is a semi-group and  $e$  is a neutral element for the law  $\cdot$  which means that, for every  $m \in M, m \cdot e = e \cdot m = m$ . A monoid  $(M, \cdot, e)$  is called cancellative iff, for every  $x, y, z \in M, x \cdot y = x \cdot z \Rightarrow y = z$  and  $y \cdot x = z \cdot x \Rightarrow y = z$ . A submonoid of a monoid  $(M, \cdot, e)$  is a monoid  $(N, \circ, f)$  such that  $N \subseteq M, \forall n, n' \in N, n \circ n' = n \cdot n'$  and  $e = f$ . A subgroup of a monoid  $(M, \cdot, e)$  is a submonoid  $(N, \circ, e)$  of  $(M, \cdot, e)$  which is a group i.e. such that,  $\forall x \in N, \exists x' \in N, x \circ x' = x' \circ x = e$ . Let  $(M, \cdot, 1)$  be a monoid. Let us consider some elements  $s \in M$  and define  $D(s) := \{(m, m') \in M \times M \mid m \cdot s = s \cdot m'\}$ . This subset  $D(s)$  is always a sub-monoid of the product monoid  $M \times M$ . Moreover, when  $M$  is cancellative, for every  $s \in M, D(s)$  is a partial isomorphism.

**HNN-extensions** Let us fix throughout this section, a monoid  $\mathbb{H}$  (the base monoid), two finite subgroups  $A \leq \mathbb{H}, B \leq \mathbb{H}$  and an isomorphism  $\varphi : A \rightarrow B$ . We then consider the HNN-extension

$$\mathbb{G} = \langle \mathbb{H}, t; t^{-1}at = \varphi(a) (a \in A) \rangle \quad (1)$$

We denote by

$$\pi_G : \mathbb{H} * \{t, \bar{t}\}^* \rightarrow \mathbb{G}$$

the homomorphism sending every  $h \in \mathbb{H}$  on itself in  $\mathbb{G}$  and mapping  $t$  to  $t$  (resp.  $\bar{t}$  to  $t^{-1}$ ).

The kernel of  $\pi_G$  coincides with the congruence  $\approx$  over  $\mathbb{H} * \{t, \bar{t}\}^*$  generated by the set of rules

$$t\bar{t} \approx \bar{t}t \approx 1, \quad (2)$$

$$at \approx t\varphi(a), \quad \text{for all } a \in A \text{ and} \quad (3)$$

$$b\bar{t} \approx \bar{t}\varphi^{-1}(b), \quad \text{for all } b \in B. \quad (4)$$

An element of  $s \in \mathbb{H} * \{t, \bar{t}\}^*$  can be viewed as a word over the alphabet  $\mathbb{H} \cup \{t, \bar{t}\}$  which has the form:

$$s = h_0 t^{\alpha_1} h_1 \dots t^{\alpha_i} h_i \dots t^{\alpha_n} h_n, \quad (5)$$

where  $n \in \mathbb{N}, \alpha_i \in \{+1, -1\}$ ,  $t^{-1}$  means the letter  $\bar{t}$  and  $h_i \in \mathbb{H}$ .

We name  $t$ -sequence every such  $s \in \mathbb{H} * \{t, \bar{t}\}^*$ . The  $t$ -sequence  $s$  is said to be a *reduced sequence* iff it does not contain any factor of the form  $\bar{t}at$  (with  $a \in A$ ) nor  $tb\bar{t}$  (with  $b \in B$ ). We denote by  $\text{Red}(\mathbb{H}, t)$  the subset of  $\mathbb{H} * \{t, \bar{t}\}^*$  consisting of all reduced sequences. Let us denote by  $\sim$  the congruence over  $\mathbb{H} * \{t, \bar{t}\}^*$  generated by all the rules of type (3),(4) above. The set  $\text{Red}(\mathbb{H}, t)$  is saturated by the congruence  $\sim$ . The following lemma is fundamental.

**Lemma 1.** *Let  $s, s'$  be some reduced sequences. Then  $s \approx s'$  if and only if  $s \sim s'$ .*

This lemma could be named “Britton’s lemma for monoids”. (See [?, Appendix A], for example, for a proof).

**Lemma 2.** *If the monoid  $\mathbb{H}$  is cancellative then the extension monoid  $\mathbb{G}$  is cancellative too.*

*Proof.* Let us use the properties of normal forms established in [?, Appendix A]. We recall that  $\mathcal{N}$  denotes the set of *normal forms* w.r.t.  $\approx$  (which is also a set of normal forms for elements of  $\mathbb{H} * \{t, \bar{t}\}^*$  w.r.t.  $\sim$ ) and  $\rho : \mathbb{H} * \{t, \bar{t}\}^* \rightarrow \mathcal{N}$  is the *reduction* map, associating to every  $t$ -sequence its normal form. Let us assume that  $\mathbb{H}$  is cancellative. We show in (1) that  $\mathbb{G}$  is right-cancellative and in (2) that it is left-cancellative.

1- Let  $s, s' \in \mathcal{N}$  and  $h \in \mathbb{H}$ :

$$s = h_0 t^{\alpha_1} \dots t^{\alpha_n} h_n, \quad s' = h'_0 t^{\alpha'_1} \dots t^{\alpha'_m} h'_m$$



where  $h_0 \in R_{A(\alpha_1)}, \dots, h_{n-1} \in R_{A(\alpha_n)}, h_n \in \mathbb{H}, h'_0 \in R_{A(\alpha'_1)}, \dots, h'_{m-1} \in R_{A(\alpha'_m)}, h'_m \in \mathbb{H}$ . For every  $h \in \mathbb{H}$ :

$$\begin{aligned}
& \rho(s \cdot h) = \rho(s' \cdot h) \\
& \Leftrightarrow \rho(h_0 t^{\alpha_1} \dots t^{\alpha_n} h_n \cdot h) = \rho(h'_0 t^{\alpha'_1} \dots t^{\alpha'_m} h'_m \cdot h) \\
& \Leftrightarrow h_0 t^{\alpha_1} \dots t^{\alpha_n} \cdot (h_n \cdot h) = h'_0 t^{\alpha'_1} \dots t^{\alpha'_m} \cdot (h'_m \cdot h) \\
& \Leftrightarrow n = m \wedge (\forall i \in [1, n], \alpha_i = \alpha'_i) \wedge (\forall i \in [1, n], h_{i-1} = h'_{i-1}) \wedge h_n \cdot h = h'_n \cdot h \text{ ( prop. of the free product )} \\
& \Leftrightarrow n = m \wedge (\forall i \in [1, n], \alpha_i = \alpha'_i) \wedge (\forall i \in [1, n], h_{i-1} = h'_{i-1}) \wedge h_n = h'_n \text{ ( cancellativity of } \mathbb{H} \text{ )}.
\end{aligned}$$

We have thus established that, for every  $g, g' \in \mathbb{G}, h \in \mathbb{H}$

$$g \cdot h = g' \cdot h \Rightarrow g = g' \quad (6)$$

Since  $\mathbb{G}$  is generated by  $\mathbb{H} \cup \{t, t^{-1}\}$ , properties (6-??) imply that  $\mathbb{G}$  is right-cancellative.

2- Using a notion of left-normal form, dual to the notion of right-normal form used in (1), one can also show that  $\mathbb{G}$  is left-cancellative.

We define the norm of a given sequence  $s \in \mathbb{H} * \{t, \bar{t}\}^*$  by:

$$\|s\| = |s|_{\{t, \bar{t}\}}. \quad (7)$$

One can easily check that, for every  $s, s' \in \mathbb{H} * \{t, \bar{t}\}^*$

$$\|s \cdot s'\| = \|s\| + \|s'\|; \quad \|s\| = 0 \Leftrightarrow s \in H. \quad (8)$$

The boolean norm of a t-sequence  $s$  is the boolean defined by

$$\| \|s\| \| = 1 \Leftrightarrow \|s\| \geq 1. \quad (9)$$

**Amalgamated products** Let us consider two monoids  $\mathbb{H}_1, \mathbb{H}_2$ , two finite subgroups  $A_1 \leq \mathbb{H}_1, A_2 \leq \mathbb{H}_2$ , and an isomorphism  $\varphi : A_1 \rightarrow A_2$ . The corresponding amalgamated product

$$\mathbb{G} = \langle \mathbb{H}_1, \mathbb{H}_2; a = \varphi(a) (a \in A_1) \rangle \quad (10)$$

is defined by  $G = (H_1 * H_2) / \approx$ , where  $\approx$  is the congruence on the free product  $H_1 * H_2$  generated by the equations  $a = \varphi(a)$  for  $a \in A_1$ . An  $(H_1, H_2)$ -sequence is an element  $s \in H_1 * H_2$ ; it has a unique decomposition of the form:

$$s = h_0 k_1 h_1 \dots k_i h_i \dots k_n h_n, \quad (11)$$

where  $n \geq 0, h_1, \dots, h_i, \dots, h_{n-1} \in \mathbb{H}_2 - \{1\}, k_1, \dots, k_i, \dots, k_n \in \mathbb{H}_1 - \{1\}$  and  $h_0, h_n \in \mathbb{H}_2$ . We name *reduced*  $(H_1, H_2)$ -sequence every  $s \in \mathbb{H}_1 * \mathbb{H}_2$  of the form:

$$s = h_0 k_1 h_1 \dots k_i h_i \dots k_n h_n, \quad (12)$$

where  $n \geq 0, h_1, \dots, h_i, \dots, h_{n-1} \in \mathbb{H}_2 - A_2, k_1, \dots, k_i, \dots, k_n \in \mathbb{H}_1 - A_1$  and  $h_0, h_n \in \mathbb{H}_2$ . We denote by  $\text{Red}(\mathbb{H}_1 * \mathbb{H}_2)$  the set of all reduced  $(H_1, H_2)$ -sequences.

It is well-known that  $\mathbb{G}$  is embedded into the HNN-extension

$$\hat{\mathbb{G}} = \langle \mathbb{H}_1 * \mathbb{H}_2, t; t^{-1}at = \varphi(a)(a \in A_1) \rangle$$

by the map

$$h_1 \in \mathbb{H}_1 \mapsto t^{-1}h_1t; \quad h_2 \in \mathbb{H}_2 \mapsto h_2 \quad (13)$$

(see [LS77, Theorem 2.6. p. 187] in the case where  $\mathbb{H}_1, \mathbb{H}_2$  are groups and [LS08] for the adaptation to the free product of monoids with amalgamation over subgroups). Further basic terminology and results on free products with amalgamation are given in [LS08], section 5.

### 2.3 Rational subsets of a monoid

Let  $\mathbb{M} = (M, \cdot, 1_M)$  be some monoid. The set

$$\text{Rat}(\mathbb{M}) \in \mathcal{P}(\mathcal{P}(M))$$

is the smallest element of  $\mathcal{P}(\mathcal{P}(M))$  which possesses the finite subsets of  $M$  and which is closed under the operations  $\cup$  (the union operation),  $\cdot$  (the product operation) and  $*$  (the star operation, associating with a subset  $P$  the smallest submonoid of  $\mathbb{M}$  containing  $P$ ).

We introduced in [LS08], in the particular case where  $\mathbb{M}$  is an HNN-extension, a kind of finite automata called *t-automata*, which recognize exactly the rational subsets of  $\mathbb{M}$ . We postpone to §3.4 a precise normal form for these automata. Given a normal finite t-automaton  $\mathcal{A}$  and an element  $g \in \mathbb{G}$  we set:

$$\mu_{\mathcal{A}, \mathbb{G}}(g) = \mu_{\mathcal{A}, 1}((1, H, \|s\|, 1, 1), s), \quad (14)$$

where  $s$  is any reduced t-sequence representing  $g$ . Since  $\mathcal{A}$  is  $\sim$ -saturated, the value of  $\mu_{\mathcal{A}, 1}(s)$  does not depend of the chosen representative  $s$ .

### 2.4 Equations and disequations over a monoid

**Equations** Let  $\mathbb{M} = (M, \cdot, 1_M)$  be some monoid and let

$$\mathcal{C} \in \mathcal{P}(\mathcal{P}(M)).$$

A *system of equations*  $\mathcal{S}$ , over  $\mathbb{M}$ , with variables in a set  $\mathcal{U}$ , is a family  $((u_i, u'_i))_{i \in I}$  of elements of  $\mathcal{U}^* \times \mathcal{U}^*$ . This system is said to be *quadratic* if, for every  $i \in I$ ,

$$|u_i| = 1, \quad |u'_i| = 2.$$

A  $\mathcal{C}$ -constraint over  $\mathcal{U}$  is a map  $C : \mathcal{U} \rightarrow \mathcal{C}$ . A  $\mathbb{M}$ -solution of the system  $\mathcal{S}$  with  $\mathcal{C}$ -constraint  $C$  is any monoid homomorphism

$$\sigma_{\mathbb{M}} : \mathcal{U}^* \rightarrow \mathbb{M}$$

fulfilling both conditions:

$$\forall i \in I, \sigma_{\mathbb{M}}(u_i) = \sigma_{\mathbb{M}}(u'_i) \quad (15)$$

$$\forall U \in \mathcal{U}, \sigma_{\mathbb{M}}(U) \in C(U). \quad (16)$$

**Disequations** A *system of equations and disequations* over  $\mathbb{M}$  is a family  $((u_i, c_i, u'_i))_{i \in I}$  of elements of  $\mathcal{U}^* \times \{=, \neq\} \times \mathcal{U}^*$ , where  $\mathcal{U}$  is a set of variables.

A  $\mathbb{M}$ -solution of the system  $((u_i, c_i, u'_i))_{i \in I}$  with constraint  $C$  is any monoid homomorphism

$$\sigma_{\mathbb{M}} : \mathcal{U}^* \rightarrow \mathbb{M}$$

fulfilling both conditions:

$$\forall i \in I, \sigma_{\mathbb{M}}(u_i) c_i \sigma_{\mathbb{M}}(u'_i) \quad (17)$$

and (16) above. One sometimes also consider systems of equations and disequations with partial involution. This means that some variables  $u \in \mathcal{U}$  have a formal inverse  $u^{-1} \in \mathcal{U}$  and that a solution  $\sigma_{\mathbb{M}}$  of the system is asked to respect the partial involution i.e. to map the variable  $u^{-1}$  onto the inverse of  $\sigma_{\mathbb{M}}(u)$ . Such a system “with partial involution” can be reduced to a system of the form above by adding the equations  $uu^{-1} = 1$  and  $u^{-1}u = 1$  in the system and removing the explicit constraint that  $\sigma_{\mathbb{M}}$  respects some partial involution.

**Special constraints** In the case where  $\mathcal{C} = \{\{m\} \mid m \in M\} \cup \{M\}$ , any system of equations with constraints in  $\mathcal{C}$  is called a system of equations with *constants* (since the variables  $U \in \mathcal{U}$  such that  $C(U)$  is a singleton are seen as constants in  $\mathbb{M}$  while the variables  $U \in \mathcal{U}$  such that  $C(U) = M$  are seen as variables without any constraint).

In the case where  $\mathcal{C} = \mathcal{B}(\text{Rat}(\mathbb{M}))$ , (i.e. the boolean closure of the set of rational subsets of  $\mathbb{M}$ ), any system of equations with constraints in  $\mathcal{C}$  is called a system of equations with *rational constraints*.

In the case where  $\mathcal{C} = \text{Rat}(\mathbb{M})$ , in order to emphasize the fact that we do not use constraints that are complement of rational subsets, any system of equations with constraints in  $\mathcal{C}$  is called a system of equations with *positive* rational constraints.

**Definable subsets** Let  $\mathbb{M}$  be a monoid and let  $\mathcal{C} \in \mathcal{P}(\mathcal{P}(\mathbb{M}))$ . We denote by  $\text{EQ}(\mathbb{M}, \mathcal{C})$  the set of all subsets of  $\mathbb{M}$  which can be defined by a system of equations with constants and with constraints in  $\mathcal{C}$ .

We denote by  $\text{Def}_{\exists+}(\mathbb{M}, \mathcal{C})$  the set of all subsets of  $\mathbb{M}$  which can be defined by

a logical formula of the form  $\exists w_1 \cdot \exists w_2 \cdots \exists w_n \Psi$  where  $\Psi$  is a positive boolean combination of statements which are either equations with constants or of the form  $v \in P$  (for some variable  $v$  and some element  $P \in \mathcal{C}$ ). The elements of  $\text{EQ}(\mathbb{M}, \mathcal{C})$  are called the *equational* subsets (with constraints in  $\mathcal{C}$ ); the elements of  $\text{Def}_{\exists+}(\mathbb{M}, \mathcal{C})$  are called the *positively definable* subsets (with constraints in  $\mathcal{C}$ ).

## 2.5 Reductions among decision problems

A one tape Turing machine  $M$  *with oracle* is a Turing-machine, with three different special state  $q_?, q_y, q_n$  such that, when the current state of  $M$  is  $q_?$ ,  $M$  makes a transition that does not move the two tape heads, does not print anything, and enters the state  $q_y$  or the state  $q_n$  according to whether the word on tape 2 belongs to  $L_2$  or not (see, for example [HU79, §8.9, p. 209-210] or [Rog87, p. 128] for a more precise definition). Such an oracle machine  $M$  is called a (Turing)-reduction from  $L_1$  to  $L_2$  if the language recognized by  $M$ , using the oracle  $L_2$ , is the language  $L_1$ . When such a reduction exists we say that  $L_1$  is Turing-reducible to  $L_2$ . The underlying idea is that, if somebody knows both  $M$  and a machine  $M_2$  that recognizes  $L_2$ , then he can combine them into a Turing machine  $M_1$  that recognizes  $L_1$ . Let us consider three languages  $L_1, L_2, L_3$ . We call Turing reduction from  $L_1$  to  $(L_2, L_3)$  any Turing-reduction from  $L_1$  to the union of a copy of  $L_2$  over an alphabet  $A_2$  with a copy of  $L_3$  over an alphabet  $A_3$  such that  $A_2 \cap A_3 = \emptyset$ . Given decision problems  $P_1, P_2, P_3$ , we say that  $P_1$  is Turing-reducible to  $P_2$  (or to  $(P_2, P_3)$ ) when the formal languages  $L_1, L_2, L_3$  that encode the set of instances where the correct answer is “yes” are fulfilling the above definition of the notion of reduction.

### 3 AB-algebras

We define here the notion of  $AB$ -algebra, which we devised for handling equations with rational constraints in an HNN-extension.

#### 3.1 Types

Let us consider the finite set of types  $\mathcal{T}_6$  defined in [LS08]. We define a finite partial semi-group  $\langle \mathcal{T}, \cdot \rangle$  as follows:

$$\mathcal{T} = \mathcal{T}_6 \times \mathbb{B} \times \mathcal{T}_6$$

where  $\mathbb{B} = \langle \{0, 1\}, \cdot \rangle$  is the monoid of booleans. The partial product is defined by: for every  $(p, b, q), (p', b', q') \in \mathcal{T}_6 \times \mathbb{B} \times \mathcal{T}_6$ , if  $q = p'$  then

$$(p, b, q) \cdot (p', b', q') = (p, b + b', q'),$$

otherwise the product is undefined. As we noticed in §2.1,  $\langle \mathcal{P}(\mathcal{T}), \cdot \rangle$  is thus a semi-group.

We define an involutory map  $\mathbb{I}_{\mathcal{R}} : \mathcal{T}_6 \rightarrow \mathcal{T}_6$  by:

$$(A, T) \mapsto (A, H), (A, H) \mapsto (A, T), (B, T) \mapsto (B, H), (B, H) \mapsto (B, T), (1, H) \mapsto (1, 1), (1, 1) \mapsto (1, H).$$

We then define an involution  $\mathbb{I}_{\mathcal{T}} : \mathcal{T} \rightarrow \mathcal{T}$  by:

$$\mathbb{I}_{\mathcal{T}}(p, b, q) = (\mathbb{I}_{\mathcal{R}}(q), b, \mathbb{I}_{\mathcal{R}}(p)).$$

One can check that  $\mathbb{I}_{\mathcal{T}}$  is an involutory anti-automorphism of  $\mathcal{T}$ . This involution induces an involutory semi-group anti-automorphism of  $\langle \mathcal{P}(\mathcal{T}), \cdot \rangle$  that will be denoted by  $\mathbb{I}_{\mathcal{T}}$  too. We associate to every element  $\theta$  of  $\mathcal{T}$  an “initial type”  $\tau i(\theta) \in \mathcal{T}_6$ , an “end type”  $\tau e(\theta) \in \mathcal{T}_6$ , an “initial group”  $\text{Gi}(\theta) \in \{\{1\}, A, B\}$  and an “end group”  $\text{Ge}(\theta) \in \{\{1\}, A, B\}$ :

$$\tau i(p, b, q) = p, \quad \text{Gi}(p, b, q) = p_1(p), \quad \tau e(p, b, q) = q, \quad \text{Ge}(p, b, q) = p_1(q).$$

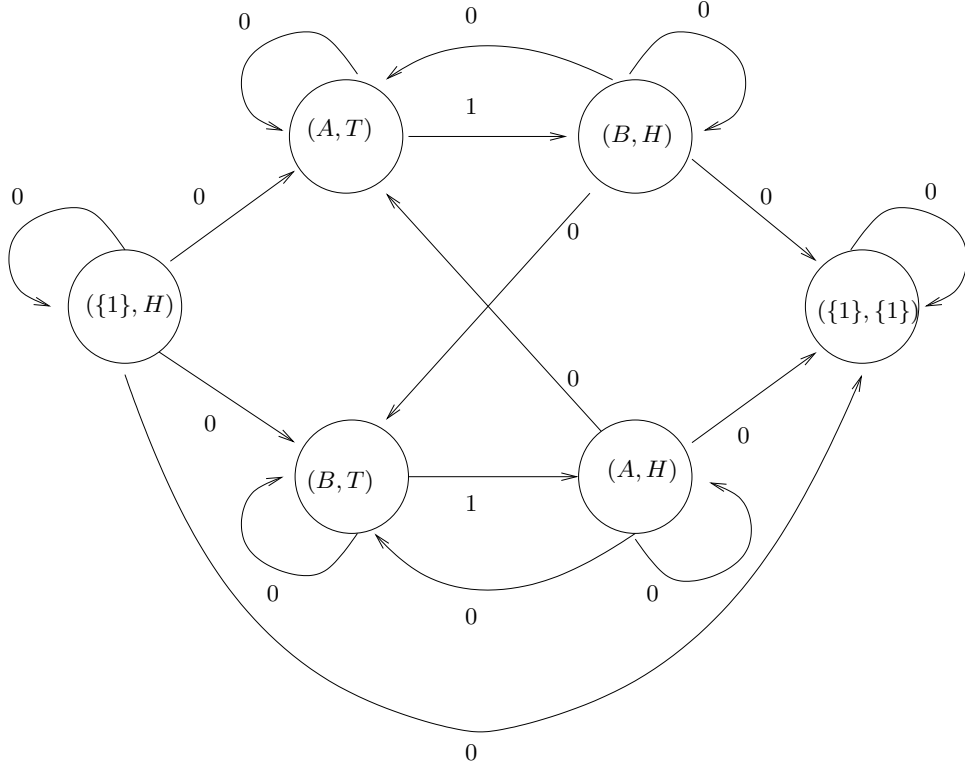
Each element of  $\mathcal{T}$  is called a *path-type* while the elements of  $\mathcal{T}_6$  are called *vertex-types*. This terminology refers to the graph  $\mathcal{R}$  exhibited on Figure 1. (It is a variant of the t-automaton  $\mathcal{R}_6$  defined in [LS08], which recognizes the set of reduced t-sequences,  $\text{Red}(\mathbb{H}, t)$ ). Let us call *atomic types* the path-types corresponding to the edges of  $\mathcal{R}$  i.e. :

$$(A, T, 1, B, H), (B, T, 1, A, H) \tag{18}$$

$$(A, H, 0, B, T), (B, H, 0, A, T), (A, H, 0, A, T), (B, H, 0, B, T), \tag{19}$$

$$(1, H, 0, A, T), (1, H, 0, B, T), (B, H, 0, 1, 1), (A, H, 0, 1, 1), (1, H, 0, 1, 1) \tag{20}$$

$$(1, H, 0, 1, H), (A, T, 0, A, T), (B, T, 0, B, T), (B, H, 0, B, H), (A, H, 0, A, H), (1, 1, 0, 1, 1). \tag{21}$$



**Fig. 1.** graph  $\mathcal{R}$

This set is closed under  $\mathbb{I}_{\mathcal{T}}$ . It is denoted by  $\mathcal{TA}$ . The partial submonoid generated by this set of atomic path-types will be denoted by  $\mathcal{TR}$ . It is closed under the involution  $\mathbb{I}_{\mathcal{T}}$ . The only path-types used in this work are those from  $\mathcal{TR}$ . We call  $T$ -types all the atomic types listed in (18),  $H$ -types all the atomic types listed in (19)(20),  $A \cup B$ -types all the atomic types listed in (21). Note that some types are non-atomic: for example  $(A, T, 1, A, H) = (A, T, 1, B, H) \cdot (B, H, 0, B, T) \cdot (B, T, 1, A, H)$  is an element of  $\mathcal{TR} - \mathcal{TA}$ .

### 3.2 AB-algebra axioms

Let  $A, B$  be two groups (what we have in mind are the two subgroups  $A, B$  of  $\mathbb{H}$  leading to the HNN-extension  $\mathbb{G}$  defined by (1)) and  $Q$  be some finite set (we have in mind the set of states of some t-automaton  $\mathcal{A}$  over  $\mathbb{H} * \{t, \bar{t}\}^*$ ). Let us denote by  $\mathbf{B}(Q)$  the monoid  $(\mathcal{P}(Q \times Q))$  of binary relations over  $Q$  and by  $\mathbf{B}^2(Q)$  the direct product of the monoid  $\mathbf{B}(Q)$  by itself. Given  $m \in \mathbf{B}(Q)$ ,  $m^{-1}$  is the binary relation  $m^{-1} = \{(p, q) \in Q \times Q \mid (q, p) \in m\}$ . We consider the involutory

monoid anti-isomorphism  $\mathbb{I}_Q : B^2(Q) \rightarrow B^2(Q)$  defined by

$$\forall m, m' \in B(Q), \quad \mathbb{I}_Q(m, m') = (m'^{-1}, m^{-1}).$$

We call  $AB$ -algebra a structure of the form

$$\langle \mathbb{M}, \cdot, 1_{\mathbb{M}}, \mathbb{I}, \iota_A, \iota_B, \gamma, \mu, \delta \rangle \quad (22)$$

where  $\iota_A : A \rightarrow \mathbb{M}, \iota_B : B \rightarrow \mathbb{M}$  are total maps,  $\mathbb{I} : \mathbb{M} \rightarrow \mathbb{M}$  is a partial map,  $\gamma : \mathbb{M} \rightarrow \mathcal{P}(\mathcal{T})$  is a total map,  $\mu : \mathcal{T} \times \mathbb{M} \rightarrow B^2(Q)$  is a total map,  $\delta : \mathcal{T} \times \mathbb{M} \rightarrow \text{PGI}(A, B)$  is a total map ;  
fulfilling the eleven axioms (23-33) below.

**monoid:**

$$(\mathbb{M}, \cdot, 1_{\mathbb{M}}) \text{ is a monoid ,} \quad (23)$$

**embeddings:**

$$\iota_A, \iota_B \text{ are injective monoid homomorphisms ,} \quad (24)$$

**involution I:**

$$\iota_A(A) \cup \iota_B(B) \subseteq \text{dom}(\mathbb{I}) \subseteq \mathbb{M} \setminus \gamma^{-1}(\{\emptyset\}) \quad (25)$$

for every  $m, m' \in \mathbb{M}$ ,

$$[\gamma(m) \cdot \gamma(m') \neq \emptyset] \Rightarrow [m \cdot m' \in \text{dom}(\mathbb{I}) \Leftrightarrow (m \in \text{dom}(\mathbb{I}) \wedge m' \in \text{dom}(\mathbb{I}))] \quad (26)$$

$\mathbb{I} : (\text{dom}(\mathbb{I}), \cdot, 1_{\mathbb{M}}) \rightarrow (\text{dom}(\mathbb{I}), \cdot, 1_{\mathbb{M}})$  is a monoid anti-isomorphism,  $\mathbb{I} \circ \mathbb{I} = \text{Id}_{\text{dom}(\mathbb{I})}$ ,  
(27)

**almost homomorphisms:**

for every  $m, m' \in \mathbb{M}$ ,

$$\gamma(m \cdot m') \supseteq \gamma(m) \cdot \gamma(m'), \quad (28)$$

for every  $m, m' \in \mathbb{M}, \theta \in \gamma(m), \theta' \in \gamma(m')$ , such that  $(\theta, \theta') \in D(\cdot)$ ,

$$\mu(\theta \cdot \theta', m \cdot m') = \mu(\theta, m) \cdot \mu(\theta', m'), \quad (29)$$

$$\text{dom}(\delta(\theta, m)) \subseteq \text{Gi}(\theta), \text{im}(\delta(\theta, m)) \subseteq \text{Ge}(\theta) \quad (30)$$

$$\delta(\theta \cdot \theta', m \cdot m') = \delta(\theta, m) \circ \delta(\theta', m'). \quad (31)$$

**commutation with I:**

for every  $a \in A, b \in B, m \in \text{dom}(\mathbb{I}), \theta \in \gamma(m)$ ,

$$\mathbb{I}(\iota_A(a)) = \iota_A(a^{-1}); \quad \mathbb{I}(\iota_B(b)) = \iota_B(b^{-1}) \quad (32)$$

$$\gamma(\mathbb{I}(m)) = \mathbb{I}_{\mathcal{T}}(\gamma(m)); \quad \mu(\mathbb{I}_{\mathcal{T}}(\theta), \mathbb{I}(m)) = \mathbb{I}_Q(\mu(\theta, m)); \quad \delta(\mathbb{I}_{\mathcal{T}}(\theta), \mathbb{I}(m)) = \delta(\theta, m)^{-1}. \quad (33)$$

Axiom (27) includes the assumption that  $\text{dom}(\mathbb{I})$  is a submonoid. From now on, we denote by  $\hat{\mathbb{M}}$  this submonoid.

### 3.3 AB-homomorphisms

Let  $\mathcal{M}_1 = \langle \mathbb{M}_1, \cdot, 1_{\mathbb{M}_1}, \iota_{A,1}, \iota_{B,1}, \mathbb{I}_1, \gamma_1, \mu_1, \delta_1 \rangle$ ,  $\mathcal{M}_2 = \langle \mathbb{M}_2, \cdot, 1_{\mathbb{M}_2}, \iota_{A,2}, \iota_{B,2}, \mathbb{I}_2, \gamma_2, \mu_2, \delta_2 \rangle$  be two  $AB$ -algebras with the same underlying groups  $A, B$  and set  $\mathbf{Q}$ . We call  $AB$ -homomorphism from  $\mathcal{M}_1$  to  $\mathcal{M}_2$  any map  $\psi : \mathbb{M}_1 \rightarrow \mathbb{M}_2$  fulfilling the seven properties (34-40) below:

**$m$ -homomorphism:**

$$\psi : (\mathbb{M}_1, \cdot, 1_{\mathbb{M}_1}) \rightarrow (\mathbb{M}_2, \cdot, 1_{\mathbb{M}_2}) \text{ is a monoid homomorphism} \quad (34)$$

**$\iota$ -preservation:**

$$\forall a \in A, \forall b \in B, \psi(\iota_{A,1}(a)) = \iota_{A,2}(a), \quad \psi(\iota_{B,1}(b)) = \iota_{B,2}(b) \quad (35)$$

**I-preservation:**

$$\forall m \in \mathbb{M}_1 - \gamma_1^{-1}(\{\emptyset\}), \quad m \in \text{dom}(\mathbb{I}_1) \Leftrightarrow \psi(m) \in \text{dom}(\mathbb{I}_2) \quad (36)$$

$$\forall m \in \hat{\mathbb{M}}_1, \quad \mathbb{I}_2(\psi(m)) = \psi(\mathbb{I}_1(m)) \quad (37)$$

**$\gamma$ -compatibility:**

$$\forall m \in \mathbb{M}_1, \gamma_2(\psi(m)) \supseteq \gamma_1(m) \quad (38)$$

**$\mu$ -preservation:**

$$\forall m \in \mathbb{M}_1, \forall \theta \in \gamma_1(m), \mu_2(\theta, \psi(m)) = \mu_1(\theta, m), \quad (39)$$

**$\delta$ -preservation:**

$$\forall m \in \mathbb{M}_1, \forall \theta \in \gamma_1(m), \delta_2(\theta, \psi(m)) = \delta_1(\theta, m). \quad (40)$$

$\mathcal{M}_1$  is said to be a *sub-AB-algebra* of  $\mathcal{M}_2$  if  $\mathbb{M}_1 \subseteq \mathbb{M}_2$  and the inclusion map  $\iota : \mathbb{M}_1 \rightarrow \mathbb{M}_2$  is an  $AB$ -homomorphism.

Given a submonoid  $(\mathbb{M}_1, \cdot, 1)$  of  $(\mathbb{M}_2, \cdot, 1)$  which contains  $\iota_2(A) \cup \iota_2(B)$  and is closed under  $\mathbb{I}_2$ , there is a natural way to endow  $\mathbb{M}_1$  with a structure of sub-AB-algebra of  $\mathcal{M}_2$ : it suffices to set  $\iota_1 := \iota \circ \iota_2$ ,  $\mathbb{I}_1 := \iota \circ \mathbb{I}_2$ ,  $\gamma_1 := \iota \circ \gamma_2$ ,  $\mu_1 := \iota \circ \mu_2$  and  $\delta_1 := \iota \circ \delta_2$  (where  $\iota$  denotes the inclusion map from  $\mathbb{M}_1$  into  $\mathbb{M}_2$ ). This structure is called the  $AB$ -structure *induced* by  $\mathcal{M}_2$  on  $\mathcal{M}_1$ .

### 3.4 Finite t-automata

Given an HNN-extension of the form (1), we have defined in §4.1 of [LS08] a notion of finite automata that recognize subsets of  $H * \{t, t^{-1}\}^*$ . We recall here the main definitions and refer to [LS08] for further details and proofs. A *finite t-automaton* over  $\mathbb{H} * \{t, t\}^*$  with labeling set  $\mathcal{F} \subseteq \mathcal{P}(\mathbb{H})$  is a 5-tuple

$$\mathcal{A} = \langle \mathcal{L}, \mathbf{Q}, \Delta, \mathbf{I}, \mathbf{T} \rangle, \quad (41)$$

where:

- (i)  $\mathcal{L}$  is a finite subset of  $\mathcal{F} \cup \mathcal{P}(A) \cup \mathcal{P}(B) \cup \{\{t\}, \{t^{-1}\}\}$ ,



- (ii)  $Q$  is a finite set of states,
- (iii)  $I \subseteq Q$  is the set of initial states,
- (iv)  $T \subseteq Q$  is the set of terminal states, and
- (v)  $\Delta \subseteq Q \times \mathcal{L} \times Q$  is the set of transitions.

Such an automaton induces a representation map  $\mu_{\mathcal{A}} : \mathbb{H} * \{t, t^{-1}\}^* \rightarrow \mathcal{P}(Q \times Q)$  defined by: for every  $x \in \mathbb{H} \cup \{t, t^{-1}\} \setminus \{1\}$  and every  $s \in \mathbb{H} * \{t, t^{-1}\}^*$  of the form (5):

$$\begin{aligned}\mu_{\mathcal{A},0}(1) &= \{(q, q) \mid q \in Q\} \cup \{(q, r) \in Q \times Q \mid \exists(q, L, r) \in \Delta : 1 \in L\} \\ \mu_{\mathcal{A},0}(x) &= \{(q, r) \in Q \times Q \mid \exists(q, L, r) \in \Delta : x \in L\} \\ \mu_{\mathcal{A}}(s) &= \mu_{\mathcal{A},0}(h_0) \circ \mu_{\mathcal{A},0}(t^{\alpha_1}) \circ \mu_{\mathcal{A},0}(h_1) \cdots \mu_{\mathcal{A},0}(t^{\alpha_n}) \circ \mu_{\mathcal{A},0}(h_n).\end{aligned}$$

$\mathcal{A}$  recognizes the set

$$L(\mathcal{A}) = \{s \in \mathbb{H} * \{t, t^{-1}\}^* \mid (I \times T) \cap \mu_{\mathcal{A}}(s) \neq \emptyset\}.$$

We recall that a *partitioned finite t-automaton* over  $\mathcal{F}$  is a 6-tuple  $\mathcal{A} = \langle \mathcal{L}, Q, \tau, \Delta, I, T \rangle$ , where  $\langle \mathcal{L}, Q, \Delta, I, T \rangle$  is as in (41) and  $\tau : Q \rightarrow \mathcal{T}_6$  maps each state to a vertex-type in such a way that

$$\tau(I) \subseteq \{(\{1\}, H)\}, \tau(T) \subseteq \{(\{1\}, \{1\})\}, \forall(q, L, r) \in \Delta : \{\tau(q)\} \times L \times \{\tau(r)\} \subseteq \widehat{\mathcal{E}}_6.$$

(here  $\widehat{\mathcal{E}}_6$  is, roughly speaking, the set of transitions of the natural t-automaton  $\mathcal{R}_6$  recognizing the set of all reduced sequences; see [LS08] §4.1).

The representation map  $\mu_{\mathcal{A}}$  associated to such a partitioned t-automaton is just the map  $\mu_{\mathcal{A}}$  associated to its underlying t-automaton (obtained by forgetting the map  $\tau$ ). For every state  $q \in Q$ , we denote by  $\gamma(q)$  the subgroup

$$\gamma(q) = p_1(\tau(q)) \in \{1, A, B\}$$

where  $p_1$  denotes the projection onto the first component of a vertex-type. We define an additional function  $\mu_{\mathcal{A},1} : \mathcal{T} \times \mathbb{H} * \{t, \bar{t}\}^* \rightarrow \mathcal{B}(Q_{\mathcal{A}})$  by: for every  $s \in \mathbb{H} * \{t, \bar{t}\}^*$ ,  $\theta \in \mathcal{T}$

$$\mu_{\mathcal{A},1}(\theta, s) = \mu_{\mathcal{A}}(s) \cap (\tau^{-1}(\tau i(\theta)) \times \tau^{-1}(\tau e(\theta))).$$

Let us define a map  $\gamma_t$  associating to every sequence  $s \in \mathbb{H} * \{t, \bar{t}\}^*$  the set of all path-types that can be realized by  $s$  in the automaton  $\mathcal{R}_6$ :

$$\gamma_t(s) = \{(p, b, q) \in \mathcal{T}_6 \times \mathbb{B} \times \mathcal{T}_6 \mid (p, q) \in \mu_{\mathcal{R}_6}(s) \wedge b = (\|s\| \neq 0)\} \quad (42)$$

where  $(\|s\| \neq 0)$  is the boolean 1 if and only if it is true that  $(\|s\| \neq 0)$ . We now define some properties of t-automata that play a role in the process of solving equations with rational constraints in  $\mathbb{G}$ .

The automaton  $\mathcal{A}$  is said  *$\approx$ -compatible* iff:

$$[L(\mathcal{A})]_{\approx} = [L(\mathcal{A}) \cap \text{Red}(\mathbb{H}, t)]_{\approx}, \quad (43)$$

$\mathcal{A}$  is said  $\sim$ -saturated iff:

$$\forall s, s' \in \mathbb{H} * \{t, t^{-1}\}^*, s \sim s' \Rightarrow \mu_{\mathcal{A}}(s) = \mu_{\mathcal{A}}(s'), \quad (44)$$

$\mathcal{A}$  is said *unitary* iff:

$$\forall \theta \in \mathcal{T}_6, \mu_{\mathcal{A},1}((\theta, 0, \theta), 1) = \text{id}_{\tau^{-1}(\theta)}. \quad (45)$$

$\mathcal{A}$  is said *subgroups-compatible* iff, for every subgroup  $C \in \{A, B\}$ , there exists a right-action  $\odot$  of the subgroup  $C$  over the set of states  $\{q \in Q \mid \gamma(q) = C\}$  such that: for every  $q, r \in Q, c \in C, h \in H$ ,

$$\gamma(q) = C \Rightarrow q \xrightarrow{c}_{\mathcal{A}} q \odot c \quad (46)$$

$$(\gamma(q) = C \wedge q \xrightarrow{h}_{\mathcal{A}} r) \Rightarrow q \odot c^{-1} \xrightarrow{ch}_{\mathcal{A}} r \quad (47)$$

$$(\gamma(r) = C \wedge q \xrightarrow{h}_{\mathcal{A}} r) \Rightarrow q \xrightarrow{hc}_{\mathcal{A}} r \odot c \quad (48)$$

$\mathcal{A}$  is said *multiplicative* iff for every  $\theta \in \gamma_t(s), \theta' \in \gamma_t(s')$  such that  $\theta \cdot \theta'$  is defined in  $\mathcal{T}$ :

$$\mu_{\mathcal{A},1}(\theta \cdot \theta', s \cdot s') = \mu_{\mathcal{A},1}(\theta, s) \cdot \mu_{\mathcal{A},1}(\theta', s'), \quad (49)$$

$\mathcal{A}$  is said *strict* if,

$$\text{L}(\mathcal{A}) \subseteq \text{Red}(\mathbb{H}, t). \quad (50)$$

(note that every strict fta (50) is  $\approx$ -compatible (43)). Finally, a partitioned finite  $t$ -automaton  $\mathcal{A}$  is said to be *normal* iff it is  $\approx$ -compatible,  $\sim$ -saturated, unitary and multiplicative.

**Proposition 1.** *Let  $R \in \mathcal{P}(\mathbb{G})$ .*

1-  *$R \in \text{RAT}(\mathbb{G})$  iff  $R = \pi_{\mathbb{G}}(\text{L}(\mathcal{A}))$  for some normal partitioned finite  $t$ -automaton  $\mathcal{A}$  with labeling set  $\text{RAT}(\mathbb{H})$ .*

2- *If  $R \in \mathcal{B}(\text{RAT}(\mathbb{G}))$  then  $R = \pi_{\mathbb{G}}(\text{L}(\mathcal{A}))$  for some strict normal partitioned finite  $t$ -automaton  $\mathcal{A}$  with labeling set  $\mathcal{B}(\text{RAT}(\mathbb{H}))$ .*

It is proved in [LS08, Proposition 33, points (1),(3) and (a)] that  $R$  is a rational subset of  $G$  iff  $\pi_G^{-1}(R) \cap \text{Red}(\mathbb{H}, t) = \text{L}(\mathcal{A}) \cap \text{Red}(\mathbb{H}, t)$  for some partitioned,  $\approx$ -compatible,  $\sim$ -saturated and unitary fta  $\mathcal{A}$  with labelling set  $\text{Rat}(H)$ .

Moreover, the automaton  $\mathcal{A} = \langle \mathcal{L}, Q, \tau, \delta, \text{l}, \text{T} \rangle$  can be chosen in such a way that it is subgroups-compatible: this follows from equations (39-40) in the the proof of [LS08, Proposition 22]. In order to prove Proposition 1, point (1), it remains to show that this automaton  $\mathcal{A}$  is also multiplicative. For ease of notation, we skip the index  $\mathcal{A}$  in the maps  $\mu_{\mathcal{A}}, \mu_{\mathcal{A},0}, \mu_{\mathcal{A},1}$ , up to the end of this subsection.

**Lemma 3.** *For every  $h \in H, h_i \in H, \alpha_i \in \{-1, +1\}$ ,*

$$1- \mu_0(t) = \mu_1((A, T, 1, B, H), t)$$

$$2- \mu_0(\bar{t}) = \mu_1((B, T, 1, A, H), \bar{t})$$

$$3- \mu_0(h) = \cup_{\theta \in \gamma(h)} \mu_1(\theta, h)$$

$$4- \mu_1((A, T, 1, B, H), (\prod_{i=1}^{n-1} t^{\alpha_i} h_i) t^{\alpha_n}) = \prod_{i=1}^{n-1} \mu_0(t^{\alpha_i}) \mu_0(h_i) \mu_0(t^{\alpha_n}).$$

**Sketch of proof:** Points (1)(2)(3) follow directly from the definition of  $\mu$ . Point (4) follows from the fact that  $\mathcal{A}$  is unitary.  $\square$

**Lemma 4.** *Let  $h, k \in H, \theta, \theta', \theta'' \in \mathcal{T}_6$ , such that  $(\theta, 0, \theta') \in \gamma_t(h), (\theta', 0, \theta'') \in \gamma_t(k)$  and  $(\theta, 0, \theta'') \in \mathcal{T}$ . Then  $\mu_1((\theta, 0, \theta') \cdot (\theta', 0, \theta''), h \cdot k) = \mu_1((\theta, 0, \theta'), h) \cdot \mu_1((\theta', 0, \theta''), k)$ .*

**Sketch of proof:** If  $\theta' \notin \{\theta, \theta''\}$ , then the product  $(\theta, 0, \theta'') \notin \mathcal{T}$ .

Let us suppose that  $\theta' = \theta$ . Hence  $h$  belongs to the subgroup  $p_1(\theta)$ , and thus, the equality  $\mu_1((\theta, 0, \theta''), h \cdot k) = \mu_1((\theta, 0, \theta), h) \cdot \mu_1((\theta, 0, \theta''), k)$  follows from the fact that  $\mathcal{A}$  is subgroups-compatible.

The case where  $\theta' = \theta''$  can be treated symmetrically.  $\square$

**Lemma 5.**

*Let  $n \geq 1$ ,  $\theta, \theta'$  be vertex-types and  $\alpha_1, \dots, \alpha_n \in \{-1, +1\}, h_0, h_1, \dots, h_n \in \mathbb{H}$ .*

*Let  $s = (\prod_{i=1}^{n-1} t^{\alpha_i} h_i) t^{\alpha_n}$ . Then*

$$\mu_1((\theta, 1, \theta'), h_0 s h_n) = \mu_1((\theta, 0, A(\alpha_1), T), h_0) \cdot \mu_1((A(\alpha_1), T, 1, B(\alpha_n), H), s) \cdot \mu_1((B(\alpha_n), H, 0, \theta'), h_n).$$

**Sketch of proof:** Follows immediately from the definitions of  $\mu_{\mathcal{A}}$  and  $\mu_1$ .  $\square$

**Lemma 6.** *For every path-types  $\theta, \theta'$  and every  $t$ -sequences  $s, s' \in \mathbb{H} * \{t, \bar{t}\}^*$ , if  $\theta \in \gamma(s), \theta' \in \gamma(s')$  and  $\theta \cdot \theta'$  is defined, then  $\mu_1(\theta \cdot \theta', s \cdot s') = \mu_1(\theta, s) \cdot \mu_1(\theta', s')$ .*

**Sketch of proof:** Suppose that  $\theta = (\theta, 1, \theta'), \theta' = (\theta', 1, \theta''), s = h \check{s} k, s' = h' \check{s}' k'$  where  $\check{s} = (\prod_{i=1}^{n-1} t^{\alpha_i} h_i) t^{\alpha_n}, \check{s}' = (\prod_{j=1}^{m-1} t^{\beta_j} h'_j) t^{\beta_m}$ .

We use below the notation:  $A(+1) := A, A(-1) := B, B(+1) := B, B(-1) := A$ .

**Case 1:**  $\theta' = (B(\alpha_n), H)$ .

Let us determine

$$\mu_1((\theta, 1, \theta''), s \cdot s'). \quad (51)$$

By Lemma 5 it is equal to

$$\mu_1((\theta, 0, A(\alpha_1), T), h_0) \cdot \mu_1((A(\alpha_1), T, 1, B(\beta_m), H), h) \cdot \check{s} \cdot k h \cdot \check{s}' \cdot \mu_1((B(\beta_m), H, 0, \theta''), k'). \quad (52)$$

By claim 3, point (4), this can be rewritten:

$$\mu_1((\theta, 0, A(\alpha_1), T), h_0) \cdot \prod_{i=1}^{n-1} \mu_0(t^{\alpha_i}) \mu_0(h_i) \mu_0(t^{\alpha_n}) \cdot \mu_0(kh) \cdot \prod_{j=1}^{m-1} \mu_0(t^{\beta_j}) \mu_0(h'_j) \mu_0(t^{\beta_m}) \mu_1((B(\beta_m), H, 0, \theta''), k'). \quad (53)$$

but since the image of  $\mu_0(t^{\alpha_n})$  is included in  $\tau^{-1}(B(\alpha_n), H)$  and the domain of  $\mu_0(t^{\beta_1})$  is included in  $\tau^{-1}(A(\beta_1), T)$ , the factor  $\mu_0(kh)$  in formula (53) can be replaced by

$$\mu_1((B(\alpha_n), H, 0, A(\beta_1), T), kh),$$

which, by Lemma 4 can be replaced by

$$\mu_1((B(\alpha_n), H, 0, B(\alpha_n), H), k) \cdot \mu_1((B(\alpha_n), H, 0, A(\beta_1), T), h).$$

After this replacement in formula (53) we obtain:

$$\begin{aligned} & \mu_1((\theta, 0, A(\alpha_1), T), h_0) \cdot \prod_{i=1}^{n-1} \mu_0(t^{\alpha_i}) \mu_0(h_i) \mu_0(t^{\alpha_n}) \cdot \mu_1(B(\alpha_n), H, 0, B(\alpha_n), H), k) \\ & \cdot \mu_1((B(\alpha_n), H, 0, A(\beta_1), T), h) \cdot \prod_{j=1}^{m-1} \mu_0(t^{\beta_j}) \mu_0(h'_j) \mu_0(t^{\beta_m}) \cdot \mu_1((B(\beta_m), H, 0, \theta''), k'). \end{aligned}$$

Using Lemma 5 backwards and twice, we obtain

$$\mu_1((\theta, 0, B(\alpha_n), H), s) \cdot \mu_1((B(\alpha_n), H, 0, \theta''), s') \quad (54)$$

which is exactly

$$\mu_1((\theta, 1, \theta'), s) \cdot \mu_1((\theta', 1, \theta''), s') \quad (55)$$

We have established that (51) and (55) have the same value, as required.

**Case 2:**  $\theta' = (A(\beta_1), T)$ .

Symetric arguments can be applied.

Since every other value of  $\theta'$  makes impossible that both  $(\theta, 1, \theta') \in \gamma(s)$  and  $(\theta', 1, \theta'') \in \gamma(s')$ , we have treated all the possible cases.

It remains to treat the case where  $s \in H$  or  $s' \in H$ :

**Case 3:**  $s \in H, s' \notin H$ .

By Lemma 4,

$$\mu_1((\theta, 0, A(\beta_1), T), s \cdot h') = \mu_1((\theta, 0, \theta'), s) \cdot \mu_1((\theta', 0, A(\beta_1), T), h').$$

Applying Lemma 5 we get

$$\begin{aligned} \mu_1((\theta, 0, \theta''), s \cdot s') &= \mu_1((\theta, 0, A(\beta_1), T), sh') \cdot \mu_1((A(\beta_1), T, 0, \theta''), s'k') \\ &= \mu_1((\theta, 0, \theta'), s) \cdot \mu_1((\theta', 0, \theta''), h's'k') \end{aligned}$$

as required.

**Case 4:**  $s \notin H, s' \in H$ .

can be handled as case 3.

**Case 5:**  $s \in H, s' \in H$ .

This case is treated by Lemma 4.  $\square$

*Proof.* Let us prove Proposition 1:

1- The initial properties of  $\mathcal{A}$  together with the multiplicativity property given by Lemma 6 show that, for every  $R \in \text{RAT}(\mathbb{G})$ , there exists a normal partitioned finite t-automaton  $\mathcal{A}$  such that  $R = \pi_{\mathbb{G}}(\text{L}(\mathcal{A}))$ . Conversely, by Proposition 33 of [LS08], if such an automaton  $\mathcal{A}$  exists, then  $\mathbb{G}$  is rational.

2- Let  $K$  be a boolean combination of rational subsets  $K_1, \dots, K_i, \dots, K_p$  of  $\mathbb{G}$ . By [LS08, Proposition 33, point (3)], for every  $i \in [1, p]$  there exists a partitionned,  $\sim$ -saturated, deterministic, complete, finite t-automaton  $\mathcal{C}_i$ , whose labelling set is  $\mathcal{B}(\text{Rat}(H))$ , and such that

$$\text{L}(\mathcal{C}_i) = \pi_G^{-1}(K) \cap \text{Red}(\mathbb{H}, t).$$

Since every boolean operation can be translated over partitioned,  $\sim$ -saturated, deterministic, complete, finite t-automata (see [LS08, Lemma 17, Lemma 20]), there exists a partitioned,  $\sim$ -saturated, deterministic, complete, finite t-automaton  $\mathcal{A}$ , whose labelling set is  $\mathcal{B}(\text{Rat}(H))$ , and such that

$$L(\mathcal{A}) = \pi_G^{-1}(K) \cap \text{Red}(\mathbb{H}, t). \quad (56)$$

Applying [LS08, Proposition 22] to this automaton  $\mathcal{A}$  and the set  $\mathcal{F} = \mathcal{B}(\text{Rat}(H))$ , we obtain a partitioned,  $\approx$ -compatible,  $\sim$ -saturated, unitary fta  $\mathcal{B}$ , with labelling set  $\mathcal{B}(\text{Rat}(H))$ , such that

$$[L(\mathcal{B})]_{\approx} \cap \text{Red}(\mathbb{H}, t) = \pi_G^{-1}(K) \cap \text{Red}(\mathbb{H}, t).$$

Moreover: by equations (39-40) of [LS08],  $\mathcal{B}$  is subgroups-compatible, thus, by Lemma 6, multiplicative; by [LS08, Claim 26],  $L(\mathcal{B}) \subseteq L(\mathcal{A})$  while by (56)  $L(\mathcal{A}) \subseteq \text{Red}(\mathbb{H}, t)$ , hence  $\mathcal{B}$  is also strict; finally,  $\mathcal{B}$  is strict and normal.

### 3.5 The AB-algebra $\mathbb{H}_t$

$\mathbb{H} * \{t, \bar{t}\}^*$  Given an HNN-extension (1) and a normal finite t-automaton  $\mathcal{A}$ , we define an AB-algebra with underlying monoid  $\mathbb{H} * \{t, \bar{t}\}^*$  and set of states  $Q_{\mathcal{A}}$

$$\langle \mathbb{H} * \{t, \bar{t}\}^*, \cdot, 1_{\mathbb{H}}, \iota_A, \iota_B, \mathbb{I}_t, \mu_t, \gamma, \delta_t \rangle \quad (57)$$

as follows:

$$\iota_A, \iota_B$$

are the natural injections from  $A$  (resp.  $B$ ) into  $\mathbb{H} * \{t, \bar{t}\}^*$ ,

$$\text{dom}(\mathbb{I}_t) = (I(\mathbb{H}) \cup \{t, \bar{t}\})^*$$

where  $I(\mathbb{H})$  is the set of invertible elements of  $\mathbb{H}$ ;  $\mathbb{I}_t$  is the unique monoid anti-homomorphism  $\text{dom}(\mathbb{I}_t) \rightarrow \text{dom}(\mathbb{I}_t)$  such that

$$\forall h \in I(\mathbb{H}), \mathbb{I}_t(h) = h^{-1}; \quad \mathbb{I}_t(t) = \bar{t}; \quad \mathbb{I}_t(\bar{t}) = t.$$

The map  $\gamma_t$  is the one previously defined in (42). The map  $\mu_t : \mathcal{T} \times \mathbb{H} * \{t, \bar{t}\}^* \rightarrow B^2(Q)$  is defined by:

$$\begin{aligned} \mu_t(\boldsymbol{\theta}, s) &= (\mu_1(\boldsymbol{\theta}, s), (\mu_1(\mathbb{I}_t(\boldsymbol{\theta}), \mathbb{I}_t(s))^{-1})) \quad \text{if } s \in \text{dom}(\mathbb{I}_t); \\ \mu_t(\boldsymbol{\theta}, s) &= (\mu_1(\boldsymbol{\theta}, s), \emptyset) \quad \text{if } s \notin \text{dom}(\mathbb{I}_t). \end{aligned} \quad (58)$$

where  $\mu_1$  is the representation map  $\mu_{\mathcal{A},1}$  associated with the partitioned t-automaton  $\mathcal{A}$  fixed above. The map  $\delta_t : \mathcal{T} \times \mathbb{H} * \{t, \bar{t}\}^* \rightarrow \text{PGI}(A, B)$  is defined by:

$$\delta_t(\boldsymbol{\theta}, s) = \{(g, g') \in \text{Gi}(\boldsymbol{\theta}) \times \text{Ge}(\boldsymbol{\theta}) \mid g \cdot s \sim s \cdot g'\}.$$

It is noteworthy that, for every  $s \in \mathbb{H} * \{t, \bar{t}\}^*$

$$\gamma_t(s) \neq \emptyset \Leftrightarrow s \in \text{Red}(\mathbb{H}, t). \quad (59)$$

**Proposition 2.** *The above structure  $\langle \mathbb{H} * \{t, \bar{t}\}^*, \cdot, 1_{\mathbb{H}}, \iota_A, \iota_B, \mathbb{I}_t, \mu_t, \gamma, \delta_t \rangle$  is an AB-algebra.*

In order to prove this proposition we show the following lemma.

**Lemma 7.** *For every  $s, s' \in \mathbb{H} * \{t, \bar{t}\}^*, \gamma_t(s \cdot s') \supseteq \gamma_t(s) \cdot \gamma_t(s')$ .*

**Sketch of proof:** Let  $\Gamma$  be the homomorphism from the partial semi-group of paths in  $\mathcal{R}$  into the partial semi-group  $\mathcal{T}$  which associates to every edge of  $\mathcal{R}$  the same edge, viewed as an atomic path-type. Let  $\theta \in \mathcal{T}, s \in \text{Red}(\mathbb{H}, t)$ . By  $\text{Path}(\theta, s)$  we denote the unique path in the graph  $\mathcal{R}$  such that  $\Gamma(\text{Path}(\theta, s)) = \theta$  and  $\Lambda(\text{Path}(\theta, s)) = s$  (where  $\Lambda$  is the labelling map). By definition, a path-type  $\theta$  belongs to  $\gamma_t(s)$  iff  $\text{Path}(\theta, s)$  exists. Suppose that  $s, s' \in \text{Red}(\mathbb{H}, t), \theta \in \gamma_t(s), \theta' \in \gamma_t(s')$ , and  $(\theta, \theta') \in D(\cdot)$ . Then the product  $\text{Path}(\theta, s) \cdot \text{Path}(\theta', s')$  is defined too, and

$$\Gamma(\text{Path}(\theta, s) \cdot \text{Path}(\theta', s')) = \theta \cdot \theta', \quad \Lambda(\text{Path}(\theta, s) \cdot \text{Path}(\theta', s')) = s \cdot s',$$

showing that

$$\gamma_t(s \cdot s') \supseteq \gamma_t(s) \cdot \gamma_t(s').$$

□

From the multiplicativity of  $\mu_1$  we can immediately deduce the multiplicativity of  $\mu_t$ . All the other checks are easy.

*Positive AB-structure* Another AB-structure over  $\mathbb{H} * \{t, \bar{t}\}^*$  can be defined by choosing, in place of the map  $\gamma_t$  defined in (42), the map  $\gamma_+$  defined by: for every  $s \in \mathbb{H} * \{t, \bar{t}\}^*$ ,

$$\gamma_+(s) = \{(p, b, q) \in \mathcal{T}_6 \times \mathbb{B} \times \mathcal{T}_6 \mid (p, q) \in \mu_{G_6}(s) \wedge b = (\|s\| \neq 0)\} \quad (60)$$

Assertion (59) is now replaced by

$$\forall s \in \mathbb{H} * \{t, \bar{t}\}^*, \gamma_+(s) \neq \emptyset. \quad (61)$$

We call the resulting structure

$$\langle \mathbb{H} * \{t, \bar{t}\}^*, \cdot, 1_{\mathbb{H}}, \iota_A, \iota_B, \mathbb{I}, \mu_t, \gamma_+, \delta_t \rangle \quad (62)$$

the *positive* AB-algebra structure over  $\mathbb{H} * \{t, \bar{t}\}^*$ . This variant will be used in section 9 where we deal with *positive* rational constraints.

$\mathbb{H}_t$  One can check that the monoid-congruence  $\sim$  is compatible with  $\mathbb{I}_t, \iota_A, \iota_B, \gamma_t, \mu_t, \delta_t$  in the sense that: for every  $s, s' \in \mathbb{H} * \{t, \bar{t}\}^*, a \in A, b \in B, \theta \in \gamma_t(s)$ , if  $s \sim s'$  then,

$$\mathbb{I}_t(s) \sim \mathbb{I}_t(s'), \quad s = \iota_A(a) \Leftrightarrow s' = \iota_A(a), \quad s = \iota_B(b) \Leftrightarrow s' = \iota_B(b),$$

$$\gamma_t(s) = \gamma_t(s'), \quad \mu_t(\theta, s) = \mu_t(\theta, s'), \quad \delta_t(\theta, s) = \delta_t(\theta, s').$$

Let us denote by  $\mathbb{H}_t$  the quotient set  $\mathbb{H} * \{t, \bar{t}\}^* / \sim$ . We can naturally endow  $\mathbb{H}_t$  with a structure of  $AB$ -algebra:

$$\mathcal{H}_t := \langle \mathbb{H}_t, \cdot, 1_{\mathbb{H}}, \iota_{A,\sim}, \iota_{B,\sim}, \mathbb{I}_{\sim}, \mu_{\sim}, \gamma_{\sim}, \delta_{\sim} \rangle \quad (63)$$

where all the required maps are just obtained from the corresponding map in the  $AB$ -structure of  $\mathbb{H} * \{t, \bar{t}\}^*$ , by composition by  $\pi_{\sim} : \mathbb{H} * \{t, \bar{t}\}^* \rightarrow \mathbb{H} * \{t, \bar{t}\}^* / \sim$ . In addition

$$s \sim s' \Rightarrow \|s\| = \|s'\|$$

so that the notion of norm remains well-defined in the quotient  $\mathbb{H}_t$ . In the rest of the paper we sometimes skip the subscript  $t$  when the context makes clear which  $AB$ -structure we are using.

*Positive  $AB$ -structure* Similarly, we can define the structure of  $AB$ -algebra:

$$\mathcal{H}_{t+} := \langle \mathbb{H}_t, \cdot, 1_{\mathbb{H}}, \iota_{A,\sim}, \iota_{B,\sim}, \mathbb{I}_{\sim}, \mu_{\sim}, \gamma_{+\sim}, \delta_{\sim} \rangle \quad (64)$$

where  $\gamma_{+}$  is defined via the automaton  $\mathcal{G}_6$  instead of  $\mathcal{R}_6$ , see (60).

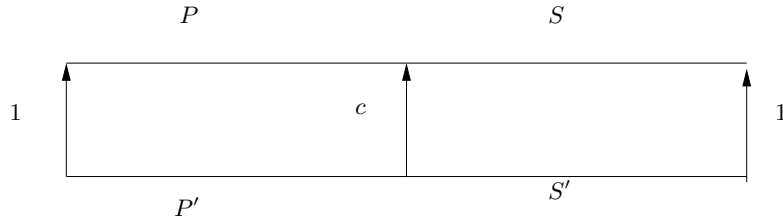
**Algebraic properties** The monoid  $(\mathbb{H}_t, \cdot, 1)$  has some properties which resemble equidivisibility. We detail here these properties.

**Lemma 8.** *Let  $P, P', S, S' \in \mathbb{H}_t, \theta \in \gamma(P) \cap \gamma(P'), \rho \in \gamma(S) \cap \gamma(S')$  such that  $\theta \cdot \rho$  is defined,  $\theta$  is a  $H$ -type and*

$$P \cdot S = P' \cdot S'.$$

*Then, there exists  $c \in \text{Ge}(\theta)$  such that*

$$P = P'c, \quad cS = S'.$$



**Fig. 2.** Lemma 8

*Proof.* Let  $p, p', s, s' \in \mathbb{H} * \{t, \bar{t}\}^*$  such that  $P = [p]_{\sim}, P' = [p']_{\sim}, S = [s]_{\sim}, S' = [s']_{\sim}$ . Since  $\theta$  is a H-type,  $p, p' \in \mathbb{H}$  and since the product  $\theta \cdot \rho$  is defined,  $\text{Gi}(\rho) = \text{Ge}(\theta)$ . Moreover the second component  $p_2(\rho)$  cannot be H, hence only one of the following two cases can occur.

**Case 1:**  $\rho = (1, 1, 0, 1, 1)$ .

Thus  $s = s' \in \text{Ge}(\theta) = \{1\}$ . Choosing  $c = 1$ , we obtain that

$$c \in \text{Ge}(\theta), \quad P = P'c, \quad cS = S'.$$

**Case 2:**  $\rho = (C, T, b, D, K)$  for some  $b \in \{0, 1\}, D \in \{A, B\}, K \in \{T, H\}$  and  $C = \text{Ge}(\theta)$ .

Suppose that

$$s = h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_i} h_i \cdots t^{\alpha_n} h_n, \quad s' = h'_0 t^{\alpha'_1} h'_1 \cdots t^{\alpha'_j} h'_j \cdots t^{\alpha'_m} h_m,$$

where  $h_i, h'_j \in \mathbb{H}, \alpha_i, \alpha'_j \in \{-1, +1\}$ . Moreover,  $h_0, h'_0 \in \text{Gi}(\rho)$ . Since  $p \cdot s \sim p' \cdot s'$ , we get that:

$$n = m, \quad \forall i \in [1, n], \alpha_i = \alpha'_i,$$

and there exist connecting elements  $c_1, \dots, c_{2n}$  between  $p \cdot s$  and  $p' \cdot s'$  as recalled in [LS08, section 3]. Hence

$$c_1 \in \text{Ge}(\theta), \quad p \cdot h_0 \cdot c_1 = p' \cdot h'_0, \quad t^{\alpha_1} h_1 \cdots t^{\alpha_i} h_i \cdots t^{\alpha_n} h_n \sim c_1 \cdot t^{\alpha_1} h'_1 \cdots t^{\alpha_i} h'_i \cdots t^{\alpha_n} h_n.$$

Let us choose  $c := h'_0 \cdot c_1^{-1} \cdot h_0^{-1} \in \text{Ge}(\theta)$ . We obtain that

$$c \in \text{Ge}(\theta), \quad P = P'c, \quad cS = S'.$$

**Lemma 9.** Let  $P, P', S, S' \in \mathbb{H}_t, \theta \in \gamma(P), \theta' \in \gamma(P'), \rho \in \gamma(S), \rho' \in \gamma(S')$  such that  $\theta \cdot \rho = \theta' \cdot \rho'$  is defined,  $\theta, \theta'$  are T-types and

$$P \cdot S = P' \cdot S'.$$

One of the following cases must occur:

1-  $\|P\| = \|P'\|$  and there exists  $c \in \text{Ge}(\theta)$  such that

$$P = P'c, \quad cS = S'$$

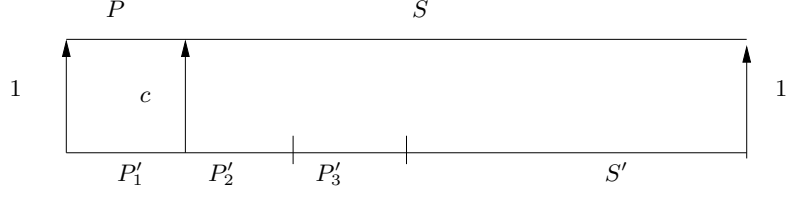
2-  $\|P\| < \|P'\|$  and there exist  $c \in \text{Ge}(\theta), P'_1, P'_2, P'_3 \in \mathbb{H}_t, P'_1$  has a T-type  $\theta'_1, P'_3$  has a T-type  $\theta'_3, P'_2$  has a H-type  $\theta'_2$  such that

$$P = P'_1 c, \quad P' = P'_1 P'_2 P'_3, \quad cS = P'_2 P'_3 S', \quad \theta' = \theta'_1 \theta'_2 \theta'_3.$$

3-  $\|P\| > \|P'\|$  and there exists  $c \in \text{Ge}(P'), P_1, P_2, P_3 \in \mathbb{H}_t, P_1$  has a T-type  $\theta_1, P_3$  has a T-type  $\theta_3, P_2$  has a H-type  $\theta_2$  such that

$$P = P_1 P_2 P_3, \quad P_1 = P'c, \quad cP_2 P_3 S = S', \quad \theta = \theta_1 \theta_2 \theta_3.$$





**Fig. 3.** Lemma 9

*Proof.* Let  $p, p', s, s' \in \mathbb{H} * \{t, \bar{t}\}^*$  such that  $P = [p]_{\sim}, P' = [p']_{\sim}, S = [s]_{\sim}, S' = [s']_{\sim}$ . Since the products  $\theta \cdot \rho, \theta' \cdot \rho'$  are defined,  $\text{Gi}(\rho) = \text{Ge}(\theta)$  and  $\text{Gi}(\rho') = \text{Ge}(\theta')$ . Suppose that

$$p = h_0 t^{\alpha_1} h_1 \dots t^{\alpha_i} h_i \dots t^{\alpha_n} h_n, \quad s = k_0 t^{\beta_1} k_1 \dots t^{\beta_j} k_j \dots t^{\beta_\ell} h_\ell,$$

$$p' = h'_0 t^{\alpha'_1} h'_1 \dots t^{\alpha'_i} h'_i \dots t^{\alpha'_\nu} h'_\nu, \quad s' = k'_0 t^{\beta'_1} k'_1 \dots t^{\beta'_\kappa} k'_\kappa \dots t^{\beta'_\lambda} h'_\lambda,$$

where  $h_i, k_j, h'_i, k'_\kappa \in \mathbb{H}, \alpha_i, \beta_j, \alpha'_i, \beta'_\kappa \in \{-1, +1\}$  and  $h_n \in \text{Ge}(\theta), h'_\nu \in \text{Ge}(\theta')$ . Since  $p \cdot s \sim p' \cdot s'$ , we get that:

$$n + \nu = \ell + \lambda, \quad (\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_\ell) = (\alpha'_1, \dots, \alpha'_\nu, \beta'_1, \dots, \beta'_\lambda)$$

and there exist connecting elements  $c_1, \dots, c_{2n+2\nu}$  between  $p \cdot s$  and  $p' \cdot s'$  (see [LS08, section 3]).

**Case 1:**  $\|P\| = \|P'\|$

Hence  $n = \nu$ . Let us choose  $c := h_n^{-1} \cdot c_{2n}^{-1} \cdot h_n$ . The fact that  $h_n, h'_n, c_{2n} \in \text{Ge}(\theta)$  ensures that  $c \in \text{Ge}(\theta)$ . Since  $c_{2n}$  is a connecting element

$$h_0 t^{\alpha_1} h_1 \dots t^{\alpha_i} h_i \dots t^{\alpha_n} c_{2n} \sim h'_0 t^{\alpha'_1} h'_1 \dots t^{\alpha'_i} h'_i \dots t^{\alpha'_n}$$

and

$$h_n k_0 t^{\beta_1} k_1 \dots t^{\beta_j} k_j \dots t^{\beta_\ell} h_\ell \sim c_{2n} h'_n k'_0 t^{\beta'_1} k'_1 \dots t^{\beta'_j} k'_j \dots t^{\beta'_\ell} h'_\ell$$

so that

$$p \sim p' c \wedge cs \sim s',$$

as required.

**Case 2:**  $\|P\| < \|P'\|$

Hence  $n < \nu$ . Let us choose

$$p'_1 := h'_0 t^{\alpha'_1} h'_1 \dots t^{\alpha'_i} h'_i \dots t^{\alpha'_n}, \quad c := c_{2n}^{-1} h_n, \quad p'_2 := h'_n, \quad p'_3 := t^{\alpha'_{n+1}} h'_{n+1} \dots t^{\alpha'_\nu} h'_\nu.$$

The fact that  $h_n, c_{2n} \in \text{Ge}(\theta)$  ensures that  $c \in \text{Ge}(\theta)$ . A possible type for  $P'_1$  is  $\theta_1 := (A(\alpha_1), T, 1, B(\alpha_n), H)$  (where we use the notation  $A(+1) := A, A(-1) := B, B(+1) := B, B(-1) := A$ ), a possible type for  $P'_2$  is  $\theta_2 := (B(\alpha_n), H, 0, A(\alpha'_{n+1}), T)$  and a possible type for  $P'_3$  is  $\theta_3 := (A(\alpha'_{n+1}), T, 1, B(\alpha'_n u), H)$ . Thus  $\theta'_1, \theta'_3$  are T-types and  $\theta'_2$  is a H-type such that  $\theta' = \theta'_1 \theta'_2 \theta'_3$ . From the fact that  $c_{2n}$  is a connecting element one deduces that  $p \sim p'_1 c$  and  $cs \sim p'_2 p'_3 s'$  (see Figure 4). Finally the classes  $P'_i = [p'_i]_{\sim}$  are fulfilling the conclusion of the lemma.

**Case 3:**  $\|P\| > \|P'\|$

This case is similar to Case 2.

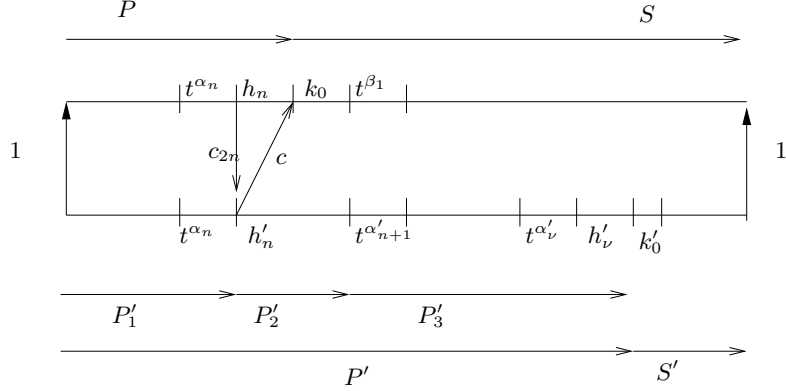


Fig. 4. Proof of Lemma 9, Case 2

### 3.6 The AB-algebra $\mathbb{W}$

$\mathcal{W}^* * A * B$  Let  $S$  be a system of equations over  $\mathbb{H}_t$  with involution and rational constraints. The rational constraints are expressed via the map  $\mu_t$  defined by (58) in §3.5. We define an alphabet of “generic” symbols  $\mathcal{W}$  with the underlying idea of representing inside each symbol the values of the functions  $\gamma_t, \mu_t, \delta_t$  for the “concrete” value (i.e. in  $\mathbb{H} * \{t, \bar{t}\}^*$ ) of that variable that leads to a solution of the system of equations.

Let  $\mathcal{V}_0$  be some starting set. Let us denote by  $\mathcal{TA}_0$  the set of all atomic types which are either H-types or T-types. We then define

$$\Omega := \mathcal{V}_0 \times \{-1, 0, 1\} \times \mathcal{TA}_0 \times \mathbf{B}^2(\mathbf{Q}) \times \text{PGI}(A, B). \quad (65)$$

$$\mathcal{W} := \{(V, \epsilon, \theta, m, \varphi) \in \Omega \mid \varphi \in \text{PIs}(\text{Gi}(\theta), \text{Ge}(\theta)), \forall (c, d) \in \varphi, \mu_A(c) \cdot m = m \cdot \mu_A(d)\}. \quad (66)$$

Let

$$\check{\mathcal{W}} = \{W \in \mathcal{W} \mid p_2(W) = 0\}, \quad \hat{\mathcal{W}} = \{W \in \mathcal{W} \mid p_2(W) \neq 0\}$$

Let us consider the free product  $\mathcal{W}^* * A * B$ . We denote by  $\iota_A : A \rightarrow \mathcal{W}^* * A * B$  the natural embedding of  $A$  into  $\mathcal{W}^* * A * B$  ( and use similarly the notation  $\iota_B$ ). Note that  $\iota_A(A) \cap \iota_B(B) = \{1\}$ . We define an AB-algebra with underlying monoid  $\mathcal{W}^* * A * B$  and set of states  $\mathbf{Q}$

$$\langle \mathcal{W}^* * A * B, \cdot, 1, \iota_A, \iota_B, \mathbb{I}, \mu, \gamma, \delta \rangle \quad (67)$$

as follows:

$$\text{dom}(\mathbb{I}) = \hat{\mathcal{W}}^* * A * B$$

(the submonoid generated by  $\hat{\mathcal{W}} \cup \iota_A(A) \cup \iota_B(B)$ );

$\mathbb{I}$  is the unique monoid anti-homomorphism  $\hat{\mathcal{W}}^* * A * B \rightarrow \hat{\mathcal{W}}^* * A * B$  such that:

$$\forall a \in A, \mathbb{I}(\iota_A(a)) = \iota_A(a^{-1}); \quad \forall b \in B, \mathbb{I}(\iota_B(b)) = \iota_B(b^{-1})$$

$$\mathbb{I}(V, \epsilon, \boldsymbol{\theta}, m, \varphi) = (V, -\epsilon, \mathbb{I}_{\boldsymbol{\theta}}(t), \mathbb{I}_{\mathbf{Q}}(m), \varphi^{-1}).$$

$$\gamma : \mathcal{W}^* * A * B \rightarrow \mathcal{P}(\mathcal{T})$$

is defined by:

$$\gamma(V, \epsilon, \boldsymbol{\theta}, m, \varphi) = \{\boldsymbol{\theta}\},$$

for every  $a \in A - \{1\}, b \in B - \{1\}$

$$\gamma(\iota_A(a)) = \{(A, T, 0, A, T), (A, H, 0, A, H)\}, \quad \gamma(\iota_B(b)) = \{(B, T, 0, B, T), (B, H, 0, B, H)\},$$

$$\gamma(1) = \{(1, H, 0, 1, H), (1, 1, 0, 1, 1), (A, T, 0, A, T), (A, H, 0, A, H), (B, T, 0, B, T), (B, H, 0, B, H)\}$$

and finally, for every  $g_1, \dots, g_i, \dots, g_n \in \mathcal{W} \cup \iota_A(A) \cup \iota_B(B)$ ,

$$\gamma\left(\prod_{i=1}^n g_i\right) = \prod_{i=1}^n \gamma(g_i) \quad (68)$$

$\mu$  is defined by

$$\mu(\boldsymbol{\theta}, \iota_A(a)) = \mu_t(\boldsymbol{\theta}, a), \quad \mu(\boldsymbol{\theta}, \iota_B(b)) = \mu_t(\boldsymbol{\theta}, b),$$

for every  $\boldsymbol{\theta}' \in \mathcal{T}, \boldsymbol{\theta}' \neq \boldsymbol{\theta}$ ,

$$\mu(\boldsymbol{\theta}, (V, \epsilon, \boldsymbol{\theta}, m, \varphi)) = m, \quad \mu(\boldsymbol{\theta}', (V, \epsilon, \boldsymbol{\theta}, m, \varphi)) = \emptyset.$$

The map  $\delta : \mathcal{T} \times \mathbb{H} * \{t, \bar{t}\}^* \rightarrow \text{PGI}(A, B)$  is defined by: for every  $a \in \iota_A(A), b \in \iota_B(B), \boldsymbol{\theta} \in \mathcal{T}$ ,

$$\delta(\boldsymbol{\theta}, \iota_A(a)) = \{(\iota_A(c), \iota_A(d)) \mid (c, d) \in \text{Gi}(\boldsymbol{\theta}) \times \text{Ge}(\boldsymbol{\theta}), ca = ad\}, \text{ if } \boldsymbol{\theta} \in \gamma(\iota_A(a))$$

$$\delta(\boldsymbol{\theta}, \iota_A(a)) = \{(1, 1)\}, \text{ if } \boldsymbol{\theta} \notin \gamma(\iota_A(a))$$

$$\delta(\boldsymbol{\theta}, \iota_B(b)) = \{(\iota_B(c), \iota_B(d)) \mid (c, d) \in \text{Gi}(\boldsymbol{\theta}) \times \text{Ge}(\boldsymbol{\theta}), ca = ad\}, \text{ if } \boldsymbol{\theta} \in \gamma(\iota_B(b))$$

$$\delta(\boldsymbol{\theta}, \iota_B(b)) = \{(1, 1)\}, \text{ if } \boldsymbol{\theta} \notin \gamma(\iota_B(b)).$$

For every  $\boldsymbol{\theta}' \in \mathcal{T}, \boldsymbol{\theta}' \neq \boldsymbol{\theta}$ ,

$$\delta(\boldsymbol{\theta}, (V, \epsilon, \boldsymbol{\theta}, m, \varphi)) = \varphi, \quad \delta(\boldsymbol{\theta}', (V, \epsilon, \boldsymbol{\theta}, m, \varphi)) = \{(1, 1)\}$$

Since for every  $W \in \mathcal{W}$ ,  $\gamma(W)$  is simply a singleton of the form  $\{\boldsymbol{\theta}\}$ , we also use the (abusive) notation

$$\tau i(W), \tau e(W), \text{Gi}(W), \text{Ge}(W), \mu(W), \delta(W)$$

for what should be denoted, in full rigor, by

$$\tau i(\boldsymbol{\theta}), \tau e(\boldsymbol{\theta}), \text{Gi}(\boldsymbol{\theta}), \text{Ge}(\boldsymbol{\theta}), \mu(\boldsymbol{\theta}, W), \delta(\boldsymbol{\theta}, W).$$

*lengths* For every  $w \in (\iota_A(A) \cup \iota_B(B) \cup \mathcal{W})^*$ , we set

$$\|w\| = |w|_{\mathcal{W}}.$$

One can check that

$$\|w \cdot w'\| = \|w\| + \|w'\|; \quad \|w\| = 0 \Leftrightarrow w \in A * B.$$

$$\chi_{AB}(w) := 1 \text{ if } w \in \iota_A(A) \cup \iota_B(B); \chi_{AB}(w) := 0 \text{ otherwise.}$$

$$\chi_H(w) := 1 \text{ if } \text{Card}(\gamma(w)) = 1 \wedge p_2(\gamma(w)) \in \{H\}; \chi_H(w) := 0 \text{ otherwise.}$$

Given  $P, S, P', S' \in \mathbb{W}$  and  $\psi_t \in \text{Hom}_{AB}(\mathbb{W}, \mathbb{H}_t)$  we define

$$\Delta(P, S, P', S', \psi_t) = 1 - \frac{1}{2}(\chi_{AB}(P) + \chi_{AB}(P')) + \chi_H(S) + \chi_H(S') + 2\|\psi_t(S)\| + 2\|\psi_t(S')\| \quad (69)$$

(this notion will serve as a “progression measure” in the induction proving Lemma 21, which is a key-point of this paper).

$\mathbb{W}$  Let us consider the monoid congruence  $\equiv$  over  $\mathcal{W}^* * A * B$  generated by the set of pairs

$$cW \equiv Wd, \quad (70)$$

for all  $W \in \mathcal{W}, (c, d) \in \delta(W)$ . We define the monoid  $\langle \mathbb{W}, \cdot, 1_{\mathbb{W}} \rangle$  as the quotient-monoid  $\mathcal{W}^* * A * B / \equiv$ . One can check that the monoid-congruence  $\equiv$  is compatible with  $\mathbb{I}, \iota_A, \iota_B, \gamma, \mu, \delta$  in the sense that: for every  $u, u' \in \mathcal{W}^* * A * B, a \in A, b \in B, \theta \in \gamma(u)$ , if  $u \equiv u'$  then,

$$\mathbb{I}(u) \equiv \mathbb{I}(u'), \quad u = \iota_A(a) \Leftrightarrow u' = \iota_A(a), \quad u = \iota_B(b) \Leftrightarrow u' = \iota_B(b), \quad (71)$$

$$\gamma(u) \equiv \gamma(u'), \quad \mu(\theta, u) = \mu(\theta, u'), \quad \delta(\theta, u) = \delta(\theta, u'). \quad (72)$$

We can naturally endow  $\mathbb{W}$  with a structure of  $AB$ -algebra:

$$\langle \mathbb{W}, \cdot, 1_{\mathbb{W}}, \iota_{A, \equiv}, \iota_{B, \equiv}, \mathbb{I}_{\equiv}, \mu_{\equiv}, \gamma_{\equiv}, \delta_{\equiv} \rangle \quad (73)$$

where all the required maps are just obtained from the corresponding map in the  $AB$ -structure of  $\mathcal{W}^* * A * B$ , by composition by  $\pi_{\equiv} : \mathcal{W}^* * A * B \rightarrow \mathcal{W}^* * A * B / \equiv$ . In addition

$$u \equiv u' \Rightarrow \|u\| = \|u'\|$$

so that the notion of norm remains well-defined in the quotient  $\mathbb{W}$ .

$\mathbb{W}_t, \mathbb{W}_{\mathbb{H}}, \hat{\mathbb{W}}$  Let us consider the set  $\mathcal{W}_t$  consisting of all the letters  $W \in \mathcal{W}$  fulfilling

$$\exists s \in \mathbb{H} * \{t, \bar{t}\}^*, W \in \text{dom}(\mathbb{I}_{\mathbb{W}}) \Leftrightarrow s \in \text{dom}(\mathbb{I}_t), \gamma(W) \subseteq \gamma(s), \quad \text{and}$$

$$\forall \theta \in \gamma(W), \mu(\theta, W) = \mu(\theta, s), \delta(\theta, W) = \delta(\theta, s).$$

We define the subset

$$\mathcal{W}_{\mathbb{H}} := \{W \in \mathcal{W}_t \mid \gamma(W) \text{ is a H-type}\}.$$

We then define the quotients

$$\mathbb{W}_t := \mathcal{W}_t^* * A * B / \equiv, \quad \mathbb{W}_{\mathbb{H}} := \mathcal{W}_{\mathbb{H}}^* * A * B / \equiv, \quad \hat{\mathbb{W}} := \hat{\mathcal{W}}^* * A * B / \equiv$$

and consider the AB-structures induced by  $\mathbb{W}$  on  $\mathbb{W}_t, \mathbb{W}_{\mathbb{H}}, \hat{\mathbb{W}}$ . One can easily check that the inclusions  $\mathbb{W}_{\mathbb{H}} \rightarrow \mathbb{W}_t$ ,  $\mathbb{W}_t \rightarrow \mathbb{W}$ ,  $\hat{\mathbb{W}} \rightarrow \mathbb{W}$  are AB-homomorphisms.

### Involutions

*Involutions over  $\hat{\mathbb{W}}$*  Apart from the natural involution  $\mathbb{I} : \hat{\mathbb{W}} \rightarrow \hat{\mathbb{W}}$  there might exist other involutory monoid anti-isomorphisms  $\mathbb{I}' : (\hat{\mathbb{W}}, \cdot, 1_{\mathbb{W}}) \rightarrow (\hat{\mathbb{W}}, \cdot, 1_{\mathbb{W}})$ . Let us consider those  $\mathbb{I}'$  defined by a partition  $\hat{\mathcal{W}} = \hat{\mathcal{W}}_0 \cup \mathcal{W}_1 \cup \overline{\mathcal{W}}_1$ ,  $\mathcal{W}_1 = \{W_1, \dots, W_p\}$ ,  $\overline{\mathcal{W}}_1 = \{\bar{W}_1, \dots, \bar{W}_p\}$ , a tuple  $(a_1, b_1, \dots, a_k, b_k, \dots, a_p, b_p)$ , with  $(a_k, b_k) \in (\text{Gi}(W_k), \text{Ge}(W_k))$  and formulas of the form

$$\mathbb{I}'(e) = e^{-1}, \quad \text{for all } e \in \iota(A) \cup \iota(B), \quad \mathbb{I}'(W) = \mathbb{I}(W), \quad \text{for all } W \in \hat{\mathcal{W}}_0 \quad (74)$$

$$\mathbb{I}'(W_k) = a_k W_k b_k; \mathbb{I}'(\bar{W}_k) = a_k^{-1} \bar{W}_k b_k^{-1} \quad \text{for all } k \in [1, p]. \quad (75)$$

**Lemma 10.** *Let us consider a partition of  $\hat{\mathcal{W}}$  and a tuple of group elements  $(a_1, b_1, \dots, a_k, b_k, \dots, a_p, b_p)$  as above.*

1- *If there exists some anti-automorphism  $\mathbb{I}' : \hat{\mathbb{W}} \rightarrow \hat{\mathbb{W}}$  satisfying (74,75) then, for every  $k \in [1, p]$*

$$\delta(W_k)^{-1} = \delta(a_k) \circ \delta(W_k) \circ \delta(b_k). \quad (76)$$

2- *If condition (76) is fulfilled, then there exists a unique anti-automorphism  $\mathbb{I}' : \hat{\mathbb{W}} \rightarrow \hat{\mathbb{W}}$  satisfying (74,75).*

3- *The monoid anti-automorphism  $\mathbb{I}'$  given in point (2) is involutive iff, for every  $k \in [1, p]$ ,*

$$(b_k^{-1} a_k, a_k b_k^{-1}) \in \delta(W_k) \quad (77)$$

4- *The involutive monoid anti-automorphism  $\mathbb{I}'$  given in point (3) makes  $\langle \mathbb{W}, \iota_A, \iota_B, \mathbb{I}', \gamma, \mu, \delta \rangle$  into an AB-algebra iff, in addition, for every  $k \in [1, p]$*

$$\gamma(W_k) = \mathbb{I}_{\mathcal{T}}(\gamma(W_k)), \quad \mu(a_k W_k b_k) = \mathbb{I}_{\mathcal{Q}}(\mu(W_k)). \quad (78)$$

**Proof:** 1- Suppose that  $\mathbb{I}'$  is an anti-isomorphism of  $(\hat{\mathbb{W}}, \cdot)$  fulfilling (74,75). Let  $k \in [1, p]$  and  $(c, d) \in \text{Gi}(W_k) \times \text{Ge}(W_k)$ . On one hand:

$$\begin{aligned} (c, d) \in \delta(\mathbb{I}'(W_k)) &\Leftrightarrow (c, d) \in \delta(a_k W_k b_k) \\ &\Leftrightarrow (c, d) \in \delta(a_k) \circ \delta(W_k) \circ \delta(b_k). \end{aligned}$$

On the other hand:

$$\begin{aligned}
(c, d) \in \delta(\mathbb{I}'(W_k)) &\Leftrightarrow c\mathbb{I}'(W_k) = \mathbb{I}'(W_k)d \\
&\Leftrightarrow \mathbb{I}'(W_k c^{-1}) = \mathbb{I}'(d^{-1}W_k) \\
&\Leftrightarrow W_k c^{-1} = d^{-1}W_k \\
&\Leftrightarrow dW_k = W_k c \\
&\Leftrightarrow (d, c) \in \mathbb{I}'(W_k) \\
&\Leftrightarrow (c, d) \in (\mathbb{I}'(W_k))^{-1}.
\end{aligned}$$

We have thus established that

$$(\mathbb{I}'(W_k))^{-1} = \delta(a_k) \circ \delta(W_k) \circ \delta(b_k).$$

2- Suppose that condition (76) is met. By the universal property of the free-product, there exists a monoid-anti-homomorphism  $I : (\hat{\mathcal{W}}^* * A * B, \cdot) \rightarrow (\hat{\mathcal{W}}^* * A * B, \cdot)$  such that,

$$\begin{aligned}
I(e) &= e, \quad \text{for all } e \in \iota(A) \cup \iota(B), \quad I(W) = W, \quad \text{for all } W \in \hat{\mathcal{W}}_0 \\
I(W_k) &= a_k W_k b_k, \quad I(\bar{W}_k) = a_k^{-1} \bar{W}_k b_k^{-1} \quad \text{for all } k \in [1, p].
\end{aligned}$$

Similarly, there exists a unique monoid-anti-homomorphism  $J : (\hat{\mathcal{W}}^* * A * B, \cdot) \rightarrow (\hat{\mathcal{W}}^* * A * B, \cdot)$  such that,

$$\begin{aligned}
J(e) &= e, \quad \text{for all } e \in \iota(A) \cup \iota(B), \quad J(W) = W, \quad \text{for all } W \in \hat{\mathcal{W}}_0 \\
J(W_k) &= b_k W_k a_k, \quad J(\bar{W}_k) = b_k^{-1} \bar{W}_k a_k^{-1} \quad \text{for all } k \in [1, p].
\end{aligned}$$

Let  $k \in [1, p]$ ,  $(c, d) \in \delta(W_k)$ .

$$I(cW_k) = a_k W_k b_k \cdot c^{-1}, I(W_k d) = d^{-1} \cdot a_k W_k b_k.$$

From  $(c, d) \in \delta(W_k)$  we get that  $(d^{-1}, c^{-1}) \in \delta(W_k)$  and by hypothesis (76) we obtain that  $(d^{-1}, c^{-1}) \in \delta(aW_k b_k)$ , so that

$$I(cW_k) = I(W_k d) \tag{79}$$

and by a similar argument

$$I(\bar{W}_k c) = I(d \bar{W}_k). \tag{80}$$

It follows from the equalities (79,80), that  $I$  induces a monoid anti-homomorphism  $\mathbb{I}' : \hat{\mathbb{W}} \rightarrow \hat{\mathbb{W}}$ .

Let us remark that condition (76) also implies the similar condition

$$\delta(W_k)^{-1} = \delta(b_k) \circ \delta(W_k) \circ \delta(a_k). \tag{81}$$

This implication can be detailed as

$$\begin{aligned}
\delta(W_k)^{-1} &= \delta(a_k) \circ \delta(W_k) \circ \delta(b_k) \Leftrightarrow \delta(W_k) = \delta(b_k)^{-1} \circ \delta(W_k)^{-1} \circ \delta(a_k)^{-1} \\
&\Leftrightarrow \delta(b_k) \circ \delta(W_k) \circ \delta(a_k) = \delta(W_k)^{-1}.
\end{aligned}$$

Hence, by same means as those used for  $I$ , one can prove that  $J$  induces a monoid anti-homomorphism  $\mathbb{J}' : \hat{\mathbb{W}} \rightarrow \hat{\mathbb{W}}$ .

Moreover the action of  $\mathbb{I}' \circ \mathbb{J}'$  over the generators of  $\mathbb{W}$  is given by:

$$\mathbb{I}' \circ \mathbb{J}'(e) = e, \quad \text{for all } e \in \iota(A) \cup \iota(B), \quad \mathbb{I}' \circ \mathbb{J}'(W) = W, \quad \text{for all } W \in \hat{\mathcal{W}}_0,$$

and, for every  $k \in [1, p]$ ,

$$\begin{aligned} \mathbb{I}' \circ \mathbb{J}'(W_k) &= \mathbb{J}'(a_k W_k b_k) = b_k^{-1} \mathbb{J}'(W_k) a_k^{-1} = W_k \\ \mathbb{I}' \circ \mathbb{J}'(\bar{W}_k) &= \mathbb{J}'(a_k^{-1} \bar{W}_k b_k^{-1}) = b_k \mathbb{J}'(\bar{W}_k) a_k = \bar{W}_k \end{aligned}$$

which shows that  $\mathbb{I}' \circ \mathbb{J}' = \text{Id}_{\hat{\mathbb{W}}}$ . By analogous calculations  $\mathbb{J}' \circ \mathbb{I}' = \text{Id}_{\hat{\mathbb{W}}}$ . Finally,  $\mathbb{I}'$  is a monoid anti-*automorphism* (with reciprocal  $\mathbb{J}'$ ). The unicity of such an anti-automorphism follows from the fact that  $\hat{\mathbb{W}}$  is generated by the images of  $\iota(A) \cup \iota(B) \cup \hat{\mathcal{W}}$  by  $\pi_{\equiv}$ .

3-  $\mathbb{I}' \circ \mathbb{I}' = \text{Id}$  iff, for every  $k \in [1, p]$ ,  $\mathbb{I}'(\mathbb{I}'(W_k)) = W_k$  i.e.  $\mathbb{I}'(a_k W_k b_k) = W_k$  i.e.  $b_k^{-1} a_k W_k b_k a_k^{-1} = W_k$ , which is equivalent to  $b_k^{-1} a_k W_k = W_k a_k b_k^{-1}$  i.e.  $(b_k^{-1} a_k, a_k b_k^{-1}) \in \delta(W_k)$ , which is exactly condition (77).

4-  $\mathbb{I}'$  is a suitable involution for making  $\langle \mathbb{W}, \iota_A, \iota_B, \mathbb{I}', \gamma, \mu, \delta \rangle$  into an AB-algebra, iff  $\mathbb{I}'$  is compatible with  $\gamma, \mu, \delta$  (as imposed by axiom (33)). It is clear that  $\mathbb{I}'$  is compatible with  $\gamma$  and  $\mu$  iff it fulfils  $\gamma(W_k) = \mathbb{I}'_{\mathcal{I}}(\gamma(W_k))$ ,  $\mu(a_k W_k b_k) = \mathbb{I}'_{\mathcal{Q}}(\mu(W_k))$  for every  $k \in [1, p]$ . The condition that  $\mathbb{I}'$  is compatible with  $\delta$  can be expressed as  $\delta(a_k W_k b_k) = (\delta(W_k))^{-1}$ , which is just the condition (76) that  $\mathbb{I}'$  is already assumed to fulfil.  $\square$

An involution  $\mathbb{I}'$  of the form (74,75), fulfilling conditions (76-78) is called *H-realizable* if, for every  $k \in [1, p]$

$$\exists h_k \in I(H), \quad \gamma(W_k) \subseteq \gamma_t(h_k), \quad \mu(W_k) = \mu_t(h_k), \quad \delta(W_k) = \delta_t(h_k), \quad a_k h_k b_k = h_k^{-1} \quad (82)$$

We denote by  $\mathcal{I}$  the set of all partial involution  $\mathbb{I}'$  of the form (74,75) satisfying the four conditions (76)(77)(78) and (82). We call the elements of  $\mathcal{I}$  the *H-involutions* of  $\mathbb{W}$ .

**Homomorphisms** Let us show here some properties of AB-homomorphisms from  $\mathcal{W}^* * A * B$  or  $\mathbb{W}$  to other AB-algebras. Let us denote by  $\mathcal{G}_{\mathbb{W}}$  the set of generators:

$$\mathcal{G}_{\mathbb{W}} = \mathcal{W} \cup \iota_A(A) \cup \iota_B(B).$$

**Lemma 11.** *Let  $\mathcal{M}_2 = \langle \mathbb{M}_2, \cdot, 1_{\mathbb{M}_2}, \iota_{A,2}, \iota_{B,2}, \mathbb{I}_2, \gamma_2, \mu_2, \delta_2 \rangle$  be some AB-algebra. Let  $\psi : \mathbb{W} \rightarrow \mathbb{M}_2$  be some monoid-homomorphism. This map  $\psi$  is an AB-homomorphism if and only if,*

$$1- \iota_A \circ \psi = \iota_{A,2}, \quad \iota_B \circ \psi = \iota_{B,2}$$

$$\text{and for every } g \in \mathcal{G}_{\mathbb{W}}, \theta \in \gamma(g):$$

$$2- g \in \text{dom}(\mathbb{I}) \Leftrightarrow \psi(g) \in \text{dom}(\mathbb{I}_2)$$

$$2'- \mathbb{I}_2(\psi(g)) = \psi(\mathbb{I}(g))$$

- 3-  $\gamma_2(\psi(g)) \supseteq \gamma(g)$
- 4-  $\mu_2(\boldsymbol{\theta}, \psi(g)) = \mu(\boldsymbol{\theta}, g)$
- 5-  $\delta_2(\boldsymbol{\theta}, \psi(g)) = \delta(\boldsymbol{\theta}, g)$ .

**Proof:** Suppose that  $\psi$  is an  $AB$ -homomorphism. By definition it must fulfill conditions (35-40). But for all  $g \in \mathcal{G}_{\mathbb{W}}$ ,  $\gamma(g) \neq \emptyset$ . Hence condition (36) implies condition (2) of the lemma. The other five conditions translate immediately into (1)(2')(3)(4)(5).

Conversely, let suppose that  $\psi$  fulfills conditions (1-5) of the lemma.

By (1), condition (35) is fulfilled.

**Extending (2) to  $\mathbb{W}$**

Let  $w \in \mathbb{W}$  with  $\gamma(w) \neq \emptyset$ . It must have a decomposition

$$w = g_1 g_2 \cdots g_n$$

with  $1 \leq n, \forall i \in [1, n], g_i \in \mathcal{G}_{\mathbb{W}}$ .

Let us suppose that

$$w \in \text{dom}(\mathbb{I}). \quad (83)$$

By definition of  $\gamma_{\mathbb{W}}$ ,  $\gamma_{\mathbb{W}}(w) = \prod_{i=1}^n \gamma(g_i)$ , hence, (83) and axiom (25) imply

$$\prod_{i=1}^n \gamma(g_i) \neq \emptyset \quad (84)$$

and, in particular

$$\forall i \in [1, n], \gamma(g_i) \neq \emptyset \quad (85)$$

Applying axiom (26) of  $AB$ -algebras, (83) and (84) give:

$$\forall i \in [1, n], g_i \in \text{dom}(\mathbb{I}). \quad (86)$$

By condition (2) of the lemma, (85) and (86) entail that

$$\forall i \in [1, n], \psi(g_i) \in \text{dom}(\mathbb{I}_2). \quad (87)$$

By condition (3) of the lemma and (84), we know that

$$\prod_{i=1}^n \gamma(\psi(g_i)) \neq \emptyset. \quad (88)$$

Using again axiom (26) and (87) we obtain that

$$\prod_{i=1}^n \psi(g_i) \in \text{dom}(\mathbb{I}_2). \quad (89)$$

But  $\psi$  is a monoid homomorphism, hence this implies that

$$\psi(w) \in \text{dom}(\mathbb{I}_2). \quad (90)$$



We have proved that, under the hypothesis that  $\gamma(w) \neq \emptyset$ , (83) implies (90). Let us establish the converse. Let us assume that

$$\gamma(w) \neq \emptyset \quad (91)$$

and (90). As  $\psi$  is a monoid-homomorphism, we obtain (89). From (91) we get (84) and, as above (88). From (89) and (88), by axiom (26) of  $AB$ -algebras we can deduce (87). By condition (2) of the lemma, (87) implies (86). From (86) and (84), by axiom (26) we obtain (83), as required.

**Extending (2') to  $\mathbb{W}$**

By the point above, we know that  $\text{im}(\mathbb{I} \circ \psi) \subseteq \text{dom}(\mathbb{I}_2)$ . Let us consider the map

$$\theta = \mathbb{I} \circ \psi \circ \mathbb{I}_2 : \hat{\mathbb{W}} \rightarrow \hat{\mathbb{M}}_2.$$

Condition (2') shows that,

$$\forall g \in \mathcal{G}_{\mathbb{W}}, \theta(g) = \psi(g).$$

As  $\theta, \psi$  are monoid-homomorphism and  $\mathcal{G}_{\mathbb{W}}$  is a set of monoid generators of  $\mathbb{W}$ , it follows that  $\theta = \psi$ , thus  $\theta \circ \mathbb{I}_2 = \psi \circ \mathbb{I}_2$  i.e.

$$\mathbb{I} \circ \psi = \psi \circ \mathbb{I}_2,$$

as required.

**Extending (3) to  $\mathbb{W}$**

Let us consider the pairs  $(\mathbb{W}, =), (\mathbb{M}_2, =), (\mathcal{P}(\mathcal{T}), \subseteq)$ . Each of them is an *ordered* monoid i.e., the second element of each pair is an ordering relation which is compatible with right(resp. left) product. Let us consider the sequence of two maps:

$$\mathbb{W} \xrightarrow{\psi} \mathbb{M}_2 \xrightarrow{\gamma_2} \mathcal{P}(\mathcal{T})$$

These two maps are *overmorphic* in the sense that:

$$\psi(w \cdot w') = \psi(w) \cdot \psi(w'), \quad \gamma_2(m \cdot m') \supseteq \gamma_2(m) \cdot \gamma_2(m').$$

(see axiom (28) for the second inequality). It follows that their composition  $\psi \circ \gamma_2$  is overmorphic too, i.e. for every  $w, w' \in \mathbb{W}$

$$\gamma_2(\psi(w \cdot w')) \supseteq \gamma_2(\psi(w)) \cdot \gamma_2(\psi(w')) \quad (92)$$

From this property (92), one can show, by induction over the integer  $n$  that, for every  $g_1, \dots, g_i, \dots, g_n$

$$\gamma_2(\psi(\prod_{i=1}^n g_i)) \supseteq \prod_{i=1}^n \gamma_2(\psi(g_i)),$$

which, by condition (3) of the lemma, and the definition of  $\gamma_{\mathbb{W}}$  implies that

$$\gamma_2(\psi(\prod_{i=1}^n g_i)) \supseteq \gamma_{\mathbb{W}}(\prod_{i=1}^n g_i),$$

as required.

**Extending (4) to  $\mathbb{W}$**

Let  $w \in \mathbb{W}$  such that

$$\gamma_{\mathbb{W}}(w) \neq \emptyset. \quad (93)$$

This  $w$  must have a decomposition

$$w = \prod_{i=1}^n g_i \quad (94)$$

where  $g_i \in \mathcal{G}_{\mathbb{W}}$ . As we saw in the extension of (3) to  $\mathbb{W}$ , hypothesis (93) entails that

$$\prod_{i=1}^n \gamma_{\mathbb{W}}(g_i) \neq \emptyset, \quad \prod_{i=1}^n \gamma_2(\psi(g_i)) \neq \emptyset. \quad (95)$$

Let  $\theta \in \gamma_{\mathbb{W}}(w)$ : by definition of  $\gamma_{\mathbb{W}}$  it must have the form

$$\theta = \prod_{i=1}^n \theta_i, \quad \forall i \in [1, n], \theta_i \in \gamma_{\mathbb{W}}(g_i). \quad (96)$$

We thus have

$$\begin{aligned} \mu_2(\theta, \psi(w)) &= \mu_2(\prod_{i=1}^n \theta_i, \prod_{i=1}^n \psi(g_i)) \quad (\psi \text{ is a monoid hom.}) \\ &= \prod_{i=1}^n \mu_2(\psi(\theta_i), \psi(g_i)) \quad (\text{axiom (29)}) \\ &= \prod_{i=1}^n \mu_{\mathbb{W}}(\theta_i, g_i) \quad (\text{by condition (4)}) \\ &= \mu_{\mathbb{W}}(\theta, w) \quad (\text{axiom (29)}), \end{aligned} \quad (97)$$

as required.

**Extending (5) to  $\mathbb{W}$**

We start again with some  $w \in \mathbb{W}$  fulfilling (93), hence (95) and consider some  $\theta \in \gamma_{\mathbb{W}}(w)$ , hence of the form (96). We thus have

$$\begin{aligned} \delta_2(\theta, \psi(w)) &= \delta_2(\prod_{i=1}^n \theta_i, \prod_{i=1}^n \psi(g_i)) \quad (\psi \text{ is a monoid hom.}) \\ &= \prod_{i=1}^n \delta_2(\theta_i, \psi(g_i)) \quad (\text{axiom (31)}) \\ &= \prod_{i=1}^n \delta(\theta_i, g_i) \quad (\text{by condition (5)}) \\ &= \delta_{\mathbb{W}}(\theta, w) \quad (\text{axiom (31)}). \end{aligned} \quad (98)$$

□

**Lemma 12.** Let  $P, S, P', S' \in \mathbb{W}$  such  $\gamma(P) = \gamma(P')$  and  $\gamma(PS) = \gamma(P'S') \neq \emptyset$ .

Then one of the following occurs

1- there exist  $\theta, \theta' \in \mathcal{T}_6$ ,  $\gamma(S), \gamma(S') \in \{\{(\theta, 0, \theta')\}, \{(\theta, 1, \theta')\}\}$ .

2-  $P, S, P', S' \in A$

3-  $P, S, P', S' \in B$

**Proof:** Let  $P, S, P', S'$  fulfill the hypothesis of the lemma.

**Case 1:**  $\|P\| \geq 1, \|P'\| \geq 1, \|S\| \geq 1, \|S'\| \geq 1$ .

Since  $\gamma(P'S) = \gamma(P'S') \neq \emptyset$  we must have  $\tau_i(S) = \tau_e(P), \tau_i(S') = \tau_e(P')$ .

Similarly we obtain that  $\tau_e(S) = \tau_e(S')$ , so that conclusion 1 holds.

**Case 2:**  $\|P\| \geq 1, \|P'\| \geq 1, \|S\| = \|S'\| = 0$ .

In this case,  $S, S' \in A \cup B$ . Moreover,  $\gamma(P) = \gamma(P') \Rightarrow \text{Ge}(P) = \text{Ge}(P') \Rightarrow S, S' \in \text{Ge}(P) \Rightarrow \gamma(S) = \gamma(S')$ .

**Case 3:**  $\|P\| \geq 1, \|P'\| \geq 1, \|S\| \geq 1, \|S'\| = 0$ .

As  $\|S'\| \geq 1, \text{Card}(\gamma(S)) = 1$  and  $\tau_e(S) \neq \tau_i(S) = \tau_e(P)$  so that

$$\tau_e(S) \neq \tau_e(P) \quad (99)$$

Since  $\|S'\| = 0$ , for every  $\theta \in \gamma(S'), \tau_i(\theta) = \tau_e(\theta)$ , hence

$$\tau_e(P'S') = \tau_e(P') \quad (100)$$

We also have  $\gamma(P'S) = \gamma(P'S') \neq \emptyset$  which implies that  $\tau_e(S) = \tau_e(P'S) = \tau_e(P'S')$  hence, taking into account (100) we get

$$\tau_e(S) = \tau_e(P') \quad (101)$$

But equations (99)(101) entail that  $\tau_e(P) \neq \tau_e(P')$  contradicting the hypothesis that  $\gamma(P) = \gamma(P')$ . This case is thus impossible.

**Case 4:**  $\|P\| = \|P'\| = 0, \|S\| \geq 1, \|S'\| \geq 1$ .

In this case  $P, P' \in A \cup B$ . The fact that  $\gamma(P) = \gamma(P')$  implies that

$$(P \in A - \{1\} \wedge P' \in A - \{1\}) \vee (P \in B - \{1\} \wedge P' \in B - \{1\}) \vee (P = P' = 1).$$

Here  $\gamma(S) = \gamma(P'S) = \gamma(P'S') = \gamma(S')$ . Hence conclusion 1 holds.

**Case 5:**  $\|P\| = \|P'\| = 0, \|S\| \geq 1, \|S'\| = 0$ .

We should then have  $\text{Card}(\gamma(P'S)) = 1$  while  $\text{Card}(\gamma(P'S')) \in \{0, 2, 6\}$ . This contradicts the hypothesis that  $\gamma(P'S) = \gamma(P'S')$ . This case is thus impossible.

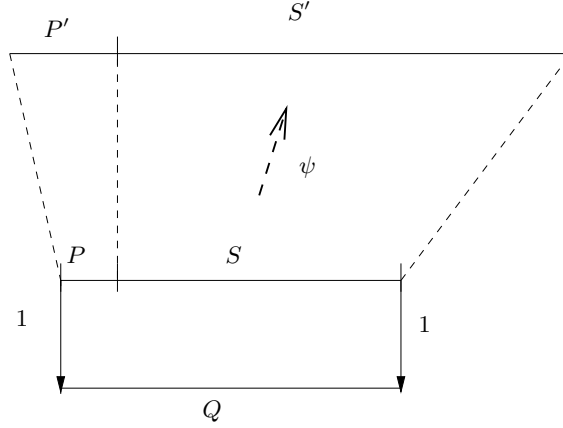
**Case 6:**  $\|P\| = \|P'\| = 0, \|S\| = \|S'\| = 0$ .

Then  $P, P', S, S' \in A \cup B$ . But  $\gamma(P'S) = \gamma(P'S')$  implies that conclusion 2 or conclusion 3 holds.  $\square$

**Lemma 13.** Let  $\psi : \mathbb{W} \rightarrow \mathbb{M}$  be some AB-homomorphism into some AB-algebra  $\mathbb{M}$ . Let  $P, S, P', S' \in \mathbb{W}$  such that  $\gamma(P) = \gamma(P'), \psi(P) = \psi(P'), \psi(P'S) = \psi(P'S')$  and  $\gamma(P'S) = \gamma(P'S') \neq \emptyset$ . Then  $\gamma(S) = \gamma(S')$ .

**Proof:** One of conclusions 1,2,3 of Lemma 12 must hold. If conclusion 1 holds,  $\|\psi(P)\| = \|\psi(P')\|, \|\psi(P'S)\| = \|\psi(P'S')\|$  imply that  $\|\psi(S)\| = \|\psi(S')\|$ . The boolean component of  $\gamma(S), \gamma(S')$  are thus equal and finally,  $\gamma(S) = \gamma(S')$ .

If conclusion 2 (resp. 3) holds, since  $\psi$  restricted to the group  $A$  (resp.  $B$ ) is a group isomorphism onto its image,  $S = S'$ .  $\square$



**Fig. 5.** Lemma 14, the statement.

**Lemma 14.** *Let  $\psi : \mathbb{W} \rightarrow \mathbb{H}_t$  be some AB-homomorphism. Let  $Q \in \mathbb{W}, P', S' \in \mathbb{H}_t, \theta \in \gamma(P'), \rho \in \gamma(S')$  such that,  $\theta$  is a H-type,  $\theta \cdot \rho$  is defined and  $\psi(Q) = P' \cdot S'$ . Then, there exist  $P, S \in \mathbb{W}$  such that:*

$$Q = P \cdot S, \quad \psi(P) = P', \quad \gamma(P) = \{\theta\}, \quad \psi(S) = S', \quad \rho \in \gamma(S).$$

**Proof:** Let us consider  $\psi, Q, P', S', \theta, \rho$  fulfilling the hypothesis of the lemma. Decomposing  $Q$  over the generators of  $\mathcal{G}_{\mathbb{W}}$  gives

$$Q = e_0 W_0 \cdot Q_1 \tag{102}$$

where  $W_0 \in \mathcal{W}$ ,  $e_0 \in \iota(A) \cup \iota(B)$ . Let us choose some reduced sequences  $s_0, s_1, p', s'$  such that

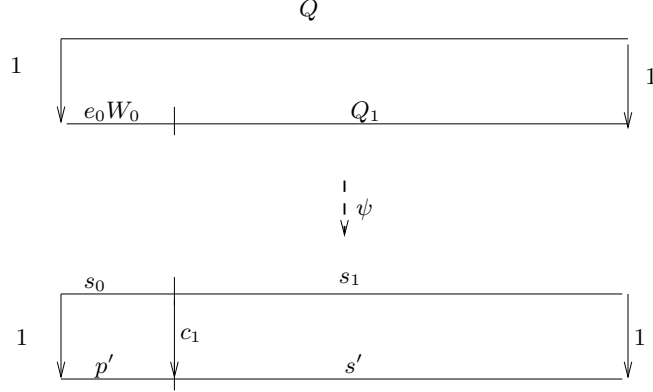
$$\psi(e_0 W_0) = [s_0]_{\sim}, \quad \psi(Q_1) = [s_1]_{\sim}, \quad P' = [p']_{\sim}, \quad S' = [s']_{\sim}, \tag{103}$$

see Figure 6. Since  $W_0 \in \mathcal{W}$ ,  $W_0$  has either a H-type or a T-type. The equality  $\gamma(W_0) \cdot \gamma(Q_1) = \{\theta \cdot \rho\}$  shows that the following equality between vertex-types holds:  $\gamma_1(W_0) = \gamma_1(\theta)$ . Hence  $\gamma(W_0)$  is a H-type. It follows that  $Q_1$  has a T-type or the type  $(1, 1, 0, 1, 1)$ . Similarly,  $p'$  has a H-type (namely  $\theta$ ) and, by the same argument,  $s'$  has a T-type or the type  $(1, 1, 0, 1, 1)$ . Let us choose the representatives  $s_1$  (resp.  $s'$ ) in such a way that it begins with a letter  $t$  or  $\bar{t}$  or it is equal to 1. We know that  $\psi(Q) = P'Q'$  i.e.

$$s_0 \cdot s_1 \sim p' \cdot s' \tag{104}$$

and the choice of representatives  $s_1, s'$  ensures the sequences  $s_0 \cdot s_1, p' \cdot s'$  are reduced. Thus there exist connecting elements  $c_1, \dots$  between  $s_0 \cdot s_1$  and  $p' \cdot s'$  ([LS08, section 3]); in particular

$$c_1 \in \text{Ge}(\theta), \quad s_0 \cdot c_1 = p', \quad c_1 s' \sim s_1 \tag{105}$$



**Fig. 6.** Lemma 14, the proof.

Let us define

$$P := e_0 W_0 c_1, \quad S := c_1^{-1} Q_1. \quad (106)$$

We obtain from (102,106) that  $Q = P \cdot S$ . We obtain from (105) that  $\psi(P) = P', \psi(S) = S'$ . It remains to determine the types of  $P, Q$ . Let us note  $\gamma(P) = \{\theta_1\}$  and let  $\rho_1 \in \gamma(S)$ . The fact that  $\psi(P \cdot S) = P' \cdot S'$  implies that

$$\theta_1 \cdot \rho_1 = \theta \cdot \rho. \quad (107)$$

Since  $\theta$  is a H-type and  $\theta \cdot \rho$  is defined,  $\rho$  must be either a T-type or the type  $(1, 1, 0, 1, 1)$ .

**Case 1:**  $\rho$  is a T-type.

$\rho, \rho_1$  are both types of  $s'$ . Since  $s'$  starts with either a letter  $t$  or a letter  $\bar{t}$ , this letter completely determines the first vertex-type  $p_1(\rho) = p_1(\rho_1)$ ; it also imposes that, concerning the middle boolean component,  $p_2(\rho) = p_2(\rho_1) = 1$ ; and finally, by (107),  $p_3(\rho) = p_3(\rho_1) = p_3(\theta \cdot \rho)$ . This establishes that  $\rho_1 = \rho$ . Using (107) we know that  $\theta_1, \theta$  have same initial and ending vertex-types and, since they are H-types, they also have the same boolean component, namely 0. Hence  $\theta_1 = \theta$ . Finally,  $\gamma(P) = \{\theta\}, \gamma(S) = \{\rho\}$ .

**Case 2:**  $\rho = (1, 1, 0, 1, 1)$ .

In this case  $Q' = 1$  and the choice of the representatives  $s', s_1$  implies  $s' = s_1 = 1$ , hence  $c_1 = 1$  and  $Q_1 = S = 1$  so that  $\rho \in \gamma(S)$ . By hypothesis,  $\gamma(Q) = \{\theta \cdot \rho\}$ , hence  $\gamma(P) = \{\theta\}$ .

In both cases the types of  $P, S$  fulfil the required property.  $\square$

**Lemma 15 (factorization).** *Let  $\tilde{\psi} : \mathcal{W}^* A^* B \rightarrow \mathbb{W}$  be some  $AB$ -homomorphism. Then, there exists a unique  $AB$ -homomorphism  $\psi : \mathbb{W} \rightarrow \mathbb{W}$  such that  $\pi_{\equiv} \circ \psi = \tilde{\psi}$ .*

**Proof:** Since  $\tilde{\psi}$  is an  $AB$ -homomorphism, for every  $W \in \mathcal{W}$ ,  $\delta(W) = \delta(\tilde{\psi}(W))$ . Hence  $\ker(\pi_{\equiv}) \subseteq \ker(\tilde{\psi})$ , which ensures the existence of  $\psi \in \text{Hom}(\mathbb{W}, \mathbb{W})$  such that  $\pi_{\equiv} \circ \psi = \tilde{\psi}$ . By hypothesis,  $\tilde{\psi}$  preserves  $\iota_A, \iota_B, \mathbb{I}, \gamma, \mu, \delta$ , over the elements of  $\mathcal{G}_{\mathbb{W}}$ . As  $\pi_{\equiv}$  does also preserves all these maps, it follows that  $\psi$  fulfills conditions (1-5) of Lemma 11, hence it is an  $AB$ -homomorphism.  $\square$

**Lemma 16 (quotient).** *Let  $\tilde{\sigma} : \mathcal{W}^* * A * B \rightarrow \mathcal{W}^* * A * B$  be some  $AB$ -homomorphism. Then, there exists a unique  $AB$ -homomorphism  $\sigma : \mathbb{W} \rightarrow \mathbb{W}$  such that  $\pi_{\equiv} \circ \sigma = \tilde{\sigma} \circ \pi_{\equiv}$ .*

**Proof:** Applying Lemma 15 to the  $AB$ -homomorphism  $\tilde{\psi} = \tilde{\sigma} \circ \pi_{\equiv}$  we obtain this lemma.  $\square$

**Lemma 17 (lifting).** *Let  $\tilde{\psi} : \mathcal{W}^* * A * B \rightarrow \mathbb{W}$  be some  $AB$ -homomorphism. Then, there exists an  $AB$ -homomorphism  $\psi : \mathcal{W}^* * A * B \rightarrow \mathcal{W}^* * A * B$  such that  $\tilde{\psi} = \psi \circ \pi_{\equiv}$ .*

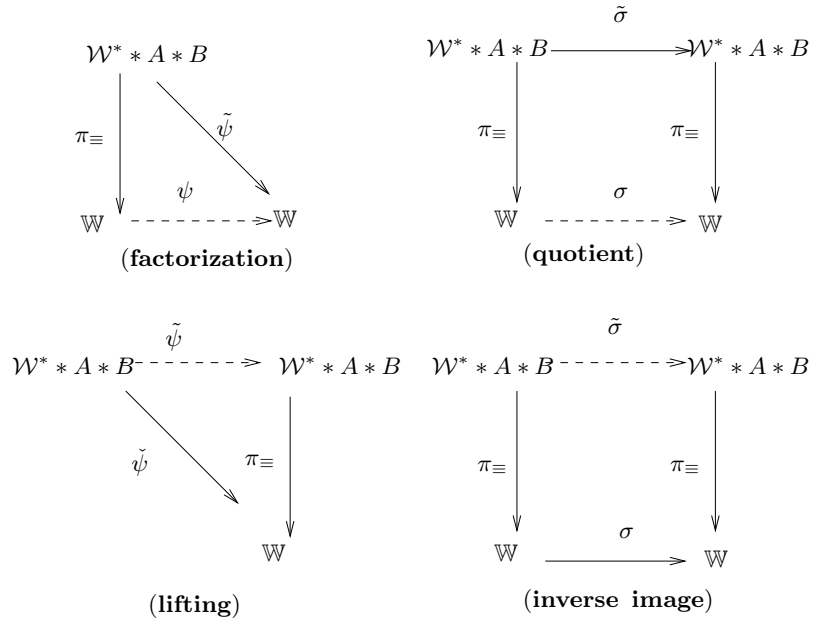
**Proof:** Let us consider some map  $\tilde{\psi} : \mathcal{G}_{\mathbb{W}} \rightarrow \mathcal{W}^* * A * B$  fulfilling, for every  $a \in A, b \in B, W \in \mathcal{W}$ :

$$\begin{aligned}\tilde{\psi}(\iota_A(a)) &= \iota_A(a), \quad \tilde{\psi}(\iota_B(b)) = \iota_B(b) \\ \tilde{\psi}(W) &\in \pi_{\equiv}^{-1}(\tilde{\psi}(W)).\end{aligned}$$

Since  $\pi_{\equiv}$  preserves  $\iota_A, \iota_B, \mathbb{I}, \gamma, \mu, \delta$  and  $\tilde{\psi}$  fulfills conditions (1-5) of Lemma 11, the map  $\tilde{\psi}$  does also fulfill conditions (1-5). By the universal property of the free product, it can be extended into a monoid homomorphism from  $\mathcal{W}^* * A * B$  to  $\mathcal{W}^* * A * B$ . By Lemma 11, it is also an  $AB$ -homomorphism from  $\mathcal{W}^* * A * B$  to  $\mathcal{W}^* * A * B$ . Moreover, for every  $g \in \mathcal{G}_{\mathbb{W}}$ ,  $\pi_{\equiv}(\tilde{\psi}(g)) = \tilde{\psi}(g)$ , hence  $\tilde{\psi} \circ \pi_{\equiv} = \tilde{\psi}$ , as required.  $\square$

**Lemma 18 (inverse image).** *Let  $\sigma : \mathbb{W} \rightarrow \mathbb{W}$  be some  $AB$ -homomorphism. Then, there exists an  $AB$ -homomorphism  $\tilde{\sigma} : \mathcal{W}^* * A * B \rightarrow \mathcal{W}^* * A * B$  such that  $\pi_{\equiv} \circ \sigma = \tilde{\sigma} \circ \pi_{\equiv}$ .*

**Proof:** Applying Lemma 17 to the  $AB$ -homomorphism  $\tilde{\psi} = \pi_{\equiv} \circ \sigma$ , we obtain this lemma.  $\square$



**Fig. 7.**  $AB$ -homomorphisms

## 4 Equations with rational constraints over $\mathbb{G}$

Let us consider a *system of equations*  $\mathcal{S}$  over  $\mathbb{G}$ :

$$((u_i, u'_i))_{i \in I}$$

where  $I$  is a finite set,  $\mathcal{U}$  is a finite set of variables and  $u_i \in \mathcal{U}^*$ ,  $u'_i \in \mathcal{U}^*$ ; let us consider also a rational constraint  $C : \mathcal{U} \rightarrow \mathcal{B}(\text{Rat}(\mathbb{G}))$ .

### 4.1 Equations with rational constraints

**Quadratic normal form** Such a system can be effectively transformed into a finite system  $\mathcal{S}'$ , with set of variables  $\mathcal{U}'$  and with rational constraint  $C' : \mathcal{U}' \rightarrow \mathcal{B}(\text{Rat}(\mathbb{G}))$  such that

- (1)  $\mathcal{S}'$  is quadratic
- (2)  $\mathcal{U} \subseteq \mathcal{U}'$
- (3) the solutions of  $(\mathcal{S}, C)$  are exactly the restrictions to  $\mathcal{U}^*$  of the solutions of  $(\mathcal{S}', C')$ .

Such a transformation consists of applying iteratively the following elementary transformations  $T_k$ , for  $1 \leq k \leq 4$ :

**T1** Suppose that  $|u'_i| \leq 1$ .

Then set  $\mathcal{U}' := \mathcal{U} \cup \{U'\}$ , where  $U'$  is a new variable, and set

$$v_j := u_j \text{ for all } j \in I, \quad v'_j := u'_j \text{ for all } j \in I - \{i\}, \quad v'_i := u'_i U',$$

$$C'(U) = C(U) \text{ for all } U \in \mathcal{U}, \quad C'(U') = \{\varepsilon\}.$$

**T2** Suppose that  $|u_i| = 0$ .

Then set  $\mathcal{U}' := \mathcal{U} \cup \{U'\}$ , where  $U'$  is a new variable, and set

$$v_j := u_j \text{ for all } j \in I - \{i\}, \quad v'_j := u'_j \text{ for all } j \in I, \quad v_i := U',$$

$$C'(U) = C(U) \text{ for all } U \in \mathcal{U}, \quad C'(U') = \{\varepsilon\}.$$

**T3** Suppose that  $|u_i| \geq 2$ .

Then set  $\mathcal{U}' := \mathcal{U} \cup \{U'\}$ , where  $U'$  is a new variable,  $I' := I \cup \{\bar{i}\}$  where  $\bar{i} \notin I$

$$v_j := u_j \text{ for all } j \in I - \{i\}, \quad v'_j := u'_j \text{ for all } j \in I - \{i\},$$

$$v_i := U', \quad v'_i := u_i, \quad v_{\bar{i}} := U', \quad v'_{\bar{i}} := u'_i,$$

$$C'(U) = C(U) \text{ for all } U \in \mathcal{U}, \quad C'(U') = \mathbb{G}.$$

**T4** Suppose that  $|u'_i| \geq 3 : u'_i = u''_i U$  for some  $U \in \mathcal{U}$ .

Then set  $\mathcal{U}' := \mathcal{U} \cup \{U'\}$ , where  $U'$  is a new variable,  $I' := I \cup \{\bar{i}\}$  where  $\bar{i} \notin I$

$$v_j := u_j \text{ for all } j \in I - \{i\}, \quad v'_j := u'_j \text{ for all } j \in I - \{i\},$$

$$v_i := u_i, \quad v'_i := U' U, \quad v_{\bar{i}} := U', \quad v'_{\bar{i}} := u''_i.$$

$$C'(U) = C(U) \text{ for all } U \in \mathcal{U}, \quad C'(U') = \mathbb{G}.$$



**Rational constraints** Let  $C : \mathcal{U} \rightarrow \mathcal{B}(\text{Rat}(\mathbb{G}))$ . By Proposition 1, for every variable  $U \in \mathcal{U}$ , one can construct some strict normal partitioned finite t-automaton  $\mathcal{A}_U$  over the labelling set  $\mathcal{B}(\text{Rat}(\mathbb{H}))$  such that:

$$C(U) = L(\mathcal{A}_U).$$

Let  $\mathcal{A}$  be the direct product of the fta  $(\mathcal{A}_U)_{U \in \mathcal{U}}$ . This fta  $\mathcal{A}$  is strict, normal partitioned and, for every  $u \in \mathcal{U}$ , there exists  $I_U \subseteq Q_{\mathcal{A}}, T_U \subseteq Q_{\mathcal{A}}$  such that

$$C(U) = \{g \in \mathbb{G} \mid (I_U \times T_U) \cap \mu_{\mathcal{A}, \mathbb{G}}(g) \neq \emptyset\}.$$

Let us define, for every  $U \in \mathcal{U}$ , the subset  $B(U) \subseteq B(Q)$  by:

$$B(U) := \{\rho \in B(Q) \mid (I_U \times T_U) \cap \rho \neq \emptyset\}.$$

Note that  $B(U)$  is *upwards-closed* i.e., if  $\rho \subseteq \rho'$  and  $\rho \in B(U)$ , then  $\rho' \in B(U)$ . It is then clear that  $\mathcal{A}$  recognizes the constraint  $C$  in the sense that, for every  $U \in \mathcal{U}$ ,

$$C(U) = \mu_{\mathcal{A}, \mathbb{G}}^{-1}(B(U)).$$

Let us define

$$M(C) := \{\mu : \mathcal{U} \rightarrow B(Q) \mid \forall U \in \mathcal{U}, \mu(U) \in B(U)\}.$$

We can thus express the initial system of equations with constraint as follows:

$$\bigvee_{\mu \in M(C)} ((u_i, u'_i)_{i \in I}, \mu_{\mathcal{A}, \mathbb{G}}, \mu_{\mathcal{U}}). \quad (108)$$

A solution of the system  $((u_i, u'_i)_{i \in I}, \mu_{\mathcal{A}, \mathbb{G}}, \mu_{\mathcal{U}})$  is now any monoid-homomorphism  $\sigma_{\mathbb{G}} : \mathcal{U}^* \rightarrow \mathbb{G}$  fulfilling both conditions:

$$\forall i \in I, \sigma_{\mathbb{G}}(u_i) = \sigma_{\mathbb{G}}(u'_i) \quad (109)$$

$$\forall U \in \mathcal{U}, \mu_{\mathcal{A}, \mathbb{G}}(\sigma_{\mathbb{G}}(U)) = \mu_{\mathcal{U}}(U). \quad (110)$$

An *over-solution* of the system  $((u_i, u'_i)_{i \in I}, \mu_{\mathcal{A}, \mathbb{G}}, \mu_{\mathcal{U}})$  is any monoid-homomorphism  $\sigma_{\mathbb{G}} : \mathcal{U}^* \rightarrow \mathbb{G}$  fulfilling the above condition (109) together with the condition

$$\forall U \in \mathcal{U}, \mu_{\mathcal{A}, \mathbb{G}}(\sigma_{\mathbb{G}}(U)) \supseteq \mu_{\mathcal{U}}(U). \quad (111)$$

Note that, for the disjunction of systems (108) built above, since each set  $B(U)$  is upwards-closed, every over-solution of the disjunction of systems is also a solution of the disjunction of systems. We have thus proved the following proposition.

**Proposition 3.** *Given a system  $\mathcal{S}_0$  of equations with rational constraints over  $\mathbb{G}$  over a set of variables  $\mathcal{U}_0$ , one can compute a finite family of systems  $(\mathcal{S}_{1,j})_{j \in J}$  of equations with rational constraints over  $\mathbb{G}$  with set of variables  $\mathcal{U}_1 \supseteq \mathcal{U}_0$ , of the form*

$$\mathcal{S}_{1,j} = ((u_i, u'_i)_{i \in I}, \mu_{\mathcal{A}, \mathbb{G}}, \mu_{\mathcal{U}_1, j}) \quad (112)$$

such that

- 1- every equation  $(u_i, u'_i)$  is quadratic,
- 2-  $\mu_{\mathcal{A}, \mathbb{G}}$  is the map associated with a strict normal finite t-automaton  $\mathcal{A}$  and  $\mu_{\mathcal{U}_1, j}$  is a map  $\mathcal{U}_1 \rightarrow \mathcal{B}(\mathcal{Q}_{\mathcal{A}})$ ,
- 3- every solution  $\sigma : \mathcal{U}_0^* \rightarrow \mathbb{G}$  of  $\mathcal{S}_0$  extends into a solution  $\sigma_1 : \mathcal{U}_1^* \rightarrow \mathbb{G}$  of  $\bigvee_{j \in J} \mathcal{S}_{1,j}$
- 4- every solution  $\sigma_1 : \mathcal{U}_1^* \rightarrow \mathbb{G}$  of  $\bigvee_{j \in J} \mathcal{S}_{1,j}$  induces a restriction  $\sigma|_{\mathcal{U}_0^*}$  which is a solution of  $\mathcal{S}_0$ .
- 5- every over-solution of  $\bigvee_{j \in J} \mathcal{S}_{1,j}$  is also a solution of  $\bigvee_{j \in J} \mathcal{S}_{1,j}$ .

Every system  $\mathcal{S} = ((u_i, u'_i)_{i \in I}, \mu_{\mathcal{A}, \mathbb{G}}, \mu_{\mathcal{U}})$  where the equations are quadratic and the map  $\mu_{\mathcal{U}}$  is defined through a strict normal partitioned finite t-automaton  $\mathcal{A}$  over the labelling set  $\mathcal{B}(\text{Rat}(\mathbb{H}))$  is said to be in *quadratic normal form*.

Every finite disjunction of systems  $\bigvee_{j \in J} ((u_i, u'_i)_{i \in I}, \mu_{\mathcal{A}, \mathbb{G}}, \mu_{\mathcal{U}, j})$  where the equations are quadratic, the map  $\mu_{\mathcal{U}}$  is defined through a strict normal partitioned finite t-automaton  $\mathcal{A}$  over the labelling set  $\mathcal{B}(\text{Rat}(\mathbb{H}))$  and such that every over-solution of the disjunction is also a solution of the disjunction is said to be in *closed quadratic normal form*.

## 4.2 Equations and disequations with rational constraints

Let us recall that a finite *system of equations and disequations*  $\mathcal{S}$  over  $\mathbb{G}$  is a family:

$$((u_i, c_i, u'_i))_{i \in I} \quad (113)$$

where  $I$  is a finite set,  $\mathcal{U}$  is a finite set of variables,  $u_i \in \mathcal{U}^*$ ,  $u'_i \in \mathcal{U}^*$  and  $c_i \in \{=, \neq\}$ ; let us consider also a rational constraint  $\mathcal{C} : \mathcal{U} \rightarrow \mathcal{B}(\text{Rat}(\mathbb{G}))$  (see §2.4). Such a system is said to be *quadratic* iff it has the form:

$$((u_i = u'_i)_{1 \leq i \leq n}, (u_i \neq u'_i)_{n+1 \leq i \leq 2n}, \mu_{\mathcal{A}, \mathbb{G}}, \mu_{\mathcal{U}}) \quad (114)$$

where, for every  $i \in [1, n]$ ,  $|u_i| = 1$ ,  $|u'_i| = 2$  and, for every  $i \in [n+1, 2n]$ ,  $|u_i| = |u'_i| = 1$ .

Using the same kind of tricks as in the previous subsection, we can prove the following normalization statement.

**Proposition 4.** *Given a system  $\mathcal{S}_0$  of equations and disequations with rational constraints over  $\mathbb{G}$  over a set of variables  $\mathcal{U}_0$ , one can compute a finite family of systems  $(\mathcal{S}_{1,j})_{j \in J}$  of equations with rational constraints over  $\mathbb{G}$  with set of variables  $\mathcal{U}_1 \supseteq \mathcal{U}_0$ , of the form*

$$\mathcal{S}_{1,j} = ((u_i = u'_i)_{1 \leq i \leq n}, (u_i \neq u'_i)_{n+1 \leq i \leq 2n}, \mu_{\mathcal{A}, \mathbb{G}}, \mu_{\mathcal{U}_1, j}) \quad (115)$$

such that

- 1- every system  $\mathcal{S}_{1,j}$  is quadratic,
- 2-  $\mu_{\mathcal{A}, \mathbb{G}}$  is the map associated with a strict normal finite t-automaton  $\mathcal{A}$  and  $\mu_{\mathcal{U}_1, j}$  is a map  $\mathcal{U}_1 \rightarrow \mathcal{B}(\mathcal{Q}_{\mathcal{A}})$ ,

- 3- every solution  $\sigma : \mathcal{U}_0^* \rightarrow \mathbb{G}$  of  $\mathcal{S}_0$  extends into a solution  $\sigma_1 : \mathcal{U}_1^* \rightarrow \mathbb{G}$  of  $\bigvee_{j \in J} \mathcal{S}_{1,j}$
- 4- every solution  $\sigma_1 : \mathcal{U}_1^* \rightarrow \mathbb{G}$  of  $\bigvee_{j \in J} \mathcal{S}_{1,j}$  induces a restriction  $\sigma|_{\mathcal{U}_0^*}$  which is a solution of  $\mathcal{S}_0$ .
- 5- every over-solution of  $\bigvee_{j \in J} \mathcal{S}_{1,j}$  is also a solution of  $\bigvee_{j \in J} \mathcal{S}_{1,j}$ .

Every finite disjunction of systems  $\bigvee_{j \in J} ((u_i, u'_i)_{i \in I}, \mu_{\mathcal{A}, \mathbb{G}}, \mu_{\mathcal{U}, j})$  where the equations/disequations are quadratic, the map  $\mu_{\mathcal{U}}$  is defined through a strict normal partitioned finite t-automaton  $\mathcal{A}$  over the labelling set  $\mathcal{B}(\text{Rat}(\mathbb{H}))$  and such that every over-solution of the disjunction is also a solution of the disjunction is said to be in *closed quadratic normal form*.

## 5 Equations over $\mathbb{H}_t$

### 5.1 t-equations

A system of t-equations is a family of ordered pairs

$$\mathcal{S} = (w_i, w'_i)_{i \in I} \quad (116)$$

where  $w_i, w'_i \in \mathbb{W}_t$ ,  $\gamma(w_i) = \gamma(w'_i) \neq \emptyset$ . A *solution* of  $\mathcal{S}$  is any *AB*-homomorphism  $\psi_t : \mathbb{W}_t \rightarrow \mathbb{H}_t$  such that, for every  $i \in I$

$$\psi_t(w_i) = \psi_t(w'_i). \quad (117)$$

Notice that here, the rational constraints are replaced by the even more restrictive conditions that define the notion of *AB*-homomorphism: beside preservation of  $\mu$  the map  $\psi_t$  must also preserve  $\mathbb{I}$ ,  $\gamma$  and  $\delta$ .

### 5.2 From $\mathbb{G}$ -equations to t-equations

Let us start with a system of equations with rational constraints, over  $\mathbb{G}$ , which is in quadratic normal form (see Proposition 3):

$$((u_i, u'_i)_{i \in I}, \mu_{\mathcal{A}, \mathbb{G}}, \mu_{\mathcal{U}}) \quad (118)$$

We suppose  $I = [1, n]$ , we denote by  $U_{i,1}$  (resp.  $U_{i,2}, U_{i,3}$ ) the unique letter of  $u_i$  (resp. the first, second letter of  $u'_i$ ). therefore, the equations of  $\mathcal{S}$  take the form

$$E_i : (U_{i,1}, U_{i,2}U_{i,3}) \text{ for all } 1 \leq i \leq n \quad (119)$$

We define here a reduction of the satisfiability problem for such systems to the satisfiability problem for systems of t-equations. The leading idea is simply that, since  $\pi_G : \text{Red}(\mathbb{H}, t) / \sim \rightarrow \mathbb{G}$  is a bijection, every solution in  $\mathbb{G}$  corresponds to a map into  $\mathbb{H}_t$ . Nevertheless the product in  $\mathbb{G}$  corresponds to a somewhat complicated operation over  $\text{Red}(\mathbb{H}, t) / \sim$  that we must deal with. Let us consider the alphabets  $\mathcal{V}_0 := I \times [1, 3] \times [1, 9]$  and the alphabet  $\mathcal{W}$  constructed from this  $\mathcal{V}_0$  in §3.6. We consider all the vectors  $(W_{i,j,k})$  where  $1 \leq i \leq n, 1 \leq j \leq 3, 1 \leq k \leq 9$

of elements of  $\mathcal{W} \cup \{1\}$  and all triple  $(e_{i,1,2}, e_{i,2,3}, e_{i,3,1}) \in (A \cup B)^3$  such that:

$$p_1(W_{i,j,k}) = (i, j, k) \in \mathcal{V}_0 \quad \text{for } W_{i,j,k} \neq 1 \quad (120)$$

$$\gamma\left(\prod_{k=1}^9 W_{i,j,k}\right) = (1, H, b, 1, 1) \quad \text{for some } b \in \{0, 1\} \quad (121)$$

$$\mu_1\left(\prod_{k=1}^9 W_{i,j,k}\right) = \mu_{\mathcal{U}}(U_{i,j}) \quad (122)$$

$$W_{i,2,k}, W_{i,3,10-k} \in \hat{\mathcal{W}} \cup \{1\} \quad \text{for } 6 \leq k \leq 9 \quad (123)$$

$$\gamma\left(\prod_{k=1}^4 W_{i,1,k}\right) = \gamma\left(\prod_{k=1}^4 W_{i,2,k}\right) \quad (124)$$

$$\gamma\left(\prod_{k=6}^9 W_{i,2,k}\right) = \gamma\left(\prod_{k=6}^9 \overline{W}_{i,3,10-k}\right) \quad (125)$$

$$\gamma\left(\prod_{k=6}^9 W_{i,1,k}\right) = \gamma\left(\prod_{k=6}^9 W_{i,3,k}\right) \quad (126)$$

$$W_{i,j,5} \in \mathcal{W} \wedge \gamma(W_{i,j,5}) \text{ is a H-type} \quad (127)$$

$$e_{i,1,2} \in \text{Gi}(W_{i,1,5}) = \text{Gi}(W_{i,2,5}) \quad (128)$$

$$e_{i,2,3} \in \text{Ge}(W_{i,2,5}) = \text{Gi}(W_{i,3,5}) \quad (129)$$

$$e_{i,3,1} \in \text{Ge}(W_{i,3,5}) = \text{Ge}(W_{i,1,5}). \quad (130)$$

A vector  $(\mathbf{W}, \mathbf{e})$  fulfilling all the properties (120-130) is called an *admissible* vector. For every admissible vector  $(\mathbf{W}, \mathbf{e})$  we define the following equations:

$$\left(\prod_{k=1}^9 W_{i,j,k}, \quad \prod_{k=1}^9 W_{i',j',k}\right) \quad \text{if } U_{i,j} = U_{i',j'} \quad (131)$$

$$(W_{i,1,1}W_{i,1,2}W_{i,1,3}W_{i,1,4}e_{i,1,2}, \quad W_{i,2,1}W_{i,2,2}W_{i,2,3}W_{i,2,4}) \quad (132)$$

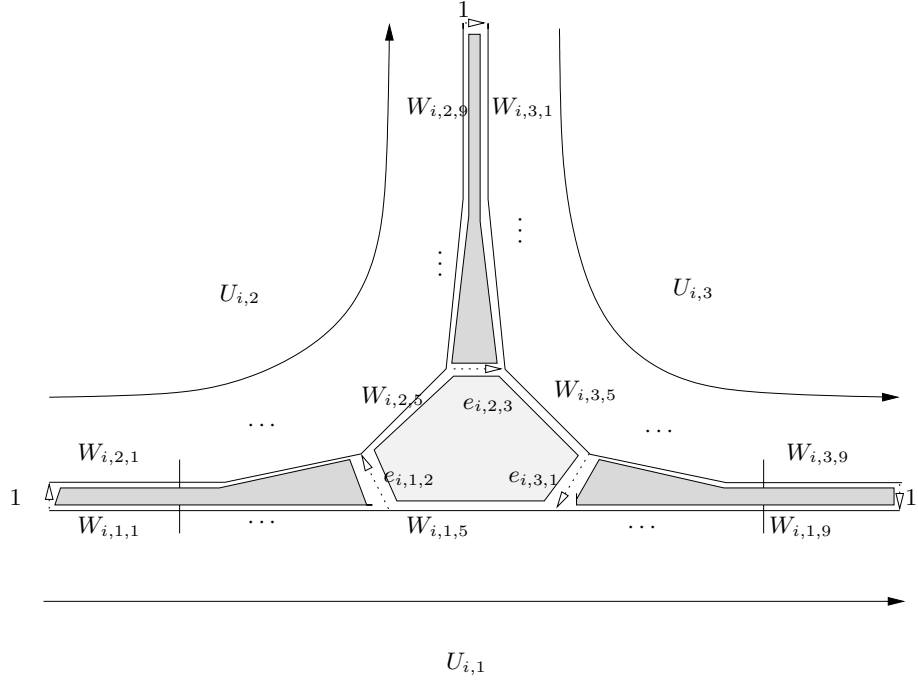
$$(W_{i,2,6}W_{i,2,7}W_{i,2,8}W_{i,2,9}, \quad e_{i,2,3}\overline{W}_{i,3,4}\overline{W}_{i,3,3}\overline{W}_{i,3,2}\overline{W}_{i,3,1}) \quad (133)$$

$$(W_{i,1,6}W_{i,1,7}W_{i,1,8}W_{i,1,9}, \quad e_{i,3,1}W_{i,3,6}W_{i,3,7}W_{i,3,8}W_{i,3,9}) \quad (134)$$

$$(W_{i,1,5}, \quad e_{i,1,2}W_{i,2,5}e_{i,2,3}W_{i,3,5}e_{i,3,1}) \quad (135)$$

for all  $1 \leq i, i' \leq n, 1 \leq j, j' \leq 3$ . Equations (132-135) correspond to a decomposition of the planar diagram associated with the relation  $U_{i,1} \approx U_{i,2}U_{i,3}$  into four pieces, as indicated on Figure 8. Equation (131) expresses the fact that some variables from  $\mathcal{U}$  are common to several equations of  $\mathcal{S}$ .

We denote by  $\mathcal{S}_t(\mathcal{S}, \mathbf{W}, \mathbf{e})$  the sequence of equations (131-134) and by  $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, \mathbf{e})$  the sequence of equations (135). For every  $(i, j) \in [1, n] \times [1, 3]$  we denote by  $\overline{i}, \overline{j}$  the smallest pair such that  $U_{i,j} = U_{\overline{i}, \overline{j}}$ . By  $\sigma_{\mathbf{W}, \mathbf{e}} : \mathcal{U}^* \rightarrow \mathbb{W}$  we denote the unique



**Fig. 8.** Equation cut into 4 pieces

monoid-homomorphism such that,

$$\sigma_{\mathbf{W},e}(U_{i,j}) = \prod_{k=1}^9 W_{i,j,k}.$$

Notice that, by the conditions imposed through the notion of “admissible vector”, the equations of  $\mathcal{S}_t(\mathcal{S}, \mathbf{W}, e)$  are really t-equations, while some of the righthand-sides of the equations of  $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, e)$  might have an empty image by  $\gamma$ .

**Lemma 19.** *Let  $\mathcal{S} = ((E_i)_{1 \leq i \leq n}, \mu_{A, \mathbb{G}}, \mu_U)$  be a system of equations over  $\mathbb{G}$ , with rational constraint. Let us suppose that  $\mathcal{S}$  is in normal form. A monoid homomorphism*

$$\sigma : \mathcal{U}^* \rightarrow \mathbb{G}$$

*is a solution of  $\mathcal{S}$  if and only if, there exists an admissible choice  $(\mathbf{W}, e)$  of variables of  $\mathcal{W}_t$  and elements of  $A \cup B$  and an AB-homomorphism*

$$\sigma_t : \mathcal{W}_t \rightarrow \mathbb{H}_t$$

*solving both systems  $\mathcal{S}_t(\mathcal{S}, \mathbf{W}, e)$  and  $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, e)$ , such that*

$$\sigma = \sigma_{\mathbf{W},e} \circ \sigma_t \circ \bar{\pi}_{\mathbb{G}}.$$

(We denote by  $\bar{\pi}_{\mathbb{G}} : \mathbb{H}_t \rightarrow \mathbb{G}$  the canonical projection; see Figure 9). We prove

$$\begin{array}{ccc}
 \mathcal{U}^* & \xrightarrow{\sigma_{\mathbf{W},e}} & \mathbb{W}_t \\
 \sigma \downarrow & & \downarrow \\
 \mathbb{G} & \xleftarrow{\bar{\pi}_{\mathbb{G}}} & \mathbb{H}_t
 \end{array}$$

**Fig. 9.** Lemma 19

this lemma in the following two subsections.

**From  $\mathbb{G}$ -solutions to  $\mathbf{t}$ -solutions** Let  $\sigma : \mathcal{U}^* \rightarrow \mathbb{G}$  be a monoid homomorphism solving the system  $\mathcal{S}$ . Let us fix some equation from  $\mathcal{S}$ , i.e. some integer  $1 \leq i \leq n$ . Let us construct the vectors  $(W_{i,*,*}), (e_{i,*,*})$  corresponding to this equation. Let us choose, for every  $j \in [1, 3]$ , some  $s_{i,j} \in \text{Red}(\mathbb{H}, t)$  such that:

$$\sigma(U_{i,j}) = \pi_G(s_{i,j}).$$

Let us consider decompositions of the form (5) for  $s_{i,2}, s_{i,3}$ :

$$s_{i,2} = h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_\lambda} h_\lambda \cdots t^{\alpha_\ell} h_\ell, \quad (136)$$

$$s_{i,3} = k_0 t^{\beta_1} k_1 \cdots t^{\beta_\rho} k_\rho \cdots t^{\beta_m} k_m. \quad (137)$$

We know that  $s_{i,1} \approx s_{i,2} s_{i,3}$ . There exist some integers  $\lambda \in [1, \ell], \rho \in [1, m]$  such that

$$\alpha_\lambda + \beta_\rho = 0, \quad (138)$$

$$t^{\alpha_\lambda} h_\lambda \cdots t^{\alpha_\ell} h_\ell \cdot k_0 t^{\beta_1} k_1 \cdots t^{\beta_\rho} \approx e_{i,2,3} \in A(\beta_\rho), \quad (139)$$

$$h_0 \cdots t^{\alpha_{\lambda-1}} (h_{\lambda-1} e_{i,2,3} k_\rho) t^{\beta_{\rho+1}} \cdots t^{\beta_m} k_m \in \text{Red}(\mathbb{H}, t), \quad (140)$$

We include in the above notation the following “degenerated” cases:

- [Left-degenerated case]:  $\lambda = 1$ ; then  $h_0 \cdots t^{\alpha_{\lambda-1}}$  must be understood as 1
- [Right-degenerated case]:  $\rho = m$ ; then  $t^{\beta_{\rho+1}} \cdots t^{\beta_m} k_m$  must be understood as 1,
- [Middle-degenerated case]:  $\alpha_\ell + \beta_1 \neq 0$  or ( $\alpha_\ell + \beta_1 = 0$  and  $h_\ell \cdot k_0 \notin A(\beta_1)$ ); we then consider that  $\lambda = \ell + 1, \rho = 0, e_{i,2,3} = 1$ . Equality (138) disappears, (139) becomes the trivial equation  $1 = 1$  while (140) remains valid.
- [LM-degenerated case]:  $\ell = 0$ ;

We then consider that  $\lambda = \rho = 0, e_{i,2,3} = 1$  and equation (139) becomes the trivial equation  $1 = 1$ . The lefthand-side of assertion (140) consists just of  $s_{i,3}$ .

• [MR-degenerated case]:  $m = 0$ ;

Same notation as for LM. The l.h.s. of (140) consists just of  $s_{i,2}$ .

Notice that these cases are not disjoint; in particular, when  $\ell = m = 0$  the three kinds of degeneracy occur simultaneously. Each kind of degeneracy can be visualized on Figure 10 as one of the three triangular pieces consisting of a trivial relation.

Let us consider the following factors of the reduced sequences  $s_{i,2}, s_{i,3}$ :

$$P_{i,2} = h_0 \cdots t^{\alpha_\lambda - 1}, \quad M_{i,2} = h_{\lambda-1}, \quad S_{i,2} = t^{\alpha_\lambda} \cdots t^{\alpha_\ell} h_\ell,$$

$$P_{i,3} = k_0 \cdots t^{\beta_\rho}, \quad M_{i,3} = k_\rho, \quad S_{i,3} = t^{\beta_{\rho+1}} \cdots t^{\beta_m} k_m.$$

Since  $s_{i,1} \approx s_{i,2}s_{i,3} \approx P_{i,2}(M_{i,2}e_{i,2,3}M_{i,3})S_{i,3}$  and  $s_{i,1}, P_{i,2}(M_{i,2}e_{i,2,3}M_{i,3})S_{i,3}$  are reduced sequences, by Lemma 1 we get:

$$s_{i,1} \sim P_{i,2}(M_{i,2}e_{i,2,3}M_{i,3})S_{i,3}.$$

**Case 1**[standard case]  $\lambda \in [2, \ell], \rho \in [1, m-1]$ .

There must exist  $P_{i,1}, S_{i,1} \in \text{Red}(\mathbb{H}, t), M_{i,1} \in \mathbb{H}$  and connecting elements  $e_{i,1,2} \in B(\alpha_{\lambda-1}), e_{i,2,3} \in A(\alpha_\lambda)$  such that:

$$P_{i,1}e_{i,1,2} \sim P_{i,2}, \tag{141}$$

$$e_{i,1,2}M_{i,2}e_{i,2,3}M_{i,3}e_{i,3,1} =_{\mathbb{H}} M_{i,1} \tag{142}$$

$$e_{i,3,1}S_{i,1} \sim S_{i,3}, \tag{143}$$

while relation (139) can be rewritten as:

$$S_{i,2} \sim e_{i,2,3}\mathbb{I}_t(P_{i,3}), \tag{144}$$

see Figure 10. Let  $\pi_T : \mathbb{H} * \{t, \bar{t}\}^* \rightarrow \{t, \bar{t}\}^*$  be the natural projection. By (141), (resp. (143), (144)) we know that

$$\pi_T(P_{i,1}) = \pi_T(P_{i,2}), \quad \pi_T(S_{i,1}) = \pi_T(S_{i,3}), \quad \pi_T(S_{i,2}) = \pi_T(\mathbb{I}_t(P_{i,3})).$$

Hence the t-automaton  $\mathcal{R}_6$  has computations of the following forms:

$$(1, H) \xrightarrow{P_{i,1}} q_{i,1} \xrightarrow{M_{i,1}} r_{i,1} \xrightarrow{S_{i,1}} (1, 1) \tag{145}$$

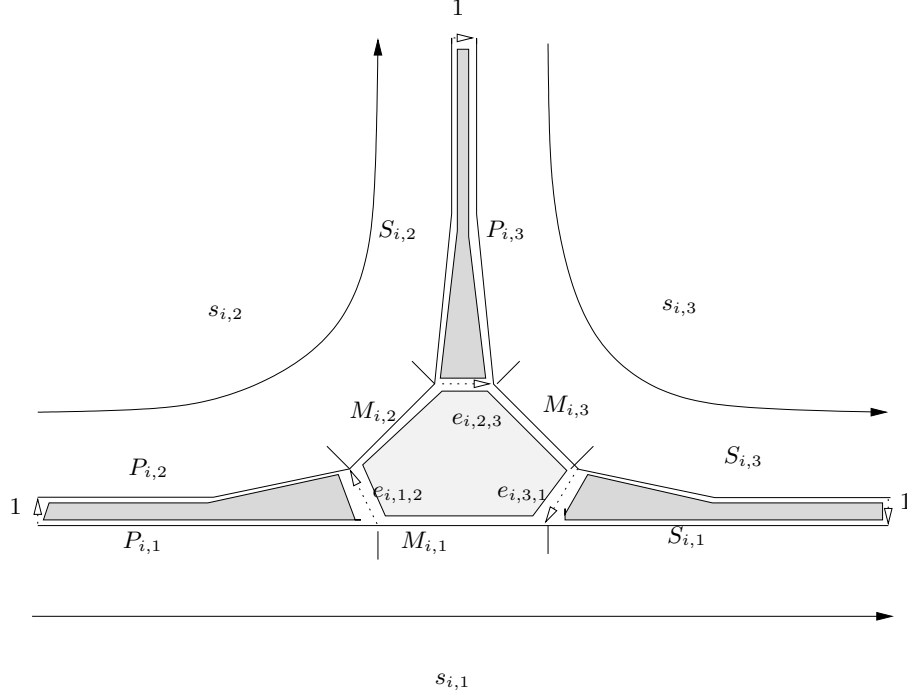
$$(1, H) \xrightarrow{P_{i,2}} q_{i,1} \xrightarrow{M_{i,2}} r_{i,2} \xrightarrow{S_{i,2}} (1, 1) \tag{146}$$

$$(1, H) \xrightarrow{P_{i,3}} \mathbb{I}_{\mathcal{R}}(r_{i,2}) \xrightarrow{M_{i,3}} r_{i,1} \xrightarrow{S_{i,3}} (1, 1). \tag{147}$$

Since  $q_{i,1} \neq (1, 1)$ , an easy inspection of the automaton  $\mathcal{R}_6$  shows that the computation  $(1, H) \xrightarrow{P_{i,1}} q_{i,1}$  can be factored into four subcomputations

$$(1, H) = q_{i,1,0} \xrightarrow{P_{i,1,1}} q_{i,1,1} \xrightarrow{P_{i,1,2}} q_{i,1,2} \xrightarrow{P_{i,1,3}} q_{i,1,3} \xrightarrow{P_{i,1,4}} q_{i,1,4} = q_{i,1} \tag{148}$$





**Fig. 10.** Cutting the solution into three factors

such that each  $(q_{i,1,k}, |||P_{i,1,k+1}|||, q_{i,1,k+1})$  is an edge of  $\mathcal{R}$ . Any decomposition having this property w.r.t. its projection on  $\mathcal{R}$  will be called  $\mathcal{R}$ -compatible. Similarly the computations  $r_{i,1} \xrightarrow{S_{i,1}} (1, 1)$  ( resp.  $r_{i,2} \xrightarrow{S_{i,2}} (1, 1)$ ) have  $\mathcal{R}$ -compatible decompositions:

$$q_{i,1,5} \xrightarrow{P_{i,1,6}} q_{i,1,6} \xrightarrow{P_{i,1,7}} q_{i,1,7} \xrightarrow{P_{i,1,8}} q_{i,1,8} \xrightarrow{P_{i,1,9}} q_{i,1,9} = (1, 1), \quad (149)$$

$$q_{i,2,5} \xrightarrow{P_{i,2,6}} q_{i,2,6} \xrightarrow{P_{i,2,7}} q_{i,2,7} \xrightarrow{P_{i,2,8}} q_{i,2,8} \xrightarrow{P_{i,2,9}} q_{i,2,9} = (1, 1). \quad (150)$$

Combining decomposition (148) with equation (141), (149) with (143), (150) with (144), we get the three  $\mathcal{R}$ -compatible decompositions:

$$(1, H) = q_{i,1,0} \xrightarrow{P_{i,2,1}} q_{i,1,1} \xrightarrow{P_{i,2,2}} q_{i,1,2} \xrightarrow{P_{i,2,3}} q_{i,1,3} \xrightarrow{P_{i,2,4}} q_{i,1,4} = q_{i,1} \quad (151)$$

$$r_{i,1} = q_{i,1,5} \xrightarrow{P_{i,3,6}} q_{i,1,6} \xrightarrow{P_{i,3,7}} q_{i,1,7} \xrightarrow{P_{i,3,8}} q_{i,1,8} \xrightarrow{P_{i,3,9}} q_{i,1,9} = (1, 1), \quad (152)$$

$$\begin{aligned} (1, H) &= \mathbb{I}(q_{i,2,9}) = q_{i,3,0} \xrightarrow{P_{i,3,1}} \mathbb{I}(q_{i,2,8}) = q_{i,3,1} \xrightarrow{P_{i,3,2}} \\ &\mathbb{I}(q_{i,2,7}) = q_{i,3,2} \xrightarrow{P_{i,3,3}} \mathbb{I}(q_{i,2,6}) = q_{i,3,3} \xrightarrow{P_{i,3,4}} \mathbb{I}(r_{i,2}) = q_{i,3,4}. \end{aligned} \quad (153)$$

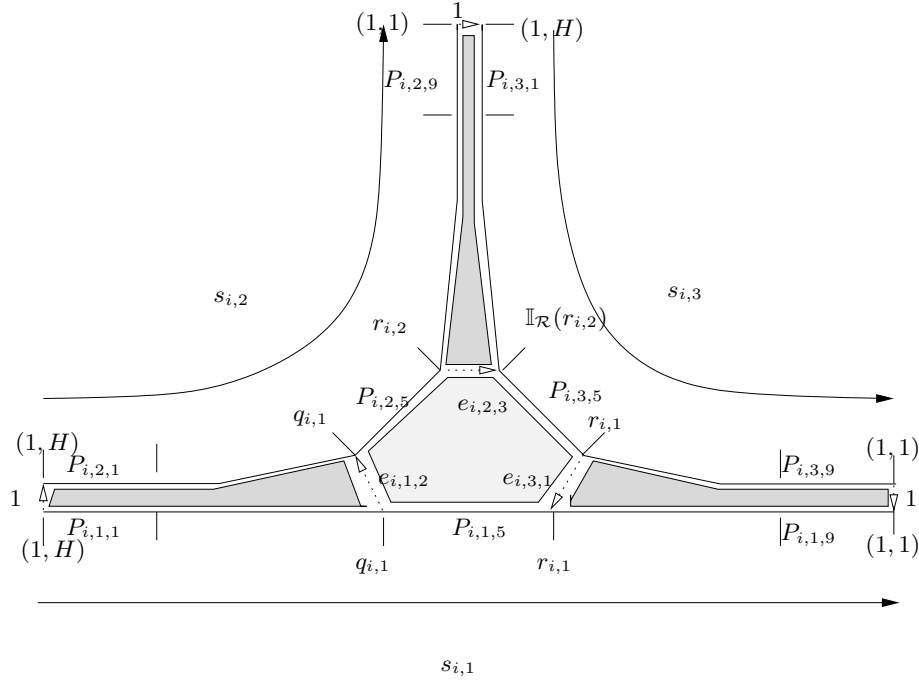
Finally, we define  $P_{i,j,5} := M_{i,j}$ . We summarize on Figure 11 the above decompositions and relations. Let us extract from these the vector  $(\mathbf{W}, e)$  and the AB-homomorphism  $\sigma_t$ :

- we choose for  $W_{i,j,k}$  a letter from  $\mathcal{W}$  with  $\gamma(W_{i,j,k}) = (q_{i,j,k-1}, \|P_{i,j,k}\|, q_{i,j,k})$  and which can be mapped by some AB-homomorphism on the t-sequence  $P_{i,j,k}$ .
- we define  $\sigma_t(W_{i,j,k}) := [P_{i,j,k}]_{\sim}$ ; the choice of the letters  $W_{i,j,k}$  together with Lemma 11 imply that any extension of  $\sigma_t$  on the alphabet  $\mathcal{W}_t$  (respecting conditions 1-5 of Lemma 11), will possess a unique extension as an AB-homomorphism from  $\mathbb{W}_t$  to  $\mathbb{H}_t$ .

One can check that  $(\mathbf{W}, e)$  is an admissible vector, that  $\sigma_t$  solves the systems of equations  $\mathcal{S}_t(\mathcal{S}, \mathbf{W}, e)$  and  $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, e)$  and that

$$\sigma = \sigma_{\mathbf{W}, e} \circ \sigma_t \circ \bar{\pi}_{\mathbb{G}}.$$

We indicate now how these arguments must be adapted to the degenerated



**Fig. 11.** Cutting the solution into nine factors

cases.

**Case 2**[L]:  $\lambda = 1$ .

We take:  $P_{i,2} = P_{i,1} = 1$ ,  $e_{i,1,2} = 1$  and, accordingly

$$P_{i,2,k} = P_{i,1,k} = 1, \quad W_{i,2,k} = W_{i,1,k} = 1$$

for  $1 \leq k \leq 4$ .

**Case 3[R]:**  $\rho = m$ .

We take:  $S_{i,3} = S_{i,1} = 1$ ,  $e_{i,3,1} = 1$  and, accordingly

$$S_{i,3,k} = S_{i,1,k} = 1, \quad W_{i,3,k} = W_{i,1,k} = 1$$

for  $6 \leq k \leq 9$ .

**Case 4[M]:**  $\alpha_\ell + \beta_1 \neq 0$  or  $(\alpha_\ell + \beta_1 = 0 \text{ and } h_\ell \cdot k_0 \notin A(\beta_1))$ .

We take:  $S_{i,2} = P_{i,3} = 1$ ,  $e_{i,2,3} = 1$  and, accordingly

$$S_{i,2,k} = P_{i,3,10-k} = 1, \quad W_{i,2,k} = W_{i,3,10-k} = 1$$

for  $6 \leq k \leq 9$ .

**Case 5[LM]:**  $\ell = 0$ .

We choose all the special values chosen in Case 2 and Case 4 i.e.  $P_{i,2} = P_{i,1} = S_{i,2} = P_{i,3} = 1$ ,  $e_{i,1,2} = e_{i,2,3} = 1$  and the resulting choices for  $W_{i,*,*}$ .

**Case 6[MR]:**  $m = 0$ .

We choose all the special values chosen in Case 3 and Case 4.

**From t-solutions to G-solutions** Let  $\sigma_t : \mathbb{W}_t \rightarrow \mathbb{H}_t$  be an  $AB$ -homomorphism solving both systems  $\mathcal{S}_t(\mathcal{S}, \mathbf{W}, \mathbf{e})$  and  $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, \mathbf{e})$ .

1- Let us show that, for every  $i \in [1, n]$ ,

$$\sigma_t(\sigma_{\mathbf{W}, \mathbf{e}}(U_{i,1})) \approx \sigma_t(\sigma_{\mathbf{W}, \mathbf{e}}(U_{i,2}U_{i,3})). \quad (154)$$

Let us fix such an integer  $i$ . The conjunction of equivalences (132-135), implies that

$$\sigma_t\left(\prod_{k=1}^9 W_{i,1,k}\right) \approx \sigma_t\left(\prod_{k=1}^9 W_{i,2,k} \prod_{k=1}^9 W_{i,3,k}\right).$$

(Figure 8 gives a decomposition of the Van-Kampen diagram corresponding to the above equivalence into four diagrams corresponding to (132-135)). Using equation (131) we get:

$$\sigma_t\left(\prod_{k=1}^9 W_{\overline{1,1},k}\right) \approx \sigma_t\left(\prod_{k=1}^9 W_{\overline{1,2},k} \prod_{k=1}^9 W_{\overline{1,3},k}\right).$$

Taking into account the definition of  $\sigma_{\mathbf{W}, \mathbf{e}}$  and the fact that  $\sigma_t$  is a monoid-homomorphism, we get a proof of (154).

2- Let us show that, for every  $i \in [1, n]$

$$\mu_{\mathcal{A}, \mathbb{G}}(\pi_{\mathbb{G}}(\sigma_t(\sigma_{\mathbf{W}, \mathbf{e}}(U_{i,j})))) = \mu_{\mathcal{U}}(U_{i,j}).$$

By definition (14) this means that the value of

$$\mu_{\mathcal{A}, 1}((1, H, b, 1, 1), \sigma_t(\sigma_{\mathbf{W}, \mathbf{e}}(U_{i,j}))), \quad (155)$$

where  $b = \|\sigma_t(\sigma_{\mathbf{W},e}(U_{i,j}))\|$  is equal to  $\mu_{\mathcal{U}}(U_{i,j})$ .  
We first remark that

$$\begin{aligned}\sigma_t(\sigma_{\mathbf{W},e}(U_{i,j})) &= \sigma_t(\prod_{k=1}^9 U_{i,j,k}) \text{ by definition of } \sigma_{\mathbf{W},e} \\ &= \sigma_t(\prod_{k=1}^9 U_{i,j,k}) \text{ by condition (131)}\end{aligned}\quad (156)$$

As  $\sigma_t$  is an AB-homomorphism

$$\mu_{\mathcal{A},1}((1, H, b, 1, 1), \sigma_t(\prod_{k=1}^9 U_{i,j,k})) = \mu_{\mathcal{A},1}((1, H, b, 1, 1), \prod_{k=1}^9 U_{i,j,k}). \quad (157)$$

Using now the conditions defining the notion of admissible vector we get:

$$\begin{aligned}\mu_{\mathcal{A},1}((1, H, b, 1, 1), \prod_{k=1}^9 U_{i,j,k}) &= \mu_{\mathcal{A},1}(\prod_{k=1}^9 U_{i,j,k}) \text{ by (121)} \\ &= \mu_{\mathcal{U}}(U_{i,j}) \text{ by (122)}\end{aligned}\quad (158)$$

Putting together (156)(157)(158), we obtain that the value of term (155) is exactly  $\mu_{\mathcal{U}}(U_{i,j})$ , as required.

## 6 Equations over $\mathbb{W}$

We suppose here that a system of equations with rational constraints over  $\mathbb{G}$  is fixed. Thus the AB-algebras  $\mathbb{W}$  and  $\mathbb{H}_t$  are completely defined (from the variable alphabet of the system and the t-automaton expressing the constraints). Given an  $H$ -involution  $\mathbb{I}'$  (this notion is defined at the end of subsubsection 3.6) we abbreviate as  $(\mathbb{W}, \mathbb{I}')$  the AB-algebra obtained from the AB-algebra  $\mathbb{W}$  by replacing the standard involution  $\mathbb{I}$  by  $\mathbb{I}'$  (see Lemma 10, point (4)).

### 6.1 $\mathbb{W}$ -equations

A system of  $\mathbb{W}$ -equations is a family of ordered pairs together with an involution:

$$\mathcal{S} = ((w_i, w'_i)_{i \in I}, \mathbb{I}') \quad (159)$$

where  $w_i, w'_i \in \mathbb{W}_t, \gamma(w_i) = \gamma(w'_i) \neq \emptyset, \mathbb{I}' \in \mathcal{I}$ .

A solution of  $\mathcal{S}$  is any AB-homomorphism  $\sigma_{\mathbb{W}} : (\mathbb{W}_t, \mathbb{I}) \rightarrow (\mathbb{W}_t, \mathbb{I}')$  such that, for every  $i \in I$

$$\sigma_{\mathbb{W}}(w_i) = \sigma_{\mathbb{W}}(w'_i). \quad (160)$$

### 6.2 From t-equations to $\mathbb{W}$ -equations

#### From t-solutions to $\mathbb{W}$ -solutions

**Lemma 20 (factorisation of t-solutions).** *Let  $\mathcal{S} = ((w_i, w'_i)_{1 \leq i \leq n})$  be a system of t-equations of the form (116). Let us suppose that  $\sigma_t : \mathbb{W}_t \rightarrow \mathbb{H}_t$  is an AB-homomorphism solving the system  $\mathcal{S}$ . Then there exists an involution  $\mathbb{I}' \in \mathcal{I}$  and AB-homomorphisms*

$$\sigma_{\mathbb{W}} : (\mathbb{W}_t, \mathbb{I}) \rightarrow (\mathbb{W}_t, \mathbb{I}'), \quad \psi_t : (\mathbb{W}_t, \mathbb{I}') \rightarrow (\mathbb{H}_t, \mathbb{I}_t)$$

such that,  $\sigma_t = \sigma_{\mathbb{W}} \circ \psi_t$  and

$$\sigma_{\mathbb{W}}(w_i) = \sigma_{\mathbb{W}}(w'_i) \text{ for all } 1 \leq i \leq n.$$

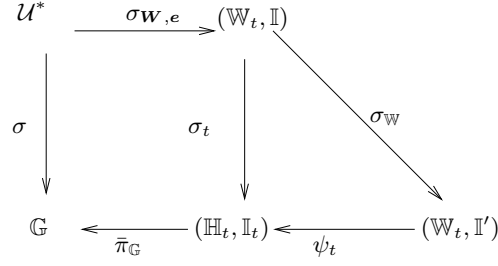
In other words: every solution in  $\mathbb{H}_t$  of a system of t-equations factorizes through a solution in  $\mathbb{W}_t$  of the same system of equations, with an involution in  $\mathcal{I}$ .

This factorization lemma is obtained via the more technical Lemma 21 below. For every  $w \in \mathbb{W}$  let us note

$$A(w) := \text{Card}\{W \in \check{\mathcal{W}} \mid |w|_W \neq 0\} + \frac{1}{2} \text{Card}\{W \in \hat{\mathcal{W}} \mid |w|_{W, \bar{W}} \neq 0\}.$$

**Lemma 21.** *Let  $K_0$  be an integer such that  $K_0 < \text{Card}(\mathcal{V}_0)$  and  $((w_i, w'_i)_{1 \leq i \leq n+m})$  be a sequence of pairs  $(w_i, w'_i) \in \mathbb{W} \times \mathbb{W}$  such that  $\gamma(w_i) = \gamma(w'_i) \neq \emptyset$ . Let us suppose that  $\lambda_i : (\mathbb{W}_t, \mathbb{I}) \rightarrow (\mathbb{W}_t, \mathbb{I})$  (for  $1 \leq i \leq n+m$ ) and  $\theta_t : (\mathbb{W}_t, \mathbb{I}) \rightarrow (\mathbb{H}_t, \mathbb{I}_t)$  are AB-homomorphisms such that*

$$\theta_t(\lambda_i(w_i)) = \theta_t(\lambda_i(w'_i)) \text{ for all } 1 \leq i \leq n+m,$$



**Fig. 12.** Lemma 20

$$\lambda_i = \lambda_j \text{ for all } 1 \leq i \leq n, 1 \leq j \leq n,$$

$$A(\prod_{i=1}^{n+m} \lambda_i(w_i w'_i)) \leq K_0.$$

Then there exists an involution  $\mathbb{I}' \in \mathcal{I}$  and AB homomorphisms

$$\lambda'_i : (\mathbb{W}_t, \mathbb{I}) \rightarrow (\mathbb{W}_t, \mathbb{I}'), \quad \theta'_t : (\mathbb{W}_t, \mathbb{I}') \rightarrow (\mathbb{H}_t, \mathbb{I}_t)$$

such that,

$$\lambda_i \circ \theta_t = \lambda'_i \circ \theta'_t, \quad (161)$$

$$\lambda'_i(w_i) = \lambda'_i(w'_i) \text{ for all } 1 \leq i \leq n+m, \quad (162)$$

$$\lambda'_i = \lambda'_j \text{ for all } 1 \leq i \leq n, 1 \leq j \leq n. \quad (163)$$

**Proof:** Let  $\mathcal{S} = ((w_i, w'_i))_{1 \leq i \leq n+m}$  be a sequence of pairs  $(w_i, w'_i) \in \mathbb{W}_t \times \mathbb{W}_t$  such that  $\gamma(w_i) = \gamma(w'_i)$  and let  $\boldsymbol{\lambda} = (\lambda_i)_{1 \leq i \leq n+m}$  be a sequence of AB-homomorphisms from  $\mathbb{W}_t$  to  $\mathbb{W}_t$ .

*Distinguishing pair* For every  $i \in [1, n+m]$  we define  $\equiv_i$  as the least monoid congruence over  $\mathbb{W}$  containing  $\{(\lambda_j(w_j), \lambda_j(w'_j)) \mid i+1 \leq j \leq n+m\}$ . For every  $i \in [1, n+m]$  let us consider some decompositions

$$\lambda_i(w_i) = P_i \cdot S_i, \quad \lambda_i(w'_i) = P'_i \cdot S'_i \quad (164)$$

such that  $P_i \equiv_i P'_i$ , and this choice of the decomposition (164) minimizes the integer

$$\Delta(P_i, S_i, P'_i, S'_i, \theta_t).$$

(this integer was defined by equation (69)). Such a  $(P_i, P'_i)$  is called a *distinguishing pair* for  $(\lambda_i(w_i), \lambda_i(w'_i))$  and we denote by

$$\Delta_i(\mathcal{S}, \boldsymbol{\lambda}, \theta_t)$$

the corresponding value of  $\Delta(P_i, S_i, P'_i, S'_i, \theta_t)$ .

*Size* We call *size* of the triple  $(\mathcal{S}, \lambda, \theta_t)$  the multiset of natural integers:

$$\|(\mathcal{S}, \lambda, \theta_t)\| = \{\{\Delta_1(\mathcal{S}, \lambda, \theta_t), \dots, \Delta_i(\mathcal{S}, \lambda, \theta_t), \dots, \Delta_{n+m}(\mathcal{S}, \lambda, \theta_t)\}\}. \quad (165)$$

For every  $w \in \mathbb{W}$  we use the notation

$$\begin{aligned} \text{Alph}(w) &:= \{W \in \hat{\mathcal{W}} \mid |w|_W \neq 0\} \cup \{W \in \hat{\mathcal{W}} \mid |w|_{W, \bar{W}} \neq 0\}, \\ w(\mathcal{S}, \lambda) &:= \prod_{i=1}^{n+m} \lambda_i(w_i w'_i), \\ \text{Alph}(\mathcal{S}, \lambda) &:= \text{Alph}(w(\mathcal{S}, \lambda)), \\ A(\mathcal{S}, \lambda) &:= A(w(\mathcal{S}, \lambda)). \end{aligned}$$

*Induction* Let us prove Lemma 21 by induction over  $\|(\mathcal{S}, \lambda, \theta_t)\|$ , with respect to the partial ordering over multisets of integers induced by the natural ordering over  $\mathbb{N}$  (it is known that this ordering is well-founded). Let  $(\mathcal{S}, \lambda, \theta_t)$  fulfill the hypothesis of the lemma.

**Case 1:** In this case we suppose that, for every  $i \in [1, n+m]$ , one of the two following situations occurs:

$$\lambda_i(w_i) \equiv_i \lambda_i(w'_i) \quad (166)$$

$$\lambda_i(w_i) = e_i W f_i, \quad \lambda_i(w'_i) = c_i^{-1} \bar{W} d_i^{-1} \quad (167)$$

for some  $W \in \hat{\mathcal{W}}$ ,  $(e_i, f_i), (d_i, c_i) \in (\text{Gi}(W), \text{Ge}(W))$ .

Let us consider the partition

$$\hat{\mathcal{W}} = \hat{\mathcal{W}}_0 \cup \mathcal{W}_1 \cup \bar{\mathcal{W}}_1, \quad \mathcal{W}_1 = \{W_1, \dots, W_p\}$$

where  $\mathcal{W}_1 \cup \bar{\mathcal{W}}_1$  is exactly the set of variables occurring in the equations of type (167). We can modify the system  $\mathcal{S}$  in such a way that in every equation of type (167),  $e_i = f_i = 1$ , with preservation of the hypothesis of the lemma (with the same morphisms) and also of the size of  $(\mathcal{S}, \lambda, \theta_t)$ . We can also suppose that  $\mathcal{W}_1$  is exactly the set of lefthand-sides of the equations (167). For every  $k \in [1, p]$ , let  $(W_k, c_{i(k)}^{-1} \bar{W}_k d_{i(k)}^{-1})$  be the equation of type (167) with smallest index,  $i(k) \in [1, n+m]$ , such that  $\lambda_{i(k)}(w_{i(k)}) = W_k$ . We thus have  $\lambda_{i(k)}(w'_{i(k)}) = c_{i(k)}^{-1} \bar{W}_k d_{i(k)}^{-1}$ . Let us notice that, since  $\theta_t$  is an  $AB$ -homomorphism and  $\theta_t(W_k) = \theta_t(\lambda_{i(k)}(w_{i(k)})) = \theta_t(\lambda_{i(k)}(w'_{i(k)})) = \theta_t(c_{i(k)}^{-1} \bar{W}_k d_{i(k)}^{-1})$  we know that

$$\theta_t(\bar{W}_k) = \theta_t(c_{i(k)} W_k d_{i(k)}). \quad (168)$$

As  $\theta_t$  preserves  $\delta$ , for every  $e \in \text{Gi}(W_k), e' \in \text{Ge}(W_k)$ ,

$$e \bar{W}_k = \bar{W}_k e' \Leftrightarrow e c_{i(k)} W_k d_{i(k)} = c_{i(k)} W_k d_{i(k)} e'. \quad (169)$$

It follows that there exists a unique monoid homomorphism  $\lambda' : \mathbb{W} \rightarrow \mathbb{W}$  fulfilling:

$$\lambda'(e) = e \quad \text{for all } e \in \iota_A(A) \cup \iota_B(B) \quad (170)$$

$$\lambda'(W) = W \quad \text{for all } W \in \mathcal{W} - \mathcal{W}_1 \quad (171)$$

$$\lambda'(W_k) = W_k \quad \text{for all } 1 \leq k \leq p \quad (172)$$

$$\lambda'(\bar{W}_k) = c_{i(k)} W_k d_{i(k)} \quad \text{for all } 1 \leq k \leq p. \quad (173)$$

The involutory anti-isomorphism  $\mathbb{I}_t$  defined on  $\mathbb{H}_t$ , maps  $\theta_t(W_k)$  to  $\theta_t(c_{i(k)}W_kd_{i(k)})$  and  $\theta_t(\bar{W}_k)$  to  $\theta_t(c_{i(k)}^{-1}W_kd_{i(k)}^{-1})$ . The arguments used for proving points (1)(3)(4) of Lemma 10 show that the tuple  $(c_{i(1)}, d_{i(1)}, \dots, c_{i(k)}, d_{i(k)}, \dots, c_{i(p)}, d_{i(p)})$  fulfils the three conditions (76-77-78). Hence, by Lemma 10, there exists a unique involutive monoid anti-isomorphism  $\mathbb{I}' : \hat{\mathbb{W}} \rightarrow \hat{\mathbb{W}}$  such that

$$\mathbb{I}'(e) = e^{-1} \quad \text{for all } e \in \iota_A(A) \cup \iota_B(B) \quad (174)$$

$$\mathbb{I}'(W) = \mathbb{I}(W) \quad \text{for all } W \in \hat{\mathcal{W}}_0 \quad (175)$$

$$\mathbb{I}'(W_k) = c_{i(k)}W_kd_{i(k)} \quad \text{for all } 1 \leq k \leq p \quad (176)$$

$$\mathbb{I}'(\bar{W}_k) = c_{i(k)}^{-1}\bar{W}_kd_{i(k)}^{-1} \quad \text{for all } 1 \leq k \leq p. \quad (177)$$

and which makes  $\langle \mathbb{W}, \iota_A, \iota_B, \mathbb{I}', \gamma, \mu, \delta \rangle$  into an  $AB$ -algebra. Using (168), we can see that this involution  $\mathbb{I}'$  also meets condition (82) with the choice  $h_k := \theta_t(W_k)$ . Hence  $\mathbb{I}'$  belongs to the set  $\mathcal{I}$  (this set of “ $H$ -involutions” is defined at the end of §3.6). It is clear that  $\lambda'$  preserves  $\iota_A, \iota_B$ . The fact that

$$\mathbb{I} \circ \lambda' = \lambda' \circ \mathbb{I}' \quad (178)$$

can be checked over the generators of  $\mathbb{W}$ . The only non-trivial verification is for  $W = \bar{W}_k$ :

$$\begin{aligned} \lambda'(\mathbb{I}(\bar{W}_k)) &= \lambda'(W_k) = W_k \\ \mathbb{I}'(\lambda'(\bar{W}_k)) &= \mathbb{I}'(c_{i(k)}W_kd_{i(k)}) = d_{i(k)}^{-1}c_{i(k)}W_kd_{i(k)}c_{i(k)}^{-1}, \end{aligned}$$

and by condition (77), the righthand-side of this last equality is  $W_k$ . Thus (178) is established. The fact that  $\lambda'$  preserves  $\mu, \gamma, \delta$  is ensured by:

- the hypothesis that  $\theta_t$  does so,
- the fact that all the monoid generators  $W \in \mathcal{W}$  are mapped by  $\gamma$  into a singleton
- the fact that, for  $e \in \iota_A(A) \cup \iota_B(B)$ ,  $\gamma_t(e) = \gamma_{\mathbb{W}}(e)$ , and for all  $\theta \in \gamma(e)$ ,  $\mu_t(\theta, e) = \mu_{\mathbb{W}}(\theta, e)$ ,  $\delta_t(\theta, e) = \delta_{\mathbb{W}}(\theta, e)$ .

We have thus established that

$$\lambda' : (\mathbb{W}, \mathbb{I}) \rightarrow (\mathbb{W}, \mathbb{I}') \text{ is an } AB\text{-homomorphism.}$$

Let us define

$$\lambda'_i = \lambda_i \circ \lambda', \theta'_t = \theta_t.$$

As every  $\lambda'_i$  is a composite of two  $AB$ -homomorphisms, it is an  $AB$ -homomorphism from  $(\mathbb{W}_t, \mathbb{I})$  to  $(\mathbb{W}_t, \mathbb{I}')$ . By hypothesis,  $\theta_t : \mathbb{W}_t \rightarrow \mathbb{H}_t$  is a monoid-homomorphism which preserves  $\iota, \mu, \gamma, \delta$ . It is clear that  $\theta_t \circ \mathbb{I}$  is equal to  $\mathbb{I}' \circ \theta_t$  over  $\iota_A(A) \cup \iota_B(B) \cup \hat{\mathcal{W}}_0$ . Moreover

$$\mathbb{I}(\theta_t(W_k)) = \theta_t(\mathbb{I}(W_k)) = \theta_t(\bar{W}_k), \quad \text{while}$$

$$\theta_t(\mathbb{I}'(W_k)) = \theta_t(c_{i(k)}^{-1}W_kd_{i(k)}^{-1}).$$

But the hypothesis that  $\theta_t(\lambda_{i(k)}(w_{i(k)})) = \theta_t(\lambda_{i(k)}(w'_{i(k)}))$  ensures that  $\theta_t(\bar{W}_k) = \theta_t(c_{i(k)}^{-1}W_kd_{i(k)}^{-1})$ . We have established that

$$\theta_t : (\mathbb{W}_t, \mathbb{I}') \rightarrow (\mathbb{H}_t, \mathbb{I}_t) \text{ is an } AB\text{-homomorphism.}$$



Let us check now that  $(\lambda'_i, \theta'_t)$  fulfill conclusions (161),(162),(163) of the lemma. Let us show that

$$\theta_t = \lambda' \circ \theta_t. \quad (179)$$

The only non-trivial verification is for generators of the form  $\bar{W}_k$ : from (168) we get that  $\theta_t(\bar{W}_k) = \theta_t(\lambda'(\bar{W}_k))$ , which establishes (179). This equality (179) and the fact that  $\lambda'_i = \lambda_i \circ \lambda'$  prove (161).

Let  $1 \leq i \leq n + m$ . Suppose that  $(w_i, w'_i)$  is one of the pairs of the form (167) (recall we reduced to the case where  $e_i = f_i = 1$ ): there exists some  $k \in [1, p]$  such that

$$\lambda_i(w_i) = W_k, \quad \lambda_i(w'_i) = c_i^{-1} \bar{W}_k d_i^{-1}$$

Therefore

$$\lambda'(\lambda_i(w_i)) = W_k, \quad \lambda'(\lambda_i(w'_i)) = c_i^{-1} c_{i(k)} W_k d_{i(k)} d_i^{-1} \quad (180)$$

Applying  $\lambda_i \circ \theta_t$  on  $(w_i, w'_i)$ , on one hand, on  $(w_{i(k)}, w'_{i(k)})$  on the other hand, we obtain

$$\theta_t(W_k) = c_i^{-1} \theta_t(\bar{W}_k) d_i^{-1} = c_{i(k)}^{-1} \theta_t(\bar{W}_k) d_{i(k)}^{-1}$$

hence

$$\theta_t(W_k) = c_i^{-1} c_{i(k)} \theta_t(W_k) d_{i(k)} d_i^{-1}.$$

This shows that  $(c_i^{-1} c_{i(k)}, d_i d_{i(k)}^{-1}) \in \delta(\theta_t(W_k))$  which, as  $\theta_t$  is an  $AB$ -homomorphism, implies that  $(c_i^{-1} c_{i(k)}, d_i d_{i(k)}^{-1}) \in \delta(W_k)$ , which finally proves that both righthand-sides of the two equalities in (180) are equal. We have thus established (162).

By hypothesis  $\lambda_i = \lambda_j$  for all  $1 \leq i, j \leq n$ , which immediately implies (163).

**Case 2:** We suppose here that, there exists some  $i \in [1, n + m]$ , such that none of conditions (166)(167) does hold.

Let  $i \in [1, n + m]$  be the minimal integer fulfilling  $\neg(166) \wedge \neg(167)$ .

Let  $(P_i, P'_i)$  be a distinguishing pair for  $(\lambda_i(w_i), \lambda_i(w'_i))$ . The hypothesis that  $P_i \equiv_i P'_i$  implies that  $\gamma(P_i) = \gamma(P'_i)$ ,  $\theta_t(P_i) = \theta_t(P'_i)$ . By Lemma 2,  $\mathbb{G}$  is left-cancellative, so that  $\theta_t(P_i) = \theta_t(P'_i)$  implies that  $\pi_{\mathbb{G}}(\theta_t(S_i)) = \pi_{\mathbb{G}}(\theta_t(S'_i))$ . But, since  $\theta_t(S_i), \theta_t(S'_i)$  have a non-empty set of types they are classes of reduced sequences, hence

$$\theta_t(S_i) = \theta_t(S'_i). \quad (181)$$

Lemma 13 applied on  $P_i, S_i, P'_i, S'_i \in \mathbb{W}$  asserts that  $\gamma(S_i) = \gamma(S'_i)$ . As  $\theta_t$  restricted to  $\iota_A(A)$  (resp. to  $\iota_B(B)$ ) is injective, the value  $\|S_i\| = 0$  would lead to  $S_i = S'_i$ , which contradicts the choice of  $i$ . Finally we must have:

$$\|S_i\| \geq 1, \quad \|S'_i\| \geq 1, \quad \gamma(S_i) = \gamma(S'_i).$$

Decomposing  $S_i, S'_i$  over the set of generators  $\mathcal{G}_{\mathbb{W}}$  we must have

$$S_i = cW \cdot L_i; \quad S'_i = c'W' \cdot L'_i \quad (182)$$

where

$$W, W' \in \mathcal{W}, \gamma(W) = \gamma(W') \in \mathcal{TA}_0, \gamma(L_i) = \gamma(L'_i) \in \mathcal{TR}, c, c' \in Gi(W).$$

**Subcase 2.1:**  $W' = W, \gamma(W)$  is a H-type.

Equation (181), decomposition (182) and Lemma 8 imply that there exists  $d, d' \in \text{Ge}(W)$  such that

$$\theta_t(cWd) = \theta_t(c'Wd'); \quad \theta_t(d^{-1}L_i) = \theta_t(d'^{-1}L'_i).$$

As  $\theta_t$  is  $\delta$ -preserving, this implies that  $cWd = c'Wd'$ . Taking  $Q_i = P_i cWd, T_i = d^{-1}L_i, Q'_i = P'_i c'Wd', T'_i = d'^{-1}L'_i$ , we obtain a decomposition of  $\lambda_i(w_i), \lambda_i(w'_i)$  such that  $2\|\psi_t(T_i)\| + 2\|\psi_t(T'_i)\| \leq 2\|\psi_t(S_i)\| + 2\|\psi_t(S'_i)\|$  and  $\chi_H(T_i) + \chi_H(T'_i) < \chi_H(S_i) + \chi_H(S'_i)$  (because  $T_i, T'_i$  cannot begin with a letter having a H-type). This is enough to entail

$$\Delta(Q_i, T_i, Q'_i, T'_i, \theta_t) < \Delta(P_i, S_i, P'_i, S'_i, \theta_t)$$

and  $Q_i \equiv_i Q'_i$ , violating the hypothesis of minimality in the choice of decomposition (164). This subcase is thus impossible.

**Subcase 2.2:**  $W' = \bar{W}, \gamma(W)$  is a H-type.

Reasoning as in subcase 2.1, we obtain  $d, d' \in \text{Ge}(W)$  such that

$$\theta_t(cWd) = \theta_t(c'\bar{W}d'); \quad \theta_t(d^{-1}L_i) = \theta_t(d'^{-1}L'_i).$$

Let us define a new equation

$$w_{n+m+1} = cWd; \quad w'_{n+m+1} = c'\bar{W}d',$$

and the  $AB$ -morphisms:

$$\lambda'_i = \lambda_i \text{ for all } 1 \leq i \leq n+m, \lambda'_{n+m+1} = \text{Id}_{\mathbb{W}_t}, \theta'_t = \theta_t.$$

The new system  $\mathcal{S}' = ((w_i, w'_i))_{1 \leq i \leq n+m+1}$  together with  $\lambda' = (\lambda_i)_{1 \leq i \leq n+m+1}$  and  $\theta'_t$  fulfills the hypothesis of Lemma 21.

$$P_i cWd \equiv_i P'_i c'\bar{W}d'$$

$$\|\theta_t(\lambda_i(L_i))\| = \|\theta_t(\lambda_i(S_i))\| \tag{183}$$

$$2\chi_H(L_i) = 0 \leq 2\chi_H(S_i) - 2 \tag{184}$$

$$1 - \chi_{AB}(P_i cWd) = 1 \leq (1 - \chi_{AB}(P_i)) + 1. \tag{185}$$

Adding up comparisons (183)(184)(185), we obtain:

$$\Delta(P_i cWd, P'_i c'W'd', d^{-1}L_i, d'^{-1}L'_i, \theta_t) < \Delta(P_i, P'_i, S_i, S'_i, \theta_t)$$

hence, by definition of  $\Delta_i$ ,

$$\Delta_i(\mathcal{S}', \lambda', \theta'_t) < \Delta_i(\mathcal{S}, \lambda, \theta_t). \tag{186}$$

The integer  $i$  was supposed to do not fullfil (167), hence

$$1 \leq 1 - \chi_{AB}(P_i) + 4\|\theta_t(L_i)\|,$$

which implies

$$\Delta_{n+m+1}(\mathcal{S}', \lambda', \theta_t) < \Delta_i(\mathcal{S}, \lambda, \theta_t). \quad (187)$$

The above inequalities (186)(187) prove that

$$\{\{\Delta_i(\mathcal{S}', \lambda', \theta'_t), \Delta_{n+m+1}(\mathcal{S}', \lambda', \theta'_t)\}\} < \{\{\Delta_i(\mathcal{S}, \lambda, \theta_t)\}\}.$$

Hence

$$\|(\mathcal{S}', \lambda', \theta'_t)\| < \|(\mathcal{S}, \lambda, \theta_t)\|.$$

By induction hypothesis, the conclusion of the lemma holds for  $(\mathcal{S}', \lambda', \theta'_t)$ . This proves that it holds for  $(\mathcal{S}, \lambda, \theta_t)$  too.

**Subcase 2.3:**  $W' \notin \{W, \bar{W}\}$ ,  $\gamma(W)$  is a H-type.

As in subcase 2.1 we obtain that there exists  $d, d' \in \text{Ge}(W)$  such that

$$\theta_t(cWd) = \theta_t(c'W'd'); \quad \theta_t(d^{-1}L_i) = \theta_t(d'^{-1}L'_i). \quad (188)$$

Let us consider the monoid homomorphism  $\lambda' : \mathbb{W} \rightarrow \mathbb{W}$  fulfilling:

$$\lambda'(e) = e \quad \text{for all } e \in \iota_A(A) \cup \iota_B(B) \quad (189)$$

$$\lambda'(W) = c^{-1}c'W'd'd^{-1} \quad (190)$$

$$\lambda'(\bar{W}) = dd'^{-1}\bar{W}'c'^{-1}c \quad (191)$$

(this definition is written for the case where  $W \in \hat{\mathcal{W}}$ , in the case where  $W \notin \hat{\mathcal{W}}$ , last line of this definition must be cancelled). Such an homomorphism exists because (188) ensures that  $(W, c^{-1}c'W'd'd^{-1})$  (resp.  $(\bar{W}, dd'^{-1}\bar{W}'c'^{-1}c)$  in case  $W \in \hat{\mathcal{W}}$ ) have the same image by  $\delta$ . Unicity of  $\lambda'$  is straightforward. Such an homomorphism  $\lambda'$  also preserves  $\mu, \gamma, \delta$  because  $\theta_t$  does so. It preserves the partial involution because  $dd'^{-1}\bar{W}'c'^{-1}c = \mathbb{I}(c^{-1}c'W'd'd^{-1})$ . Hence  $\lambda'$  is an  $AB$ -homomorphism. Let us define:

$$\lambda'_i = \lambda_i \circ \lambda' \text{ for all } 1 \leq i \leq n+m, \quad \theta'_t = \theta_t.$$

Since  $\text{Alph}(\mathcal{S}, \lambda') = \text{Alph}(\mathcal{S}, \lambda) - \{W, \bar{W}\}$ , the inequality  $A(\mathcal{S}, \lambda') \leq K_0$  still holds.

In this sytem we now have:

$$P_i c W d \equiv_i P'_i c' W' d'$$

$$\|\theta_t(\lambda_i(d^{-1}L_i))\| = \|\theta_t(\lambda_i(S_i))\| \quad (192)$$

$$2\chi_H(d^{-1}L_i) = 0 \leq 2\chi_H(S_i) - 2 \quad (193)$$

The conjunction of comparisons (192) (193) imply

$$\Delta_i(\mathcal{S}', \lambda', \theta'_t) < \Delta_i(\mathcal{S}, \lambda, \theta_t). \quad (194)$$

and finally

$$\|(\mathcal{S}', \lambda', \theta'_t)\| < \|(\mathcal{S}, \lambda, \theta_t)\|.$$

The system  $\mathcal{S}' = \mathcal{S}$  together with  $\boldsymbol{\lambda}' = (\lambda'_i)_{1 \leq i \leq n+m}$  and  $\theta'_t$  fulfills the hypothesis of Lemma 21 and has smaller size. By induction hypothesis the conclusion of the lemma holds for  $(\mathcal{S}', \boldsymbol{\lambda}', \theta'_t)$ . This proves that it holds for  $(\mathcal{S}, \boldsymbol{\lambda}, \theta_t)$  too.

**Subcase 2.4:**  $W' = W, \gamma(W)$  is a T-type.

Let us observe that  $\|\theta_t(cWd)\| = \|\theta_t(c'Wd')\|$ . In view of equation (181), decomposition (182) and the above equality, point (1) of Lemma 9 applies: there exists  $d, d' \in \gamma_3(W)$  such that

$$\theta_t(cWd) = \theta_t(c'Wd'); \quad \theta_t(d^{-1}L_i) = \theta_t(d'^{-1}L'_i).$$

We can then conclude as in subcase 2.1.

**Subcase 2.5:**  $W' = \bar{W}, \gamma(W)$  is a T-type.

Then  $\gamma(W) = \gamma(\bar{W}) = \mathbb{I}_{\mathcal{T}}(\gamma(W))$ . But the two atomic T-types are exchanged by the involution  $\mathbb{I}_{\mathcal{T}}$ , which makes this subcase impossible.

**Subcase 2.6:**  $W' \notin \{W, \bar{W}\}, \gamma(W)$  is a T-type  $\boldsymbol{\theta}'$ .

By (181)  $\theta_t(cWL_i) = \theta_t(c'W'L'_i)$ . Using that  $\gamma(W) = \gamma(W')$  is a T-type, we can apply Lemma 9 on  $P = \theta_t(cW), P' = \theta_t(cW'), S = \theta_t(L_i), S' = \theta_t(L'_i)$ . We distinguish 3 subsubcases according to which point of Lemma 9 occurs.

**subsubcase 2.6.1:**  $\|\theta_t(cW)\| = \|\theta_t(cW')\|$ .

This corresponds to point (1) of Lemma 9: there exists some  $d \in \text{Ge}(W)$  such that,

$$\theta_t(cW) = \theta_t(cW')d, \quad d\theta_t(L_i) = \theta_t(L'_i). \quad (195)$$

We can end this subsubcase as for case 2.3.

**subsubcase 2.6.2:**  $\|\theta_t(cW)\| < \|\theta_t(cW')\|$ .

This corresponds to point (2) of Lemma 9:  $\exists d \in \text{Ge}(W), P'_1, P'_2, P'_3 \in \mathbb{H}_t, P'_1$  has a T-type  $\boldsymbol{\theta}'_1, P'_3$  has a T-type  $\boldsymbol{\theta}'_3, P'_2$  has a H-type  $\boldsymbol{\theta}'_2$  such that

$$\theta_t(cW) = P'_1d, \quad \theta_t(c'W') = P'_1 \cdot P'_2 \cdot P'_3, \quad d\theta_t(L_i) = P'_2P'_3\theta_t(L'_i), \quad \boldsymbol{\theta}' = \boldsymbol{\theta}'_1\boldsymbol{\theta}'_2\boldsymbol{\theta}'_3 \quad (196)$$

Let us apply Lemma 14 over the AB-homomorphism  $\theta_t$ , the equality  $\theta_t(dL_i) = P'_2 \cdot (P'_3\theta_t(L'_i))$ , the H-type  $\boldsymbol{\theta} = \boldsymbol{\theta}'_2$  and the T-type  $\boldsymbol{\rho}$  such that  $\gamma_t(P'_3\theta_t(L'_i)) = \{\boldsymbol{\rho}\}$ . We obtain some  $P_2, S \in \mathbb{W}$  such that:

$$dL_i = P_2 \cdot S, \quad \theta_t(P_2) = P'_2, \quad \theta_t(S) = P'_3\theta_t(L'_i). \quad (197)$$

### First step

Let us assume, in this step, that  $W' \in \hat{\mathbb{W}}$ .

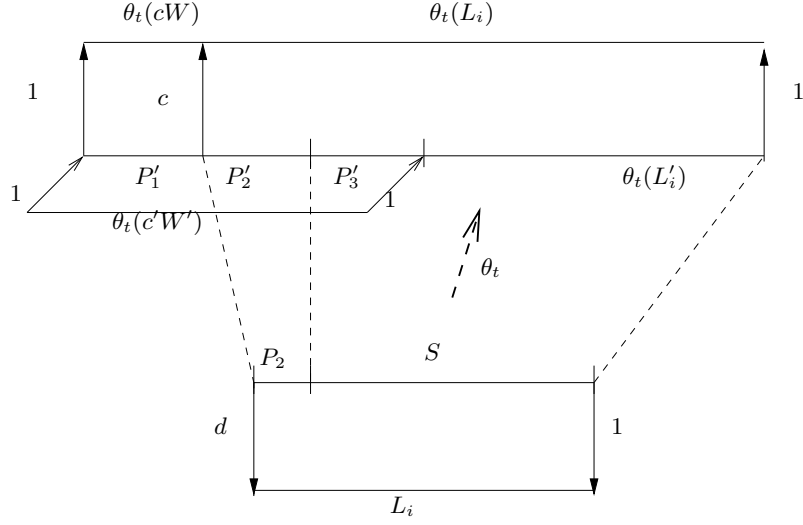
By axiom (25),  $c' \in \hat{\mathbb{W}}$ , by axiom (26)  $c'W' \in \hat{\mathbb{W}}$ . Axiom (36) on AB-homomorphisms implies that  $P'_1 \cdot P'_2 \cdot P'_3 \in \text{dom}(\mathbb{I}_t)$ . Axiom (26) implies that all the  $P'_i$  ( $1 \leq i \leq 3$ ) belong to  $\text{dom}(\mathbb{I}_t)$  and axiom (36) implies that

$$W, P_2 \in \hat{\mathbb{W}}. \quad (198)$$

We saw above that  $\gamma(P'_3)$  is a T-type and, by hypothesis,  $A(\mathcal{S}, \boldsymbol{\lambda}) \leq K_0 < \text{Card}(\mathcal{V}_0)$ .

Hence, we can choose a letter  $W_3 \in \mathcal{W}$  such that

$$W_3 \notin \text{Alph}(\mathcal{S}, \boldsymbol{\lambda}), \quad \gamma(W_3) = \gamma(P'_3), \quad \mu(W_3) = \mu(P'_3), \quad \delta(W_3) = \delta(P'_3).$$



**Fig. 13.** subsubcase 2.6.2

We define a monoid-homomorphism  $\lambda' : \mathbb{W} \rightarrow \mathbb{W}$  by

$$\begin{aligned} \lambda'(e) &= e && \text{for all } e \in \iota_A(A) \cup \iota_B(B) \\ \lambda'(W'') &= W'' && \text{for all } W'' \in \mathcal{W} - \{W', \bar{W}'\} \\ \lambda'(W') &= c'^{-1}cWd^{-1}P_2W_3 && (199) \\ \lambda'(\bar{W}') &= \mathbb{I}(c'^{-1}cWd^{-1}P_2W_3) . && (200) \end{aligned}$$

and we define a new monoid-homomorphism  $\theta' : \mathbb{W}_t \rightarrow \mathbb{H}_t$  by

$$\begin{aligned} \theta'(\iota_A(a)) &= a && \text{for all } a \in A \\ \theta'(\iota_B(b)) &= b && \text{for all } b \in B \\ \theta'(W'') &= W'' && \text{for all } W'' \in \mathcal{W} - \{W_3, \bar{W}_3\} \\ \theta'(W_3) &= P'_3 && (201) \\ \theta'(\bar{W}_3) &= \mathbb{I}_t(P'_3) . && (202) \end{aligned}$$

As in the above cases we can check that  $\lambda', \theta'_t$  are  $AB$ -homomorphisms. Let us check that, for every  $W'' \in \text{Alph}(\mathcal{S}, \lambda)$

$$\theta'_t(\lambda'(W'')) = \theta_t(W'') . \quad (203)$$

Since  $W_3 \notin \text{Alph}(\mathcal{S}, \lambda)$ ,  $\bar{W}_3 \notin \text{Alph}(\mathcal{S}, \lambda)$ , for every  $W'' \in \text{Alph}(\mathcal{S}, \lambda) - \{W', \bar{W}'\}$ ,  $\theta'_t(\lambda'(W'')) = \theta'_t(W'') = \theta_t(W'')$ .

Moreover

$$\begin{aligned}
\theta'_t(\lambda'(W')) &= \theta'_t(c'^{-1}cWd^{-1}P_2W_3) \quad \text{by (201)} \\
&= c'^{-1}\theta_t(cW)d^{-1}\theta'_t(P_2)P'_3 \quad \text{by (201)} \\
&= c'^{-1}\theta_t(cW)d^{-1}\theta_t(P_2)P'_3 \quad (\text{no occurrence of } W_3, \bar{W}_3 \text{ in } P_2) \\
&= c'^{-1}\theta_t(cW)d^{-1}P'_2P'_3 \quad \text{by (197), second equation} \\
&= c'^{-1}P'_1dd^{-1}P'_2P'_3 \quad \text{by (196), first equation} \\
&= \theta_t(W') \quad \text{by (196), second equation.}
\end{aligned}$$

Finally, since  $\lambda', \theta'_t, \theta_t$  preserve the involutions  $\mathbb{I}_W, \mathbb{I}_t$ , we also get

$$\theta'_t(\lambda'(\bar{W}')) = \theta_t(\bar{W}').$$

Let us define

$$\lambda'_i = \lambda_i \circ \lambda' \text{ for all } 1 \leq i \leq n + m.$$

Let us notice that  $\gamma(W')$  is a T-type while  $\gamma(P_2)$  is a H-type. Hence  $\|\theta_t(P_2)\| = 0 < \|\theta_t(W')\|$  which proves that

$$W', \bar{W}' \notin \text{Alph}(P_2)$$

Hence  $\text{Alph}(\mathcal{S}', \lambda') = \text{Alph}(\mathcal{S}, \lambda) \cup \{W_3, \bar{W}_3\} - \{W', \bar{W}'\}$ . We thus obtain

$$A(\mathcal{S}', \lambda') \leq K_0. \quad (204)$$

Equality (203) and inequality (204) ensure that the new triple  $(\mathcal{S}, \lambda', \theta')$  fulfills the hypothesis of Lemma 21.

Let us evaluate now the size of this new triple.

$$\begin{aligned}
(\lambda'_i(w_i), \lambda'_i(w'_i)) &= (\lambda'(P_i c W L_i), \lambda'(P'_i c' W' L'_i)) \\
&= (\lambda'(P_i) c W \lambda'(d^{-1} P_2 S), \lambda'(P'_i) c' (c'^{-1} c W d^{-1} P_2 W_3) \lambda'(L'_i)) \\
&= (\lambda'(P_i) c W d^{-1} P_2 \cdot \lambda'(S), \lambda'(P'_i) c W d^{-1} P_2 \cdot W_3 \lambda'(L'_i)) \quad \text{by (6.2)}
\end{aligned}$$

Let us set

$$Q_i = \lambda'(P_i) c W d^{-1} P_2, \quad T_i = \lambda'(S), \quad Q'_i = \lambda'(P'_i) c W d^{-1} P_2, \quad T'_i = W_3 \lambda'(L'_i)$$

$$\begin{aligned}
\Delta(Q_i, T_i, Q'_i, T'_i, \theta'_t) &\leq 3 + 4\|\theta'_t(W_3)\theta'_t(\lambda'(L'_i))\| \\
&= 3 + 4\|P'_3\| + 4\|\theta_t(L'_i)\| \quad (\text{by (201), (203)}) \\
&< 4(\|P'_3\| + \|P'_3\| + \|P'_3\|) + 4\|\theta_t(L'_i)\| \quad (\text{because } \|P'_1\| \geq 1) \\
&\leq \Delta(P_i, S_i, P'_i, S'_i, \theta_t). \quad (205)
\end{aligned}$$

The hypothesis that  $P_i, P'_i$  are related by the monoid-congruence generated by the set of pairs  $\{(\lambda_j(w_j), \lambda_j(w'_j)) \mid i + 1 \leq j \leq n + m\}$  implies that

$\lambda'(P_i), \lambda'(P'_i)$  are related by the monoid-congruence generated by the set of pairs  $\{(\lambda'(\lambda_j(w_j)), \lambda'(\lambda_j(w'_j))) \mid i+1 \leq j \leq n+m\}$ . It follows that

$$\Delta_i(\mathcal{S}, \lambda', \theta'_t) \leq \Delta(Q_i, T_i, Q'_i, T'_i, \theta'_t) < \Delta(P_i, S_i, P'_i, S'_i, \theta_t) = \Delta_i(\mathcal{S}, \lambda, \theta_t)$$

and thus:

$$\|(\mathcal{S}', \lambda', \theta')\| < \|(\mathcal{S}, \lambda, \theta)\|.$$

By induction hypothesis, conclusions (161-163) are true for  $(\mathcal{S}, \lambda')$ , which also implies that they hold for  $(\mathcal{S}, \lambda)$ .

**second step**

Let us handle the situation where  $W'$  does not belong to  $\hat{\mathbb{W}}$ .

We just cancel the last line of (200) and can conclude as in first step.

**subsubcase 2.6.3:**  $\|\theta_t(cW)\| > \|\theta_t(c'W')\|$ .

Symmetric to subsubcase 2.6.2.  $\square$

Let us prove Lemma 20.

**Proof:** Let us suppose that  $\sigma_t : \mathbb{W}_t \rightarrow \mathbb{H}_t$  is an  $AB$ -homomorphism solving the system  $\mathcal{S}$ . Let us define  $m := 0, \lambda_i := \text{Id}$  for  $1 \leq i \leq n, \theta_t := \sigma_t, K_0 := A(\prod_{i=1}^n w_i w'_i)$ . Since

$$A(\prod_{i=1}^n w_i w'_i) \leq \text{Card}(\mathcal{W}) < \text{Card}(\mathcal{V}_0),$$

the integers  $n, m$ , the maps  $(\lambda_i)_{1 \leq i \leq n+m}, \theta_t$  and the integer  $K_0$  are fulfilling the hypothesis of Lemma 21. Let us consider the maps  $\mathbb{I}', \lambda'_i, \theta'_t$  given by the conclusion of Lemma 21 and choose:

$$\sigma_{\mathbb{W}} := \lambda'_1, \psi_t := \theta'_t.$$

These objects are fulfilling the properties asserted in Lemma 20, as required.  $\square$

**From  $\mathbb{W}$ -solutions to  $\mathbf{t}$ -solutions** Conversely, every  $\mathbb{W}$ -solution of a given system  $\mathcal{S}$  of the form (116) provides a  $\mathbf{t}$ -solution of the same system. Let us state this formally.

**Lemma 22 ( $\mathbb{W}$ -solutions provide  $\mathbf{t}$ -solutions).** *Let  $\mathcal{S} = ((w_i, w'_i))_{1 \leq i \leq n}$  be a system of  $t$ -equations of the form (116). Let us suppose that there exists an  $H$ -involution  $\mathbb{I}' \in \mathcal{I}$  and an  $AB$ -homomorphism  $\sigma_{\mathbb{W}} : (\mathbb{W}_t, \mathbb{I}) \rightarrow (\mathbb{W}_t, \mathbb{I}')$  such that*

$$\sigma_{\mathbb{W}}(w_i) = \sigma_{\mathbb{W}}(w'_i) \text{ for all } 1 \leq i \leq n.$$

*Then, there exists an  $AB$ -homomorphism  $\psi_t : (\mathbb{W}_t, \mathbb{I}') \rightarrow (\mathbb{H}_t, \mathbb{I}_t)$  such that  $\sigma_{\mathbb{W}} \circ \psi_t$  solves the system  $\mathcal{S}$ .*

**Proof:** Let  $\mathbb{I}' \in \mathcal{I}$  and  $\sigma_{\mathbb{W}} : (\mathbb{W}_t, \mathbb{I}) \rightarrow (\mathbb{W}_t, \mathbb{I}')$  fulfil the hypothesis of the lemma. We define a monoid-homomorphism  $\varphi : \mathcal{W}_t^* * A * B \rightarrow \mathbb{H}_t$  in the following way: -for every  $a \in A, \varphi(\iota(a)) = a$

-for every  $b \in B$ ,  $\varphi(\iota(b)) = b$   
 -for every  $W \in \mathcal{W}_t \setminus \hat{\mathcal{W}}$ , we choose some t-sequence  $s \in \mathbb{H} * \{t, \bar{t}\}^*$  which realizes  $W$  in the sense that

$$s \notin \text{dom}(\mathbb{I}_t), \gamma(W) \subseteq \gamma(s),$$

$$\forall \theta \in \gamma(W), \mu(\theta, W) = \mu(\theta, s), \delta(\theta, W) = \delta(\theta, s),$$

and we set  $\varphi(W) = [s]_{\sim}$ .

-for every  $W \in \mathcal{W}_t \cap \bar{\mathcal{W}}_0$ , we choose some t-sequence  $s \in \mathbb{H} * \{t, \bar{t}\}^*$  such that

$$s \in \text{dom}(\mathbb{I}_t), \gamma(W) \subseteq \gamma(s),$$

$$\forall \theta \in \gamma(W), \mu(\theta, W) = \mu(\theta, s), \delta(\theta, W) = \delta(\theta, s),$$

and we set  $\varphi(W) = [s]_{\sim}$ .

-for every  $k \in [1, p]$ , we choose some element  $h_k \in H$  such that

$$h_k \in I(H), a_k h_k b_k = h_k^{-1}, \quad \gamma(W) \subseteq \gamma(h_k),$$

$$\forall \theta \in \gamma(W), \mu(\theta, W) = \mu(\theta, h_k), \delta(\theta, W) = \delta(\theta, h_k),$$

and we set  $\varphi(W_k) = [h]_{\sim}$ ,  $\varphi(\bar{W}_k) = [h_k^{-1}]_{\sim}$ . Since, for every  $W \in \mathcal{W}$  and every  $(c, d) \in \delta(W)$ ,  $c\varphi(W) \sim \varphi(W)d$ , the map  $\varphi$  induces a monoid-homomorphism  $\psi_t : \mathbb{W}_t \rightarrow \mathbb{H}_t$ . This monoid homomorphism clearly fulfils conditions (35,36,38,39,40) by our choices. It is also compatible with the involutions (condition (37)) because,

$$\psi_t(\mathbb{I}'(W_k)) = \psi_t(a_k W_k b_k) = [a_k h_k b_k]_{\sim} = [h_k^{-1}]_{\sim} = I_t(\psi_t(W_k))$$

and, analogously

$$\psi_t(\mathbb{I}'(\bar{W}_k)) = \psi_t(a_k^{-1} \bar{W}_k b_k^{-1}) = [a_k^{-1} h_k^{-1} b_k^{-1}]_{\sim} = [h_k]_{\sim} = I_t(\psi_t(\bar{W}_k)).$$

Thus  $\psi_t$  is an AB-homomorphism. Since  $\sigma_{\mathbb{W}}$  solves  $\mathcal{S}$  it is clear that  $\sigma_{\mathbb{W}} \circ \psi_t$  solves  $\mathcal{S}$  too.

□



## 7 Equations over $\mathbb{U}$

### 7.1 The group $\mathbb{U}$

Let us adjoin to  $\check{W}$  an alphabet of inverses  $\overline{\check{W}}$ . The extended alphabet  $\mathcal{W}' := \check{W} \cup \overline{\check{W}} \cup \hat{W}$  is now endowed with a total involution  $W \mapsto \bar{W}$ , which extends the partial involution  $\mathbb{I}_{\mathbb{W}}$ . The maps  $\gamma, \mu, \delta$  are extended to  $\mathcal{W}'$  in such a way that the axiom (33) of  $AB$ -algebras is fulfilled by  $\mathcal{W}'^* * A * B$  endowed with this involution. We define the group

$$\mathbb{U} := \langle A * B, \mathcal{W}'; \bar{W}eW = \delta(W)(e) \quad (e \in \text{Gi}(W), W \in \mathcal{W}) \rangle \quad (206)$$

i.e. it is an HNN-extension of the free product  $A * B$  with, as stable letters, all the letters  $W$  from  $\mathcal{W}'$  and as partial isomorphisms, the maps  $\delta(W)$ . We identify  $\iota_A$  (resp.  $\iota_B$ ) with the natural embedding of  $A$  (resp.  $B$ ) into  $A * B$ . We denote by  $\equiv_{\mathbb{U}}$  the monoid-congruence over  $\mathcal{W}'^* * A * B$  generated by the set of relations (206). We denote by

$$\pi_U : \mathcal{W}'^* * A * B \rightarrow \mathbb{U}$$

the homomorphism  $z \mapsto [z]_{\equiv_{\mathbb{U}}}$ . All the pairs of (70) also belong to  $\equiv_{\mathbb{U}}$ , hence  $\equiv_{\mathbb{U}} \subseteq \equiv_{\mathbb{U}}$ . Thus, there exists a unique map  $\bar{\pi}_U : \mathbb{W} \rightarrow \mathbb{U}$  such that

$$\pi_U|_{\mathcal{W}'^* * A * B} = \pi_{\equiv} \circ \bar{\pi}_U.$$

An element  $z \in \mathcal{W}'^* * A * B$  is said to be a *reduced sequence* iff it does not contain any factor of the form  $\bar{W}eW$  with  $W \in \mathcal{W}', e \in \text{Gi}(W)$ . We denote by  $\text{Red}(A * B, \mathcal{W}')$  the subset of  $\mathcal{W}'^* * A * B$  consisting of all reduced sequences.

**Lemma 23.** *Let  $z, z'$  be some reduced sequences in  $\mathcal{W}'^* * A * B$ . Then  $z \equiv_{\mathbb{U}} z'$  if and only if  $z \equiv z'$ .*

This lemma is obtained via the analogue of lemma 1, but in the case of an HNN-extension with a set  $\mathcal{W}'$  of stable letters (instead of just  $\{t, \bar{t}\}$ ). Such an analogue can be obtained from lemma 1, by induction over the number of stable letters.

**Lemma 24.** *Let  $z, z' \in \mathcal{W}'^* * A * B$  such that  $\gamma(z) = \gamma(z') \neq \emptyset$ . Then  $z \equiv_{\mathbb{U}} z'$  if and only if  $z \equiv z'$ .*

Every  $z$  such that  $\gamma(z) \neq \emptyset$  is a reduced sequence. This lemma is thus a direct corollary of lemma 23.

### 7.2 From $\mathbb{W}$ -equations to $\mathbb{U}$ -equations

We use here the notion of system of equations with rational constraint over  $\mathbb{U}$ , as defined in §2.4 for any monoid. Let us consider a system of  $\mathbb{W}$ -equations of the form described in (159), together with a morphism:

$$\mathcal{S}_{\mathbb{W}} = ((w_i, w'_i)_{i \in I}, \mathbb{I}'); \quad \sigma_H \in \text{Hom}_{AB}((\mathbb{W}_H, \mathbb{I}), (\mathbb{W}_H, \mathbb{I}')).$$

The involution  $\mathbb{I}'$  is given by formulas (75). Let us notice that every letter  $W_k \in \mathcal{W}_1$ , i.e. on which  $\mathbb{I}'$  has a “non-standard” value, fulfills (78), so that  $\gamma(W_k)$  must be a H-type and  $\text{Gi}(W_k) = \text{Ge}(W_k)$ .

Let  $z_i, z'_i \in \mathcal{W}_t^* * A * B$  be some representatives, modulo  $\equiv$ , of  $w_i, w'_i$ . By lemma 18, we can also choose an  $AB$ -homomorphism  $\tilde{\sigma}_H : \mathcal{W}_t^* * A * B \rightarrow \mathcal{W}_t^* * A * B$  such that  $\pi_{\equiv} \circ \sigma_H = \tilde{\sigma}_H \circ \pi_{\equiv}$ . For every  $W \in \mathcal{W}_t$  we consider the following rational subsets of  $\mathcal{W}_t^* * A * B$ :

$$\begin{aligned} R_{\mathbb{I},W} &:= \{z \in \mathcal{W}_t^* * A * B \mid \gamma(z) = \gamma(W) \wedge z \in \hat{\mathcal{W}}_t^* * A * B \Leftrightarrow W \in \hat{\mathcal{W}}_t\}, \\ R_{\mu,W} &:= \{z \in \mathcal{W}_t^* * A * B \mid \gamma(z) = \gamma(W) \wedge \mu(z) = \mu(W)\}, \\ R_{\delta,W} &:= \{z \in \mathcal{W}_t^* * A * B \mid \gamma(z) = \gamma(W) \wedge \delta(z) = \delta(W)\}. \\ R_{H,W} &:= \{\tilde{\sigma}_H(W)\} \text{ if } W \in \mathcal{W}_H; \quad R_{H,W} := \mathcal{W}_t^* * A * B \text{ if } W \notin \mathcal{W}_H \end{aligned}$$

We define the rational constraint  $C : \mathcal{W}_t^* * A * B \rightarrow \text{Rat}(\mathbb{U})$  by:

$$\begin{aligned} \forall W \in \mathcal{W}_t, \quad C(W) &:= \pi_{\mathbb{U}}(R_{\mathbb{I},W}) \cap \pi_{\mathbb{U}}(R_{\mu,W}) \cap \pi_{\mathbb{U}}(R_{\delta,W}) \cap \pi_{\mathbb{U}}(R_{H,W}), \\ \forall e \in \iota_A(A) \cup \iota_B(B), \quad C(e) &:= \pi_{\mathbb{U}}(\{e\}). \end{aligned}$$

Let us define a system of equations over  $\mathbb{U}$  with rational constraint:

$$\mathcal{S}_{\mathbb{U}}(\sigma_H) := ((z_i, z'_i)_{1 \leq i \leq n}, C),$$

(note that  $\mathcal{S}_{\mathbb{U}}(\sigma_H)$  does really depend on  $\mathcal{S}_{\mathbb{W}}$  and  $\sigma_H$ , but not on the choice of  $\tilde{\sigma}_H$ ).

**Lemma 25.** *The map  $\Phi : \text{Hom}_{AB}((\mathbb{W}_t, \mathbb{I}), (\mathbb{W}_t, \mathbb{I}')) \rightarrow \text{Hom}(\mathcal{W}_t^* * A * B, \mathbb{U})$ ,  $\sigma_{\mathbb{W}} \mapsto \pi_{\mathbb{W}} \circ \sigma_{\mathbb{W}} \circ \bar{\pi}_{\mathbb{U}}$  induces a bijection from the set of solutions of  $\mathcal{S}_{\mathbb{W}}$  which extend  $\sigma_H$ , into the set of solutions of  $\mathcal{S}_{\mathbb{U}}(\sigma_H)$ .*

We prove this lemma in the subsequent three subsections; see figure 14 for the general context and figure 15 for the details of the proof.

**From  $\mathbb{W}$ -solutions to  $\mathbb{U}$ -solutions** Let  $\sigma_{\mathbb{W}}$  be a solution of  $\mathcal{S}_{\mathbb{W}}$ , extending  $\sigma_H$ . Let  $\sigma_{\mathbb{U}} := \Phi(\sigma_{\mathbb{W}})$  i.e.

$$\sigma_{\mathbb{U}} := \pi_{\equiv} \circ \sigma_{\mathbb{W}} \circ \bar{\pi}_{\mathbb{U}}.$$

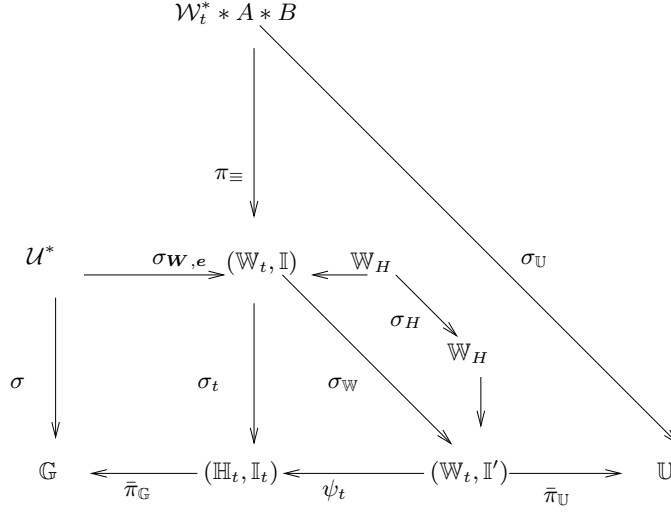
From the definitions of  $z_i, z'_i$  we get

$$\sigma_{\mathbb{U}}(z_i) = \bar{\pi}_{\mathbb{U}}(\sigma_{\mathbb{W}}(w_i)) = \bar{\pi}_{\mathbb{U}}(\sigma_{\mathbb{W}}(w'_i)) = \sigma_{\mathbb{U}}(z'_i), \quad (207)$$

thus  $\sigma_{\mathbb{U}}$  is a solution of the system of equations  $(z_i, z'_i)_{1 \leq i \leq n}$ .

The map  $\pi_{\equiv} \circ \sigma_{\mathbb{W}}$  is an  $AB$ -homomorphism, hence it maps  $\mathbb{I}$  on  $\mathbb{I}'$  and preserves  $\gamma, \mu, \delta$ . It follows that, for every  $W \in \mathcal{W}_t$ :

$$\sigma_{\mathbb{W}}(\pi_{\equiv}(W)) \in \pi_{\equiv}(R_{\mathbb{I},W}) \cap \pi_{\equiv}(R_{\mu,W}) \cap \pi_{\equiv}(R_{\delta,W}).$$



**Fig. 14.** lemma 25: the context

As  $\sigma_{\mathbb{W}}$  extends  $\sigma_H$  we get, for every  $W \in \mathcal{W}$ :

$$\sigma_{\mathbb{W}}(\pi_{\equiv}(W)) \in \pi_{\equiv}(R_{H,W}).$$

Applying  $\bar{\pi}_{\mathbb{U}}$  on both sides of the above membership relations we obtain that, for every  $W \in \mathcal{W}_t$ :

$$\sigma_{\mathbb{U}}(W) \in \mathbb{C}(W). \quad (208)$$

Moreover the three maps  $\pi_{\equiv}, \sigma_{\mathbb{W}}, \bar{\pi}_{\mathbb{U}}$  are fixing every element of  $A \cup B$ , so that, for every  $e \in A \cup B$ :

$$\sigma_{\mathbb{U}}(e) \in \mathbb{C}(e). \quad (209)$$

By (207)(208)(209)  $\sigma_{\mathbb{U}}$  is a solution of  $\mathcal{S}_{\mathbb{U}}(\sigma_H)$ .

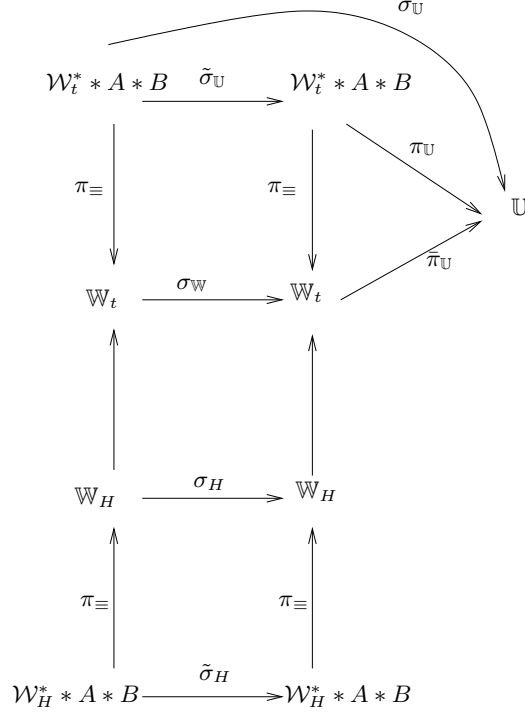
**From  $\mathbb{U}$ -solutions to  $\mathbb{W}$ -solutions** Let  $\sigma_{\mathbb{U}}$  be a solution of  $\mathcal{S}_{\mathbb{U}}(\sigma_H)$ .

Since, for every  $W \in \mathcal{W}_t$ ,  $\sigma_{\mathbb{U}}(W) \in \mathbb{C}(W) \subseteq \pi_{\mathbb{U}}(R_{\mu,W})$ , there is a choice map  $\tilde{\sigma}_{\mathbb{U}} : \mathcal{W}_t \rightarrow \mathcal{W}_t^* * A * B$  fulfilling:

$$\forall W \in \mathcal{W}_t, \tilde{\sigma}_{\mathbb{U}}(W) \in R_{\mu,W}, \quad \pi_{\mathbb{U}}(\tilde{\sigma}_{\mathbb{U}}(W)) = \sigma_{\mathbb{U}}(W). \quad (210)$$

Let us denote by  $\tilde{\sigma}_{\mathbb{U}}$  the unique monoid homomorphism fixing every element of  $A * B$  and extending the above choice map. Since  $\sigma_{\mathbb{U}}(W) \in \mathbb{C}(W)$ , there exist  $z_{\mathbb{I},W} \in R_{\mathbb{I},W}, z_{\delta,W} \in R_{\delta,W}, z_{H,W} \in R_{H,W}$  fulfilling

$$\pi_{\mathbb{U}}(\tilde{\sigma}_{\mathbb{U}}(W)) = \pi_{\mathbb{U}}(z_{\mathbb{I},W}) = \pi_{\mathbb{U}}(z_{\delta,W}) = \pi_{\mathbb{U}}(z_{H,W}).$$



**Fig. 15.** lemma 25: the proof

All these  $z_{\mathbb{I},W}, z_{\delta,W}, z_{H,W}$  have a non-empty image by  $\gamma$  and are equivalent with  $\tilde{\sigma}_{\mathbb{U}}(W)$  modulo  $\equiv_{\mathbb{U}}$ . By lemma 24:

$$\tilde{\sigma}_{\mathbb{U}}(W) \equiv z_{\mathbb{I},W} \equiv z_{\delta,W} \equiv z_{H,W}.$$

The equivalence  $\equiv$  preserves the  $AB$ -structure of  $\mathcal{W}^* * A * B$  (see (71-72)), hence, for every  $W \in \mathcal{W}_t$ ,

$$\tilde{\sigma}_{\mathbb{U}}(W) \in \hat{\mathcal{W}}_t * A * B \Leftrightarrow W \in \hat{\mathcal{W}}_t$$

$$\delta(\tilde{\sigma}_{\mathbb{U}}(W)) = \delta(W)$$

$$\pi_{\equiv}(\tilde{\sigma}_{\mathbb{U}}(W)) = \pi_{\equiv}(\tilde{\sigma}_H(W)) \text{ if } W \in \mathcal{W}_H. \quad (211)$$

The map  $\tilde{\sigma}_{\mathbb{U}} : \mathcal{W}_t \rightarrow \mathcal{W}_t^* * A * B$  defined by (210) can thus be extended into an  $AB$ -homomorphism  $\tilde{\sigma}_{\mathbb{U}} : \mathcal{W}_t^* * A * B \rightarrow \mathcal{W}_t^* * A * B$ . By lemma 16 it defines a unique  $AB$ -homomorphism  $\sigma_{\mathbb{W}} : \mathbb{W}_t \rightarrow \mathbb{W}_t$  fulfilling:

$$\pi_{\equiv} \circ \sigma_{\mathbb{W}} = \tilde{\sigma}_{\mathbb{W}} \circ \pi_{\equiv}. \quad (212)$$

By (211)(212)  $\sigma_{\mathbb{W}}$  extends  $\sigma_H$ .

By hypothesis  $\tilde{\sigma}_{\mathbb{U}} \circ \pi_{\mathbb{U}}$  is a solution of  $\mathcal{S}_{\mathbb{U}}(\sigma_H)$  hence:

$$\pi_{\mathbb{U}}(\tilde{\sigma}_{\mathbb{U}}(z_i)) = \pi_{\mathbb{U}}(\tilde{\sigma}_{\mathbb{U}}(z'_i))$$

i.e.  $\tilde{\sigma}_{\mathbb{U}}(z_i) \equiv_{\mathbb{U}} \tilde{\sigma}_{\mathbb{U}}(z'_i)$ . We know that  $\gamma(z_i) = \gamma(z'_i) \neq \emptyset$  and that  $\tilde{\sigma}_{\mathbb{U}}$  preserves  $\gamma$ . Using lemma 24 we conclude that  $\tilde{\sigma}_{\mathbb{U}}(z_i) \equiv \tilde{\sigma}_{\mathbb{U}}(z'_i)$ , hence

$$\sigma_{\mathbb{U}}(w_i) = \sigma_{\mathbb{U}}(w'_i).$$

Using (212),  $\pi_{\equiv} \circ \sigma_{\mathbb{W}} \circ \bar{\pi}_{\mathbb{U}} = \tilde{\sigma}_{\mathbb{W}} \circ \pi_{\equiv} \circ \bar{\pi}_{\mathbb{U}} = \tilde{\sigma}_{\mathbb{W}} \circ \pi_{\mathbb{U}} = \sigma_{\mathbb{U}}$ . Finally,  $\sigma_{\mathbb{W}}$  is a solution of  $\mathcal{S}_{\mathbb{W}}$  which extends  $\sigma_H$  and

$$\sigma_{\mathbb{U}} = \Phi(\sigma_{\mathbb{W}}).$$

**Bijection  $\Phi$**  Subsubsection 7.2 established that  $\Phi$  is surjective. Let us check it is injective.

Suppose that  $\sigma_{\mathbb{W}}, \sigma'_{\mathbb{W}} \in \text{Hom}_{AB}(\mathbb{W}_t, \mathbb{W}_t)$  fulfill:

$$\pi_{\equiv} \circ \sigma_{\mathbb{W}} \circ \bar{\pi}_{\mathbb{U}} = \pi_{\equiv} \circ \sigma'_{\mathbb{W}} \circ \bar{\pi}_{\mathbb{U}}$$

As  $\pi_{\equiv}$  is surjective we get

$$\sigma_{\mathbb{W}} \circ \bar{\pi}_{\mathbb{U}} = \sigma'_{\mathbb{W}} \circ \bar{\pi}_{\mathbb{U}}.$$

By lemma 24,  $\bar{\pi}_{\mathbb{U}}$  is injective over  $\{z \in \mathbb{W}_t \mid \gamma(z) \neq \emptyset\}$ , hence, for every  $g \in \mathcal{W}_t \cup \iota_A(A) \cup \iota_B(B)$ ,

$$\sigma_{\mathbb{W}}(g) = \sigma'_{\mathbb{W}}(g),$$

which implies

$$\sigma_{\mathbb{W}} = \sigma'_{\mathbb{W}}.$$

By the above three subsubsections, Lemma 25 is proved.

## 8 Transfer of solvability

### 8.1 The structure of $\mathbb{U}$

Since  $\mathbb{U}$  is built from two finite groups  $A, B$  by a finite number of operations which are either a free product or an HNN-extension,  $\mathbb{U}$  is a virtually free group. Let us notice that, for the particular virtually free groups  $\mathbb{K}$  of the form:

$$\mathbb{K} = A \rtimes F(\mathcal{V}) \quad (213)$$

i.e. a semi-direct product of a finite group  $A$  by a free group with finite rank, the decidability of the satisfiability problem for equations with rational constraints in  $\mathbb{K}$  is Turing-reducible to the same problem in the free group  $F(\mathcal{V})$ . Hence, by the main theorem of [DHG05], this problem is decidable. By successive sequences of Tietze transformations, we show that  $\mathbb{U}$  can be constructed from a group  $\mathbb{K}$  of the form (213) by a finite number of HNN-extensions, with associated subgroups of *strictly smaller* cardinality than  $A$ .

*First transformation* Let  $t \in \mathcal{W}$  such that  $\delta(t)$  is a full isomorphism  $A \rightarrow B$ , for example we can choose  $t$  such that  $\delta(t) = \varphi$ . Let us apply the Tietze transformation:

$$b \mapsto t^{-1}\varphi^{-1}(b)t \text{ for all } b \in B \setminus \{1\}$$

we obtain a group-presentation with  $A \cup \{W \in \mathcal{W}' \mid \text{Gi}(W) = A\}$  as set of generators and relations of the form:

$$\begin{aligned} W^{-1}aW &= \delta(W)(a); & \text{for } \text{Gi}(W) = \text{Ge}(W) = A \\ W^{-1}aW &= t^{-1}\varphi^{-1}(\delta(W)(a))t; & \text{for } \text{Gi}(W) = A, \text{Ge}(W) = B, W \neq t \\ aa' &= a''; & \text{for } a, a', a'' \in A \text{ such that } aa' = a'' \end{aligned}$$

*Second transformation* Taking as new set of generators:

$$A \cup \{t\} \cup \{W \in \mathcal{W}' \mid \text{Gi}(W) = \text{Ge}(W) = A\} \cup \{tW^{-1} \mid \text{Gi}(W) = A, \text{Ge}(W) = B, W \neq t\}$$

we obtain a set of generators of the form  $A \cup \mathcal{V}$  and a set of relations of the form

$$\bar{V}aV = \delta'(V)(a) \text{ for } V \in \mathcal{V},$$

with  $\delta' : \mathcal{V} \rightarrow \text{PIs}(A, A)$  together with the basic relations

$$aa' = a''; \text{ for } a, a', a'' \in A \text{ such that } aa' = a''.$$

Let us denote by  $\text{PHNN}(A)$  the set of all such presentations of a multiple HNN-extension of a group  $A$ .

*Decomposition* Let us consider a presentation  $P \in \text{PHNN}(A)$ . Let  $\mathcal{V}_A := \{V \in \mathcal{V}, \text{dom}(\delta'(V)) = \text{im}(\delta'(V)) = A\}$  and

$$\mathbb{K} := \langle A; \bar{V}aV = \delta'(V)(a) \text{ for } V \in \mathcal{V}_A \rangle.$$

We claim that  $\mathbb{K}$  is of the form (213) and the group  $\mathbb{U}$  presented by  $P$  is obtained from  $\mathbb{K}$  by a finite number of HNN-extension operations, with associated subgroups of cardinality  $< |A|$ .

## 8.2 Transfer results

We prove now a general transfer theorem for systems of equations with rational constraints. We first treat the case of groups since it is technically simpler.

### Transfer for groups

**Proposition 5.** *Let  $\mathbb{H}$  be a group and  $\mathbb{G}$  an HNN-extension of  $\mathbb{H}$  with finite associated subgroups  $A, B$ . The satisfiability problem for systems of equations with rational constraints in  $\mathbb{G}$  is Turing-reducible to the pair of problems  $(Q_1, Q_2)$ , where*

- 1-  $Q_1$  is the SAT-problem for systems of equations with rational constraints in a group defined by a presentation in  $\text{PHNN}(A)$
- 2-  $Q_2$  is the SAT-problem for systems of equations with rational constraints in  $\mathbb{H}$

**Proof:** Let us consider a system  $\mathcal{S}_0$  of equations with rational constraints in  $\mathbb{G}$ . By Proposition 3 it can be reduced to a finite disjunction of systems in quadratic normal form. By Lemma 19, solving one system  $\mathcal{S}_{\mathbb{G}}$  in quadratic normal form reduces to problem P1 and the auxiliary problem AP1:

**P1** Compute the alphabet  $\mathcal{W}_t$ .

**AP1** Solve the disjunction of all the pairs of systems  $\mathcal{S}_t(\mathcal{S}, \mathbf{W}, \mathbf{e}), \mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, \mathbf{e})$  by a common  $\sigma_t \in \text{Hom}_{AB}(\mathbb{W}_t, \mathbb{H}_t)$ .

For every value of  $\mathbf{W}, \mathbf{e}$ , by Lemma 20 AP1 reduces to:

**AP2** Find an involution  $\mathbb{I}' \in \mathcal{I}$  and a solution  $\sigma_{\mathbb{W}} \in \text{Hom}_{AB}((\mathbb{W}_t, \mathbb{I}), (\mathbb{W}_t, \mathbb{I}'))$  to the system  $\mathcal{S}_t(\mathcal{S}, \mathbf{W}, \mathbf{e})$ , and find a  $\psi_t \in \text{Hom}_{AB}((\mathbb{W}_t, \mathbb{I}'), (\mathbb{H}_t, \mathbb{I}_t))$  such that  $\sigma_{\mathbb{W}} \circ \psi_t$  solves  $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, \mathbf{e})$ .

By Lemma 25, and a (finite) enumeration of all the  $\mathbb{I}' \in \mathcal{I}$ , and  $\sigma_H \in \text{Hom}_{AB}(\mathbb{W}_H, \mathbb{W}_H)$ , AP2 reduces to

**P2**

**P2.1** Solve the system  $\mathcal{S}_{\mathbb{U}}(\sigma_H)$ ,

**P2.2** Find a  $\psi_{H,t} \in \text{Hom}_{AB}((\mathbb{W}_H, \mathbb{I}'), (\mathbb{H}_t, \mathbb{I}_t))$ , solving  $\sigma_H(\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, \mathbf{e}))$ . Let us examine now the remaining problems P1, P2.1, P2.2.

Problem P1 consists, for every letter  $W \in \hat{\mathcal{W}}$ , in deciding whether there exists an AB-homomorphism from the induced sub-AB-algebra  $\langle W, \bar{W} \rangle$  into  $\mathbb{H}_t$ . Let us

suppose  $\mathbb{I}'$  is given by the formulas (75) of §3.6. For every  $W \in \mathcal{W}_H$  we define the sets

$$\begin{aligned} C_I(W) &:= \mathbb{H}; \quad \text{if } W \in \hat{\mathcal{W}}_0, \\ C_I(W_k) &:= \{h \in \mathbb{H} \mid a_k h b_k = h^{-1}\}; \quad \text{for } k \in [1, p], \\ C_I(\bar{W}_k) &:= \{h \in \mathbb{H} \mid a_k^{-1} h b_k^{-1} = h^{-1}\}; \quad \text{for } k \in [1, p], \\ C_\gamma(W) &:= \{h \in \mathbb{H} \mid \gamma(W) \subseteq \gamma_t(h)\}, \\ C_\mu(W) &:= \{h \in \mathbb{H} \mid \mu(W) = \mu_t(h)\}, \\ C_\delta(W) &:= \{h \in \mathbb{H} \mid \forall \theta \in \gamma(W), \delta(\theta, W) = \delta_t(\theta, h)\}, \\ C(W) &:= C_I(W) \cap C_\gamma(W) \cap C_\mu(W) \cap C_\delta(W). \end{aligned}$$

Recall the notions of equational and positively definable subsets of a monoid were defined in §2.4. Next lemma uses these notions as well as the notation introduced for them.

**Lemma 26.** *For every group  $\mathbb{H}$ ,  $\mathcal{B}(\text{EQ}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))) \subseteq \text{Def}_{\exists+}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))$ .*

In words: a boolean combination of equational subsets of  $\mathbb{H}$  (with rational constraints) is positively definable (with rational constraints).

**Proof:** Every disequation  $u \neq v$  in  $\mathbb{H}$  can be translated as the formula

$$\exists v' \cdot \exists w \cdot v v' = 1 \wedge u v' = w \wedge w \in (\mathbb{H} \setminus \{1\}) \quad (214)$$

Hence, if  $P$  is defined by a positive boolean combination of equations and rational constraints, its complement is definable by a positive boolean combination of statements of the form (214) above, of equations and of rational constraints. This positive boolean combination can be put in existential prenex form, showing that  $\mathbb{H} \setminus P$  belongs to  $\text{Def}_{\exists+}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))$ .  $\square$

We observe that  $C_I$  take values in  $\text{EQ}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))$ ,  $C_\gamma$  take values in  $\mathcal{B}(\{\{1\}, A, B, \mathbb{H}\})$  and  $C_\mu$  take values in  $\mathcal{B}(\text{Rat}(\mathbb{H}))$ . The map  $C_\delta$  take values which are intersections of subsets of the form

$$CD_H(c, d) := \{h \in \mathbb{H} \mid ch =_{\mathbb{H}} hd\} \quad (215)$$

for  $c, d \in A \cup B$  and of subsets of the form  $\mathbb{H} - CD_H(c, d)$ . It is clear that  $CD_H(c, d) \in \text{EQ}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))$  and, by Lemma 26,  $\mathbb{H} - CD_H(c, d)$  belongs to  $\text{Def}_{\exists+}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))$ . Therefore, each of the four subsets  $C_I(W)$ ,  $C_\gamma(W)$ ,  $C_\mu(W)$ ,  $C_\delta(W)$  belongs to  $\text{Def}_{\exists+}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))$ , so that  $C(W)$  also belongs to  $\text{Def}_{\exists+}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))$ .

Deciding whether  $C(W) = \emptyset$  is thus an instance of  $Q_2$ .

Let  $W \in \mathcal{W} - \mathcal{W}_H$ . We set now

$$\begin{aligned} C_I(W) &:= \mathbb{H} * \{t, \bar{t}\}^*, \\ C_\gamma(W) &:= \{s \in \mathbb{H} * \{t, \bar{t}\}^* \mid \gamma(W) \subseteq \gamma_t(s)\}, \\ C_\mu(W) &:= \{s \in \mathbb{H} * \{t, \bar{t}\}^* \mid \mu_1(W) = \mu_A(s)\}, \\ C_\delta(W) &:= \{s \in \mathbb{H} * \{t, \bar{t}\}^* \mid \forall \theta \in \gamma(W), \delta(\theta, W) = \delta_t(\theta, s)\}, \\ C(W) &:= C_I(W) \cap C_\gamma(W) \cap C_\mu(W) \cap C_\delta(W). \end{aligned}$$



*Claim 1 ( $\gamma$ -constraint).* For every  $W \in \mathcal{W} - \mathcal{W}_H$ ,  $C_\gamma(W)$  is recognized by some t-automaton with labels in  $\text{EQ}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))$ .

For every type  $\theta \in \mathcal{T}_6$ , the subset  $CG(\theta) := \{s \in \mathbb{H} * \{t, \bar{t}\}^* \mid \theta \in \gamma(s)\}$  is recognized by a variant of the t-automaton  $\mathcal{R}_6$  where we choose as initial vertex the initial vertex-type of  $\theta$ , as terminal vertex the ending vertex-type of  $\theta$ , and on which we apply a direct product with a finite automaton that memorizes whether at least one letter  $t$  or  $\bar{t}$  has been encountered. The subset  $C_\gamma(W)$  can be described as an intersection of the subsets  $CG(\theta)$ :

$$C_\gamma(W) = \left( \bigcap_{\theta \in \gamma(W)} CG(\theta) \right).$$

Each set  $CG(\theta)$  is recognized by some fta with labelling set  $\text{EQ}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))$ . By Lemma 3 of [LS08] (property of closure under intersection) the set  $C_\gamma(W)$  is thus recognized by a fta with labelling set  $\text{EQ}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))$ .

*Claim 2 ( $\mu$ -constraint).* For every  $W \in \mathcal{W} - \mathcal{W}_H$ ,  $C_\mu(W)$  is recognized by some t-automaton with labels in  $\text{Def}_{\exists+}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))$ .

For every states  $q, r \in \mathcal{Q}$  the set

$$CM(q, r) := \{s \in \mathbb{H} * \{t, \bar{t}\}^* \mid (q, r) \in \mu_{\mathcal{A}}(s)\}$$

is recognized by the variant of the strict automaton  $\mathcal{A}$  obtained just by taking  $q$  as initial state and  $r$  as terminal state. Similarly, the set

$$\overline{CM}(q, r) := \{s \in \mathbb{H} * \{t, \bar{t}\}^* \mid (q, r) \in (\mu_{\mathcal{A}})^{-1}(\mathbb{I}_t(s))\}$$

is recognized by the variant of the fta  $\mathcal{A}$  obtained by replacing the labels by their inverses, the vertex-type of every state by its image by  $\mathbb{I}_{\mathcal{R}}$ , taking  $q$  as initial state and  $r$  as terminal state. The subset  $C_\mu(W)$  can be described as:

$$\begin{aligned} C_\mu(W) = & \left( \bigcap_{(q,r) \in \mu_1(W)} CM(q, r) \right) \cap \left( \bigcap_{(q,r) \notin \mu_1(W)} (\mathbb{H} * \{t, \bar{t}\}^* \setminus CM(q, r)) \right) \\ & \left( \bigcap_{(q,r) \in (\mu_1(\bar{W}))^{-1}} \overline{CM}(q, r) \right) \cap \left( \bigcap_{(q,r) \notin (\mu_1(\bar{W}))^{-1}} (\mathbb{H} * \{t, \bar{t}\}^* \setminus \overline{CM}(q, r)) \right) \end{aligned}$$

By Proposition 1 and Proposition 2 of [LS08], each  $CM(q, r)$  is recognized by a partitioned, saturated, deterministic and complete fta with labelling set  $\mathcal{B}(\text{EQ}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H}))))$ . Hence every subset  $\mathbb{H} * \{t, \bar{t}\}^* \setminus CM(q, r)$  or  $\mathbb{H} * \{t, \bar{t}\}^* \setminus \overline{CM}(q, r)$  is also recognized by a partitioned, saturated, deterministic and complete fta with labelling set  $\mathcal{B}(\text{EQ}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H}))))$ . By Lemma 26 this labeling set is included in  $\text{Def}_{\exists+}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))$  and by Lemma 3 of [LS08], we conclude that  $C_\mu(W)$  is recognized by some t-automaton with labels in  $\text{Def}_{\exists+}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))$ .

*Claim 3 ( $\delta$ -constraint).* For every  $W \in \mathcal{W} - \mathcal{W}_H$ ,  $C_\delta(W)$  is recognized by some t-automaton with labels in  $\text{Def}_{\exists+}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))$ .

The subset  $C_\delta(W)$  is a boolean combination of subsets of the form:

$$CD(c, d) := \{s \in \mathbb{H} * \{t, \bar{t}\}^* \mid cs \sim sd\} \quad (216)$$

for some  $c, d \in A \cup B$ . Each set  $CD(c, d)$  is recognized by some t-automaton with  $A \cup B$  as set of states, with  $c$  as initial state,  $d$  as terminal state, and with deterministic transitions such that, the state reached after reading the sequence  $s \in \mathbb{H} * \{t, \bar{t}\}^*$ , either is undefined (if  $s^{-1}cs \notin A \cup B$ ) or is equal to  $s^{-1}cs$  (if  $s^{-1}cs \in A \cup B$ ). Such a fta has labels in  $\text{EQ}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))$ . The claim follows by the same arguments as for the previous claim.

Finally, due to the claims 1,2,3 and to Lemma 3 of [LS08], the subset  $C(W)$  is recognized by some t-automaton  $\mathcal{D}$  with labels in  $\text{Def}_{\exists+}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))$ . The emptiness problem for  $C(W) = L(\mathcal{D})$  reduces to the emptiness problem for elements of  $\text{Def}_{\exists+}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))$  (given by a system of equations with rational constraints), which are themselves instances of  $Q_2$ .

The problem P2.1, first line, is an instance of  $Q_1$ , while P2.2 is an instance of  $Q_2$ .

□

**Proposition 6.** *Let  $\mathbb{H}$  be a group with decidable SAT-problem for systems of equations with rational constraints and let  $\mathbb{G}$  an HNN-extension of  $\mathbb{H}$  with finite associated subgroups. Then, the satisfiability problem for systems of equations with rational constraints in  $\mathbb{G}$  is decidable.*

**Proof:** We prove this proposition by induction over the size of the finite associated subgroups  $A, B$  used in the HNN-extension leading from  $\mathbb{H}$  to  $\mathbb{G}$ .

**Basis:**  $|A| = 1$ .

In this case  $\mathbb{G}$  is the free product of  $\mathbb{H}$  by  $\mathbb{Z}$ . It is known that the additive group  $\mathbb{Z}$  has a decidable SAT-problem for systems of equations with rational constraints (see, for example, [ES69]). It is proved in [DL03] that a free product of two groups having decidable SAT-problem for systems of equations with rational constraints has also a decidable SAT-problem for systems of equations with rational constraints. Hence  $\mathbb{G}$  has decidable SAT-problem for systems of equations with rational constraints.<sup>1</sup>

**Induction step:**  $|A| > 1$ .

By Proposition 5, the SAT-problem for systems of equations with rational constraints reduces to two other decision problems  $Q_1, Q_2$ . By hypothesis, here, problem  $Q_2$  is decidable.

$Q_1$  is the SAT-problem for systems of equations with rational constraints in the group  $\mathbb{U}$ , which has a presentation in  $\text{PHNN}(A)$ . By §8.1,  $\mathbb{U}$  is obtained from the group  $\mathbb{K}$  by a finite number of HNN-extension operations, with associated

<sup>1</sup> the original formulation of [DL03, Theorem 2] deals with the existential first order theory, with rational constraints, of a group  $\mathbb{G} = \mathbb{H}_1 * \mathbb{H}_2$ . By the trick of formula (214), decidability of this fragment is equivalent to the decidability of the SAT-problem for systems of equations with rational constraints in  $\mathbb{G}$ .

subgroups of cardinality  $< |A|$ . We know that  $\mathbb{K}$  has a decidable satisfiability problem for equations with rational constraints (see subsection 8.1) and, by induction hypothesis, each of the HNN-extension operations preserves this decidability property. Hence  $\mathbb{U}$  has a decidable satisfiability problem for equations with rational constraints. Thus problem  $Q_1$  is decidable too, so that  $\mathbb{G}$  has a decidable satisfiability problem for equations with rational constraints.  $\square$

**Theorem 1.** *Let  $\mathbb{H}$  be a group and  $\mathbb{G}$  an HNN-extension of  $\mathbb{H}$  with finite associated subgroups. The satisfiability problem for systems of equations with rational constraints in  $\mathbb{G}$  is Turing-reducible to the SAT-problem for systems of equations with rational constraints in  $\mathbb{H}$ .*

**Proof:** By Proposition 5 the satisfiability problem for systems of equations with rational constraints in  $\mathbb{G}$  is Turing-reducible to a pair of problems  $Q_1, Q_2$  (precisely defined in the proposition). But  $Q_1$  is the SAT-problem for systems of equations with rational constraints in  $\mathbb{U}$ , where  $\mathbb{U}$  is a group obtained from a finite group  $A$  by a finite number  $n$  of successive HNN-extension operations with finite associated subgroups. It is clear that any finite group has a decidable SAT-problem for equations with rational constraints. Starting from  $\mathbb{H} := A$  and applying Proposition 6  $n$  times, we obtain that  $Q_1$  is decidable. Thus the satisfiability problem for systems of equations with rational constraints in  $\mathbb{G}$  is Turing-reducible to the single problem  $Q_2$ , i.e. to the SAT-problem for systems of equations with rational constraints in  $\mathbb{H}$ .  $\square$

**Transfer for cancellative monoids** We will prove the extension of Proposition 5 to cancellative monoids:

**Proposition 7.** *Let  $\mathbb{H}$  be a cancellative monoid and  $\mathbb{G}$  an HNN-extension of  $\mathbb{H}$  with finite associated subgroups. The satisfiability problem for systems of equations with rational constraints in  $\mathbb{G}$  is Turing-reducible to the pair of problems  $(Q_1, Q_2)$ , where*

- 1-  $Q_1$  is the SAT-problem for systems of equations with rational constraints in a group defined by a presentation in  $\text{PHNN}(A)$
- 2-  $Q_2$  is the SAT-problem for systems of equations with rational constraints in  $\mathbb{H}$

What becomes difficult here is the computation of  $\mathcal{W}_t$ : it requires to determine, for a given symbol  $W \in \mathcal{W}$  whether there exists a  $t$ -sequence  $s$  such that:  $s \in \mathbb{H}$  ( if  $\gamma(W)$  is a H-type),  $s$  is not invertible ( if  $\gamma(W)$  specifies that  $W$  does not belong to the domain of  $\mathbb{I}_{\mathbb{W}}$ ), and  $cs \neq sd$  for some  $c, d \in A \cup B$  ( if the value of  $\delta(W)$  imposes this). The non-invertibility condition is expressed via an universally quantified formula  $(\forall h', h \cdot h' \neq 1)$ , and the non-commutation condition is a disequation. Since no hypothesis ensures that the satisfiability of such formulas over  $\mathbb{H}$  is decidable, we give up the hope to compute  $\mathcal{W}_t$ . Instead, we enumerate

all the subalphabets  $\mathcal{W}' \subseteq \mathcal{W}$  ( closed under  $\mathbb{I}_{\mathbb{W}}$  ) and apply the above method in the induced sub-AB-algebra  $\mathbb{W}'$  generated by  $\mathcal{W}'$  instead of the sub-AB-algebra  $\mathbb{W}_t$ . But the above difficulty arises in the computation of  $\psi_t : \mathbb{W}' \rightarrow \mathbb{H}_t$ . We have to compute, for every  $W' \in \mathcal{W}'$ , an image  $\psi_t(W')$  having the same behaviour as  $W'$  w.r.t.  $\mathbb{I}, \gamma, \mu, \delta$ , while Lemma 26 is no more ensured when  $\mathbb{H}$  is not assumed to be a group. We avoid here this difficulty by computing a *weak* AB-homomorphism  $\psi_t : \mathbb{W}' \rightarrow \mathbb{H}_t$ .

We call *weak AB-homomorphism* from  $\mathcal{M}_1$  to  $\mathcal{M}_2$  any map  $\psi : \mathbb{M}_1 \rightarrow \mathbb{M}_2$  fulfilling the seven properties (217-223) below:

$$\psi : (\mathbb{M}_1, \cdot, 1_{\mathbb{M}_1}) \rightarrow (\mathbb{M}_2, \cdot, 1_{\mathbb{M}_2}) \text{ is a monoid homomorphism} \quad (217)$$

$$\forall a \in A, \forall b \in B, \psi(\iota_{A,1}(a)) = \iota_{A,2}(a), \quad \psi(\iota_{B,1}(b)) = \iota_{B,2}(b) \quad (218)$$

$$\forall m \in \mathbb{M}_1 - \gamma_1^{-1}(\{\emptyset\}), \quad m \in \text{dom}(\mathbb{I}_1) \Rightarrow \psi(m) \in \text{dom}(\mathbb{I}_2) \quad (219)$$

$$\forall m \in \hat{\mathbb{M}}_1, \quad \mathbb{I}_2(\psi(m)) = \psi(\mathbb{I}_1(m)) \quad (220)$$

$$\forall m \in \mathbb{M}_1, \gamma_2(\psi(m)) \supseteq \gamma_1(m) \quad (221)$$

$$\forall m \in \mathbb{M}_1, \forall \theta \in \gamma_1(m), \mu_2(\theta, \psi(m)) \supseteq \mu_1(\theta, m), \quad (222)$$

$$\forall m \in \mathbb{M}_1, \forall \theta \in \gamma_1(m), \delta_2(\theta, \psi(m)) \supseteq \delta_1(\theta, m). \quad (223)$$

We have thus replaced the axioms (36),(39),(40) by the weaker axioms (219),(222),(223). It remains true that the above list of axioms can be checked on the generators only, i.e. the following analogue of Lemma11 is true.

**Lemma 27.** *Let  $\mathcal{M}_2 = \langle \mathbb{M}_2, \cdot, 1_{\mathbb{M}_2}, \iota_{A,2}, \iota_{B,2}, \mathbb{I}_2, \gamma_2, \mu_2, \delta_2 \rangle$  be some AB-algebra. Let  $\mathbb{W}'$  be the sub-AB-algebra generated by some subalphabet  $\mathcal{W}' \subseteq \mathcal{W}$ , which is closed under  $\mathbb{I}_{\mathbb{W}}$ . Let  $\psi : \mathbb{W}' \rightarrow \mathbb{M}_2$  be some monoid-homomorphism. This map  $\psi$  is a weak AB-homomorphism if and only if,*

- 1-  $\iota_A \circ \psi = \iota_{A,2}, \quad \iota_B \circ \psi = \iota_{B,2}$
- and for every  $g \in \mathcal{W}' \cup A \cup B, \theta \in \gamma(g)$ :
- 2-  $g \in \text{dom}(\mathbb{I}) \Rightarrow \psi(g) \in \text{dom}(\mathbb{I}_2)$
- 2'-  $\mathbb{I}_2(\psi(g)) = \psi(\mathbb{I}(g))$
- 3-  $\gamma_2(\psi(g)) \supseteq \gamma(g)$
- 4-  $\mu_2(\theta, \psi(g)) \supseteq \mu(\theta, g)$
- 5-  $\delta_2(\theta, \psi(g)) \supseteq \delta(\theta, g)$ .

Given two AB-algebras  $\mathcal{M}_1, \mathcal{M}_2$ , we denote by  $\text{WHom}_{AB}(\mathcal{M}_1, \mathcal{M}_2)$  the set of all weak AB-homomorphisms from  $\mathcal{M}_1$  to  $\mathcal{M}_2$ .

Accordingly, we weaken the notion of  $H$ -involution. An involution  $\mathbb{I}'$  of the form (74,75), fulfilling conditions (76-78) is called *weakly  $H$ -realizable* if, for every  $k \in [1, p]$

$$\exists h_k \in I(H), \quad \gamma(W_k) \subseteq \gamma(h_k), \quad \mu(W_k) \subseteq \mu_t(h_k), \quad \delta(W_k) \subseteq \delta(h_k), \quad a_k h_k b_k = h_k^{-1}. \quad (224)$$

We denote by  $\mathcal{WI}$  the set of all partial involution  $\mathbb{I}'$  of the form (74,75) satisfying the four conditions (76)(77)(78) and (224). We call the elements of  $\mathcal{WI}$  the *weak  $H$ -involutions* of  $\mathbb{W}$ . We can then express the solutions of the original equation over  $\mathbb{G}$  via some *AB-* (resp. *weak AB-*) homomorphisms.

**Lemma 28.** Let  $\mathcal{DS} = \bigvee_{j \in J} \mathcal{DS}_j$  be a finite disjunction of systems of equations over  $\mathbb{G}$ , with rational constraint, where  $\mathcal{S}_j := ((E_i)_{1 \leq i \leq n}, \mu_A, \mu_{\mathcal{U}, j})$ . Let us suppose that  $\mathcal{DS}$  is in closed quadratic normal form. A monoid homomorphism

$$\sigma : \mathcal{U}^* \rightarrow \mathbb{G}$$

is a solution of  $\mathcal{S}$  if and only if, there exists an index  $j \in J$ , an admissible choice  $(\mathbf{W}, \mathbf{e})$  of variables of  $\mathcal{W}$  (resp. elements of  $A \cup B$ ), an alphabet  $\mathcal{W}' \subseteq \mathcal{W}$  possessing all these variables and closed under  $\mathbb{I}_{\mathbb{W}}$ , an involution  $\mathbb{I}' \in \mathcal{WT}$ , an AB-homomorphism  $\sigma_{\mathbb{W}} : (\langle \mathcal{W}' \rangle, \mathbb{I}) \rightarrow (\langle \mathcal{W}' \rangle, \mathbb{I}')$  and a weak AB-homomorphism  $\psi_t : (\langle \mathcal{W}' \rangle, \mathbb{I}') \rightarrow \mathbb{H}_t$  such that:

- (S1)  $\sigma_{\mathbb{W}}$  is a solution of  $\mathcal{S}_t(\mathcal{S}_j, \mathbf{W}, \mathbf{e})$ ,
- (S2)  $\sigma_{\mathbb{W}} \circ \psi_t$  is a solution of  $\mathcal{S}_{\mathbb{H}}(\mathcal{S}_j, \mathbf{W}, \mathbf{e})$ ,
- (S3)  $\sigma = \sigma_{\mathbf{W}, \mathbf{e}} \circ \sigma_{\mathbb{W}} \circ \psi_t \circ \bar{\pi}_{\mathbb{G}}$ .

(These maps were summarized on Figure 12 and form the left-lower part of Figure 16).

**Proof:** 1- Suppose that a monoid-homomorphism

$$\sigma : \mathcal{U}^* \rightarrow \mathbb{G}$$

is a solution of  $\mathcal{S}$ . By Lemma19, there exists an admissible choice  $(\mathbf{W}, \mathbf{e})$  of variables of  $\mathcal{W}_t$  and an AB-homomorphism  $\sigma_t : \mathbb{W}_t \rightarrow \mathbb{H}_t$  such that:

$$\sigma_t \text{ solves } \mathcal{S}_t(\mathcal{S}, \mathbf{W}, \mathbf{e}) \wedge \mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, \mathbf{e}) \quad (225)$$

$$\sigma = \sigma_{\mathbf{W}, \mathbf{e}} \circ \sigma_t \circ \bar{\pi}_{\mathbb{G}} \quad (226)$$

By Lemma20  $\sigma_t$  can be decomposed as

$$\sigma_t = \sigma_{\mathbb{W}} \circ \psi_t \quad (227)$$

where

$$\sigma_{\mathbb{W}} \in \text{Hom}_{AB}((\mathbb{W}_t, \mathbb{I}), (\mathbb{W}_t, \mathbb{I}')) \quad (228)$$

$$\mathbb{I}' \in \mathcal{I}. \quad (229)$$

such that

$$\sigma_{\mathbb{W}} \text{ solves } \mathcal{S}_t(\mathcal{S}, \mathbf{W}, \mathbf{e}) \quad (230)$$

Let us choose  $\mathcal{W}' := \mathcal{W}_t$ . By (230), (S1) is true; by (225) and (227) (S2) is true; by (226) and (227) (S3) is true.

2- Conversely, suppose that  $(\mathbf{W}, \mathbf{e}), \mathcal{W}', \mathbb{I}' \in \mathcal{WT}$ ,  $\sigma_{\mathbb{W}}, \psi_t$  are fulfilling (S1)(S2)(S3) and let us define  $\sigma_t := \sigma_{\mathbb{W}} \circ \psi_t, \sigma := \sigma_{\mathbf{W}, \mathbf{e}} \circ \sigma_t \circ \bar{\pi}_{\mathbb{G}}$ .

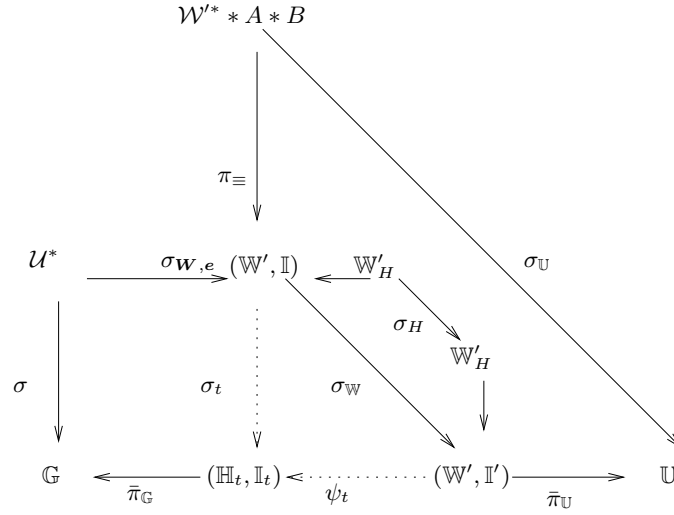
By (S1)(S2), the map  $\sigma_t$  is a weak-AB-homomorphism solving  $\mathcal{S}_t(\mathcal{S}, \mathbf{W}, \mathbf{e}) \wedge \mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, \mathbf{e})$ . The arguments given in subsubsection 5.2, adapted to a weak-H-involution  $\mathbb{I}'$  and a weak-AB-homomorphism  $\psi_t$  from a sub-AB-algebra  $(\langle \mathcal{W}' \rangle, \mathbb{I}')$  into  $\mathbb{H}_t$  show that  $\sigma$  is an over-solution of  $\mathcal{DS}$ , which is assumed in closed quadratic normal form, thus  $\sigma$  is a solution of  $\mathcal{DS}$ .  $\square$

By Proposition 3, every system  $\mathcal{S}_0$  of equations with rational constraints can be

reduced to a disjunction  $\mathcal{DS} = \bigvee_{j \in J} \mathcal{S}_j$  in closed quadratic normal form where  $\mathcal{S}_j = (\mathcal{S}, \mu_A, \mu_{\mathcal{U}, j})$  (i.e. the different systems are differing by their map  $\mu_{\mathcal{U}, j}$  only). This disjunction  $\mathcal{DS}$  can thus be solved by the following

**Algorithm Scheme:**

- 1- **Enumerate** the subalphabets  $\mathcal{W}'$  which are closed under the involutin  $\mathbb{I}_{\mathcal{W}}$ .
  - 2- **Enumerate** the involutions  $\mathbb{I}' \in \mathcal{WI}$ , the indices  $j \in J$  and the admissible vectors  $\mathbf{W}, e$ .
  - 3- **For** every value of  $\mathcal{W}', \mathbb{I}', j, \mathbf{W}, e$  :
  - 4-  $\mathbb{W}' := \langle \mathcal{W}' \rangle$ .
  - 5- **Find** a solution  $\sigma_{\mathbb{W}} \in \text{Hom}_{AB}((\mathbb{W}', \mathbb{I}), (\mathbb{W}', \mathbb{I}'))$  to the system  $\mathcal{S}_t(\mathcal{S}_j, \mathbf{W}, e)$  by the following procedure
    - 5.1- **Enumerate** all the  $\sigma_H \in \text{Hom}_{AB}((\mathbb{W}'_H, \mathbb{I}), (\mathbb{W}'_H, \mathbb{I}'))$ ,
    - 5.2- **Find** a solution  $\sigma_{\mathbb{U}}$  for the system  $\mathcal{S}_{\mathbb{U}}(\sigma_H)$ ,
    - 5.3-  $\sigma_{\mathbb{W}} := \Phi^{-1}(\sigma_{\mathbb{U}})$
  - 6- **Find** a  $\psi_t \in \text{WHom}_{AB}((\mathbb{W}', \mathbb{I}'), (\mathbb{H}_t, \mathbb{I}_t))$  such that  $\sigma_{\mathbb{W}} \circ \psi_t$  solves  $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, e)$ .
  - 7- **Endfor**
  - 8- **If** some pair  $\sigma_{\mathbb{W}}, \psi_t$  is found **then**  $\mathcal{DS}$  is satisfiable
  - 9- **else**  $\mathcal{DS}$  is unsatisfiable.
- (We summarize on Figure 16 the different maps to be found; dotted arrows cor-



**Fig. 16.** the algorithm: monoid case

respond to weak  $AB$ -homomorphisms). Let us precise how one can achieve every line of this scheme.

Line 5.2 is an instance of  $Q_1$ . Let us show that line 6 can be achieved by a Turing-reduction to  $Q_2$ .

By Lemma 27, line 6 amounts to find some tuple  $(\psi_t(W))_{W \in \mathcal{W}'}$  such that conditions 1-5 of Lemma 27 are fulfilled and  $(\psi_t(W))_{W \in \mathcal{W}'_H}$  is a solution of  $\sigma_{\mathbb{W}}(\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, e))$ . Conditions 1-5 can be expressed by the following constraints. For every  $W \in \mathcal{W}'_H$ :

$$C_I(W) := \mathbb{H} \quad \text{if } W \in \mathcal{W}' - \hat{\mathcal{W}}, \quad (231)$$

$$C_I(W) := I(\mathbb{H}) \quad \text{if } W \in \hat{\mathcal{W}}_0, \quad (232)$$

$$C_I(W_k) := \{h \in I(\mathbb{H}) \mid a_k h b_k = h^{-1}\}, \quad (233)$$

$$C_I(\bar{W}_k) := \{h \in I(\mathbb{H}) \mid a_k^{-1} h b_k^{-1} = h^{-1}\}, \quad \text{if } W_k \in \hat{\mathcal{W}}_0, \quad (234)$$

$$C_\gamma(W) := \{h \in \mathbb{H} \mid \gamma(W) \subseteq \gamma_t(h)\}, \quad (235)$$

$$C_\mu(W) := \{h \in \mathbb{H} \mid \mu(W) \subseteq \mu_t(h)\}, \quad (236)$$

$$C_\delta(W) := \{h \in \mathbb{H} \mid \forall \boldsymbol{\theta} \in \gamma(W), \delta(\boldsymbol{\theta}, W) \subseteq \delta_t(\boldsymbol{\theta}, h)\}. \quad (237)$$

$$C(W) := C_I(W) \cap C_\gamma(W) \cap C_\mu(W) \cap C_\delta(W). \quad (238)$$

For every  $W \in \mathcal{W}' - \mathcal{W}'_H$ :

$$C_I(W) := \{s \in \mathbb{H} * \{t, \bar{t}\}^* \mid W \in \text{dom}(\mathbb{I}') \Rightarrow s \in \text{dom}(\mathbb{I}_t)\}, \quad (239)$$

$$C_\gamma(W) := \{s \in \mathbb{H} * \{t, \bar{t}\}^* \mid \gamma(W) \subseteq \gamma_t(s)\}, \quad (240)$$

$$C_\mu(W) := \{s \in \mathbb{H} * \{t, \bar{t}\}^* \mid \mu(W) \subseteq \mu_t(s)\}, \quad (241)$$

$$C_\delta(W) := \{s \in \mathbb{H} * \{t, \bar{t}\}^* \mid \forall \boldsymbol{\theta} \in \gamma(W), \delta(\boldsymbol{\theta}, W) \subseteq \delta_t(\boldsymbol{\theta}, s)\}, \quad (242)$$

$$C(W) := C_I(W) \cap C_\gamma(W) \cap C_\mu(W) \cap C_\delta(W). \quad (243)$$

The values of the  $C_*(W)$  have been modified in such a way that, now, every subset  $C(W)$  with  $W \in \mathcal{W}'_H$  belongs to  $\text{EQ}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))$  while every subset  $C(W)$  with  $W \in \mathcal{W}' - \mathcal{W}'_H$  is recognized by some t-automaton with labels in  $\text{EQ}(\mathbb{H}, \mathcal{B}(\text{Rat}(\mathbb{H})))$ . Line 6 amounts thus to:

- find a solution in  $\mathbb{H}$  to the system  $\sigma_{\mathbb{W}}(\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, e))$  with the additional constraints  $C(W)$  for  $W \in \mathcal{W}'_H$ - this is an instance of  $Q_2$
- find an element in the set  $C(W)$  for  $W \in \mathcal{W}' - \mathcal{W}'_H$ - this reduces to finitely many instances of  $Q_2$ .

We have thus proved Proposition 7.

**Theorem 2.** *Let  $\mathbb{H}$  be a cancellative monoid and  $\mathbb{G}$  an HNN-extension of  $\mathbb{H}$  with finite associated subgroups  $A, B$ . The satisfiability problem for systems of equations with rational constraints in  $\mathbb{G}$  is Turing-reducible to the SAT-problem for systems of equations with rational constraints in  $\mathbb{H}$*

**Proof:** Let  $\mathbb{H}$  be a cancellative monoid and  $\mathbb{G}$  an HNN-extension of  $\mathbb{H}$  with finite associated subgroups. By Proposition 7 the satisfiability problem for systems of equations with rational constraints in  $\mathbb{G}$  is Turing-reducible to a certain pair of problems  $(Q_1, Q_2)$ , where  $Q_1$  is the SAT-problem for systems of equations with rational constraints in a group  $\mathbb{U}$  having a presentation in  $\text{PHNN}(A)$ . But, due to the structure of  $\mathbb{U}$  (see §8.1) and to Theorem 1, this problem  $Q_1$  is decidable. Thus the pair  $(Q_1, Q_2)$  is Turing-reducible to the single problem  $Q_2$ , i.e. the

SAT-problem for systems of equations with rational constraints in  $\mathbb{H}$ .  $\square$

The two following sections are stating some variants of the main Theorem 2. The variations consist in considering:

- other kinds of constraints: *positive* rational constraints, positive *subgroup* constraints, *constant* constraints,
- not only equations but also *disequations*
- the operation of free product with *amalgamation* instead of the operation of HNN-extension.

It turns out that all these variations lead to an analogue of Theorem 2.



## 9 Equations with positive rational constraints over $\mathbb{G}$

### 9.1 Positive rational constraints

We consider here constraints over the variables consisting of a rational subset of the monoid (while in Theorem 2 the constraints were consisting in *boolean combinations* of rational subsets). More formally, we call system of equations with *positive* rational constraints in the monoid  $\mathbb{M}$ , any system of equations  $\mathcal{S}$  with constraints in  $\mathcal{C} = \text{Rat}(\mathbb{M})$ .

**Theorem 3.** *Let  $\mathbb{H}$  be a cancellative monoid and  $\mathbb{G}$  an HNN-extension of  $\mathbb{H}$  with finite associated subgroups. The satisfiability problem for systems of equations with positive rational constraints in  $\mathbb{G}$  is Turing-reducible to the SAT-problem for systems of equations with positive rational constraints in  $\mathbb{H}$ .*

**Sketch of proof:** It suffices to adapt the reduction given in the proof of Theorem 2:

- the *strict normal* partitioned finite  $t$ -automaton  $\mathcal{A}$  with labeling set  $\mathcal{B}(\text{Rat}(\mathbb{H}))$  is replaced by, merely, a *normal* partitioned finite  $t$ -automaton  $\mathcal{A}$  with labeling set  $\text{Rat}(\mathbb{H})$ ; the existence of such a  $t$ -automaton recognizing the given positive constraints is ensured by Proposition 1, point (1).
- the AB-algebra  $\mathbb{H}_t$  is replaced by the AB-algebra  $\mathbb{H}_{t+}$ .
- the notion of *weakly  $H$ -realizable* involution is replaced by the following notion of *weakly positively  $H$ -realizable* involution:  
an involution  $\mathbb{I}'$  of the form (74,75), fulfilling conditions (76-78) is called *weakly positively  $H$ -realizable* if, for every  $k \in [1, p]$ ,

$$\exists h_k \in I(H), \gamma(W_k) \subseteq \gamma_+(h_k), \mu(W_k) \subseteq \mu_t(h_k), \delta(W_k) \subseteq \delta_t(h_k), a_k h_k b_k = h_k^{-1}. \quad (244)$$

- for every  $W \in \mathcal{W}'_H$ :  $\mathcal{C}_\gamma(W) := \{h \in \mathbb{H} \mid \gamma(W) \subseteq \gamma_+(h)\}$ ,
- for  $W \in \mathcal{W}' \setminus \mathcal{W}'_H$ :  $\mathcal{C}_\gamma(W) := \{s \in \mathbb{H} * \{t, \bar{t}\}^* \mid \gamma(W) \subseteq \gamma_+(s)\}$ ,
- for  $W \in \mathcal{W}' \setminus \mathcal{W}'_H$ , each of the sets  $\mathcal{C}_I(W), \mathcal{C}_\gamma(W), \mathcal{C}_\mu(W), \mathcal{C}_\delta(W)$  is recognized by a  $t$ -automaton with labels in  $\text{EQ}(\mathbb{H}, \text{Rat}(\mathbb{H}))$ .  $\square$

### 9.2 Positive subgroup constraints

We consider here the case where  $\mathbb{G}$  is the HNN-extension of a group  $\mathbb{H}$  by an isomorphism  $\varphi : A \rightarrow A$  from a finite subgroup  $A$  of  $\mathbb{H}$  into itself. Let  $C_1, \dots, C_n$  be finitely generated subgroups of  $\mathbb{H}$  containing  $A$ ; let us consider the sets:

$$\mathcal{C}_{\mathbb{H}} := \{C_1, \dots, C_n\}; \quad \mathcal{C}_{\mathbb{G}} := \{C_1, \dots, C_n, \langle C_1, t \rangle, \dots, \langle C_n, t \rangle\}.$$

The set of constraints  $\mathcal{C}_{\mathbb{G}}$  turns out to be useful for the decidability of the positive first-order theory of  $\mathbb{G}$  (see [LS05]).

**Theorem 4.** *Let  $\mathbb{H}$  be a group and  $\mathbb{G}$  an HNN-extension of  $\mathbb{H}$  with finite associated subgroups  $A = B$ . The satisfiability problem for systems of equations over  $\mathbb{G}$  with constraints in  $\mathcal{C}_{\mathbb{G}}$  is Turing-reducible to the SAT-problem for systems of equations over  $\mathbb{H}$  with constraints in  $\mathcal{C}_{\mathbb{H}}$ .*

**Sketch of proof:** It suffices to adapt the reduction given in the proof of Theorem 2:

- the *strict normal* partitioned finite  $t$ -automaton  $\mathcal{A}$  with labeling set  $\mathcal{B}(\text{Rat}(\mathbb{H}))$  is replaced by a *normal* partitioned finite  $t$ -automaton  $\mathcal{A}$  with labeling set  $\{\{a\} \mid a \in A\} \cup \mathcal{C}_{\mathbb{H}}$ .
- the AB-algebra  $\mathbb{H}_t$  is replaced by the AB-algebra  $\mathbb{H}_{t+}$ .
- the notion of weakly  $H$ -realizable involution is replaced by the notion of weakly *positively*  $H$ -realizable involution.

Let us describe more precisely the necessary adaptations. Given a finitely generated subgroup  $C_i$ , we consider the fta  $\mathcal{A}_i$  that possesses exactly two states  $(1, H)$  (its initial state) and  $(1, 1)$  (its terminal state) and one transition  $((1, H), C_i, (1, 1))$ . This fta  $\mathcal{A}_i$  is trivially partitioned,  $\approx$ -compatible  $\sim$ -saturated, unitary and it recognizes the subgroup  $C_i$ . Let us consider now the fta  $\mathcal{B}_i$  obtained from the fta  $\mathcal{G}_6$  by replacing each occurrence of the label  $\mathbb{H}$  by the label  $C_i$ . This fta  $\mathcal{B}_i$  is partitioned,  $\approx$ -compatible (because  $A \subseteq C_i$ ),  $\sim$ -saturated (because each of the four states  $(A, T), (B, H), (B, T), (A, H)$  has a loop labeled by  $A$ ) unitary (because, for every vertex-type  $\theta$ , there exists only one state mapped to the type  $\theta$  by  $\tau$ ) and recognizes the subgroup  $\langle C_i, t \rangle$ .

Let  $\mathcal{A}$  be the direct product of all these partitioned fta  $\mathcal{A}_i$  and  $\mathcal{B}_i$ .

The fta  $\mathcal{A}$  is a partitioned fta which is also  $\approx$ -compatible and  $\sim$ -saturated (by Lemma 5 of [LS08]) and unitary (because unitarity is also preserved by direct product). Given a finite set of constraints  $\mu : \mathcal{U}^* \rightarrow \mathcal{C}_{\mathbb{G}}$ , there exists  $I_U \subseteq Q_{\mathcal{A}}, T_U \subseteq Q_{\mathcal{A}}$  such that

$$\mathbf{C}(U) = \{g \in \mathbb{G} \mid (I_U \times T_U) \cap \mu_{\mathcal{A}, \mathbb{G}}(g) \neq \emptyset\}.$$

Any system of equations  $\mathcal{S}_0$  over  $\mathbb{G}$  with constraints in  $\mathcal{C}_{\mathbb{G}}$  can thus be reduced to a disjunction  $\bigvee_{j \in J} \mathcal{S}_{1,j}$  of systems of equations with rational constraints over  $\mathbb{G}$  with set of variables  $\mathcal{U}_1 \supseteq \mathcal{U}_0$ , of the form (115), fulfilling points (1-3-4-5) of Proposition 3 and point (2), with the modification that the finite  $t$ -automaton  $\mathcal{A}$  is a normal partitioned finite  $t$ -automaton (which might be non-strict) over the labelling set  $\{\{a\} \mid a \in A\} \cup \mathcal{C}_{\mathbb{H}}$ . Line 6 of the Algorithm Scheme amounts to:

- find a solution in  $\mathbb{H}$  to the system  $\sigma_{\mathbb{W}}(\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, \mathbf{e}))$  with the additional constraints  $\mathbf{C}(W)$  for  $W \in \mathcal{W}'_H$ ; this is an instance of the SAT-problem for systems of equations with constraints in  $\mathcal{C}_{\mathbb{H}}$
- find an element in the set  $\mathbf{C}(W)$  for  $W \in \mathcal{W}' - \mathcal{W}'_H$ ; the set  $\mathbf{C}(W)$  is recognized by a finite  $t$ -automaton where each label is the set of solutions of a system of equations in  $\mathbb{H}$  with constraints in  $\mathcal{C}_{\mathbb{H}}$ ; this problem thus reduces to finitely many instances of the SAT-problem for systems of equations with constraints in  $\mathcal{C}_{\mathbb{H}}$ .

□

### 9.3 Constants

The sets of constraints corresponding to so-called equations *with constants* are

$$\mathcal{C}_{\mathbb{H}} := \{\{h\} \mid h \in \mathbb{H}\} \cup \{\mathbb{H}\}; \quad \mathcal{C}_{\mathbb{G}} := \{\{g\} \mid g \in \mathbb{G}\} \cup \{\mathbb{G}\}.$$

**Theorem 5.** *Let  $\mathbb{H}$  be a cancellative monoid and  $\mathbb{G}$  an HNN-extension of  $\mathbb{H}$  with finite associated subgroups. The satisfiability problem for systems of equations with constants in  $\mathbb{G}$  is Turing-reducible to the SAT-problem for systems of equations with constants in  $\mathbb{H}$ .*

**Sketch of proof:** It suffices to adapt the reduction given in the proof of Theorem 2:

- the *strict normal* partitioned finite  $t$ -automaton  $\mathcal{A}$  with labeling set  $\mathcal{B}(\text{Rat}(\mathbb{H}))$  is replaced by, merely, a *normal* partitioned finite  $t$ -automaton  $\mathcal{A}$  with labeling set  $\mathcal{C}_{\mathbb{H}}$ .
- the AB-algebra  $\mathbb{H}_t$  is replaced by the AB-algebra  $\mathbb{H}_{t+}$ .
- the notion of weakly  $H$ -realizable involution is replaced by the notion of weakly *positively*  $H$ -realizable involution.

□

## 10 Equations and disequations with rational constraints over $\mathbb{G}$

We recall that the notion of systems of equations and disequations with rational constraints over a monoid has been defined in §2.4.

### 10.1 Rational constraints

Let us show how to reduce a system of equations and disequations (with rational constraints) over  $\mathbb{G}$  to a systems of equations (with rational constraints) over  $\mathbb{H}_t$  together with a system of equations/disequations (with rational constraints) over  $\mathbb{H}$ .

Let us start with a system of equations/disequations with rational constraints, over  $\mathbb{G}$ , which is in normal form (see Proposition 4):

$$((E_i)_{1 \leq i \leq n}, (\bar{E}_i)_{n+1 \leq i \leq 2n}, \mu_{\mathcal{A}, \mathbb{G}}, \mu_{\mathcal{U}}) \quad (245)$$

The equations  $E_i$  have the form

$$E_i : (U_{i,1}, U_{i,2} U_{i,3}) \text{ for all } 1 \leq i \leq n \quad (246)$$

while the disequations  $\bar{E}_i$  have the form

$$\bar{E}_i : (U_{i,1}, U_{i,2}) \text{ for all } n+1 \leq i \leq 2n \quad (247)$$

where, for every  $i \in [1, n]$ , the symbols  $U_{i,1}, U_{i,2}, U_{i,3}, U_{n+i,1}, U_{n+i,2}$  belong to the alphabet of unknowns  $\mathcal{U}$ . Let us consider the alphabet  $\mathcal{V}_0 := [1, 2n] \times [1, 3] \times [1, 9]$  and the alphabet  $\mathcal{W}$  constructed from this  $\mathcal{V}_0$  in §3.6. We consider all the vectors  $(W_{i,j,k})$  where  $1 \leq i \leq 2n, 1 \leq j \leq 3, 1 \leq k \leq 9$  of elements of  $\mathcal{W} \cup \{1\}$  and all triple  $(e_{i,1,2}, e_{i,2,3}, e_{i,3,1}) \in (A \cup B)^3$  such that: the vectors

$$(W_{i,j,k})_{1 \leq i \leq n, 1 \leq j \leq 3, 1 \leq k \leq 9}, (e_{i,1,2}, e_{i,2,3}, e_{i,3,1})_{1 \leq i \leq n}$$

fulfill conditions (120-130) and their counterpart for disequations

$$(W_{i,j,k})_{n+1 \leq i \leq 2n, 1 \leq j \leq 2, 1 \leq k \leq 9}, (e_{i,1,2})_{n+1 \leq i \leq 2n}$$

fulfill the analogous conditions:

$$p_1(W_{i,j,k}) = (i, j, k) \in \mathcal{V}_0 \quad \text{for } W_{i,j,k} \neq 1 \quad (248)$$

$$\gamma\left(\prod_{k=1}^9 W_{i,j,k}\right) = (1, H, b, 1, 1) \quad \text{for some } b \in \{0, 1\} \quad (249)$$

$$\mu\left(\prod_{k=1}^9 W_{i,j,k}\right) = \mu_{\mathcal{U}}(U_{i,j}) \quad (250)$$

$$\gamma\left(\prod_{k=1}^4 W_{i,1,k}\right) = \gamma\left(\prod_{k=1}^4 W_{i,2,k}\right) \quad (251)$$

$$W_{i,j,5} \in \mathcal{W} \wedge \gamma(W_{i,j,5}) \text{ is a H-type} \quad (252)$$

$$e_{i,1,2} \in \text{Gi}(W_{i,1,5}) = \text{Gi}(W_{i,2,5}) \quad (253)$$

A vector  $(\mathbf{W}, \mathbf{e})$  fulfilling (120-130) for the indices  $i \in [1, n]$  and (248-253) for the indices  $i \in [n+1, 2n]$ , is called an *admissible* vector. For every admissible vector  $(\mathbf{W}, \mathbf{e})$  we define the following equations and disequations:

$$\prod_{k=1}^9 W_{i,j,k} = \prod_{k=1}^9 W_{i',j',k} \quad \text{if } U_{i,j} = U_{i',j'} \quad (254)$$

$$W_{i,1,1} W_{i,1,2} W_{i,1,3} W_{i,1,4} e_{i,1,2} = W_{i,2,1} W_{i,2,2} W_{i,2,3} W_{i,2,4} \quad (255)$$

for all  $1 \leq i \leq 2n$

$$W_{i,2,6} W_{i,2,7} W_{i,2,8} W_{i,2,9} = e_{i,2,3} \overline{W}_{i,3,4} \overline{W}_{i,3,3} \overline{W}_{i,3,2} \overline{W}_{i,3,1} \quad (256)$$

$$W_{i,1,5} W_{i,1,6} W_{i,1,7} W_{i,1,8} = e_{i,1,3} W_{i,3,6} W_{i,3,7} W_{i,3,8} W_{i,3,9} \quad (257)$$

$$W_{i,1,5} = e_{i,1,2} W_{i,2,5} e_{i,2,3} W_{i,3,5} e_{i,3,1} \quad (258)$$

for all  $1 \leq i \leq n$

$$\bigwedge_{d \in \text{Ge}(W_{i,1,5})} W_{i,1,5} \cdot d \neq e_{i,1,2} \cdot W_{i,2,5} \quad (259)$$

for all  $n+1 \leq i \leq 2n$  such that  $\tau e(W_{i,1,5}) = \tau e(W_{i,2,5})$ .

We denote by  $\mathcal{S}_t(\mathcal{S}, \mathbf{W}, \mathbf{e})$  the sequence of equations (254-257), by  $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, \mathbf{e})$  the sequence of equations and disequations (258-259). For every  $(i, j) \in [1, n] \times [1, 3] \cup [n+1, 2n] \times [1, 2]$  we denote by  $\overline{i, j}$  the smallest pair such that  $U_{i,j} = U_{\overline{i, j}}$ . By  $\sigma_{\mathbf{W}, \mathbf{e}} : \mathcal{U}^* \rightarrow \mathbb{W}$  we denote the unique monoid-homomorphism such that,

$$\sigma_{\mathbf{W}, \mathbf{e}}(U_{i,j}) = \prod_{k=1}^9 W_{\overline{i, j}, k}.$$

**Lemma 29.** *Let  $\mathcal{S} = ((E_i)_{1 \leq i \leq n}, (\bar{E}_i)_{n+1 \leq i \leq 2n}, \mu_{\mathcal{A}, \mathbb{G}}, \mu_{\mathcal{U}})$  be a system of equations and disequations over  $\mathbb{G}$ , with rational constraint. Let us suppose that  $\mathcal{S}$  is in quadratic normal form. A monoid homomorphism*

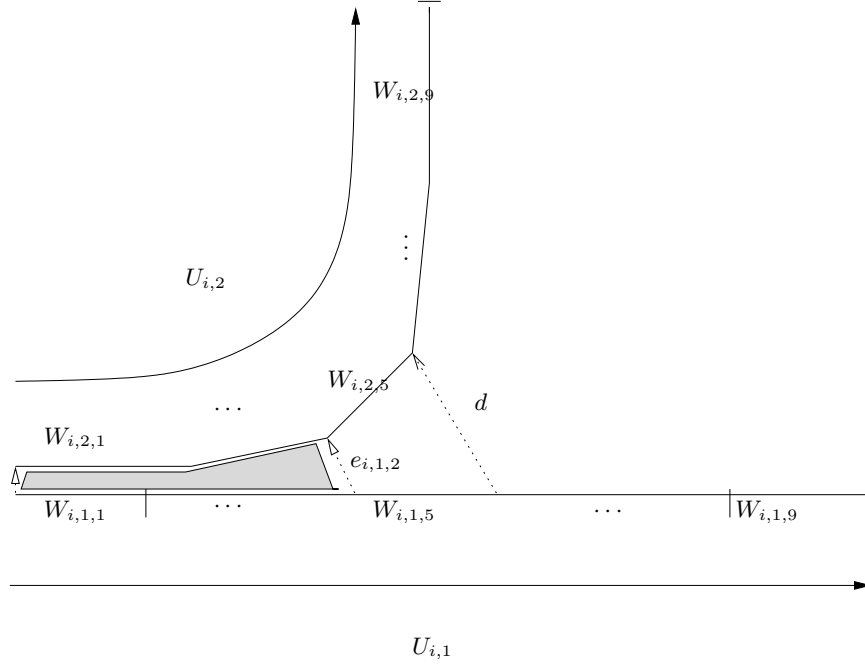
$$\sigma : \mathcal{U}^* \rightarrow \mathbb{G}$$

*is a solution of  $\mathcal{S}$  if and only if, there exists an admissible choice  $(\mathbf{W}, \mathbf{e})$  of variables of  $\mathcal{W}_t$  and elements of  $A \cup B$  and an AB-homomorphism*

$$\sigma_t : \mathbb{W}_t \rightarrow \mathbb{H}_t$$

*solving simultaneously the system  $\mathcal{S}_t(\mathcal{S}, \mathbf{W}, \mathbf{e})$  of equations over  $\mathbb{H}_t$  and the system  $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, \mathbf{e})$  of equations and disequations over  $\mathbb{H}$ , and such that*

$$\sigma = \sigma_{\mathbf{W}, \mathbf{e}} \circ \sigma_t \circ \bar{\pi}_{\mathbb{G}}.$$



**Fig. 17.** Disequation cut into 3 parts

**From  $\mathbb{G}$ -solutions to  $\mathbf{t}$ -solutions** Let  $\sigma : \mathcal{U}^* \rightarrow \mathbb{G}$  be a monoid homomorphism solving the system  $\mathcal{S}$ . For every  $1 \leq i \leq n$  we construct the vector  $(W_{i,*,*}, e_{i,*,*})$  as in §5.2. Let us fix now some disequation from  $\mathcal{S}$ , i.e. some integer  $n+1 \leq i \leq 2n$ . Let us choose, for every  $j \in [1, 2]$ , some  $s_{i,j} \in \text{Red}(\mathbb{H}, t)$  such that:

$$\sigma(U_{i,j}) = \pi_G(s_{i,j}).$$

Let us consider some decomposition of the form (5) for  $s_{i,2}, s_{i,1}$ :

$$s_{i,2} = h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_\lambda} h_\lambda \cdots t^{\alpha_\ell} h_\ell, \quad (260)$$

$$s_{i,1} = h'_0 t^{\alpha'_1} h'_1 \cdots t^{\alpha'_\lambda} h'_\lambda \cdots t^{\alpha'_{\ell'}} h'_{\ell'}, \quad (261)$$

We know that  $s_{i,1} \not\approx s_{i,2}$ . Let us distinguish the possible forms for  $s_{i,1}$ , as represented on figures 18-20.

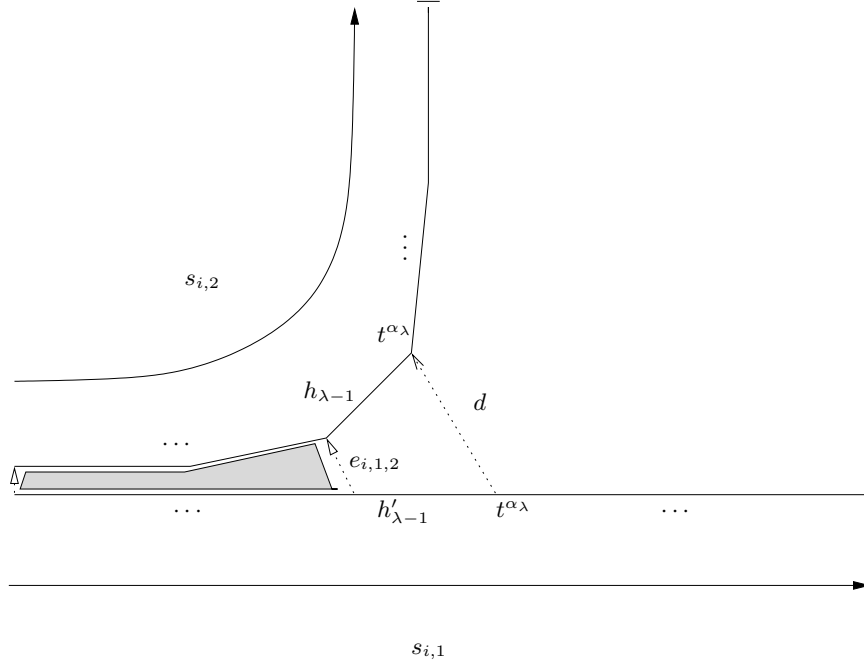
**Case 1:** there exists some integer  $\lambda \in [2, \ell]$ , some  $e_{i,1,2} \in B(\alpha_{\lambda-1})$  such that

$$h_0 \cdots t^{\alpha_{\lambda-1}} h_{\lambda-1} = h'_0 \cdots t^{\alpha_{\lambda-1}} h'_{\lambda-1} e_{i,1,2}, \quad \alpha_\lambda = \alpha'_\lambda$$

$$e_{i,1,2} h_{\lambda-1} \neq h'_{\lambda-1} d \quad \text{for all } d \in A(\alpha_\lambda).$$

We consider the following factors of  $s_{i,2}, s_{i,1}$ :

$$P_{i,2} = h_0 \cdots t^{\alpha_{\lambda-1}}, \quad M_{i,2} = h_{\lambda-1}, \quad S_{i,2} = t^{\alpha_\lambda} \cdots t^{\alpha_\ell} h_\ell.$$



**Fig. 18.** Disequations, case 1

$$P_{i,1} = h'_0 \cdots t^{\alpha_{\lambda-1}}, \quad M_{i,1} = h'_{\lambda-1}, \quad S_{i,1} = t^{\alpha_\lambda} \cdots t^{\alpha_{\ell'}} h'_{\ell'}.$$

Following the lines of §5.2, these reduced sequences can be cut into nine factors  $(P_{i,j,k})$ ,  $1 \leq j \leq 2, 1 \leq k \leq 9$ , and subsequently lifted to nine letters  $(W_{i,j,k})$ ,  $1 \leq j \leq 2, 1 \leq k \leq 9$ , such that the vector  $(W_{i,*,*}, e_{i,1,2})$  fulfills conditions (248-253) and the classes  $([P_{i,*,*}]_{\sim})$  fulfill equations and disequations (255),(259). We can define  $\sigma_t(W_{i,j,k}) = [P_{i,j,k}]_{\sim}$ ;  $\sigma_t$  can be extended into an AB-homomorphism solving both systems  $\mathcal{S}_t(\mathcal{S}, \mathbf{W}, \mathbf{e})$ ,  $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, \mathbf{e})$  and such that

$$\sigma = \sigma_{\mathbf{W}, \mathbf{e}} \circ \sigma_t \circ \bar{\pi}_{\mathbb{G}}.$$

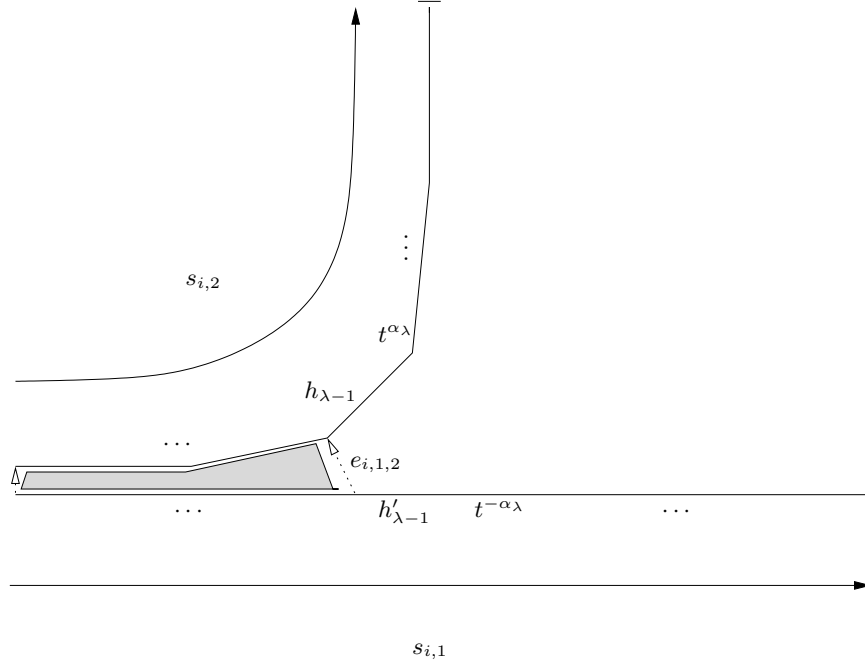
**Case 2:** there exists  $\lambda \in [2, \ell]$ , some  $e_{i,1,2} \in B(\alpha_{\lambda-1})$  such that

$$h_0 \cdots t^{\alpha_{\lambda-1}} h_{\lambda-1} = h'_0 \cdots t^{\alpha_{\lambda-1}} h'_{\lambda-1} e_{i,1,2}, \quad \alpha_\lambda = -\alpha'_\lambda$$

We consider the factors  $P_{i,2}, M_{i,2}, S_{i,2}, P_{i,1}, M_{i,1}$  defined by the same formulas as in case 1, and define

$$S_{i,1} = t^{-\alpha_\lambda} \cdots t^{\alpha_{\ell'}} h'_{\ell'}.$$

This time we obtain a vector  $(W_{i,*,*})$  such that  $\tau e(W_{i,1,5}) \neq \tau e(W_{i,2,5})$ . It follows there is no disequation (259) associated to this index  $i$ . The vector  $(W_{i,*,*}, e_{i,1,2})$  fulfills conditions (248-253) and the classes  $([P_{i,*,*}]_{\sim})$  fulfill equation (255).



**Fig. 19.** Disequations, case 2

**Case 3:** there exists  $\lambda \in [2, \ell]$ , such that

$$s_{i,1} = h_0 \cdots t^{\alpha_{\lambda-1}} h_{\lambda-1}.$$

This case can be treated similarly as case 2. We just define  $S_{i,1} = 1$  and, correspondingly  $W_{i,1,k} = 1$ , for  $6 \leq k \leq 9$ .

**Case 4:** there exists some integer  $\lambda \in [2, \ell']$ , such that

$$s_{i,2} = h_0 \cdots t^{\alpha_{\lambda-1}} h_{\lambda-1}.$$

This case is obtained from case 3 by exchanging  $s_{i,1}$  with  $s_{i,2}$ .

It remains to treat some degenerated cases.

**Case 5:**  $\lambda = 1 \leq \ell$ , fulfills one of the conditions defining cases 1-3 (except beeing smaller than 2) or  $\lambda = 1 \leq \ell'$  fulfills the conditions defining case 4 (except beeing smaller than 2).

We take:  $P_{i,1} = P_{i,2} = 1$ ,  $e_{i,1,2} = 1$ ,  $S_{i,1} = 1$  (under the condition of case 3),  $S_{i,2} = 1$  (under the condition of case 4).

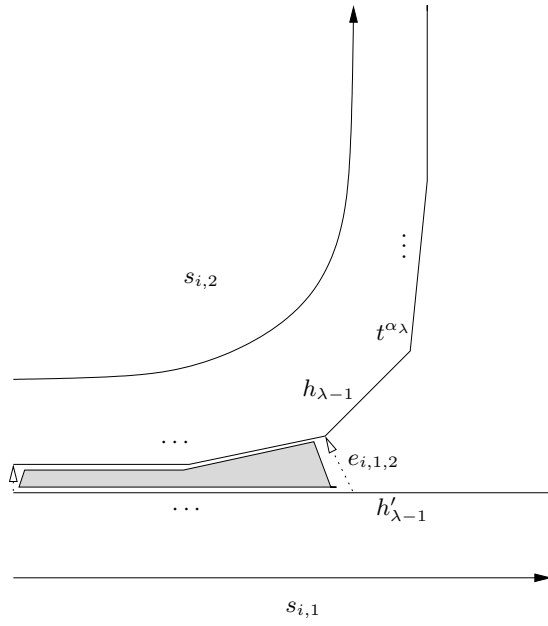
The construction is ended as in the degenerated cases of §5.2.

**Case 6:**  $\ell = \ell' = 0$ .

We take:  $P_{i,1} = P_{i,2} = 1$ ,  $e_{i,1,2} = 1$ ,  $S_{i,1} = S_{i,2} = 1$ .

The construction is ended as in the degenerated cases of §5.2.





**Fig. 20.** Disequations, case 3

**From t-solutions to  $\mathbb{G}$ -solutions** Let  $\sigma_t : \mathbb{W}_t \rightarrow \mathbb{H}_t$  be an  $AB$ -homomorphism solving both systems  $\mathcal{S}_t(\mathcal{S}, \mathbf{W}, e)$  and  $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, e)$ . Owing to the proofs of §5.2, we just have to prove that for every  $i \in [n+1, 2n]$ ,

$$\sigma_t(\sigma_{\mathbf{W},e}(U_{i,1})) \not\approx \sigma_t(\sigma_{\mathbf{W},e}(U_{i,2})).$$

Using equation (254) and the definition of  $\sigma_{\mathbf{W},e}$ , the above inequalities are equivalent with

$$\sigma_t\left(\prod_{k=1}^9 W_{i,1,k}\right) \not\approx \sigma_t\left(\prod_{k=1}^9 W_{i,2,k}\right). \quad (262)$$

Equation (255) states that

$$\sigma_t\left(\prod_{k=1}^4 W_{i,1,k}\right) e_{i,1,2} \approx \sigma_t\left(\prod_{k=1}^4 W_{i,2,k}\right). \quad (263)$$

Let us distinguish several cases according to the values of  $\tau e(W_{i,j,5})$ . Since, by (252),  $\gamma(W_{i,j,5})$  are H-types, one of the following cases must occur.

**Case 1:**  $\tau e(W_{i,2,5}) = \tau e(W_{i,1,5}) = (1, 1)$

By (249),  $\gamma(\prod_{k=6}^9 W_{i,j,k}) = (1, 1, 0, 1, 1)$  for  $j \in [1, 2]$ , which implies that, for every  $j \in [1, 2]$ :

$$\sigma_t\left(\prod_{k=1}^9 W_{i,j,k}\right) = \sigma_t\left(\prod_{k=1}^5 W_{i,j,k}\right), \quad (264)$$

But disequation (259) reads:

$$\sigma_t(W_{i,1,5}) \neq_{\mathbb{H}_t} e_{i,1,2} \cdot \sigma_t(W_{i,2,5}). \quad (265)$$

The conjunction of (263)(264)(265) proves inequality (262).

**Case 2:**  $\tau e(W_{i,2,5}) = \tau e(W_{i,1,5}) = (A, T)$

Since  $\sigma_t$  is a solution of equation (255) and disequation (259), two representatives of  $\sigma_t(\prod_{k=1}^5 W_{i,2,k})$ , ( resp.  $\sigma_t(\prod_{k=1}^5 W_{i,1,k})$ ) cannot be prefixes of two reduced sequences which are equivalent modulo  $\sim$ . Thus (262) is established.

**Case 3:**  $\tau e(W_{i,2,5}) = \tau e(W_{i,1,5}) = (B, T)$

Same argument as for case 2.

**Case 4:**  $\tau e(W_{i,2,5}) \neq \tau e(W_{i,1,5})$

This shows that the projections of  $\sigma_t(\prod_{k=1}^9 W_{i,2,k})$ ,  $\sigma_t(\prod_{k=1}^9 W_{i,1,k})$  on  $\{t, \bar{t}\}^*$  are non-equal, so that, a fortiori, inequality (262) holds.

**Theorem 6.** *Let  $\mathbb{H}$  be a cancellative monoid and  $\mathbb{G}$  an HNN-extension of  $\mathbb{H}$  with finite associated subgroups  $A, B$ . The satisfiability problem for systems of equations and disequations with rational constraints in  $\mathbb{G}$  is Turing-reducible to the SAT-problem for systems of equations and disequations with rational constraints in  $\mathbb{H}$*

In order to prove this theorem we must, as for proving Theorem 2, cope with the fact that we do not know an algorithm testing the satisfiability over  $\mathbb{H}$  of an equation with the constraint  $\mathbb{H} \setminus \mathbb{I}(\mathbb{H})$  (the set of non-units of the monoid  $\mathbb{H}$ ). Therefore we use again the notion of *weak-AB-homomorphism*<sup>2</sup>. We first adapt Lemma 28 into the following

**Lemma 30.** *Let  $\mathcal{DS} = \bigvee_{j \in J} \mathcal{S}_j$  be a finite disjunction of systems of equations and disequations over  $\mathbb{G}$ , with rational constraint defined by a strict normal fta  $\mathcal{A}$  with labelling set  $\mathcal{B}(\text{Rat}(\mathbb{H}))$  and where  $\mathcal{S}_j := ((E_i)_{1 \leq i \leq n}, (\bar{E}_i)_{n+1 \leq i \leq 2n}, \mu_A, \mu_{\mathcal{U}, j})$ . Let us suppose that  $\mathcal{DS}$  is in closed quadratic normal form. A monoid homomorphism*

$$\sigma : \mathcal{U}^* \rightarrow \mathbb{G}$$

*is a solution of  $\mathcal{DS}$  if and only if, there exists and index  $j \in J$ , an admissible choice  $(\mathbf{W}, \mathbf{e})$  of variables of  $\mathcal{W}$  (resp. elements of  $A \cup B$ ), an alphabet  $\mathcal{W}' \subseteq \mathcal{W}$  possessing all these variables and closed under  $\mathbb{I}_{\mathbb{W}}$ , an involution  $\mathbb{I}' \in \mathcal{WI}$ , an AB-homomorphism  $\sigma_{\mathbb{W}} : (\langle \mathcal{W}' \rangle, \mathbb{I}) \rightarrow (\langle \mathcal{W}' \rangle, \mathbb{I}')$  and a weak AB-homomorphism  $\psi_t : (\langle \mathcal{W}' \rangle, \mathbb{I}') \rightarrow \mathcal{H}_t$  such that:*

- (S1)  $\sigma_{\mathbb{W}}$  is a solution of the system of equations  $\mathcal{S}_t(\mathcal{S}_j, \mathbf{W}, \mathbf{e})$ ,
- (S2)  $\sigma_{\mathbb{W}} \circ \psi_t$  is a solution of the system of equations and disequations  $\mathcal{S}_{\mathbb{H}}(\mathcal{S}_j, \mathbf{W}, \mathbf{e})$ ,
- (S3)  $\sigma = \sigma_{\mathbf{W}, \mathbf{e}} \circ \sigma_{\mathbb{W}} \circ \psi_t \circ \bar{\pi}_{\mathbb{G}}$ .

<sup>2</sup> though we might also use a notion weaker than AB-hom and stronger than weak-AB-hom, since we are able to translate the conditions over  $\gamma, \mu, \delta$  by equations and disequations with rational constraints.

This lemma can be proved in the same way as Lemma 28.

**Sketch of proof** of Theorem 6: It suffices to adapt the reductions given in the proof of Theorem 2 as follows:

- Lemma 28 is replaced by Lemma 30
  - Instead of a system of equations with rational constraints in  $\mathbb{H}$  we use the system  $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, \mathbf{e})$  of equations and disequations with rational constraints in  $\mathbb{H}$  supplied by Lemma 29.
- 

## 10.2 Positive rational constraints

Here we consider  $\mathcal{C}_{\mathbb{G}} := \text{Rat}(\mathbb{G})$  and  $\mathcal{C}_{\mathbb{H}} := \text{Rat}(\mathbb{H})$ .

**Theorem 7.** *Let  $\mathbb{H}$  be a cancellative monoid and  $\mathbb{G}$  an HNN-extension of  $\mathbb{H}$  with finite associated subgroups  $A, B$ . The satisfiability problem for systems of equations and disequations with positive rational constraints in  $\mathbb{G}$  is Turing-reducible to the SAT-problem for systems of equations and disequations with positive rational constraints in  $\mathbb{H}$*

In order to prove this theorem we must, as for proving Theorem 2, cope with the fact that we do not know an algorithm testing a set of the form  $\{s \in \mathbb{H} * \{t, \bar{t}\}^* \mid \mu_t(s) = \mu(W)\}$  for emptiness: such a set is not known to be recognized by a t-automaton with labels which are defined by equations, disequations and positive rational constraints over  $\mathbb{H}$ . Therefore we use the notion of *weak-AB-homomorphism*.

**Lemma 31.** *Let  $\mathcal{DS} = \bigvee_{j \in J} \mathcal{S}_j$  be a finite disjunction of systems of equations and disequations over  $\mathbb{G}$ , with positive rational constraint defined by a normal fta  $\mathcal{A}$  with labelling set  $\text{Rat}(\mathbb{H})$  and where  $\mathcal{S}_j := ((E_i)_{1 \leq i \leq n}, (\bar{E}_i)_{n+1 \leq i \leq 2n}, \mu_A, \mu_{\mathcal{U}, j})$ . Let us suppose that  $\mathcal{DS}$  is in closed quadratic normal form. A monoid homomorphism*

$$\sigma : \mathcal{U}^* \rightarrow \mathbb{G}$$

*is a solution of  $\mathcal{DS}$  if and only if, there exists an index  $j \in J$ , an admissible choice  $(\mathbf{W}, \mathbf{e})$  of variables of  $\mathcal{W}$  (resp. elements of  $A \cup B$ ), an alphabet  $\mathcal{W}' \subseteq \mathcal{W}$  possessing all these variables and closed under  $\mathbb{I}_{\mathbb{W}}$ , an involution  $\mathbb{I}' \in \mathcal{WT}$ , an AB-homomorphism  $\sigma_{\mathbb{W}} : (\langle \mathcal{W}' \rangle, \mathbb{I}) \rightarrow (\langle \mathcal{W}' \rangle, \mathbb{I}')$  and a weak AB-homomorphism  $\psi_t : (\langle \mathcal{W}' \rangle, \mathbb{I}') \rightarrow \mathcal{H}_t$  such that:*

- (S1)  $\sigma_{\mathbb{W}}$  is a solution of the system of equations  $\mathcal{S}_t(\mathcal{S}_j, \mathbf{W}, \mathbf{e})$ ,
- (S2)  $\sigma_{\mathbb{W}} \circ \psi_t$  is a solution of the system of equations and disequations  $\mathcal{S}_{\mathbb{H}}(\mathcal{S}_j, \mathbf{W}, \mathbf{e})$ ,
- (S3)  $\sigma = \sigma_{\mathbf{W}, \mathbf{e}} \circ \sigma_{\mathbb{W}} \circ \psi_t \circ \bar{\pi}_{\mathbb{G}}$ .

**Sketch of proof** of Theorem 7: It suffices to adapt the reductions given in the proof of Theorem 2 as follows:

- Lemma 28 is replaced by Lemma 31

- Instead of a system of equations with rational constraints in  $\mathbb{H}$  we use the system  $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \mathbf{W}, \mathbf{e})$  of equations and disequations with positive rational constraints in  $\mathbb{H}$  supplied by Lemma 29.
- for every  $W \in \mathcal{W}'_H$ ,  $C(W)$  belongs to  $\text{DEQ}(\mathbb{H}, \text{Rat}(\mathbb{H}))$ .
- for every  $W \in \mathcal{W}' \setminus \mathcal{W}'_H$ ,  $C(W)$  is recognized by a finite t-automaton with labels in  $\text{DEQ}(\mathbb{H}, \text{Rat}(\mathbb{H}))$ : this is clear for  $C_I(W), C_\mu(W), C_\delta(W)$ ; for  $C_\gamma(W)$ , the trick consists just in seeing the subset  $\mathbb{H} \setminus A$  (resp.  $\mathbb{H} \setminus B$ ) as defined by the system of disequations  $\bigwedge_{a \in A} v \neq a$ .  $\square$

### 10.3 Constants

The set of constraints here are  $\mathcal{C}_{\mathbb{G}} := \{\{g\} \mid g \in \mathbb{G}\} \cup \{\mathbb{G}\}$  and  $\mathcal{C}_{\mathbb{H}} := \{\{h\} \mid h \in \mathbb{H}\} \cup \{\mathbb{H}\}$

**Theorem 8.** *Let  $\mathbb{H}$  be a cancellative monoid and  $\mathbb{G}$  an HNN-extension of  $\mathbb{H}$  with finite associated subgroups. The satisfiability problem for systems of equations and disequations with constants in  $\mathbb{G}$  is Turing-reducible to the SAT-problem for systems of equations and disequations with constants in  $\mathbb{H}$ .*

**Sketch of proof:** We adapt the reductions given in the proof of Theorem 2 as follows:

- Lemma 28 is replaced by Lemma 30
- for every  $W \in \mathcal{W}'$ ,  $C(W)$  is recognized by a finite t-automaton with labeling set  $\text{DEQ}(\mathbb{H}, \mathcal{C}_{\mathbb{H}})$ , i.e. the set of subsets of  $\mathbb{H}$  which are definable by systems of equations and disequations with constants.  $\square$

## 11 Equations and disequations over an amalgamated product

In this section we adapt the transfer result about the operation of HNN-extension (i.e. Theorem 6) as a transfer result about *free product with amalgamation* (see Theorem 10 below).

### 11.1 Free product

In [LS08, section 6.1] we defined a notion of  $(\mathbb{H}_1, \mathbb{H}_2)$ -automata which is the direct adaptation to the operation of free product (possibly with amalgamation) of the notion of t-automaton. Let us formulate with the help of these automata a result about free-products which is a particular case of [DL03, Theorem 2] (where the more general operation of *graph product* is treated). Given two sets  $\mathcal{C}_{\mathbb{H}_1} \in \mathcal{P}(\mathbb{H}_1), \mathcal{C}_{\mathbb{H}_2} \in \mathcal{P}(\mathbb{H}_2)$ , we denote by  $\mathcal{L}(\mathcal{C}_{\mathbb{H}_1}, \mathcal{C}_{\mathbb{H}_2})$  the set of subsets of  $\text{Red}(\mathbb{H}_1, \mathbb{H}_2)$  which are recognized by partitioned,  $\approx$ -compatible and finite  $(\mathbb{H}_1, \mathbb{H}_2)$ -automata with labelling set  $(\mathcal{C}_{\mathbb{H}_1}, \mathcal{C}_{\mathbb{H}_2})$ . Informally, such an automaton  $\mathcal{A}$  is a finite automaton over the alphabet  $\mathcal{C}_{\mathbb{H}_1} \cup \mathcal{C}_{\mathbb{H}_2}$  which has transitions labeled alternatively by elements of  $\mathcal{C}_{\mathbb{H}_1}$  and by elements of  $\mathcal{C}_{\mathbb{H}_2}$ ;  $\approx$ -compatibility means that, if it recognizes some  $(H_1, H_2)$ -sequence  $s$  it also recognizes the reduced sequence  $s'$  such that  $s \approx s'$ ; the language recognized by  $\mathcal{A}$  is obtained by substituting, in the ordinary language recognized by  $\mathcal{A}$ , each letter by its value in  $\mathcal{P}(\mathbb{H}_1) \cup \mathcal{P}(\mathbb{H}_2)$ .

**Theorem 9.** *Let us consider two monoids  $\mathbb{H}_1, \mathbb{H}_2$ . The satisfiability problem for systems of equations and disequations with constraints in  $\mathcal{B}(\mathcal{L}(\mathcal{C}_{\mathbb{H}_1}, \mathcal{C}_{\mathbb{H}_2}))$  over the free product  $\mathbb{H}_1 * \mathbb{H}_2$  is Turing-reducible to the pair of problems  $(S_1, S_2)$  where*

- 1-  $S_1$  *is the SAT-problem for systems of equations and disequations with constraints in  $\mathcal{B}(\mathcal{C}_{\mathbb{H}_1})$*
- 2-  $S_2$  *is the SAT-problem for systems of equations and disequations with constraints in  $\mathcal{B}(\mathcal{C}_{\mathbb{H}_2})$*

Note that when  $\mathcal{C}_{\mathbb{H}_i} = \text{Rat}(\mathbb{H}_i)$  (for  $i \in \{1, 2\}$ ), then  $\mathcal{L}(\mathcal{C}_{\mathbb{H}_1}, \mathcal{C}_{\mathbb{H}_2}) = \text{Rat}(\mathbb{H}_1 * \mathbb{H}_2)$ .

### 11.2 Free product with amalgamation

**Theorem 10.** *Let us consider two cancellative monoids  $\mathbb{H}_1, \mathbb{H}_2$ , two finite subgroups  $A_1 \leq \mathbb{H}_1, A_2 \leq \mathbb{H}_2$ , and an isomorphism  $\varphi : A_1 \rightarrow A_2$ . The satisfiability problem for systems of equations and disequations with rational constraints in the amalgamated product  $\mathbb{G} := \langle \mathbb{H}_1, \mathbb{H}_2; a = \varphi(a)(a \in A_1) \rangle$  is Turing-reducible to the pair of problems  $(S_1, S_2)$  where*

- 1-  $S_1$  *is the SAT-problem for systems of equations and disequations with rational constraints in  $\mathbb{H}_1$*
- 2-  $S_2$  *is the SAT-problem for systems of equations and disequations with rational constraints in  $\mathbb{H}_2$*

**Proof:** Let us use the embedding  $\eta : \mathbb{G} \rightarrow \hat{\mathbb{G}}$  defined in subsection 2.2 by formula (13), where  $\hat{\mathbb{G}} := \langle \mathbb{H}_1 * \mathbb{H}_2, t; t^{-1}at = \varphi(a)(a \in A_1) \rangle$ . For every  $R \in \text{Rat}(\mathbb{G})$ , the constraint  $R$  is translated by the rational constraint  $\eta(R)$  over  $\hat{\mathbb{G}}$  and the constraint  $\mathbb{G} \setminus R$  is translated by the constraint  $\eta(\mathbb{G}) \setminus \eta(R)$ , which is a constraint in  $\mathcal{B}(\text{Rat}(\hat{\mathbb{G}}))$ . The SAT problem for systems of equations and disequations with rational constraints in  $\mathbb{G}$  is thus reduced to the same problem in  $\hat{\mathbb{G}}$ . By Theorem 2 this problem reduces to the same problem in the product  $\mathbb{H}_1 * \mathbb{H}_2$  and by Theorem 9 this last problem reduces to the same problem in every factor i.e.  $(S_1, S_2)$ .  $\square$

Note that when  $\mathcal{C}_{\mathbb{H}_i} = \{\{h\} \mid h \in \mathbb{H}_i\} \cup \{\mathbb{H}_i\}$  then  $\mathcal{L}(\mathcal{C}_{\mathbb{H}_1}, \mathcal{C}_{\mathbb{H}_2}) \supseteq \{\{g\} \mid g \in \mathbb{G}\} \cup \{\mathbb{G}\}$ . Hence, by similar arguments as above, one can prove the variant of Theorem 10 where equations and disequations *with constants* are considered.

### 11.3 Equations over an amalgamated product

We strongly believe that one can adapt the main transfer result about equations and the operation of HNN-extension (i.e. Theorem 2) as a transfer result about *free product with amalgamation*. Since we lack such a theorem even in the case of a free product, the most natural method would consist in adapting all the method developed in sections 3-6 to the case of a free product with amalgamation over finite subgroups. As well, analogues of Theorem 3, dealing with equations with positive rational constraints, and of Theorem 5, dealing with equations with constants, should hold for free products with amalgamation.

## 12 Equations and disequations over a graph of groups

Let us recall a graph of groups  $\mathcal{G}$  is a directed graph  $G = (V, E)$  endowed with a family of groups  $(G_v)_{v \in V}$  and a family  $(\varphi_e)_{e \in E}$  of maps, such that, for every  $e \in E$ ,  $\varphi_e$  is a partial isomorphism from  $G_{\iota(e)}$  into  $G_{\tau(e)}$  (here  $\iota(e)$  denotes the initial vertex of edge  $e$  and  $\tau(e)$  denotes the terminal vertex of edge  $e$ ). For every vertex  $v$ , we denote by  $\pi_1(\mathcal{G}, v)$  the fundamental group of  $\mathcal{G}$  with base-point  $v$  (see [Ser77] or [DD90] for background on graphs of groups).

**Theorem 11.** *Let  $\mathcal{G} := (V, E, (G_v)_{v \in V}, (\varphi_e)_{e \in E})$  be a finite graph of groups where all the edge partial isomorphisms  $\varphi_e$  have finite domain and let  $v_0 \in V$ . The satisfiability problem for systems of equations and disequations with rational constraints in the fundamental group  $\pi_1(\mathcal{G}, v_0)$  is Turing-reducible to the join of the problems  $(S_v)_{v \in V}$  where  $S_v$  is the SAT-problem for systems of equations and disequations with rational constraints in  $G_v$ .*

**Proof:** We can assume that  $(V, E)$  is connected (otherwise adding some edges with trivial partial isomorphisms would preserve the fundamental group and make the graph connected). Let  $T \subseteq E$  be a covering tree. The group  $\pi_1(\mathcal{G}, v_0)$  can be obtained as a  $k$ -fold HNN-extension of a  $\ell$ -fold free product with amalgamation of the vertex groups  $(G_v)$ , where the associated (or amalgamated) subgroups are pairs of the form  $(\text{dom}(\varphi_e), \text{im}(\varphi_e))$  for  $e \in E$ ,  $k = |T| - |E|$  and  $\ell = |T|$ . Hence, using  $k$  times Theorem 6 and  $\ell$  times Theorem 10, we obtain the desired Turing reduction.  $\square$

**Corollary 1.** *If  $\mathbb{G}$  is a virtually-free group of finite type, then the satisfiability problem for systems of equations and disequations with rational constraints in  $\mathbb{G}$  is decidable.*

**Proof:** Recall that the virtually-free groups of finite type are exactly the fundamental groups of finite graphs of groups with finite vertex-groups ([DD90]). Corollary 1 follows from Theorem 11 since, in a finite group, systems of equations and disequations with rational constraints are algorithmically solvable.  $\square$  Note that another proof of this result has been exposed in [DG07].

### *Related works*

In [DG07] F. Dahmani and V. Guirardel are proving Corollary 1 by geometrical methods. They claim that, using this result, they get an algorithm that solves equations in any word hyperbolic group (even with torsion). As mentioned in the introduction, A. Myasnikov and O. Karlapovich have shown that the full first-order theory of a free group of finite rank is decidable. Their solution includes ([KM05a, KM05b]) methods for solving equations in so-called fully residually finite groups (these groups generalize free groups).

### *Perspectives*

We think that part of the techniques exposed here will be extendable to the HNN-extensions where the subgroups  $A, B$  are infinite but assumed to be nicely embedded in the base group (or monoid)  $\mathbb{H}$ .

We extend in [LS05] our transfer theorems to the positive first-order theory of HNN-extensions (or free products with amalgamation) of groups. Whether an extension to the full first-order theory is true (or not) is a fascinating open question.



## References

- [DD90] W. Dicks and M.J. Dunwoody. *Groups acting on graphs*. Cambridge University Press, 1990.
- [DG07] F. Dahmani and V. Guirardel. Geometric Makanin algorithm for solving equations in virtually free groups. In *Talk given on November 08, 2007*. MSRI, Lecture nr 12581, 2007.
- [DHG05] V. Diekert, C. Hagenah, and C. Gutierrez. The existential theory of equations with rational constraints in free groups is PSPACE-complete. *TOCS*, pages 1–45, 2005.
- [DL03] Volker Diekert and Markus Lohrey. Word equations over graph products. In *Proceedings FSTTCS*, pages 156–167. LNCS 2914, 2003.
- [DL04] Volker Diekert and Markus Lohrey. Word equations over graph products. *Theory of Computing Systems*, 37(1):133–156, 2004.
- [DM06] Volker Diekert and Anca Muscholl. Solvability of equations in graph groups is decidable. *Internat. J. Algebra Comput.*, 16(6):1047–1069, 2006.
- [ES69] Samuel Eilenberg and M. P. Schützenberger. Rational sets in commutative monoids. *J. Algebra*, 13:173–191, 1969.
- [Gre90] Elisabeth R. Green. *Graph Products of Groups*. PhD thesis, The University of Leeds, 1990.
- [HNN49] Graham Higman, B. H. Neumann, and Hanna Neumann. Embedding theorems for groups. *J. London Math. Soc.*, 24:247–254, 1949.
- [HU79] J.E. Hopcroft and J.D. Ullman. *Introduction to Automata Theory, Languages and Computation*. Addison-Wesley, Reading, Mass., 1979.
- [KM98] Olga G. Kharlampovich and Alexei Myasnikov. Tarski’s problem about the elementary theory of free groups has a positive solution. *Electronic Research Announcements of the American Mathematical Society*, 4:101–108, 1998.
- [KM05a] Olga Kharlampovich and Alexei Myasnikov. Implicit function theorem over free groups. *J. Algebra*, 290(1):1–203, 2005.
- [KM05b] Olga Kharlampovich and Alexei G. Myasnikov. Effective JSJ decompositions. In *Groups, languages, algorithms*, volume 378 of *Contemp. Math.*, pages 87–212. Amer. Math. Soc., Providence, RI, 2005.
- [KMS05] B. Khan, A. G. Myasnikov, and D. E. Serbin. On positive theories of groups with regular free length function. Manuscript, 2005.
- [KP98] Antoni Kościelski and Leszek Pacholski. Makanin’s algorithm is not primitive recursive. *Theoretical Computer Science*, 191(1-2):145–156, 1998.
- [LS77] Roger C. Lyndon and Paul E. Schupp. *Combinatorial group theory*. Springer-Verlag, Berlin, 1977. *Ergebnisse der Mathematik und ihrer Grenzgebiete*, Band 89.
- [LS05] M. Lohrey and G. Sénizergues. Positive theories of HNN-extensions and amalgamated free products. Manuscript, 2005.
- [LS06] M. Lohrey and G. Sénizergues. Theories of HNN-extensions and amalgamated products. In *Proceedings ICALP’06*, volume 4052 of *LNCS*, pages 504–515. Springer-Verlag, 2006.
- [LS08] Markus Lohrey and Géraud Sénizergues. Rational subsets in HNN-extensions and amalgamated products. *Internat. J. Algebra Comput.*, 18(1):111–163, 2008.
- [Mak83] Gennadii Semyonovich Makanin. Equations in a free group. *Izv. Akad. Nauk SSR, Ser. Math.* 46:1199–1273, 1983. In Russian; English translation in *Math. USSR Izvestija* 21, 1983.

- [Mak84] Gennadii Semyonovich Makanin. Decidability of the universal and positive theories of a free group. *Izv. Akad. Nauk SSSR, Ser. Mat.* 48:735–749, 1984. In Russian; English translation in *Math. USSR Izvestija*, 25, 75–88, 1985.
- [Mer66] Y. I. Merzlyakov. Positive formulas on free groups. *Algebra i Logika Sem.*, 5(4):25–42, 1966. In Russian.
- [MS83] 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.
- [Pla99] Wojciech Plandowski. Satisfiability of word equations with constants is in PSPACE. In *40th Annual Symposium on Foundations of Computer Science (FOCS 99)*, pages 495–500. IEEE Computer Society Press, 1999.
- [Rog87] Hartley Rogers, Jr. *Theory of recursive functions and effective computability*. MIT Press, Cambridge, MA, second edition, 1987.
- [RS95] E. Rips and Z. Sela. Canonical representatives and equations in hyperbolic groups. *Inventiones Mathematicae*, 120:489–512, 1995.
- [Ser77] Jean-Pierre Serre. *Arbres, amalgames,  $SL_2$* . Société Mathématique de France, Paris, 1977. Avec un sommaire anglais, Rédigé avec la collaboration de Hyman Bass, Astérisque, No. 46.
- [Sta71] J. R. Stallings. *Group Theory and Three-Dimensional Manifolds*. Number 4 in Yale Mathematical Monographs. Yale University Press, 1971.