Equations in HNN-extensions.

Markus Lohrey and Géraud Sénizergues

[1] Institut für Informatik, Universität Leipzig, Germany
[2] 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 where the edge groups are finite and the vertex groups have a decidable existential first-order theory.

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

Date: February 25, 2018

Table of Contents

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 5: 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 8) and for systems of equations and disequations with rational constraints (Theorem 9);

– A similar theorem is proved for systems of equations and disequations with rational constraints in an amalgamated product (Theorem 12).

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 13).

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 $\mathbb{W}$. The essential statement of this section, which is also the key-step of the present paper, is Lemma 46 asserting that any solution σ_t of an equation in $\mathbb{H}_t$ factorizes through a solution of the same equation, but in the structure $\mathbb{W}$. Most of the technical lemmas of section 3 establish some algebraic properties of $\mathbb{W}$ and of $\mathbb{H}_t$ in order to enable the proof of this factorization lemma. In Section 7.1 we reduce equations over the the AB-algebra $\mathbb{W}$ to equations over some finitely generated group $\mathbb{E}$ which turns out to be virtually-free. In Section 9 we show, by induction over the size of the associated subgroups A,B, that equations in $\mathbb{E}$ are algorithmically solvable. We then prove a transfer theorem concerning groups only and prove finally our main Theorem 5 concerning cancellative monoids. In Section 10 we adapt the proof-techniques developed in the previous sections in order to prove some variants of Theorem 5 where the constraints can be positive only, in particular to the case of equations with constants. In Section 11 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 12 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 13 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.

2 Preliminaries

The power set of a set A is denoted by 2^A. For an equivalence relation R on A we denote with $[A]_R$ the set of all equivalence classes of R. For $C \subseteq 2^A$ we denote with $\mathsf{bool}(C)$ the set of all boolean combinations of sets from C, which is the smallest boolean subalgebra of 2^A containing C. For a partial mapping f we denote with $\mathrm{dom}(f)$ and $\mathrm{im}(f)$ the domain and image (or range), respectively, of the mapping f. Let us denote by $\mathsf{B}(\mathsf{Q})$ the monoid $2^{\mathsf{Q}\times\mathsf{Q}}$ of

binary relations over the set Q and let $\mathsf{B}^2(\mathsf{Q}) = \mathsf{B}(\mathsf{Q}) \times \mathsf{B}(\mathsf{Q})$. For $R \in \mathsf{B}(\mathsf{Q})$ and $R' \in \mathsf{B}(\mathsf{Q}')$ we define

$$R \otimes R' = \{((p,p'),(q,q')) \mid (p,q) \in R, (p',q') \in R'\}.$$

We will use the following simple lemma:

Lemma 1. *Let $R, S \in \mathsf{B}(\mathsf{Q})$ and $R', S' \in \mathsf{B}(\mathsf{Q}')$. Then $(R \circ S) \otimes (R' \circ S') = (R \otimes R') \circ (S \otimes S')$.*

Proof. We have $((p,p'),(r,r')) \in (R \circ S) \otimes (R' \circ S')$ if and only if $(p,r) \in R \circ S$ and $(p',r') \in R' \circ S'$ if and only if there exist $q \in \mathsf{Q}$ and $q' \in \mathsf{Q}'$ with $(p,q) \in R$, $(q,r) \in S$, $(p',q') \in R'$, and $(q',r') \in S'$ if and only if there exist $(q,q') \in \mathsf{Q} \times \mathsf{Q}'$ with $((p,p'),(q,q')) \in R \otimes R'$ and $((q,q'),(r,r')) \in S \otimes S'$ if and only if $((p,p'),(r,r')) \in (R \otimes R') \circ (S \otimes S')$. □

For a string $s \in \Sigma^*$ and $\Gamma \subseteq \Sigma$ we denote with $|s|_\Gamma$ the number of occurrences of symbols from Γ in s. For a tuple $\overline{a} = (a_1, \ldots, a_n)$ and $1 \leq i \leq n$ we denote with $p_i(\overline{a}) = a_i$ the projection onto the i-th component.

In the following subsections, we recall all the needed definitions and classical results concerning partial semigroups, semigroups, monoids, and groups.

2.1 Partial semigroups

Let $\langle P, * \rangle$ be a set endowed with a partial operation $* : P \times P \to P$. By $\mathrm{dom}(*) \subseteq P \times P$ we denote the domain of $*$. The structure $\langle P, * \rangle$ is a *partial semigroup* if for all $p, q, r \in P$:

$$(p,q) \in \mathrm{dom}(*) \wedge ((p * q), r) \in \mathrm{dom}(*) \iff (q,r) \in \mathrm{dom}(*) \wedge (p, (q * r)) \in \mathrm{dom}(*) \text{ and}$$
$$(p,q) \in \mathrm{dom}(*) \wedge ((p * q), r) \in \mathrm{dom}(*) \implies (p * q) * r = p * (q * r).$$

Let us notice that, when P is a partial semigroup, the structure $\langle 2^P, * \rangle$ with

$$\forall R, S \in 2^P : R * S = \{r * s \mid (r,s) \in (R \times S) \cap \mathrm{dom}(*)\}$$

is a semigroup.

Given two partial semigroups $\langle P, * \rangle$ and $\langle Q, \circ \rangle$, a *partial semigroup homomorphism* from P to Q is a total mapping $h : P \to Q$ such that for all $p, q \in P$ with $(p,q) \in \mathrm{dom}(*)$ the following holds: $(h(p), h(q)) \in \mathrm{dom}(\circ)$ and $h(p * q) = h(p) \circ h(q)$.

Let A, B be two groups. We denote by $\mathrm{PGI}(A,B)$ the set of all partial group isomorphisms φ with $\mathrm{dom}(\varphi) \subseteq A$ and $\mathrm{im}(\varphi) \subseteq B$. Let

$$\mathrm{PGI}\{A,B\} = \mathrm{PGI}(A,A) \cup \mathrm{PGI}(A,B) \cup \mathrm{PGI}(B,A) \cup \mathrm{PGI}(B,B).$$

The pair $\langle \mathrm{PGI}\{A,B\}, \circ \rangle$, where $\circ$ is the composition operator, is a partial semigroup.

The following property will be useful for dealing with product-automata.

Lemma 2. *Let $\langle S, * \rangle$ be a partial semigroup and let Q and R be sets. Let $\mu : S \to \mathsf{B}(\mathsf{Q})$ and $\eta : S \to \mathsf{B}(\mathsf{R})$ be two homomorphisms. Let us define $\mu \otimes \eta : S \to \mathsf{B}(\mathsf{Q} \times \mathsf{R})$ by*

$$\forall s \in S : (\mu \otimes \eta)(s) = \mu(s) \otimes \eta(s).$$

Then $\mu \otimes \eta$ is a homomorphism too.

Proof. Let $(s, s') \in \mathrm{dom}(*)$. We have

$$\begin{aligned}
(\mu \otimes \eta)(s * s') &= \mu(s * s') \otimes \eta(s * s') && \text{(by definition)} \\
&= (\mu(s) \circ \mu(s')) \otimes (\eta(s) \circ \eta(s')) && \text{(since } \mu, \eta \text{ are homomorphisms)} \\
&= (\mu(s) \otimes \eta(s)) \circ (\mu(s') \otimes \eta(s')) && \text{(by Lemma 1)} \\
&= (\mu \otimes \eta)(s) \circ (\mu \otimes \eta)(s') && \text{(by definition),}
\end{aligned}$$

which proves the lemma □

2.2 Monoids and groups

Let $\mathbb{M}$ be a monoid with identity element $1 \in \mathbb{M}$. The product of two elements $x, y \in \mathbb{M}$ is just written as xy. The monoid $\mathbb{M}$ is called *cancellative* if ($xy = xz$ or $yx = zx$) implies $y = z$ for all $x, y, z \in \mathbb{M}$. A *submonoid* of $\mathbb{M}$ is given by a subset $A \subseteq \mathbb{M}$ such that (i) $1 \in A$ and (ii) $xy \in A$ for all $x, y \in A$. If for every $x \in A$ there exists $y \in A$ with $xy = yx = 1$ (i.e., A is a group), then we call A a *subgroup* of $\mathbb{M}$.[1] With $\mathrm{Hom}(\mathbb{M}_1, \mathbb{M}_2)$ we denote the set of all monoid homomorphims from the monoid $\mathbb{M}_1$ to the monoid $\mathbb{M}_2$. An *anti-homomorphism* between monoids $\mathbb{M}_1$ and $\mathbb{M}_2$ is a mapping $h : \mathbb{M}_1 \to \mathbb{M}_2$ that maps the identity of $\mathbb{M}_1$ to the identity of $\mathbb{M}_2$ and moreover satisfies $h(xy) = h(y)h(x)$. If h is a bijection, then it is called an *anti-isomorphism*. If moreover $h^2(x) = x$ for all $x \in \mathbb{M}_1$ then it is called an *involutive anti-isomorphism*.

Given a subset $P \subseteq \mathbb{M} \times \mathbb{M}$, we denote by $\equiv_P$ the smallest monoid congruence over $\mathbb{M}$ that contains P. The following lemma is trivial.

Lemma 3. *Let $h : \mathbb{M}_1 \to \mathbb{M}_2$ be some monoid homomorphism and $P \subseteq \mathbb{M}_1 \times \mathbb{M}_1$. Then, $h(\equiv_P) \subseteq \equiv_{h(P)}$.*

Also the following fact is well-known, it will be useful for our investigations on equations over *cancellative* monoids.

Lemma 4. *Let $\mathbb{H}$ be a cancellative monoid and let $\mathsf{I}(\mathbb{H})$ be its subset of invertible elements. For every $x, y \in \mathbb{H}$, if $xy \in \mathsf{I}(\mathbb{H})$ then $x, y \in \mathsf{I}(\mathbb{H})$.*

Proof. Suppose that $\mathbb{H}$ is cancellative and that $xy \in \mathsf{I}(\mathbb{H})$. This implies that xy has some inverse $z \in \mathbb{H}$, i.e., $xyz = 1$. Hence, $xyzx = x$, so that by left-cancellation $yzx = 1$, which shows that x and yz are inverses in $\mathbb{H}$. Hence $x \in \mathsf{I}(\mathbb{H})$. By a similar argument, y and zx are inverses in $\mathbb{H}$, hence $y \in \mathsf{I}(\mathbb{H})$. □

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

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

[1] Note that usually, a subgroup A of $\mathbb{M}$ is defined to be a subsemigroup of $\mathbb{M}$, which forms a group. In particular, the identity element of A may be an idempotent of $\mathbb{M}$ different from the identity of 1 of $\mathbb{M}$. Nevertheless, we prefer to use the term subgroup for our definition in order to avoid too many different notions.

can be defined as the quotient monoid $\mathbb{H} * \{t, t^{-1}\}^*/_{\approx}$, of the free product of $\mathbb{H}$ and the free monoid $\{t, t^{-1}\}^*$ by the smallest congruence $\approx$ over $\mathbb{H} * \{t, t^{-1}\}^*$ such that:

$$tt^{-1} \approx t^{-1}t \approx 1 \tag{2}$$

$$at \approx t\varphi(a) \qquad \text{for all } a \in A \tag{3}$$

$$bt^{-1} \approx t^{-1}\varphi^{-1}(b) \text{ for all } b \in B \tag{4}$$

Note that (2) and (3) together imply (4) but below we will need (3) and (4) without assuming (2). There exists a canonical morphism

$$\pi_{\mathbb{G}} : \mathbb{H} * \{t, t^{-1}\}^* \to \mathbb{G},$$

where the kernel of $\pi_{\mathbb{G}}$ coincides with $\approx$.

An element of $s \in \mathbb{H} * \{t, t^{-1}\}^*$ can be viewed as a word over the alphabet $\mathbb{H} \cup \{t, t^{-1}\}$ which has the form

$$s = h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_n} h_n, \tag{5}$$

where $n \geq 0, \alpha_i \in \{1, -1\}$, and $h_i \in \mathbb{H}$. Such an element $s \in \mathbb{H} * \{t, t^{-1}\}^*$ is also called a *t-sequence*. The t-sequence s is said to be a *reduced sequence* if it neither contains a factor of the form $t^{-1}at$ (with $a \in A$) nor tbt^{-1} (with $b \in B$). Let

$$\mathrm{Red}(\mathbb{H}, t) = \{s \in \mathbb{H} * \{t, t^{-1}\}^* \mid s \text{ is reduced}\}.$$

For the further considerations, it is useful to define

$$A(+1) = B(-1) = A, \quad A(-1) = B(+1) = B.$$

Note that $\varphi^\alpha : A(\alpha) \to B(\alpha)$ for $\alpha \in \{1, -1\}$.

Definition 1. *Let $\sim$ be the congruence on the monoid $\mathbb{H} * \{t, t^{-1}\}^*$ generated by all the rules of type (3) and (4) above.*

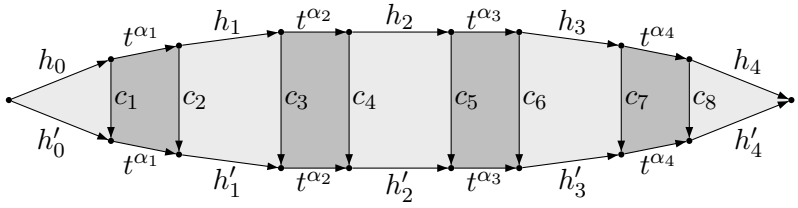
The congruence $\sim$ coincides with reflexive and transitive closure of the binary relation $\overset{1}{\sim}$ over $\mathbb{H} * \{t, t^{-1}\}^*$, which is defined as follows, where $s, s' \in \mathbb{H} * \{t, t^{-1}\}^*$:

$$s \overset{1}{\sim} s' \iff \exists u, v \in \mathbb{H} * \{t, t^{-1}\}^*, \alpha \in \{1, -1\}, c \in A(\alpha) : s = ut^\alpha v \wedge s' = uc^{-1}t^\alpha \varphi^\alpha(c)v.$$

Equivalently, if $s = h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_n} h_n$ and $s' = h'_0 t^{\alpha'_1} h'_1 \cdots t^{\alpha'_m} h'_m$ (with $n, m \geq 0$, $\alpha_i, \alpha'_j \in \{1, -1\}$ and $h_i, h'_j \in \mathbb{H}$), then $s \sim s'$ if and only if $n = m$, $\alpha_i = \alpha'_i$ for $1 \leq i \leq n$, and there exist $c_1, \ldots, c_{2n} \in A \cup B$ such that:

- $h_k c_{2k+1} = c_{2k} h'_k$ in $\mathbb{H}$ for $0 \leq k \leq n$ (here we set $c_0 = c_{2n+1} = 1$)
- $c_{2k-1} \in A(\alpha_k)$ and $c_{2k} = \varphi^{\alpha_k}(c_{2k-1}) \in A(-\alpha_k)$ for $1 \leq k \leq n$.

This situation can be visualized by a diagram of the following form (also called a van Kampen diagram, see [LS77] for more details), where $n = m = 4$. Light-shaded (resp. dark-shaded) areas represent relations in $\mathbb{H}$ (resp. relations of the form $at = t\varphi(a)$ $(a \in A)$ or $bt^{-1} = t^{-1}\varphi^{-1}(b)$ $(b \in B)$).



(†)

The elements $c_1, \ldots, c_{2n}$ in such a diagram are also called *connecting elements*.

The set $\mathrm{Red}(\mathbb{H}, t)$ is saturated by the congruence $\sim$, i.e.,

$$s \sim s' \quad \Longrightarrow \quad (s \in \mathrm{Red}(\mathbb{H}, t) \Longleftrightarrow s' \in \mathrm{Red}(\mathbb{H}, t)).$$

Just notice that, since A and B are groups, $aha' \in A \Longleftrightarrow h \in A$ for all $h \in \mathbb{H}, a, a' \in A$ and $bhb' \in B \Longleftrightarrow h \in B$ for all $h \in \mathbb{H}, b, b' \in B$. This property would fail if A and B were assumed to be merely submonoids of $\mathbb{H}$.

One has $\sim \subseteq \approx$. Moreover, for reduced sequences the following fundamental lemma holds.

Lemma 5. *Let $s, s' \in \mathrm{Red}(\mathbb{H}, t)$. Then $s \approx s'$ if and only if $s \sim s'$.*

See [LS08, Appendix A] for a proof. Let us define the quotient monoid

$$\mathbb{H}_t = \mathbb{H} * \{t, t^{-1}\}^* / \sim. \tag{6}$$

Lemma 6. *If the monoid $\mathbb{H}$ is cancellative then the monoid $\mathbb{H}_t$ is cancellative too.*

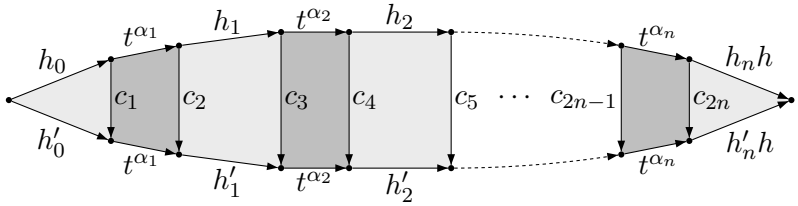
Proof. We will only prove right-cancellativity, left-cancellativity can be shown analogously. We first prove that $sh \sim s'h$ implies $s \sim s'$ for all $s, s' \in \mathbb{H} * \{t, t^{-1}\}^*$ and $h \in \mathbb{H}$. Assume that

$$s = h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_n} h_n \quad \text{and} \quad s' = h'_0 t^{\alpha'_1} h'_1 \cdots t^{\alpha'_m} h'_m.$$

Hence, $sh \sim s'h$ implies

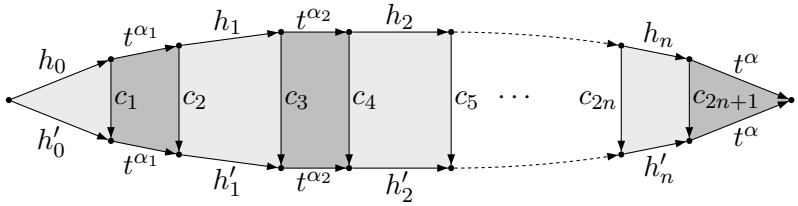
$$h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_n} h_n h \sim h'_0 t^{\alpha'_1} h'_1 \cdots t^{\alpha'_m} h'_m h.$$

This implies $n = m$ and $\alpha_i = \alpha'_i$ for $1 \leq i \leq n$. Moreover, there exists a van Kampen diagram of the following form:



In particular, we obtain the $\mathbb{H}$-identity $h_n h = c_{2n} h'_n h$. Since $\mathbb{H}$ is cancellative, we get $h_n = c_{2n} h'_n$. Thus, the above van Kampen diagram can be turned into a diagram for $s \sim s'$.

Next, assume that $st^\alpha \sim s't^\alpha$. Again, we get $n = m$ and $\alpha_i = \alpha'_i$ for $1 \leq i \leq n$ and a van Kampen diagram of the form



Since we must have $\varphi^\alpha(c_{2n+1}) = 1$ we get $c_{2n+1} = 1$. Hence, again the above van Kampen diagram can be turned into a diagram for $s \sim s'$.

Finally, since $\mathbb{H}_t$ is generated by $\mathbb{H} \cup \{t, t^{-1}\}$, it follows that $\mathbb{H}_t$ is indeed right-cancellative. □

A simple consequence of Lemma 6 and Lemma 5 is:

Lemma 7. *If the monoid $\mathbb{H}$ is cancellative then the HNN-extension $\mathbb{G}$ is cancellative too.*

Proof. We only prove right-cancellativity. Let $g, g' \in \mathbb{G}$. First assume that $gt^\alpha = g't^\alpha$ in $\mathbb{G}$. Since $t^\alpha t^{-\alpha} = 1$ in $\mathbb{G}$, we obtain $g = g'$. Now assume that $gh = g'h$ in $\mathbb{G}$ for $h \in \mathbb{H}$. Choose $s, s' \in \mathrm{Red}(\mathbb{H}, t)$ with $\pi_{\mathbb{G}}(s) = g$ and $\pi_{\mathbb{G}}(s') = g'$. Then, also $sh, s'h \in \mathrm{Red}(\mathbb{H}, t)$. Since $gh = g'h$ in $\mathbb{G}$, we have $sh \approx s'h$. Lemma 5 implies $sh \sim s'h$, i.e., $sh = s'h$ in $\mathbb{H}_t$. Lemma 6 implies $s = s'$ in $\mathbb{H}_t$, i.e., $g = g'$ in $\mathbb{G}$. □

We define the norm of a given t-sequence $s \in \mathbb{H} * \{t, t^{-1}\}^*$ by

$$\|s\| = |s|_{\{t,t^{-1}\}}. \tag{7}$$

Clearly, for all $s, s' \in \mathbb{H} * \{t, t^{-1}\}^*$, we have

$$\|ss'\| = \|s\| + \|s'\| \quad \text{and} \quad \|s\| = 0 \Longleftrightarrow s \in \mathbb{H}. \tag{8}$$

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

$$\|s\|_b = \min\{1, \|s\|\}. \tag{9}$$

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

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

is defined by $\mathbb{G} = (\mathbb{H}_1 * \mathbb{H}_2)/_\approx$, where $\approx$ is the congruence on the free product $\mathbb{H}_1 * \mathbb{H}_2$ generated by the equations $a = \varphi(a)$ for $a \in A_1$. An $(\mathbb{H}_1, \mathbb{H}_2)$-*sequence* is an element $s \in \mathbb{H}_1 * \mathbb{H}_2$; it has a unique decomposition of the form

$$s = h_0 k_1 h_1 \cdots k_n h_n, \tag{11}$$

where $n \geq 0, h_1, \ldots, h_{n-1} \in \mathbb{H}_2 \setminus \{1\}$, $k_1, \ldots, k_n \in \mathbb{H}_1 \setminus \{1\}$ and $h_0, h_n \in \mathbb{H}_2$. If, in addition, we have $h_1, \ldots, h_{n-1} \in \mathbb{H}_2 \setminus A_2$ and $k_1, \ldots, k_n \in \mathbb{H}_1 \setminus A_1$, then s is a *reduced* $(\mathbb{H}_1, \mathbb{H}_2)$-sequence. We denote by $\mathrm{Red}(\mathbb{H}_1; \mathbb{H}_2)$ the set of all reduced $(\mathbb{H}_1, \mathbb{H}_2)$-sequences.

The following statement can be found in [LS77, Theorem 2.6. p. 187] in the case where $\mathbb{H}_1$ and $\mathbb{H}_2$ are groups and in [LS08] for an amalgamated free product of monoids with amalgamation over subgroups.

Lemma 8. *The amalgamated free product $\mathbb{G} = \langle \mathbb{H}_1, \mathbb{H}_2; a = \varphi(a)(a \in A_1) \rangle$ embeds into the HNN-extension*

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

by the map with

$$h_1 \mapsto t^{-1}h_1 t \text{ for all } h_1 \in \mathbb{H}_1 \quad \text{and} \quad h_2 \mapsto h_2 \text{ for all } h_2 \in \mathbb{H}_2 \tag{12}$$

Further basic terminology and results on amalgamated free products are given in [LS08, Section 5].

2.3 Rational subsets of a monoid

Let $\mathbb{M}$ be some monoid. The set

$$\mathsf{Rat}(\mathbb{M}) \subseteq 2^{\mathbb{M}}$$

is the smallest subset of $2^{\mathbb{M}}$ which contains all finite subsets of $\mathbb{M}$ 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). Note that in case $\mathbb{M}$ is finitely generated, $\mathbb{M}$ itself is rational. We will need the following lemma.

Lemma 9. *Let c be an invertible element of $\mathbb{M}$ and let $F \subseteq \mathbb{M}$ belong to the boolean closure of $\mathsf{Rat}(\mathbb{M})$. Then the subsets cF and Fc belong to the boolean closure of $\mathsf{Rat}(\mathbb{M})$ as well.*

Proof. Let $\mathcal{F} = \mathsf{bool}(\mathsf{Rat}(\mathbb{M}))$ denote the boolean closure of the set of rational subsets of $\mathbb{M}$. Let c be an invertible element of M. Let us consider

$$\mathcal{F}_c = \{F \subseteq \mathbb{M} \mid cF \in \mathcal{F}\}.$$

Then the following hold:

(i) Since $\{c\}$ is rational and $\mathsf{Rat}(\mathbb{M})$ is closed by product, $\mathsf{Rat}(\mathbb{M}) \subseteq \mathcal{F}_c$.
(ii) Let $F \in \mathcal{F}_c$. Since c is invertible, we have $c(\mathbb{M} \setminus F) = c\mathbb{M} \setminus cF = \mathbb{M} \setminus cF$, where $cF \in \mathcal{F}$. But $\mathcal{F}$ is closed by complement. Hence, $c(\mathbb{M} \setminus F) \in \mathcal{F}$, which shows that $\mathbb{M} \setminus F \in \mathcal{F}_c$.
(iii) Let $F, G \in \mathcal{F}_c$. Then $c(F \cup G) = cF \cup cG$. Since $cF, cG \in \mathcal{F}$ and $\mathcal{F}$ is closed under union, we have $c(F \cup G) \in \mathcal{F}$, which shows that $F \cup G \in \mathcal{F}_c$.

We have proved that $\mathcal{F}_c$ contains $Rat(\mathbb{M})$ (i) and is a boolean algebra ((ii) and (iii)). Hence, it is included in the smallest boolean algebra containg $\mathsf{Rat}(\mathbb{M})$, i.e., $\mathcal{F}_c \subseteq \mathcal{F}$. Thus, $\mathcal{F}$ is closed under left multiplication by c. By the same kind of arguments one can show that $\mathcal{F}$ is closed under right multiplication by c. □

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 $\mathbb{M}$. In Section 2.5, we will introduce the basic facts concerning these automata.

2.4 Types

For this section, we assume all definitions from Section 2.2 on HNN-extensions. Following [LS08], let

$$\mathcal{T}_6 = \{(A,T), (B,T), (1,H), (1,1), (A,H), (B,H)\} \tag{13}$$

Elements of $\mathcal{T}_6$ are called *vertex types*. Note that the first component $p_1(\theta)$ of a vertex type $\theta \in \mathcal{T}_6$ is one of the three groups $1, A, B$.

We define a finite partial semigroup

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

where $\mathbb{B} = \langle \{0,1\}, \vee \rangle$ is the monoid of booleans with OR. The partial product on $\mathcal{T}$ is defined as follows, where $(\theta, b, \rho), (\theta', b', \rho') \in \mathcal{T}_6 \times \mathbb{B} \times \mathcal{T}_6$:

$$(\theta, b, \rho)(\theta', b', \rho') = \begin{cases} (\theta, b \vee b', \rho') & \text{if } \rho = \theta' \\ \text{undefined} & \text{otherwise.} \end{cases} \tag{14}$$

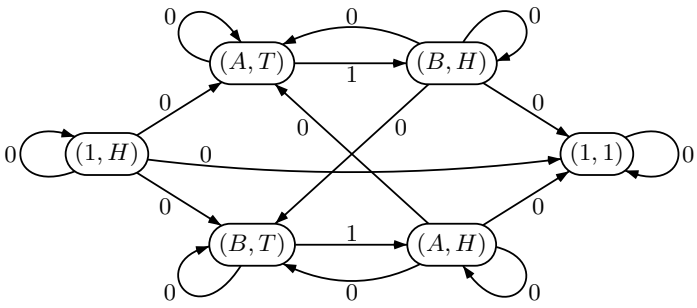


Fig. 1. The graph $\mathcal{B}_6$

As we noticed in Section 2.1, $2^{\mathcal{T}}$ is thus a semigroup. In fact, $2^{\mathcal{T}}$ is a monoid, the neutral element is $\{(\theta, 0, \theta) \mid \theta \in \mathcal{T}_6\}$.

We define an involution $\mathbb{I}_{\mathcal{R}} : \mathcal{T}_6 \to \mathcal{T}_6$ by:

$$(A,T) \mapsto (A,H) \mapsto (A,T) \tag{15}$$

$$(B,T) \mapsto (B,H) \mapsto (B,T) \tag{16}$$

$$(1,H) \mapsto (1,1) \quad \mapsto (1,H). \tag{17}$$

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

$$\mathbb{I}_{\mathcal{T}}(\theta, b, \rho) = (\mathbb{I}_{\mathcal{R}}(\rho), b, \mathbb{I}_{\mathcal{R}}(\theta)). \tag{18}$$

One can check that $\mathbb{I}_{\mathcal{T}}$ is an involutory anti-automorphism of the partial semigroup $\mathcal{T}$. This involution induces an involutory monoid anti-automorphism of $2^{\mathcal{T}}$ that will be denoted by $\mathbb{I}_{\mathcal{T}}$ too. We associate to every element $\boldsymbol{\theta}$ of $\mathcal{T}$ an *initial type* $\tau\mathrm{i}(\boldsymbol{\theta}) \in \mathcal{T}_6$, an *end type* $\tau\mathrm{e}(\boldsymbol{\theta}) \in \mathcal{T}_6$, an *initial group* $\mathrm{Gi}(\boldsymbol{\theta}) \in \{1, A, B\}$ and an *end group* $\mathrm{Ge}(\boldsymbol{\theta}) \in \{1, A, B\}$:

$$\tau\mathrm{i}(\theta_1, b, \theta_2) = \theta_1, \;\; \mathrm{Gi}(\theta_1, b, \theta_2) = p_1(\theta_1), \;\; \tau\mathrm{e}(\theta_1, b, \theta_2) = \theta_2, \;\; \mathrm{Ge}(\theta_1, b, \theta_2) = p_1(\theta_2).$$

Note that

$$\mathrm{Gi}(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta})) = \mathrm{Ge}(\boldsymbol{\theta}) \quad \text{and} \quad \mathrm{Ge}(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta})) = \mathrm{Gi}(\boldsymbol{\theta}). \tag{19}$$

Elements of $\mathcal{T}$ are called *path types*. This terminology refers to the graph $\mathcal{B}_6$ exhibited in Figure 1. The following 17 types are called *atomic types*; they correspond to the 17 edges of the graph $\mathcal{B}_6$:

$$(A(\alpha), T, 1, A(-\alpha), H) \text{ for } \alpha \in \{+1, -1\} \tag{20}$$

$$(C, H, 0, D, T) \text{ for } C \in \{1, A, B\},\ D \in \{A, B\} \tag{21}$$

$$(C, H, 0, 1, 1) \text{ for } C \in \{1, A, B\}, \tag{22}$$

$$(\theta, 0, \theta) \text{ for } \theta \in \mathcal{T}_6 \tag{23}$$

This set is closed under $\mathbb{I}_{\mathcal{T}}$. The partial subsemigroup of $\mathcal{T}$ generated by the 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 $\mathcal{TR}$. The following four types are called *T-types*:

$$(A,T,1,B,H), (B,T,1,A,H), (A,T,1,A,H), (B,T,1,B,H). \tag{24}$$

H-types are all atomic types listed in (21) and (22). Note that some types from $\mathcal{TR}$ are not atomic: for example the T-type $(A,T,1,A,H) = (A,T,1,B,H)(B,H,0,B,T)(B,T,1,A,H)$ is not atomic.

2.5 Finite t-automata

Given an HNN-extension of the form (1), we have defined in Section 4.1 of [LS08] finite automata that recognize subsets of $\mathbb{H} * \{t, t^{-1}\}^*$. We recall here the main definitions and refer to [LS08] for further details and proofs.

Let $\mathcal{F} \subseteq 2^{\mathbb{H}}$ be a set of subsets of $\mathbb{H}$ such that

$$\forall c \in A \cup B : \{c\} \in \mathcal{F}.$$

A *finite t-automaton*, briefly *fta*, over $\mathbb{H} * \{t, t^{-1}\}^*$ with labelling set $\mathcal{F}$ is a 5-tuple

$$\mathcal{A} = \langle \mathcal{L}, \mathsf{Q}, \delta, \mathsf{I}, \mathsf{T} \rangle, \tag{25}$$

where $\mathcal{L} \subseteq \mathcal{F} \cup \{\{t\}, \{t^{-1}\}\}$ is finite, Q is a finite set of states, $\mathsf{I} \subseteq \mathsf{Q}$ is the set of initial states, $\mathsf{T} \subseteq \mathsf{Q}$ is the set of terminal states, and δ (the set of transitions) is a subset of $\mathsf{Q} \times \mathcal{L} \times \mathsf{Q}$ such that

$$\forall q \in \mathsf{Q}\ \exists L \in \mathcal{L} : 1 \in L\ \wedge\ (q, L, q) \in \delta. \tag{26}$$

We define

$$\widehat{\delta} = \{(p, x, q) \in \mathsf{Q} \times (\mathbb{H} \cup \{t, t^{-1}\}) \times \mathsf{Q} \mid \exists L \in \mathcal{L} : x \in L\ \wedge\ (p, L, q) \in \delta\}. \tag{27}$$

The automaton $\mathcal{A}$ induces a representation map

$$\mu_{\mathcal{A}} : \mathbb{H} * \{t, t^{-1}\}^* \to \mathsf{B}(\mathsf{Q})$$

defined as follows: First, define $\mu_{\mathcal{A},0} : \mathbb{H} \cup \{t, t^{-1}\} \to \mathsf{B}(\mathsf{Q})$ as follows, where $x \in \mathbb{H} \cup \{t, t^{-1}\}$:

$$\mu_{\mathcal{A},0}(x) = \{(q, r) \in Q \times Q \mid (q, x, r) \in \widehat{\delta}\,\} \tag{28}$$

Note that $\mathrm{Id}_{\mathsf{Q}} \subseteq \mu_{\mathcal{A},0}(1)$ due to (26). For $x \in \mathbb{H} \cup \{t, t^{-1}\}$ and $q, r \in \mathsf{Q}$ we will also write $q \xrightarrow{x}_{\mathcal{A}} r$ instead of $(q, r) \in \mu_{\mathcal{A},0}(x)$.

Now, let $s = h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_n} h_n$ be a t-sequence of the form (5). Then

$$\mu_{\mathcal{A}}(s) = \mu_{\mathcal{A},0}(h_0) \circ \mu_{\mathcal{A},0}(t^{\alpha_1}) \circ \mu_{\mathcal{A},0}(h_1) \cdots \mu_{\mathcal{A},0}(t^{\alpha_i}) \circ \mu_{\mathcal{A},0}(h_i) \cdots \mu_{\mathcal{A},0}(t^{\alpha_n}) \circ \mu_{\mathcal{A},0}(h_n).$$

The subset of $\mathbb{H} * \{t, t^{-1}\}^*$ recognized by $\mathcal{A}$ is

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

On the set $\mathcal{T}_6$ of vertex types, we define a directed, edge-labeled graph $\mathcal{G}_6 = (\mathcal{T}_6, \mathcal{E}_6)$ by (we write for instance (A, T, t, B, H) instead of $((A, T), t, (B, H))$)

$$\begin{aligned}
\mathcal{E}_6 = \quad & \{(A(\alpha), T, t^{\alpha}, A(-\alpha), H) \mid \alpha \in \{+1, -1\}\} \\
& \cup \{(C, H, \mathbb{H}, D, T) \mid C \in \{1, A, B\}, D \in \{A, B\}\} \\
& \cup \{(C, H, \mathbb{H}, 1, 1) \mid C \in \{1, A, B\}\} \\
& \cup \{(\theta, p_1(\theta), \theta) \mid \theta \in \mathcal{T}_6\}.
\end{aligned}$$

The graph $\mathcal{G}_6$ is represented in Figure 2. We sometimes use also the graph $\mathcal{R}_6 = (\mathcal{T}_6, \mathcal{E}'_6)$ where

$$\begin{aligned}
\mathcal{E}'_6 = (\mathcal{E}_6 \setminus \{(A, H, \mathbb{H}, A, T), (B, H, \mathbb{H}, B, T))\}) \cup \\
\{(A, H, \mathbb{H} \setminus A, A, T), (B, H, \mathbb{H} \setminus B, B, T)\};
\end{aligned}$$

it is shown in Figure 3. One can check that the graph $\mathcal{G}_6$ (resp. $\mathcal{R}_6$) endowed with the set of initial states $\mathsf{I}_6 = \{(1, H)\}$ and the set of final states $\mathsf{T}_6 = \{(1, 1)\}$ is an fta recognizing $\mathbb{H} * \{t, t^{-1}\}^*$ (resp. $\mathrm{Red}(\mathbb{H}, t)$).

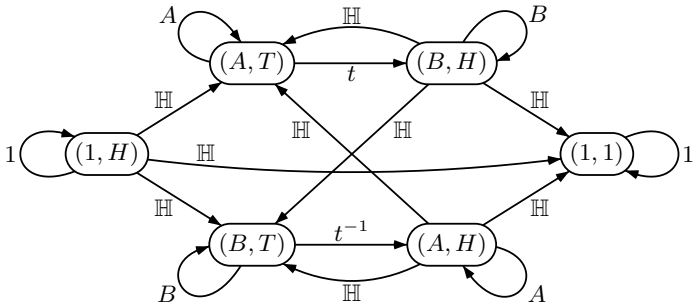


Fig. 2. The graph $\mathcal{G}_6 = (\mathcal{T}_6, \mathcal{E}_6)$

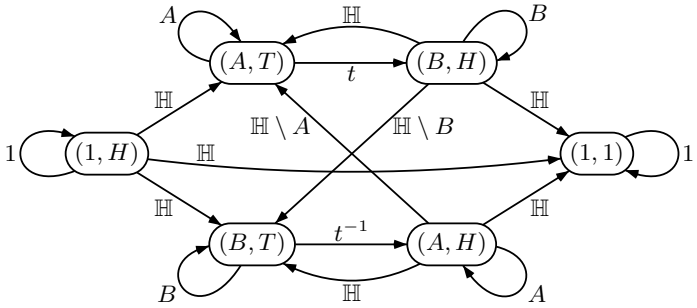


Fig. 3. The graph $\mathcal{R}_6 = (\mathcal{T}_6, \mathcal{E}'_6)$

Definition 2 (partitionned fta). *A* partitioned fta *with labelling set $\mathcal{F}$ is a 6-tuple*

$$\mathcal{A} = \langle \mathcal{L}, \mathsf{Q}, \tau, \delta, \mathsf{I}, \mathsf{T} \rangle, \tag{29}$$

where $\langle \mathcal{L}, \mathsf{Q}, \delta, \mathsf{I}, \mathsf{T} \rangle$ is an fta with labelling set $\mathcal{F}$, $\tau : Q \to \mathcal{T}_6$ assigns a vertex type to every state, and the transitions in δ and the sets I and T respect the types in the following sense:

$$\forall (q,h,r) \in \widehat{\delta} : (\tau(q), h, \tau(r)) \in \widehat{\mathcal{E}}_6 \tag{30}$$

$$\tau(\mathsf{I}) = \{(1,H)\} \ \wedge \ \tau(\mathsf{T}) = \{(1,1)\}. \tag{31}$$

For a partitioned fta $\mathcal{A}$ as in (29) and a state $q \in \mathsf{Q}$, we denote by $\gamma(q)$ the subgroup

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

The following lemma follows directly from the structure of the graph $\mathcal{G}_6$:

Lemma 10. *Let $\theta_1, \theta_2, \theta_3 \in \mathcal{T}_6$ and let $h, h' \in \mathbb{H}$ such that $\theta_1 \xrightarrow{h}_{\mathcal{G}_6} \theta_2 \xrightarrow{h'}_{\mathcal{G}_6} \theta_3$. Then ($\theta_1 = \theta_2$ and $h \in p_1(\theta_2)$) or ($\theta_2 = \theta_3$ and $h' \in p_1(\theta_2)$).*

We define an additional function $\mu_{\mathcal{A},1} : \mathcal{T} \times \mathbb{H} * \{t, t^{-1}\}^* \to \mathsf{B}(\mathsf{Q})$ as follows: For all $s \in \mathbb{H} * \{t, t^{-1}\}^*$ and $(\theta, b, \theta') \in \mathcal{T}$ let

$$\mu_{\mathcal{A},1}((\theta, b, \theta'), s) = \mu_{\mathcal{A}}(s) \cap (\tau^{-1}(\theta) \times \tau^{-1}(\theta')). \tag{32}$$

Note that the boolean component b from (θ, b, θ') has no influence on the value of $\mu_{\mathcal{A},1}((\theta, b, \theta'), s)$. Let us define maps γ_+ and γ_t that associate to every sequence $s \in \mathbb{H} * \{t, t^{-1}\}^*$ the set of all

path types that can be realized by s in the automaton $\mathcal{G}_6$ (resp. $\mathcal{R}_6$):

$$\gamma_+(s) = \{(\theta, \|s\|_b, \theta') \in \mathcal{T} \mid (\theta, \theta') \in \mu_{\mathcal{G}_6}(s)\} \in 2^{\mathcal{T}} \tag{33}$$
$$\gamma_t(s) = \{(\theta, \|s\|_b, \theta') \in \mathcal{T} \mid (\theta, \theta') \in \mu_{\mathcal{R}_6}(s)\} \in 2^{\mathcal{T}} \tag{34}$$

Clearly, we have $\gamma_t(s) \subseteq \gamma_+(s)$. Moreover, note that

$$\gamma_+(h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_n} h_n) = \gamma_+(h_0)\gamma_+(t^{\alpha_1})\gamma_+(h_1)\cdots\gamma_+(t^{\alpha_n})\gamma_+(h_n) \text{ and} \tag{35}$$
$$\gamma_t(h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_n} h_n) = \gamma_t(h_0)\gamma_t(t^{\alpha_1})\gamma_t(h_1)\cdots\gamma_t(t^{\alpha_n})\gamma_t(h_n). \tag{36}$$

Here, we use the multiplication in the monoid $2^{\mathcal{T}}$ that is obtained from the multiplication in the partial semigroup $\mathcal{T}$; see (14).

Recall the equivalences $\sim$ and $\approx$ over $\mathbb{H} * \{t, t^{-1}\}^*$ defined in Section 2.2.

Definition 3 ($\approx$-compatible, $\sim$-saturated, strict). *An fta $\mathcal{A}$ is said to be $\approx$-compatible if and only if*

$$[\mathrm{L}(\mathcal{A})]_{\approx} = [\mathrm{L}(\mathcal{A}) \cap \mathrm{Red}(\mathbb{H}, t)]_{\approx}. \tag{37}$$

It is said to be $\sim$-saturated *if and only if*

$$\forall s, s' \in \mathbb{H} * \{t, t^{-1}\}^* : s \sim s' \Rightarrow \mu_{\mathcal{A}}(s) = \mu_{\mathcal{A}}(s'). \tag{38}$$

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

$$\mathrm{L}(\mathcal{A}) \subseteq \mathrm{Red}(\mathbb{H}, t). \tag{39}$$

Note that every strict fta is $\approx$-compatible.

In [LS08] the direct product of two fta (which is again an fta) as well as the product of two partitioned fta (which is again a partitioned fta) is defined. Let $\mathcal{A}_1 = \langle \mathcal{L}_1, \mathsf{Q}_1, \delta_1, \mathsf{I}_1, \mathsf{T}_1 \rangle$ and $\mathcal{A}' = \langle \mathcal{L}_2, \mathsf{Q}_2, \delta_2, \mathsf{I}_2, \mathsf{T}_2 \rangle$ be fta. Then,

$$\mathcal{A}_1 \times \mathcal{A}_2 = \langle \{L_1 \cap L_2 \mid L_1 \in \mathcal{L}_1, L_2 \in \mathcal{L}_2\} \setminus \{\emptyset\}, \mathsf{Q}_1 \times \mathsf{Q}_2, \delta, \mathsf{I}_1 \times \mathsf{I}_2, \mathsf{T}_1 \times \mathsf{T}_2 \rangle,$$

where

$$\delta = \{((p_1, p_2), L_1 \cap L_2, (q_1, q_2)) \mid (p_1, L_1, q_1) \in \delta_1, (p_2, L_2, q_2) \in \delta_2, L_1 \cap L_2 \neq \emptyset\}.$$

If $\mathcal{A}_1$ and $\mathcal{A}_2$ are partitioned fta, then the definition is the same, except that the state set of $\mathcal{A}_1 \times \mathcal{A}_2$ is $\bigcup_{\theta \in \mathcal{T}_6} \tau_1^{-1}(\theta) \times \tau_2^{-1}(\theta)$, where τ_i is the type mapping of $\mathcal{A}_i$. The following lemmas are shown in [LS08]:

Lemma 11. *Let $\mathcal{A}$ and $\mathcal{A}'$ be (partitioned) fta. Then, $L(\mathcal{A} \times \mathcal{A}') = L(\mathcal{A}) \times L(\mathcal{A}')$. Moreover, if $\mathcal{A}$ and $\mathcal{A}'$ are both $\sim$-saturated, then also $\mathcal{A} \times \mathcal{A}'$ is $\sim$-saturated. If $\mathcal{A}$ and $\mathcal{A}'$ are both $\sim$-saturated and $\approx$-compatible, then also $\mathcal{A} \times \mathcal{A}'$ is $\sim$-saturated and $\approx$-compatible.*

Lemma 12. *Let $\mathcal{A}$ be an fta. Then $\mathcal{A} \times \mathcal{G}_6$ (resp. $\mathcal{A} \times \mathcal{R}_6$) is a partitioned fta with $L(\mathcal{A} \times \mathcal{G}_6) = L(\mathcal{A})$ (resp. $L(\mathcal{A} \times \mathcal{R}_6) = L(\mathcal{A}) \cap \mathrm{Red}(\mathbb{H}, t)$).*

Definition 4 (unitary, subgroup-compatible, multiplicative). *The partitioned fta $\mathcal{A} = \langle \mathcal{L}, \mathsf{Q}, \tau, \delta, \mathsf{I}, \mathsf{T} \rangle$ is* unitary*, if for every vertex type $\Theta \in \mathcal{T}_6$ we have*

$$\mu_{\mathcal{A},0}(1) \cap (\tau^{-1}(\theta) \times \tau^{-1}(\theta)) = \mathrm{Id}_{\mathsf{Q}} \cap (\tau^{-1}(\theta) \times \tau^{-1}(\theta)).$$

$\mathcal{A}$ *is* subgroup-compatible *if for every vertex type $\theta \in \mathcal{T}_6$, there exists a right-action $\odot$ of the subgroup $p_1(\theta)$ on the set of states $\tau^{-1}(\theta) \subseteq \mathsf{Q}$ such that for all $q, r \in \mathsf{Q}$, $c \in p_1(\theta)$, and $h \in \mathbb{H}$,*

$$\tau(q) = \theta \implies q \xrightarrow{c}_{\mathcal{A}} q \odot c \tag{40}$$

$$(\tau(q) = \theta \wedge q \xrightarrow{h}_{\mathcal{A}} r) \implies q \odot c^{-1} \xrightarrow{ch}_{\mathcal{A}} r \tag{41}$$

$$(\tau(r) = \theta \wedge q \xrightarrow{h}_{\mathcal{A}} r) \implies q \xrightarrow{hc}_{\mathcal{A}} r \odot c \tag{42}$$

Note that in case $p_1(\theta) = 1$, these conditions are trivially satisfied by setting $q \odot 1 = q$ for all q with $\tau(q) = \theta$ ((40) follows from the existence of 1-loops; see (26)).

The partitioned fta $\mathcal{A}$ is multiplicative*, if for all $\boldsymbol{\theta} \in \gamma_+(s), \boldsymbol{\theta'} \in \gamma_+(s')$ such that $\boldsymbol{\theta\theta'}$ is defined in the partial semigroup $\mathcal{T}$:*

$$\mu_{\mathcal{A},1}(\boldsymbol{\theta\theta'}, ss') = \mu_{\mathcal{A},1}(\boldsymbol{\theta}, s) \circ \mu_{\mathcal{A},1}(\boldsymbol{\theta'}, s') \tag{43}$$

Definition 5 (normal fta). *A partitioned fta $\mathcal{A}$ is said to be* normal*, if it is $\approx$-compatible, $\sim$-saturated, unitary and multiplicative.*

Lemma 13. *Let $\mathcal{A}$ be a partitioned fta. If $\mathcal{A}$ is unitary and subgroup-compatible, then $\mathcal{A}$ is multiplicative.*

Proof. Let Q be the state set of the fta $\mathcal{A}$. Assume that $\mathcal{A}$ is unitary and subgroup-compatible, and let $\boldsymbol{\theta} \in \gamma_+(s)$, $\boldsymbol{\theta'} \in \gamma_+(s')$ such that $\boldsymbol{\theta\theta'}$ is defined in $\mathcal{T}$. We have to show that

$$\mu_{\mathcal{A},1}(\boldsymbol{\theta\theta'}, ss') = \mu_{\mathcal{A},1}(\boldsymbol{\theta}, s) \circ \mu_{\mathcal{A},1}(\boldsymbol{\theta'}, s').$$

We prove this identity by induction over $\|ss'\| = \|s\| + \|s'\|$.

First assume that $\|s\| = \|s'\| = 0$, i.e., $s = h \in \mathbb{H}$ and $s' = h' \in \mathbb{H}$. We must have $\boldsymbol{\theta} = (\theta, 0, \theta')$ and $\boldsymbol{\theta'} = (\theta', 0, \theta'')$ for some vertex types $\theta, \theta', \theta'' \in \mathcal{T}_6$. Hence, $\theta \xrightarrow{h}_{\mathcal{G}_6} \theta' \xrightarrow{h'}_{\mathcal{G}_6} \theta''$. Lemma 10 implies ($\theta = \theta'$ and $h \in p_1(\theta)$) or ($\theta' = \theta''$ and $h' \in p_1(\theta')$). Let us first assume that $\theta = \theta'$ and $h \in p_1(\theta)$. We obtain for all $(p, q) \in \mathsf{Q} \times \mathsf{Q}$:

$$\begin{aligned}
(p,q) \in \mu_{\mathcal{A},1}((\theta,0,\theta''), hh') &\implies p \xrightarrow{hh'}_{\mathcal{A}} q,\ \tau(p) = \theta,\ \tau(\theta'') = q \\
&\implies p \xrightarrow{h}_{\mathcal{A}} p \odot h = p \odot (h^{-1})^{-1} \xrightarrow{h^{-1}hh'}_{\mathcal{A}} q, \\
&\qquad \tau(p \odot h) = \tau(p) = \theta,\ \tau(\theta'') = q \\
&\implies (p,q) \in \mu_{\mathcal{A},1}((\theta,0,\theta), h) \circ \mu_{\mathcal{A},1}((\theta,0,\theta''), h') \\
&\implies \exists r \in \tau^{-1}(\theta) : (p,r) \in \mu_{\mathcal{A},1}((\theta,0,\theta), h), (r,q) \in \mu_{\mathcal{A},1}((\theta,0,\theta''), h') \\
&\implies \tau(p) = \theta, \tau(q) = \theta'', \exists r \in \tau^{-1}(\theta) : p \xrightarrow{h}_{\mathcal{A}} r \xrightarrow{h'}_{\mathcal{A}} q \\
&\implies \tau(p) = \theta, \tau(q) = \theta'', \exists r \in \tau^{-1}(\theta) : p \xrightarrow{hh^{-1}}_{\mathcal{A}} r \odot h^{-1} \xrightarrow{hh'}_{\mathcal{A}} q
\end{aligned}$$

Since $\mathcal{A}$ is unitary, $p \xrightarrow{1}_{\mathcal{A}} r \odot h^{-1}$, and $\tau(p) = \tau(r) = \tau(r \odot h^{-1}) = \theta$, we must have $p = r \odot h^{-1}$. Thus, we get:

$$\tau(p) = \theta, \quad \tau(q) = \theta'', \quad p \xrightarrow{hh'}_{\mathcal{A}} q,$$

i.e. $(p, q) \in \mu_{\mathcal{A},1}((\theta, 0, \theta''), hh')$. The case that $\theta' = \theta''$ can be dealt analogously. This settles the induction base.

Now assume that $\|s\| > 0$ or $\|s'\| > 0$. Let $\|s'\| > 0$; the case that $\|s\| > 0$ can be dealt analogously). We can factorize the sequence s' as $s' = s_1 t^\alpha h$ with $\alpha \in \{-1, 1\}$ and $h \in \mathbb{H}$. The path type $\boldsymbol{\theta'} \in \gamma_+(s')$ must be of the form $\boldsymbol{\theta'} = (\theta', 1, \theta'')$. Let $\boldsymbol{\theta} = (\theta, \|s\|_b, \theta')$. Let us assume that $\alpha = 1$, again the case $\alpha = -1$ can be dealt analogously. Since (A, T, t, B, H) is the only t-labeled edge of $\mathcal{G}_6$ and $\mathcal{A}$ is partitioned, we have

$$\begin{aligned}\mu_{\mathcal{A},1}(\boldsymbol{\theta'}, s') &= \mu_{\mathcal{A},1}((\theta', 1, \theta''), s_1 t h) \\ &= \mu_{\mathcal{A},1}((\theta', \|s_1\|_b, A, T), s_1) \circ \mu_{\mathcal{A},1}((A, T, 1, B, H), t) \circ \mu_{\mathcal{A},1}((B, H, 0, \theta''), h).\end{aligned}$$

By induction, we get:

$$\begin{aligned}\mu_{\mathcal{A},1}(\boldsymbol{\theta}, s) \circ \mu_{\mathcal{A},1}(\boldsymbol{\theta'}, s') &= \mu_{\mathcal{A},1}((\theta, \|s\|_b, \theta'), s) \circ \mu_{\mathcal{A},1}((\theta', \|s_1\|_b, A, T), s_1) \circ \\ &\qquad \mu_{\mathcal{A},1}((A, T, 1, B, H), t) \circ \mu_{\mathcal{A},1}((B, H, 0, \theta''), h) \\ &= \mu_{\mathcal{A},1}((\theta, \|s s_1\|_b, A, T), s s_1) \circ \\ &\qquad \mu_{\mathcal{A},1}((A, T, 1, B, H), t) \circ \mu_{\mathcal{A},1}((B, H, 0, \theta''), h) \\ &= \mu_{\mathcal{A},1}((\theta, 1, \theta''), s s_1 t h) \\ &= \mu_{\mathcal{A},1}(\boldsymbol{\theta\theta'}, s s')\end{aligned}$$

□

Note that the partitioned fta $\mathcal{G}_6$ and $\mathcal{R}_6$ are unitary and subgroup-compatible. For the latter, define $\theta \odot c = \theta$ for very $\theta \in \mathcal{T}_6$ and $c \in p_1(\theta)$. Hence, by Lemma 13, $\mathcal{G}_6$ and $\mathcal{R}_6$ are multiplicative. This implies the following lemma:

Lemma 14. *For all $\boldsymbol{\theta} \in \gamma_+(s), \boldsymbol{\theta'} \in \gamma_+(s')$ such that $\boldsymbol{\theta\theta'}$ is defined in the partial semigroup $\mathcal{T}$, we have $\boldsymbol{\theta\theta'} \in \gamma_+(ss')$.*

The following two lemmas complement Lemma 11 by additional preservation properties.

Lemma 15. *Let $\mathcal{A}$ and $\mathcal{A}'$ be partitioned fta. If $\mathcal{A}$ and $\mathcal{A}'$ are both unitary, then $\mathcal{A} \times \mathcal{A}'$ is a unitary partitioned fta as well.*

Proof. To show that $\mathcal{A} \times \mathcal{A}'$ is unitary, it is enough to show that

$$\mu_{\mathcal{A}\times\mathcal{A}',0}(1) \cap (\tau^{-1}(\theta) \times \tau^{-1}(\theta)) \subseteq \mathrm{Id}_{\mathsf{Q}} \cap (\tau^{-1}(\theta) \times \tau^{-1}(\theta));$$

the converse inclusion follows from (26). If $((p, p'), (q, q')) \in \mu_{\mathcal{A}\times\mathcal{A}',0}(1) \cap (\tau^{-1}(\theta) \times \tau^{-1}(\theta))$ then there exist a transition (p, L, q) in $\mathcal{A}$ with $1 \in L$ and a transition (p', L', q') in $\mathcal{A}'$ with $1 \in L'$. Since $\mathcal{A}$ and $\mathcal{A}'$ are both unitary, we get $p = q$ and $p' = q'$. Hence $\mathcal{A} \times \mathcal{A}'$ is unitary. □

Lemma 16. *Let $\mathcal{A}$ and $\mathcal{A}'$ be partitioned fta. If $\mathcal{A}$ and $\mathcal{A}'$ are both mutiplicative, then $\mathcal{A} \times \mathcal{A}'$ is multiplicative as well.*

Proof. Let $\mathcal{A} = \langle \mathcal{L}, \mathsf{Q}, \tau, \delta, \mathsf{I}, \mathsf{T} \rangle$ and $\mathcal{A}' = \langle \mathcal{L}', \mathsf{Q}', \tau', \delta', \mathsf{I}', \mathsf{T}' \rangle$ be partitioned mutiplicative fta. Let us consider the partial semigroup on the set

$$S = \{(\boldsymbol{\theta}, s) \mid s \in \mathbb{H} * \{t, t^{-1}\}^*, \boldsymbol{\theta} \in \gamma_+(s)\}.$$

The product $(\boldsymbol{\theta}, s)(\boldsymbol{\theta'}, s')$ is defined if $\boldsymbol{\theta\theta'}$ is defined in the partial semigroup $\mathcal{T}$, and in this case we set $(\boldsymbol{\theta}, s)(\boldsymbol{\theta'}, s') = (\boldsymbol{\theta\theta'}, ss')$. Note that by Lemma 14 we have $(\boldsymbol{\theta\theta'}, ss') \in S$. Also note

that $\mu_{\mathcal{A},1} : S \to \mathsf{B}(\mathsf{Q})$ is a homomorphism if and only if $\mathcal{A}$ is multiplicative. Thus, $\mu_{\mathcal{A},1}$ and $\mu_{\mathcal{A}',1}$ are homomorphisms from S to $\mathsf{B}(\mathsf{Q})$ and $\mathsf{B}(\mathsf{Q}')$, respectively. By Lemma 2, $\mu_{\mathcal{A},1} \otimes \mu_{\mathcal{A}',1}$ is a homomorphism from S to $\mathsf{B}(\mathsf{Q} \times \mathsf{Q}')$. Hence it suffices to show that $\mu_{\mathcal{A}\times\mathcal{A}',1} = \mu_{\mathcal{A},1} \otimes \mu_{\mathcal{A}',1}$. To see this, let $(\boldsymbol{\theta}, s) \in S$. If $((p,p'),(q,q')) \in \mu_{\mathcal{A}\times\mathcal{A}',1}(\boldsymbol{\theta}, s)$, then we clearly have $(p,q) \in \mu_{\mathcal{A},1}(\boldsymbol{\theta}, s)$ and $(p',q') \in \mu_{\mathcal{A}',1}(\boldsymbol{\theta}, s)$. Now assume that $(p,q) \in \mu_{\mathcal{A},1}(\boldsymbol{\theta}, s)$ and $(p',q') \in \mu_{\mathcal{A}',1}(\boldsymbol{\theta}, s)$. Let $p = p_0, p_1, \ldots, p_{n-1}, p_n = q$ be the state sequence in a run of $\mathcal{A}$ on s leading from p to q. Similarly, let $p' = p'_0, p'_1, \ldots, p'_{n-1}, p'_n = q'$ be the state sequence in a run of $\mathcal{A}'$ on s leading from p' to q'. The crucial observation is that $\tau(p_i) = \tau(p'_i)$ for all $0 \leq i \leq n$. This follows from the fact that $\mathcal{A}$ and $\mathcal{A}'$ are partitioned, and that in $\mathcal{G}_6$ there is a unique way of going from one vertex to another vertex with a certain $s \in \mathbb{H} * \{t, t^{-1}\}^*$. The above observation implies that $((p,p'),(q,q')) \in \mu_{\mathcal{A}\times\mathcal{A}',1}(\boldsymbol{\theta}, s)$. □

Lemma 17. *Let $\mathcal{A}$, $\mathcal{A}'$ be normal fta. The direct product $\mathcal{A} \times \mathcal{A}'$ of two normal fta $\mathcal{A}$, $\mathcal{A}'$, is normal too.*

Proof. This follows from Lemma 11 ($\sim$-saturation and $\approx$-compatibility), Lemma 15 (unitarity) and Lemma 16 (multiplicativity). □

Proposition 1. *Let $R \subseteq \mathbb{G}$.*

(1) $R \in \mathsf{Rat}(\mathbb{G})$ if and only if $R = \pi_{\mathbb{G}}(\mathrm{L}(\mathcal{A}))$ for some normal *partitioned fta $\mathcal{A}$ with labeling set $\mathsf{Rat}(\mathbb{H})$.*

(2) If $R \in \mathsf{bool}(\mathsf{Rat}(\mathbb{G}))$ then $R = \pi_{\mathbb{G}}(\mathrm{L}(\mathcal{B}))$ for some strict normal *partitioned fta $\mathcal{B}$ with labeling set $\mathsf{bool}(\mathsf{Rat}(\mathbb{H}))$.*

Proof. It is proved in [LS08, Prop. 33, points (1), (3), and (a)] that R is a rational subset of $\mathbb{G}$ if and only if $\pi_{\mathbb{G}}^{-1}(R) \cap \mathrm{Red}(\mathbb{H}, t) = \mathrm{L}(\mathcal{A}) \cap \mathrm{Red}(\mathbb{H}, t)$ for some partitioned, $\approx$-compatible, $\sim$-saturated, and unitary fta $\mathcal{A}$ with labelling set $\mathsf{Rat}(\mathbb{H})$. Moreover, the automaton $\mathcal{A}$ can be chosen in such a way that it is subgroup-compatible: this follows from equations (39)-(40) in the proof of [LS08, Prop. 22]. By Lemma 13, $\mathcal{A}$ is multiplicative and hence normal. Finally, (37) implies

$$\pi_{\mathbb{G}}(\mathrm{L}(\mathcal{A})) = \pi_{\mathbb{G}}(\mathrm{L}(\mathcal{A}) \cap \mathrm{Red}(\mathbb{H}, t)) = \pi_{\mathbb{G}}(\pi_{\mathbb{G}}^{-1}(R) \cap \mathrm{Red}(\mathbb{H}, t)) = R.$$

This shows point (1).

For (2), let R be a boolean combination of rational subsets $K_1, \ldots, K_p$ of $\mathbb{G}$. By [LS08, Prop. 28 and 33], for every $1 \leq i \leq p$ there exists a partitionned, $\sim$-saturated, deterministic and complete fta[2] $\mathcal{C}_i$, whose labelling set is $\mathsf{bool}(\mathsf{Rat}(H))$, and such that

$$\mathrm{L}(\mathcal{C}_i) = \pi_{\mathbb{G}}^{-1}(K_i) \cap \mathrm{Red}(\mathbb{H}, t)$$

for $1 \leq i \leq p$. Since every boolean operation can be translated over partitioned, $\sim$-saturated, deterministic and complete fta (see [LS08, Lemma 15, 17, 18, and 20]), there exists a partitioned, $\sim$-saturated, deterministic and complete, fta $\mathcal{A}$, whose labelling set is $\mathsf{bool}(\mathsf{Rat}(H))$, and such that

$$\mathrm{L}(\mathcal{A}) = \pi_{\mathbb{G}}^{-1}(R) \cap \mathrm{Red}(\mathbb{H}, t). \tag{44}$$

Moreover, since $\mathrm{L}(\mathcal{A}) \subseteq \mathrm{Red}(\mathbb{H}, t)$, $\mathcal{A}$ is also $\approx$-compatible.

[2] The definition of a deterministic and complete fta can be found in [LS08], but the precise definition is not really needed for the following arguments.

By applying [LS08, Prop. 22] to this fta $\mathcal{A}$ and the set $\mathcal{F} = \mathsf{bool}(\mathsf{Rat}(H))$, we obtain a partitioned, $\approx$-compatible, $\sim$-saturated, unitary fta $\mathcal{B}$ with labelling set $\mathcal{G} := \{cFc' \mid F \in \mathsf{bool}(\mathsf{Rat}(H)), c, c' \in A \cup B\}$ such that

$$\begin{aligned} \mathrm{L}(\mathcal{B}) \cap \mathrm{Red}(\mathbb{H}, t) &= [\mathrm{L}(\mathcal{A})]_{\approx} \cap \mathrm{Red}(\mathbb{H}, t) \\ &= [\pi_{\mathbb{G}}^{-1}(R) \cap \mathrm{Red}(\mathbb{H}, t)]_{\approx} \cap \mathrm{Red}(\mathbb{H}, t) \\ &= \pi_{\mathbb{G}}^{-1}(R) \cap \mathrm{Red}(\mathbb{H}, t). \end{aligned} \tag{45}$$

By Lemma 9, $\mathcal{G} = \mathsf{bool}(\mathsf{Rat}(H))$, so that $\mathcal{B}$ is labelled over $\mathsf{bool}(\mathsf{Rat}(H))$. Equality (45) implies $R = \pi_{\mathbb{G}}(\mathrm{L}(\mathcal{B}))$ by the same argument as for (1). Moreover, by equations (39)–(40) of [LS08], $\mathcal{B}$ is subgroup-compatible. Thus, by Lemma 13, $\mathcal{B}$ is multiplicative. By [LS08, Claim 26], $\mathrm{L}(\mathcal{B}) \subseteq [\mathrm{L}(\mathcal{A})]_{\sim} = \mathrm{L}(\mathcal{A})$ (since $\mathcal{A}$ is $\sim$-saturated), while by (44) $\mathrm{L}(\mathcal{A}) \subseteq \mathrm{Red}(\mathbb{H}, t)$. Hence $\mathcal{B}$ is also strict. Thus, $\mathcal{B}$ is strict and normal. □

The fta $\mathcal{G}_6$ and $\mathcal{R}_6$ are clearly partionned with τ the identity mapping. Moreover, these fta are $\approx$-compatible, $\sim$-saturated, unitary, and subgroup compatible. For the latter, we choose for $\odot$ the trivial action. Hence, by Lemma 13, $\mathcal{G}_6$ and $\mathcal{R}_6$ are also multiplicative. As a corollary, we obtain:

Lemma 18. *For all $s_1, s_2 \in \mathbb{H} * \{t, t^{-1}\}^*$ we have $\gamma_+(s_1)\gamma_+(s_2) \subseteq \gamma_+(s_1 s_2)$ and $\gamma_t(s_1)\gamma_t(s_2) \subseteq \gamma_t(s_1 s_2)$.*

Proof. Let us prove the statement for γ_+, the same proof also works for γ_t. Let $s_1, s_2 \in \mathbb{H} * \{t, t^{-1}\}^*$, $\boldsymbol{\theta_1} \in \gamma_+(s_1)$ and $\boldsymbol{\theta_2} \in \gamma_+(s_2)$ such that $\boldsymbol{\theta_1}\boldsymbol{\theta_2}$ is defined. We have to show that $\boldsymbol{\theta_1}\boldsymbol{\theta_2} \in \gamma_+(s_1 s_2)$. Since $\mathcal{G}_6$ is multiplicative, we have

$$\mu_{\mathcal{G}_6,1}(\boldsymbol{\theta_1}\boldsymbol{\theta_2}, s_1 s_2) = \mu_{\mathcal{G}_6,1}(\boldsymbol{\theta_1}, s_1) \circ \mu_{\mathcal{G}_6,1}(\boldsymbol{\theta_2}, s_2). \tag{46}$$

Let $\boldsymbol{\theta_1} = (\theta_1, \|s_1\|_b, \theta_2)$, $\boldsymbol{\theta_2} = (\theta_2, \|s_2\|_b, \theta_3)$, and $\boldsymbol{\theta_1}\boldsymbol{\theta_2} = (\theta_1, \|s_1 s_2\|_b, \theta_3)$. Since $\boldsymbol{\theta_1} \in \gamma_+(s_1)$, we have $(\theta_1, \theta_2) \in \mu_{\mathcal{G}_6}(s_1)$ and similarly $(\theta_2, \theta_3) \in \mu_{\mathcal{G}_6}(s_2)$. Hence, $(\theta_1, \theta_2) \in \mu_{\mathcal{G}_6,1}(\boldsymbol{\theta_1}, s_1)$ and $(\theta_2, \theta_3) \in \mu_{\mathcal{G}_6,1}(\boldsymbol{\theta_2}, s_2)$. Thus, (46) implies $(\theta_1, \theta_3) \in \mu_{\mathcal{G}_6,1}(\boldsymbol{\theta_1}\boldsymbol{\theta_2}, s_1 s_2)$. This implies $\boldsymbol{\theta_1}\boldsymbol{\theta_2} = (\theta_1, \|s_1 s_2\|_b, \theta_3) \in \gamma_+(s_1 s_2)$. □

Given a normal fta $\mathcal{A}$ and an element $g \in \mathbb{G}$ we set

$$\mu_{\mathcal{A},\mathbb{G}}(g) = \mu_{\mathcal{A},1}((1, H, \|s\|_b, 1, 1), s), \tag{47}$$

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

2.6 Equations and disequations over a monoid

Let $\mathbb{M}$ be some monoid and let

$$\mathcal{C} \subseteq 2^{\mathbb{M}}$$

be a class of constraints sets. A *system of equations and disequations* over the monoid $\mathbb{M}$ is a subset $\mathcal{S} \subseteq \mathcal{U}^* \times \{=, \neq\} \times \mathcal{U}^*$, where $\mathcal{U}$ is the set of variables of $\mathcal{S}$. Instead of $(u, =, u') \in \mathcal{S}$ (resp. $(u, \neq, u') \notin \mathcal{S}$) we just write $(u = u') \in \mathcal{S}$ (resp. $(u \neq u') \notin \mathcal{S}$). The system $\mathcal{S}$ is said to be *quadratic* if

– for every $(u = u') \in \mathcal{S}$ we have $|u| = 1$ and $|u'| = 2$, and
– for every $(u \neq u') \in \mathcal{S}$ we have $|u| = |u'| = 1$.

A system of equations and disequations over the monoid $\mathbb{M}$ with $\mathcal{C}$-*constraints* is a pair $(\mathcal{S}, \mathsf{C})$, where $\mathcal{S}$ is a system of equations and disequations over the monoid $\mathbb{M}$ and C is a map $\mathsf{C} : \mathcal{U} \to \mathcal{C}$. An $\mathbb{M}$-solution of the system $(\mathcal{S}, \mathsf{C})$ is any monoid homomorphism

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

fulfilling the following conditions:

$$\forall (u = u') \in \mathcal{S} : \sigma_{\mathbb{M}}(u) = \sigma_{\mathbb{M}}(u') \tag{48}$$
$$\forall (u \neq u') \in \mathcal{S} : \sigma_{\mathbb{M}}(u) \neq \sigma_{\mathbb{M}}(u') \tag{49}$$
$$\forall U \in \mathcal{U} : \sigma_{\mathbb{M}}(U) \in \mathsf{C}(U). \tag{50}$$

The system $\mathcal{S}$ is a *system of equations* over $\mathbb{M}$ (with $\mathcal{C}$-constraints), if

$$\mathcal{S} \subseteq \mathcal{U}^* \times \{=\} \times \mathcal{U}^*.$$

In this paper, we will consider three particular sets of constraints.

– $\mathcal{C} = \{\{m\} \mid m \in \mathbb{M}\} \cup \{\mathbb{M}\}$: In this case, a system of equations (and disequations) with $\mathcal{C}$-constraints is called a system of equations (and disequations) with *constants*, since the variables $U \in \mathcal{U}$ with $|\mathsf{C}(U)| = 1$ can be seen as constants from $\mathbb{M}$, while the variables $U \in \mathcal{U}$ with $\mathsf{C}(U) = \mathbb{M}$ can be seen as variables without any constraint.
– $\mathcal{C} = \mathsf{bool}(Rat(\mathbb{M}))$, i.e. the boolean closure of the set of rational subsets of $\mathbb{M}$: In this case, a system of equations (and disequations) with $\mathcal{C}$-constraints is called a system of equations with *rational constraints*.
– $\mathcal{C} = Rat(\mathbb{M})$, i.e. the set of rational subsets of $\mathbb{M}$: In this case, in order to emphasize the fact that we do not use constraints that are complements of rational subsets, a system of equations (and disequations) with $\mathcal{C}$-constraints is called a system of equations (and disequations) with *positive* rational constraints.

The following proposition can be shown by standard techniques:

Proposition 2. *Assume that $\mathbb{M}$ is finitely generated. Let $(\mathcal{S}, \mathsf{C})$ be a system of equations and disequations over $\mathbb{M}$ with variables from $\mathcal{U}$ and rational constraints. From $(\mathcal{S}, \mathsf{C})$ we can compute a system $(\mathcal{S}', \mathsf{C}')$ of equations and disequations over $\mathbb{M}$ with variables from $\mathcal{U}'$ and rational constraints such that:*

– *$\mathcal{S}'$ is quadratic.*
– *$\mathcal{U} \subseteq \mathcal{U}'$*
– *The solutions of $(\mathcal{S}, \mathsf{C})$ are exactly the restrictions of the solutions of $(\mathcal{S}', \mathsf{C}')$ to $\mathcal{U}^*$*
– *If $\mathcal{S}$ is a system of equations (without disequations), then also $\mathcal{S}'$ is a system of equations (without disequations).*
– *If $(\mathcal{S}, \mathsf{C})$ is a system with* positive *rational constraints, then also $(\mathcal{S}', \mathsf{C}')$ is a system with* positive *rational constraints.*

One sometimes also considers systems of equations and disequations with a 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 has to respect the partial involution i.e. to map the variable u^{-1} onto the inverse of $\sigma_{\mathbb{M}}(u)$ (in particular, $\sigma_{\mathbb{M}}(u)$ has to be contained in the group of units of $\mathbb{M}$). Such a system "with partial involution" can be reduced to a system of the form above by adding the equations $uu^{-1} = 1$ and $u^{-1}u = 1$ to the system and removing the explicit constraint that $\sigma_{\mathbb{M}}$ respects some partial involution.

Let $\mathbb{M}$ be a monoid and let $\mathcal{C} \subseteq 2^{\mathbb{M}}$. We denote by $\mathrm{EQ}(\mathbb{M}, \mathcal{C})$ (resp., $\mathrm{DEQ}(\mathbb{M}, \mathcal{C})$) the set of all subsets of $\mathbb{M}$ which can be defined by a system of equations (resp., equations and disequations) with only one free variable (common to all equations), and with constants and constraints from $\mathcal{C}$.

We denote by $\mathrm{Def}_{\exists+}(\mathbb{M}, \mathcal{C})$ the set of all subsets of $\mathbb{M}$ which can be defined by a logical formula with only one free variable x_0, and having the form $\exists x_1 \exists x_2 \cdots \exists x_n \Psi$, where Ψ is a positive boolean combination of statements which are either equations with constants or of the form $x_i \in P$ (for some variable x_i, $0 \leq i \leq n$, and some $P \in \mathcal{C}$). The sets in $\mathrm{EQ}(\mathbb{M}, \mathcal{C})$ are called the *equational* subsets (with constraints in $\mathcal{C}$). The sets in $\mathrm{Def}_{\exists+}(\mathbb{M}, \mathcal{C})$ are called the *positively definable* subsets (with constraints in $\mathcal{C}$).

Lemma 19. *For every group* $\mathbb{H}$, $\mathsf{bool}(\mathrm{EQ}(\mathbb{H}, \mathsf{bool}(\mathsf{Rat}(\mathbb{H})))) \subseteq \mathrm{Def}_{\exists+}(\mathbb{H}, \mathsf{bool}(\mathsf{Rat}(\mathbb{H}))).$

In words: a boolean combination of equational subsets of $\mathbb{H}$ (with rational constraints) is positively definable (with rational contraints).

Proof. Every disequation $u \neq v$ in $\mathbb{H}$ can be translated into the formula

$$\exists v' \, \exists w : vv' = 1 \wedge uv' = w \wedge w \in \mathbb{H} \setminus \{1\}. \tag{51}$$

Hence, if P is defined by a positive boolean combination of equations and rational contraints, its complement is definable by a positive boolean combination of statements of the form (51) 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 $\mathrm{Def}_{\exists+}(\mathbb{H}, \mathsf{bool}(\mathsf{Rat}(\mathbb{H})))$. □

2.7 Reductions among decision problems

A Turing machine M *with oracle* L_2 is a Turing machine with a distinguished oracle tape and three distinguished states $q_?, q_y, q_n$ such that, when the current state of M is $q_?$, M makes a transition that does not move the tape heads, does not print anything, and enters the state q_y or the state q_n according to whether the word on the oracle tape belongs to L_2 or not (see, for example [HU79, Section 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 one knows both M and a machine M_2 that recognizes L_2, then one can combine them into a Turing machine M_1 that recognizes L_1. Let us consider three languages L_1, L_2, L_3. A Turing-reduction from L_1 to (L_2, L_3) is a Turing-reduction from L_1 to $(L_2 \times \{0\}) \cup (L_3 \times \{1\})$. 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 fulfiling the above definition of Turing-reducibility.

2.8 Submonoids and free products

The following lemma is straightforward.

Lemma 20. *If $\mathbb{M}$ is a finitely generated submonoid of the monoid $\mathbb{M}'$ and solvability of equations (and disequations) with rational constraints in $\mathbb{M}'$ is algorithmically solvable, then solvability of equations (and disequations) with rational constraints in $\mathbb{M}$ is algorithmically solvable.*

In [LS08, Section 6.1] we defined a notion of $(\mathbb{H}_1, \mathbb{H}_2)$-automata which is the direct adaptation of the notion of t-automaton to the operation of free product (possibly with amalgamation). 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).[3] Given two sets $\mathcal{C}_1 \subseteq 2^{\mathbb{H}_1}, \mathcal{C}_2 \subseteq 2^{\mathbb{H}_2}$, we denote by $\mathcal{L}(\mathcal{C}_1, \mathcal{C}_2)$ the set of subsets of $\mathrm{Red}(\mathbb{H}_1, \mathbb{H}_2)$ which are recognized by partitioned, $\approx$-compatible and finite $(\mathbb{H}_1, \mathbb{H}_2)$-automata with labelling set $(\mathcal{C}_1, \mathcal{C}_2)$. Informally, such an automaton $\mathcal{A}$ is a finite automaton over the alphabet $\mathcal{C}_1 \cup \mathcal{C}_2$ which has transitions labeled alternatively by elements of $\mathcal{C}_1$ and by elements of $\mathcal{C}_2$; $\approx$-compatibility means that, if it recognizes some $(\mathbb{H}_1, \mathbb{H}_2)$-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 $2^{\mathbb{H}_1} \cup 2^{\mathbb{H}_2}$.

Theorem 1. *Let us consider two monoids $\mathbb{H}_1, \mathbb{H}_2$. The satisfiability problem for systems of equations and disequations with constraints in $\mathsf{bool}(\mathcal{L}(\mathcal{C}_1, \mathcal{C}_2))$ over the free product $\mathbb{H}_1 * \mathbb{H}_2$ is Turing-reducible to the pair of problems (S_1, S_2) where*

- *S_1 is the satisfiability problem for systems of equations and disequations with constraints in $\mathsf{bool}(\mathcal{C}_1)$ and*
- *S_2 is the satisfiability problem for systems of equations and disequations with constraints in $\mathsf{bool}(\mathcal{C}_2)$.*

Note that when $\mathcal{C}_{\mathbb{H}_i} = \mathsf{Rat}(\mathbb{H}_i)$ (for $i \in \{1, 2\}$), then $\mathcal{L}(\mathcal{C}_{\mathbb{H}_1}, \mathcal{C}_{\mathbb{H}_2}) = \mathsf{Rat}(\mathbb{H}_1 * \mathbb{H}_2)$.

3 AB-algebras

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

3.1 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 let Q be some finite set (we have in mind the set of states of some normal fta $\mathcal{A}$ over $\mathbb{H} * \{t, t^{-1}\}^*$). Given a binary relation $r \in \mathsf{B}(\mathsf{Q}), r^{-1}$ is the binary relation $r^{-1} = \{(p, q) \in \mathsf{Q} \times \mathsf{Q} \mid (q, p) \in r\}$. We consider the involutory monoid anti-isomorphism $\mathbb{I}_{\mathsf{Q}} : \mathsf{B}^2(\mathsf{Q}) \to \mathsf{B}^2(\mathsf{Q})$ defined by

$$\forall r_1, r_2 \in \mathsf{B}(\mathsf{Q}) : \mathbb{I}_{\mathsf{Q}}(r_1, r_2) = (r_2^{-1}, r_1^{-1}).$$

[3] The original formulation of [DL03, Theorem 2] deals with the existential first order theory with rational constraints of a group $\mathbb{G} = \mathbb{H}_1 * \mathbb{H}_2$. But the decidability of this fragment is equivalent to the decidability of the satisfiability problem for systems of equations with rational constraints in $\mathbb{G}$.

An AB-algebra is a structure of the form

$$\langle \mathbb{M}, \iota_A, \iota_B, \mathbb{I}, \gamma, \mu, \delta \rangle, \tag{52}$$

where

- $\mathbb{M}$ is a monoid,
- $\iota_A : A \to \mathbb{M}, \iota_B : B \to \mathbb{M}$ are injective monoid homomorphisms,
- $\mathbb{I} : \mathbb{M} \to \mathbb{M}$ is a partial map,
- $\gamma : \mathbb{M} \to 2^{\mathcal{T}}$ is a total map,
- $\mu : \mathcal{T} \times \mathbb{M} \to \mathsf{B}^2(\mathsf{Q})$ is a partial map with $\mathrm{dom}(\mu) = \{(\boldsymbol{\theta}, m) \mid m \in \mathbb{M}, \boldsymbol{\theta} \in \gamma(m)\}$,
- $\delta : \mathcal{T} \times \mathbb{M} \to \mathrm{PGI}\{A, B\}$ is a partial map with $\mathrm{dom}(\delta) = \{(\boldsymbol{\theta}, m) \mid m \in \mathbb{M}, \boldsymbol{\theta} \in \gamma(m)\}$.

such that the following twelve axioms (AB1)–(AB12) are satisfied.

(AB1) $\mathrm{dom}(\mathbb{I}) = \mathrm{im}(\mathbb{I})$ is a submonoid of $\mathbb{M}$.

(AB2) $\mathbb{I}$ is an involutive anti-automorphism on $\mathrm{dom}(\mathbb{I})$.

(AB3) $\iota_A(A) \cup \iota_B(B) \subseteq \mathrm{dom}(\mathbb{I})$

(AB4) $\forall a \in A : \mathbb{I}(\iota_A(a)) = \iota_A(a^{-1}), \quad \forall b \in B : \mathbb{I}(\iota_B(b)) = \iota_B(b^{-1})$

For all $m, m_1, m_2 \in \mathbb{M}$:

(AB5) $m_1 m_2 \in \mathrm{dom}(\mathbb{I}) \;\Rightarrow\; m_1 \in \mathrm{dom}(\mathbb{I})$ and $m_2 \in \mathrm{dom}(\mathbb{I})$

(AB6) $\gamma(m_1)\gamma(m_2) \subseteq \gamma(m_1 m_2)$

(AB7) $\forall \boldsymbol{\theta} \in \gamma(m) : \delta(\boldsymbol{\theta}, m) \subseteq \mathrm{Gi}(\boldsymbol{\theta}) \times \mathrm{Ge}(\boldsymbol{\theta})$

(AB8) $\forall \boldsymbol{\theta}_1 \in \gamma(m_1), \boldsymbol{\theta}_2 \in \gamma(m_2) : \boldsymbol{\theta}_1\boldsymbol{\theta}_2$ defined $\;\Rightarrow\; \mu(\boldsymbol{\theta}_1\boldsymbol{\theta}_2, m_1 m_2) = \mu(\boldsymbol{\theta}_1, m_1) \circ \mu(\boldsymbol{\theta}_2, m_2)$

(AB9) $\forall \boldsymbol{\theta}_1 \in \gamma(m_1), \boldsymbol{\theta}_2 \in \gamma(m_2) : \boldsymbol{\theta}_1\boldsymbol{\theta}_2$ defined $\;\Rightarrow\; \delta(\boldsymbol{\theta}_1\boldsymbol{\theta}_2, m_1 m_2) = \delta(\boldsymbol{\theta}_1, m_1) \circ \delta(\boldsymbol{\theta}_2, m_2)$

(AB10) $m \in \mathrm{dom}(\mathbb{I}) \;\Rightarrow\; \gamma(\mathbb{I}(m)) = \mathbb{I}_{\mathcal{T}}(\gamma(m))$

(AB11) $m \in \mathrm{dom}(\mathbb{I}) \;\Rightarrow\; \forall \boldsymbol{\theta} \in \gamma(m) : \mu(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}), \mathbb{I}(m)) = \mathbb{I}_{\mathsf{Q}}(\mu(\boldsymbol{\theta}, m))$

(AB12) $m \in \mathrm{dom}(\mathbb{I}) \;\Rightarrow\; \forall \boldsymbol{\theta} \in \gamma(m) : \delta(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}), \mathbb{I}(m)) = \delta(\boldsymbol{\theta}, m)^{-1}$

Quite often, we will identify an AB-algebra with its underlying monoid. In Section 3.4 we will show that the monoid $\mathbb{H}_t$ from (6) gives rise to an AB-algebra, which will be one of the main objects studied in this work.

3.2 AB-homomorphisms

For $i \in \{1, 2\}$ let $\mathcal{M}_i = \langle \mathbb{M}_i, \iota_{A,i}, \iota_{B,i}, \mathbb{I}_i, \gamma_i, \mu_i, \delta_i \rangle$ be an AB-algebra with the underlying groups A, B and set Q. An AB-homomorphism from $\mathcal{M}_1$ to $\mathcal{M}_2$ is a map $\psi : \mathbb{M}_1 \to \mathbb{M}_2$ fulfilling the following seven properties (Hom1)–(Hom7):

(Hom1) $\psi : \mathbb{M}_1 \to \mathbb{M}_2$ is a monoid homomorphism.

(Hom2) $\forall a \in A : \psi(\iota_{A,1}(a)) = \iota_{A,2}(a), \; \forall b \in B : \psi(\iota_{B,1}(b)) = \iota_{B,2}(b)$

(Hom3) $\forall m \in \mathbb{M}_1 : m \in \mathrm{dom}(\mathbb{I}_1) \Leftrightarrow \psi(m) \in \mathrm{dom}(\mathbb{I}_2)$

(Hom4) $\forall m \in \mathrm{dom}(\mathbb{I}_1) : \mathbb{I}_2(\psi(m)) = \psi(\mathbb{I}_1(m))$

(Hom5) $\forall m \in \mathbb{M}_1 : \gamma_1(m) \subseteq \gamma_2(\psi(m))$

(Hom6) $\forall m \in \mathbb{M}_1 : \forall \boldsymbol{\theta} \in \gamma_1(m) : \mu_2(\boldsymbol{\theta}, \psi(m)) = \mu_1(\boldsymbol{\theta}, m)$

(Hom7) $\forall m \in \mathbb{M}_1 : \forall \boldsymbol{\theta} \in \gamma_1(m) : \delta_2(\boldsymbol{\theta}, \psi(m)) = \delta_1(\boldsymbol{\theta}, m)$

With $\mathrm{Hom}_{AB}(\mathcal{M}_1, \mathcal{M}_2)$ we denote the set of all AB-homomorphisms from $\mathcal{M}_1$ to $\mathcal{M}_2$. The following lemma is easy and widely (though implicitely) used.

Lemma 21. *Let $\mathcal{M}_1, \mathcal{M}_2$, and $\mathcal{M}_3$ be AB-algebras and let $\psi_1 \in \mathrm{Hom}_{AB}(\mathcal{M}_1, \mathcal{M}_2), \psi_2 \in \mathrm{Hom}_{AB}(\mathcal{M}_2, \mathcal{M}_3)$. Then $\psi_1 \circ \psi_2 : \mathcal{M}_1 \to \mathcal{M}_3$ is an AB-homomorphism.*

Lemma 22. *Let $\mathcal{M}_1$, $\mathcal{M}_2$, and $\mathcal{M}_3$ be AB-algebras and let $\pi \in \mathrm{Hom}_{AB}(\mathcal{M}_1, \mathcal{M}_2)$, $\psi' \in \mathrm{Hom}_{AB}(\mathcal{M}_1, \mathcal{M}_3)$ such that*

(a) π is surjective, and
(b) $\gamma_1(k) = \gamma_2(\pi(k))$ for all $k \in \mathbb{M}_1$ (this strengthens (Hom5) for π).

If $\psi : \mathbb{M}_2 \to \mathbb{M}_3$ is a monoid homomorphism with $\psi' = \pi \circ \psi$, then $\psi \in \mathrm{Hom}_{AB}(\mathcal{M}_2, \mathcal{M}_3)$.

Proof. We have to check properties (Hom2)–(Hom7) for ψ.

(Hom2): For all $a \in A$ we have

$$\psi(\iota_{A,2}(a)) = \psi(\pi(\iota_{A,1}(a))) = \psi'(\iota_{A,1}(a)) = \iota_{A,3}(a).$$

For B the same argument holds.

For the following properties let $m \in \mathbb{M}_2$ be arbitrary. Since π is surjective, there exists $k \in \mathbb{M}_1$ with $\pi(k) = m$.

(Hom3): We get:

$$\begin{aligned}
\psi(m) \in \mathrm{dom}(\mathbb{I}_3) &\iff \psi(\pi(k)) \in \mathrm{dom}(\mathbb{I}_3) \\
&\iff \psi'(k) \in \mathrm{dom}(\mathbb{I}_3) \\
&\iff k \in \mathrm{dom}(\mathbb{I}_1) && (\text{(Hom3) for } \psi') \\
&\iff \pi(k) \in \mathrm{dom}(\mathbb{I}_2) && (\text{(Hom3) for } \pi) \\
&\iff m \in \mathrm{dom}(\mathbb{I}_2)
\end{aligned}$$

(Hom4): Assume that $m = \pi(k) \in \mathrm{dom}(\mathbb{I}_2)$. By (Hom3) for π we have $k \in \mathrm{dom}(\mathbb{I}_1)$. Thus, with (Hom4) for π and ψ' we get:

$$\psi(\mathbb{I}_2(m)) = \psi(\mathbb{I}_2(\pi(k))) = \psi(\pi(\mathbb{I}_1(k))) = \psi'(\mathbb{I}_1(k)) = \mathbb{I}_3(\psi'(k)) = \mathbb{I}_3(\psi(\pi(k))) = \mathbb{I}_3(\psi(m)).$$

(Hom5): With assumption (b) from the lemma and (Hom5) for ψ', we get:

$$\gamma_2(m) = \gamma_2(\pi(k)) = \gamma_1(k) \subseteq \gamma_3(\psi'(k)) = \gamma_3(\psi(\pi(k))) = \gamma_3(\psi(m)).$$

(Hom6): Let $\boldsymbol{\theta} \in \gamma_2(m) = \gamma_1(k)$. With (Hom6) for π and ψ' we get:

$$\mu_2(\boldsymbol{\theta}, m) = \mu_2(\boldsymbol{\theta}, \pi(k)) = \mu_1(\boldsymbol{\theta}, k) = \mu_2(\boldsymbol{\theta}, \psi'(k)) = \mu_2(\boldsymbol{\theta}, \psi(\pi(k))) = \mu_2(\boldsymbol{\theta}, \psi(m)).$$

(Hom7) for ψ can be verified with a similar calculation as for (Hom6). □

Later, it will be convenient to check the conditions for an AB-homomorphism only on generators. The following lemma gives conditions under which this is possible.

Lemma 23. *Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be AB-algebras as above and assume that $\mathcal{M}_1$ satisfies the following:*

(A) The monoid $\mathbb{M}_1$ is generated by the set Γ and $A \cup B \subseteq \Gamma$
(B) $\gamma_1(g) \neq \emptyset$ for all $g \in \Gamma$
(C) For every $m \in \mathbb{M}_1$ there exists a decomposition $m = g_1 \cdots g_n$ with $g_1, \ldots, g_n \in \Gamma$ such that: $\gamma_1(m) = \gamma_1(g_1) \cdots \gamma_1(g_n)$.[4]

Let $\psi : \mathbb{M}_1 \to \mathbb{M}_2$ be a monoid homomorphism. Then $\psi \in \mathrm{Hom}_{AB}(\mathcal{M}_1, \mathcal{M}_2)$ if and only if for every $g \in \Gamma$ and $\boldsymbol{\theta} \in \gamma_1(g)$ we have:

(a) $\forall a \in A : \psi(\iota_{A,1}(a) = \iota_{A_2}(a)$ and $\forall b \in B : \psi(\iota_{B,1}(b) = \iota_{B,2}(b)$
(b) $g \in \mathrm{dom}(\mathbb{I}_1) \Leftrightarrow \psi(g) \in \mathrm{dom}(\mathbb{I}_2)$
(c) If $g \in \mathrm{dom}(\mathbb{I}_1)$ then $\mathbb{I}_2(\psi(g)) = \psi(\mathbb{I}_1(g))$
(d) $\gamma_1(g) \subseteq \gamma_2(\psi(g))$
(e) $\mu_2(\boldsymbol{\theta}, \psi(g)) = \mu_1(\boldsymbol{\theta}, g)$
(f) $\delta_2(\boldsymbol{\theta}, \psi(g)) = \delta_1(\boldsymbol{\theta}, g)$

Proof. First, suppose that ψ is an AB-homomorphism. By definition it must fulfilll conditions (Hom2)–(Hom7). These six axioms imply the six conditions (a)-(f).

Conversely, let us suppose that ψ fulfills conditions (a)–(f) of the lemma. By (a), condition (Hom2) is fulfilled. For the following points consider an element $m \in \mathbb{M}_1$ and choose a decomposition

$$m = g_1 g_2 \cdots g_n \tag{53}$$

that satisfies (C) from the lemma ($g_1, \ldots, g_n \in \Gamma$).

Extending (b) to $\mathbb{M}_1$. Suppose that

$$m \in \mathrm{dom}(\mathbb{I}_1). \tag{54}$$

Axiom (AB5) of AB-algebras (which can be easily extended to products of arbitrary length), together with (54), imply

$$g_i \in \mathrm{dom}(\mathbb{I}_1) \text{ for all } 1 \leq i \leq n. \tag{55}$$

By condition (b) of the lemma, (55) implies

$$\psi(g_i) \in \mathrm{dom}(\mathbb{I}_2) \text{ for all } 1 \leq i \leq n. \tag{56}$$

Since $\mathrm{dom}(\mathbb{I}_2)$ is by axiom (AB1) a submonoid of $\mathbb{M}_2$, we get

$$\psi(g_1) \cdots \psi(g_n) \in \mathrm{dom}(\mathbb{I}_2). \tag{57}$$

But ψ is a monoid homomorphism, hence

$$\psi(m) = \psi(g_1) \cdots \psi(g_n) \in \mathrm{dom}(\mathbb{I}_2). \tag{58}$$

We have proved that (54) implies (58).

[4] If $n = 0$, i.e., $m = 1$, then $\gamma_1(g_1) \cdots \gamma_1(g_n)$ is the neutral element $\{(\theta, 0, \theta) \mid \theta \in \mathcal{T}_6\}$ of the monoid $2^{\mathcal{T}}$.

Let us now establish the converse. Assume that $\psi(m) \in \mathrm{dom}(\mathbb{I}_2)$. We thus have:

$$\psi(m) = \psi(g_1) \cdots \psi(g_n) \in \mathrm{dom}(\mathbb{I}_2).$$

Using axiom (AB5) we get $\psi(g_i) \in \mathrm{dom}(\mathbb{I}_2)$ for all $1 \leq i \leq n$. Hence, (b) from the lemma implies $g_i \in \mathrm{dom}(\mathbb{I}_1)$ for all $1 \leq i \leq n$. Since $\mathrm{dom}(\mathbb{I}_1)$ is a submonoid of $\mathbb{M}_1$, we finally get $m = g_1 \cdots g_n \in \mathrm{dom}(\mathbb{I}_1)$.

Extending (c) to $\mathbb{M}_1$. Assume that $m \in \mathrm{dom}(\mathbb{I}_1)$. By Axion (AB5) we have $g_1, \ldots, g_n \in \mathrm{dom}(\mathbb{I}_1)$. We obtain

$$\begin{aligned}
\mathbb{I}_2(\psi(m)) &= \mathbb{I}_2(\psi(g_1) \cdots \psi(g_m)) && (\psi \text{ is a monoid homomorphism}) \\
&= \mathbb{I}_2(\psi(g_m)) \cdots \mathbb{I}_2(\psi(g_1)) && (\mathbb{I}_2 \text{ is a monoid anti-automorphism}) \\
&= \psi(\mathbb{I}_1(g_m)) \cdots \psi(\mathbb{I}_1(g_1)) && (\text{condition (c) from the lemma}) \\
&= \psi(\mathbb{I}_1(g_m) \cdots \mathbb{I}_1(g_1)) && (\psi \text{ is a monoid homomorphism}) \\
&= \psi(\mathbb{I}_1(m)) && (\mathbb{I}_1 \text{ is a monoid anti-automorphism})
\end{aligned}$$

Extending (d) to $\mathbb{M}_1$. For $m = g_1 \cdots g_n$ we obtain

$$\begin{aligned}
\gamma_1(g_1 \cdots g_n) &= \gamma_1(g_1) \cdots \gamma_1(g_n) && (\text{(C) from the lemma}) \\
&\subseteq \gamma_2(\psi(g_1)) \cdots \gamma_2(\psi(g_n)) && (\text{condition (d) from the lemma}) \\
&\subseteq \gamma_2(\psi(g_1) \cdots \psi(g_n)) && (\text{axiom (AB6) for } \mathcal{M}_2) \\
&= \gamma_2(\psi(g_1 \cdots g_n)) && (\psi \text{ is a monoid homomorphism})
\end{aligned}$$

Extending (e) to $\mathbb{M}_1$. Assume that $\boldsymbol{\theta} \in \gamma_1(m) = \gamma_1(g_1) \cdots \gamma_1(g_n)$. Hence, the path type $\boldsymbol{\theta}$ must have the form

$$\boldsymbol{\theta} = \boldsymbol{\theta}_1 \cdots \boldsymbol{\theta}_n \text{ with } \boldsymbol{\theta}_i \in \gamma_1(g_i) \subseteq \gamma_2(\psi(g_i)) \text{ for } 1 \leq i \leq n. \tag{59}$$

We obtain

$$\begin{aligned}
\mu_2(\boldsymbol{\theta}, \psi(m)) &= \mu_2(\prod_{i=1} \boldsymbol{\theta}_i, \prod_{i=1}^{n} \psi(g_i)) && (\psi \text{ is a monoid homomorphism}) \\
&= \prod_{i=1}^{n} \mu_2(\boldsymbol{\theta}_i, \psi(g_i)) && (\text{axiom (AB8) for } \mathcal{M}_2) \\
&= \prod_{i=1}^{n} \mu_1(\boldsymbol{\theta}_i, g_i) && (\text{condition (e) from the lemma}) \\
&= \mu_1(\boldsymbol{\theta}, m) && (\text{axiom (AB8) for } \mathcal{M}_1)
\end{aligned}$$

as required.

Extending (f) to $\mathbb{M}_1$. A similar calculation as for (e) (using axiom (AB9) instead of axiom (AB8)) holds. □

3.3 AB-subalgebras and quotients

For $i \in \{1,2\}$ let $\mathcal{M}_i = \langle \mathbb{M}_i, \iota_{A,i}, \iota_{B,i}, \mathbb{I}_i, \gamma_i, \mu_i, \delta_i \rangle$ be an AB-algebra with the underlying groups A, B and set Q. Then, $\mathcal{M}_1$ is said to be an *AB-subalgebra* of $\mathcal{M}_2$ if $\mathbb{M}_1 \subseteq \mathbb{M}_2$ and $\iota_{A,1} = \iota_{A,2}$, $\iota_{B,1} = \iota_{B,2}$, $\mathbb{I}_1 = \mathbb{I}_2 \restriction \mathbb{M}_1$, $\gamma_1 = \gamma_2 \restriction \mathbb{M}_1$, $\mu_1 = \mu_2 \restriction \mathcal{T} \times \mathbb{M}_1$, and $\delta_1 = \delta_2 \restriction \mathcal{T} \times \mathbb{M}_1$. (In particular, the inclusion map $\iota : \mathbb{M}_1 \to \mathbb{M}_2$ is an AB-homomorphism). Vice versa, if $\mathbb{M}_1$ is a submonoid of $\mathbb{M}_2$ which contains $\iota_{A,2}(A) \cup \iota_{B,2}(B)$ and which is closed under $\mathbb{I}_2$, then there is a natural way to endow $\mathbb{M}_1$ with the structure of an AB-subalgebra of $\mathcal{M}_2$: it suffices to set $\iota_{A,1} = \iota_{A,2}$, $\iota_{B,1} = \iota_{B,2}$, $\mathbb{I}_1 = \mathbb{I}_2 \restriction \mathbb{M}_1$, $\gamma_1 = \gamma_2 \restriction \mathbb{M}_1$, $\mu_1 = \mu_2 \restriction (\mathcal{T} \times \mathbb{M}_1)$, and $\delta_1 = \delta_2 \restriction (\mathcal{T} \times \mathbb{M}_1)$. This structure is called the AB-structure *induced* by $\mathcal{M}_2$ on $\mathbb{M}_1$.

Definition 6. *Let $\equiv$ be a monoid congruence on the monoid $\mathbb{M}$ and $\mathcal{M} = \langle \mathbb{M}, \iota_A, \iota_B, \mathbb{I}, \gamma, \mu, \delta \rangle$ be an AB-algebra. We say that $\equiv$ is* compatible *w.r.t. the AB-algebra $\mathcal{M}$, if the following holds for all $m, m' \in \mathbb{M}$ with $m \equiv m'$ and all $a, a' \in A$ and $b, b' \in B$:*

(a) $m \in \mathrm{dom}(\mathbb{I}) \iff m' \in \mathrm{dom}(\mathbb{I})$ and if $m, m' \in \mathrm{dom}(\mathbb{I})$ then $\mathbb{I}(m) \equiv \mathbb{I}(m')$,
(b) $\iota_A(a) \equiv \iota_A(a') \Longrightarrow a = a'$ and $\iota_B(b) \equiv \iota_B(b') \Longrightarrow b = b'$
(c) $\gamma(m) = \gamma(m')$
(d) For all $\boldsymbol{\theta} \in \gamma(m)$: $\mu(\boldsymbol{\theta}, m) = \mu(\boldsymbol{\theta}, m')$ and $\delta(\boldsymbol{\theta}, m) = \delta(\boldsymbol{\theta}, m')$.

By (a), $\equiv$ is also a congruence on $\mathrm{dom}(\mathbb{I})$, i.e. we can consider the quotient monoid $\mathrm{dom}(\mathbb{I})/_{\equiv} \subseteq \mathbb{M}/_{\equiv}$. By (a), (c), and (d), the mappings $\mathbb{I}$, γ, μ, and δ induce quotient mappings (we use the same symbols for these quotient mappings)

$$\begin{aligned} \mathbb{I} : \mathrm{dom}(\mathbb{I})/_{\equiv} &\to \mathrm{dom}(\mathbb{I})/_{\equiv} \\ \gamma : \mathbb{M}/_{\equiv} &\to 2^{\mathcal{T}} \\ \mu : \mathcal{T} \times \mathbb{M}/_{\equiv} &\to \mathsf{B}^2(\mathsf{Q}) \\ \delta : \mathcal{T} \times \mathbb{M}/_{\equiv} &\to \mathrm{PGI}\{A, B\}. \end{aligned}$$

Moreover, by (b), ι_A and ι_B can be viewed as embeddings of A and B, respectively, into $\mathbb{M}/_{\equiv}$. It is now easy to check that

$$\mathcal{M}/_{\equiv} \;=\; \langle \mathbb{M}/_{\equiv}, \iota_A, \iota_B, \mathbb{I}, \gamma, \mu, \delta \rangle$$

is again an AB-algebra; it is called the quotient of $\mathcal{M}$ w.r.t. $\equiv$. Moreover, the projection morphism $\pi_{\equiv}$ with $\pi_{\equiv}(m) = [m]_{\equiv}$ becomes a surjective AB-homomorphism $\pi_{\equiv} : \mathcal{M} \to \mathcal{M}/_{\equiv}$ such that moreover for all $m \in \mathbb{M}$:

$$\gamma(m) = \gamma(\pi_{\equiv}(m)) \tag{60}$$

Hence, with Lemma 22 we get:

Lemma 24. *Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be AB-algebras with underlying monoids $\mathbb{M}_1$ and $\mathbb{M}_2$, respectively. Let the monoid congruence $\equiv$ on $\mathbb{M}_1$ be compatible w.r.t. $\mathcal{M}_1$. Let $\psi' \in \mathrm{Hom}_{AB}(\mathcal{M}_1, \mathcal{M}_2)$. If $\psi : \mathbb{M}_1/_{\equiv} \to \mathbb{M}_2$ is a monoid homomorphism with $\psi' = \pi_{\equiv} \circ \psi$, then $\psi \in \mathrm{Hom}_{AB}(\mathcal{M}_1/_{\equiv}, \mathcal{M}_2)$.*

Also the next lemma can be easily verified.

Lemma 25. *Let $\mathcal{M}$ be an AB-algebra with underlying monoid $\mathbb{M}$, and let the monoid congruence $\equiv$ on $\mathbb{M}$ be compatible w.r.t. $\mathcal{M}$. If $\mathcal{M}$ fulfills hypotheses (A), (B), and (C) of Lemma 23 for the set of generators Γ, then $\mathcal{M}/_{\equiv}$ fulfills (A), (B), and (C) for the set of generators $\pi_{\equiv}(\Gamma)$ of $\mathbb{M}/_{\equiv}$.*

3.4 The AB-algebra $\mathbb{H}_t$

From now on, we assume that $\mathbb{H}$ is a *cancellative monoid* with subgroups A and B. In this section, we will define an AB-algebra with the underlying monoid $\mathbb{H}_t$ from (6). This AB-algebra will be denoted by $\mathbb{H}_t$ as well. In a first step, we extend the monoid $\mathbb{H} * \{t, t^{-1}\}^*$ to an AB-algebra that we denote with $\mathbb{H} * \{t, t^{-1}\}^*$ again. The AB-algebra $\mathbb{H}_t$ will be a quotient of $\mathbb{H} * \{t, t^{-1}\}^*$.

Recall the definition of a normal partitioned fta from Definition 5. Given an HNN-extension (1) and a normal fta $\mathcal{A}$ with state set Q, we define an AB-algebra

$$\langle \mathbb{H} * \{t, t^{-1}\}^*, \iota_A, \iota_B, \mathbb{I}_t, \gamma_t, \mu_t, \delta_t \rangle \tag{61}$$

with underlying monoid $\mathbb{H} * \{t, t^{-1}\}^*$ and set of states Q as follows:

- ι_A and ι_B are the natural injections from A (resp. B) into $\mathbb{H} * \{t, t^{-1}\}^*$.
- $\mathrm{dom}(\mathbb{I}_t) = \mathsf{I}(\mathbb{H}) * \{t, t^{-1}\}^*$, where $\mathsf{I}(\mathbb{H})$ is the subgroup of invertible elements of $\mathbb{H}$.
- $\mathbb{I}_t$ is the unique involutive anti-isomorphism $\mathbb{I}_t : \mathrm{dom}(\mathbb{I}_t) \to \mathrm{dom}(\mathbb{I}_t)$ such that

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

- The map γ_t is the one previously defined in (34).
- The map $\mu_t : \mathcal{T} \times \mathbb{H} * \{t, t^{-1}\}^* \to \mathsf{B}^2(\mathsf{Q})$ is defined by:

$$\mu_t(\boldsymbol{\theta}, s) = \begin{cases} \langle \mu_1(\boldsymbol{\theta}, s), \mu_1(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}), \mathbb{I}_t(s))^{-1} \rangle & \text{if } s \in \mathrm{dom}(\mathbb{I}_t) \\ \langle \mu_1(\boldsymbol{\theta}, s), \emptyset \rangle & \text{if } s \notin \mathrm{dom}(\mathbb{I}_t). \end{cases} \tag{62}$$

  Here, μ_1 is the representation map $\mu_{\mathcal{A},1}$ associated with the partitioned fta $\mathcal{A}$ fixed above, see (32).
- The map $\delta_t : \mathcal{T} \times \mathbb{H} * \{t, t^{-1}\}^* \to \mathrm{PGI}\{A, B\}$ is defined by:

$$\delta_t(\boldsymbol{\theta}, s) = \{(c, c') \in \mathrm{Gi}(\boldsymbol{\theta}) \times \mathrm{Ge}(\boldsymbol{\theta}) \mid cs \sim sc'\}, \tag{63}$$

where $\sim$ is the congruence on $\mathbb{H} * \{t, t^{-1}\}^*$ from Definition 1. Note that $\delta_t(\boldsymbol{\theta}, s)$ is indeed a partial isomorphism from $\mathrm{PGI}\{A, B\}$: It is a partial injection, since the quotient $\mathbb{H}_t = \mathbb{H} * \{t, t^{-1}\}^*/_\sim$ is cancellative (Lemma 6). Moreover, if $c_1 s \sim s c_1'$ and $c_2 s \sim s c_2'$, then $(c_1 c_2)s \sim c_1 s c_2' \sim s(c_1' c_2')$.

It is noteworthy that for every $s \in \mathbb{H} * \{t, t^{-1}\}^*$:

$$\gamma_t(s) \neq \emptyset \iff s \in \mathrm{Red}(\mathbb{H}, t). \tag{64}$$

Before we show that $\langle \mathbb{H} * \{t, t^{-1}\}^*, \iota_A, \iota_B, \mathbb{I}_t, \mu_t, \gamma_t, \delta_t \rangle$ is indeed an AB-algebra, let us prove the following lemma:

Lemma 26. *Let $s_1, s_2 \in \mathbb{H} * \{t, t^{-1}\}^*$, $\boldsymbol{\theta}_1 \in \gamma_+(s_1)$, $\boldsymbol{\theta}_2 \in \gamma_+(s_2)$, $\boldsymbol{\theta}_1\boldsymbol{\theta}_2$ defined. Assume that $(c, c') \in \mathrm{Gi}(\boldsymbol{\theta}_1\boldsymbol{\theta}_2) \times \mathrm{Ge}(\boldsymbol{\theta}_1\boldsymbol{\theta}_2) = \mathrm{Gi}(\boldsymbol{\theta}_1) \times \mathrm{Ge}(\boldsymbol{\theta}_2)$ and $cs_1s_2 \sim s_1s_2c'$. Then there exists $c'' \in \mathrm{Ge}(\boldsymbol{\theta}_1) = \mathrm{Gi}(\boldsymbol{\theta}_2)$ such that $cs_1 \sim s_1c''$ and $c''s_2 \sim s_2c'$.*

Proof. Assume that $s_1 = h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_n} h_n$ and $s_2 = k_0 t^{\beta_1} k_1 \cdots t^{\beta_m} k_m$.

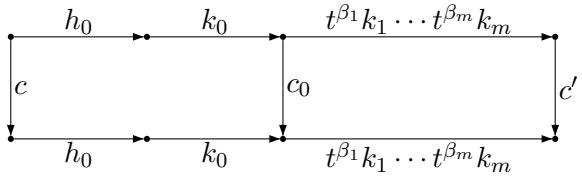
Case 1. $n = m = 0$: Thus, $ch_0k_0 = h_0k_0c'$. Since $\boldsymbol{\theta}_1\boldsymbol{\theta}_2$ is defined, Lemma 10 implies that (i) $\tau\mathrm{i}(\boldsymbol{\theta}_1) = \tau\mathrm{e}(\boldsymbol{\theta}_1)$ and $s_1 = h_0 \in \mathrm{Gi}(\boldsymbol{\theta}_1) = \mathrm{Ge}(\boldsymbol{\theta}_1) = \mathrm{Gi}(\boldsymbol{\theta}_2)$ or (ii) $\tau\mathrm{i}(\boldsymbol{\theta}_2) = \tau\mathrm{e}(\boldsymbol{\theta}_2)$ and

$s_2 = k_0 \in \mathrm{Ge}(\boldsymbol{\theta}_1) = \mathrm{Gi}(\boldsymbol{\theta}_2) = \mathrm{Ge}(\boldsymbol{\theta}_2)$. In case (i) we can set $c'' = h_0^{-1}ch_0 \in \mathrm{Ge}(\boldsymbol{\theta}_1)$. In case (ii) we set $c'' = k_0c'k_0^{-1} \in \mathrm{Ge}(\boldsymbol{\theta}_1)$.

Case 2. $n = 0$ and $m > 0$. Thus,

$$(ch_0k_0)t^{\beta_1}k_1 \cdots t^{\beta_m}k_m \sim (h_0k_0)t^{\beta_1}k_1 \cdots t^{\beta_m}(k_mc').$$

We obtain a van Kampen diagram of the form



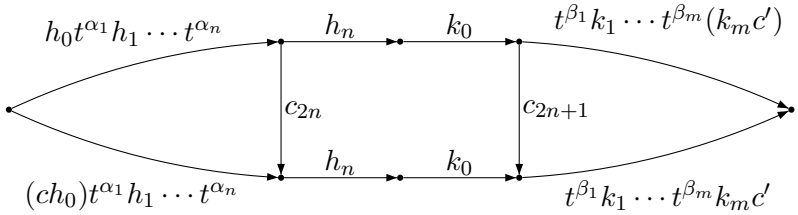
where $c_0 \in A(\beta_1)$. Note that $ch_0 = h_0k_0c_0k_0^{-1}$. As in case 1, since $\boldsymbol{\theta}_1\boldsymbol{\theta}_2$ is defined, Lemma 10 implies that (i) $\tau\mathrm{i}(\boldsymbol{\theta}_1) = \tau\mathrm{e}(\boldsymbol{\theta}_1)$ and $s_1 = h_0 \in \mathrm{Gi}(\boldsymbol{\theta}_1) = \mathrm{Ge}(\boldsymbol{\theta}_1) = \mathrm{Gi}(\boldsymbol{\theta}_2)$ or (ii) $k_0 \in \mathrm{Ge}(\boldsymbol{\theta}_1) = \mathrm{Gi}(\boldsymbol{\theta}_2) = A(\beta_1)$. In case (i) we can set $c'' = h_0^{-1}ch_0 \in \mathrm{Ge}(\boldsymbol{\theta}_1)$; in case (ii) we set $c'' = k_0c_0k_0^{-1} \in \mathrm{Ge}(\boldsymbol{\theta}_1)$.

Case 3. $n > 0$ and $m = 0$. This case can be dealt analogously to case 2.

Case 4. $n, m > 0$. Hence, we have

$$h_0t^{\alpha_1}h_1 \cdots t^{\alpha_n}(h_nk_0)t^{\beta_1}k_1 \cdots t^{\beta_m}(k_mc') = (ch_0)t^{\alpha_1}h_1 \cdots t^{\alpha_n}(h_nk_0)t^{\beta_1}k_1 \cdots t^{\beta_m}k_m.$$

We obtain a van Kampen diagram of the form



where $c_{2n} \in B(\alpha_n)$ and $c_{2n+1} \in A(\beta_1)$. Again, with Lemma 10 we get (i) $h_n, c_{2n} \in B(\alpha_n) = \mathrm{Ge}(\boldsymbol{\theta}_1) = \mathrm{Gi}(\boldsymbol{\theta}_2)$ or (ii) $k_0, c_{2n+1} \in A(\beta_1) = \mathrm{Ge}(\boldsymbol{\theta}_1) = \mathrm{Gi}(\boldsymbol{\theta}_2)$. In case (i) we set $c'' = h_n^{-1}c_{2n}h_n$; in case (ii) we set $c'' = k_0c_{2n+1}k_0^{-1}$. □

Proposition 3. *The structure* $\langle \mathbb{H} * \{t, t^{-1}\}^*, \iota_A, \iota_B, \mathbb{I}_t, \mu_t, \gamma_t, \delta_t\rangle$ *is an AB-algebra.*

Proof. We check the properties (AB1)–(AB12). Properties (AB1)–(AB4) are obvious.

(AB5): Assume that $s_1s_2 \in \mathrm{dom}(\mathbb{I})$. Let $s_1 = h_0t^{\alpha_1}h_1 \cdots t^{\alpha_n}h_n$ and $s' = h'_0t^{\alpha'_1}h'_1 \cdots t^{\alpha'_m}h'_m$. Thus

$$s_1s_2 = h_0t^{\alpha_1}h_1 \cdots t^{\alpha_n}(h_nh'_0)t^{\alpha'_1}h'_1 \cdots t^{\alpha'_m}h'_m \in \mathrm{dom}(\mathbb{I})$$

Hence, $h_0, \ldots, h_{n-1}, h_nh'_0, h'_1, \ldots, h'_m$ are invertible elements of $\mathbb{H}$. Since $\mathbb{H}$ is cancellative, by Lemma 4, $h_nh'_0 \in \mathsf{I}(\mathbb{H})$ implies that $h_n, h'_0 \in \mathsf{I}(\mathbb{H})$. It follows that $s_1 \in \mathrm{dom}(\mathbb{I})$ and $s_2 \in \mathrm{dom}(\mathbb{I})$.

(AB6): This is stated in Lemma 18.

(AB7): Follows directly from the definition of δ_t.

(AB10): Note that by (36), it suffices to show $\gamma_t(\mathbb{I}_t(s)) = \mathbb{I}_{\mathcal{T}}(\gamma_t(s))$ only for 1 and all generators $s \in \mathsf{I}(\mathbb{H}) \cup \{t, t^{-1}\}$ of $\mathrm{dom}(\mathbb{I}_t)$. This follows easily from the definition of $\mathbb{I}_{\mathcal{T}}$ in (18).

(AB8): Let $\boldsymbol{\theta}_1 \in \gamma_t(s_1)$ and $\boldsymbol{\theta}_2 \in \gamma_t(s_2)$ such that $\boldsymbol{\theta}_1\boldsymbol{\theta}_2$ is defined. First assume that $s_1 s_2 \in \mathrm{dom}(\mathbb{I}_t)$. Then, by (AB5), also $s_1, s_2 \in \mathrm{dom}(\mathbb{I}_t)$. Moreover, by (AB10), $\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}_1) \in \mathbb{I}_{\mathcal{T}}(\gamma_t(s_1)) = \gamma_t(\mathbb{I}_t(s_1))$ and $\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}_2) \in \gamma_t(\mathbb{I}_t(s_2))$. Since the fta $\mathcal{A}$ is normal and therefore multiplicative (see Definition 4), we obtain:

$$\begin{aligned}
\mu_t(\boldsymbol{\theta}_1\boldsymbol{\theta}_2, s_1 s_2) &= \langle \mu_1(\boldsymbol{\theta}_1\boldsymbol{\theta}_2, s_1 s_2), \mu_1(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}_1\boldsymbol{\theta}_2), \mathbb{I}_t(s_1 s_2))^{-1} \rangle \\
&= \langle \mu_1(\boldsymbol{\theta}_1\boldsymbol{\theta}_2, s_1 s_2), \mu_1(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}_2)\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}_1), \mathbb{I}_t(s_2)\mathbb{I}_t(s_1))^{-1} \rangle \\
&= \langle \mu_1(\boldsymbol{\theta}_1, s_1) \circ \mu_1(\boldsymbol{\theta}_2, s_2), (\mu_1(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}_2), \mathbb{I}_t(s_2)) \circ \mu_1(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}_1), \mathbb{I}_t(s_1)))^{-1} \rangle \\
&= \langle \mu_1(\boldsymbol{\theta}_1, s_1) \circ \mu_1(\boldsymbol{\theta}_2, s_2), \mu_1(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}_1), \mathbb{I}_t(s_1))^{-1} \circ \mu_1(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}_2), \mathbb{I}_t(s_2))^{-1} \rangle \\
&= \langle \mu_1(\boldsymbol{\theta}_1, s_1), \mu_1(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}_1), \mathbb{I}_t(s_1))^{-1} \rangle \circ \langle \mu_1(\boldsymbol{\theta}_2, s_2), \mu_1(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}_2), \mathbb{I}_t(s_2))^{-1} \rangle \\
&= \mu_t(\boldsymbol{\theta}_1, s_1) \circ \mu_t(\boldsymbol{\theta}_2, s_2)
\end{aligned}$$

On the other hand, if $s_1 s_2 \notin \mathrm{dom}(\mathbb{I}_t)$, then either $s_1 \notin \mathrm{dom}(\mathbb{I}_t)$ or $s_2 \notin \mathrm{dom}(\mathbb{I}_t)$. Assume that $s_1 \notin \mathrm{dom}(\mathbb{I}_t)$, i.e., $\mu_t(\boldsymbol{\theta}_1, s_1) = \langle \mu_1(\boldsymbol{\theta}_1, s_1), \emptyset \rangle$ (the other cases can be treated similarly). Again, by the fact that $\mathcal{A}$ is multiplicative, we obtain:

$$\begin{aligned}
\mu_t(\boldsymbol{\theta}_1\boldsymbol{\theta}_2, s_1 s_2) &= \langle \mu_1(\boldsymbol{\theta}_1\boldsymbol{\theta}_2, s_1 s_2), \emptyset \rangle \\
&= \langle \mu_1(\boldsymbol{\theta}_1, s_1) \circ \mu_1(\boldsymbol{\theta}_2, s_2), \emptyset \rangle \\
&= \langle \mu_1(\boldsymbol{\theta}_1, s_1), \emptyset \rangle \circ \mu_t(\boldsymbol{\theta}_2, s_2) \\
&= \mu_t(\boldsymbol{\theta}_1, s_1) \circ \mu_t(\boldsymbol{\theta}_2, s_2)
\end{aligned}$$

(AB9): The inclusion

$$\delta_t(\boldsymbol{\theta}_1\boldsymbol{\theta}_2, s_1 s_2) \subseteq \delta_t(\boldsymbol{\theta}_1, s_1) \circ \delta_t(\boldsymbol{\theta}_2, s_2)$$

follows directly from Lemma 26. For the reverse inclusion assume that $(c_1, c_2) \in \delta_t(\boldsymbol{\theta}_1, s_1)$ and $(c_2, c_3) \in \delta_t(\boldsymbol{\theta}_2, s_2)$. Hence, $c_1 s_1 \sim s_1 c_2$ and $c_2 s_2 \sim s_2 c_3$. This implies $c_1(s_1 s_2) \sim s_1 c_2 s_2 \sim (s_1 s_2) c_3$. Hence, $(c_1, c_3) \in \delta_t(\boldsymbol{\theta}_1\boldsymbol{\theta}_2, s_1 s_2)$.

(AB11): Assume that $s \in \mathrm{dom}(\mathbb{I}_t) = \mathsf{I}(\mathbb{H}) * \{t, t^{-1}\}^*$ and let $\boldsymbol{\theta} \in \gamma_t(s)$. We obtain

$$\begin{aligned}
\mathbb{I}_{\mathsf{Q}}(\mu_t(\boldsymbol{\theta}, s)) &= \mathbb{I}_{\mathsf{Q}}(\langle \mu_1(\boldsymbol{\theta}, s), \mu_1(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}), \mathbb{I}_t(s))^{-1} \rangle) \\
&= \langle \mu_1(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}), \mathbb{I}_t(s)),\ \mu_1(\boldsymbol{\theta}, s)^{-1} \rangle \\
&= \langle \mu_1(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}), \mathbb{I}_t(s)),\ \mu_1(\mathbb{I}_{\mathcal{T}}(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta})), \mathbb{I}_t(\mathbb{I}_t(s)))^{-1} \rangle \\
&= \mu_t(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}), \mathbb{I}_t(s)).
\end{aligned}$$

(AB12): Assume that $s \in \mathrm{dom}(\mathbb{I}_t) = \mathsf{I}(\mathbb{H}) * \{t, t^{-1}\}^*$ and let $\boldsymbol{\theta} \in \gamma_t(s)$. We obtain

$$\begin{aligned}
\delta_t(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}), \mathbb{I}_t(s)) &= \{(c, d) \in \mathrm{Gi}(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta})) \times \mathrm{Ge}(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta})) \mid c\mathbb{I}_t(s) \sim \mathbb{I}_t(s) d\} \\
&\overset{(19)}{=} \{(c, d) \in \mathrm{Ge}(\boldsymbol{\theta}) \times \mathrm{Gi}(\boldsymbol{\theta}) \mid \mathbb{I}_t(s c^{-1}) \sim \mathbb{I}_t(d^{-1} s)\} \\
&= \{(c, d) \in \mathrm{Ge}(\boldsymbol{\theta}) \times \mathrm{Gi}(\boldsymbol{\theta}) \mid s c^{-1} \sim d^{-1} s\} \\
&= \{(c, d) \in \mathrm{Ge}(\boldsymbol{\theta}) \times \mathrm{Gi}(\boldsymbol{\theta}) \mid ds \sim sc\} \\
&= \{(d, c) \in \mathrm{Gi}(\boldsymbol{\theta}) \times \mathrm{Ge}(\boldsymbol{\theta}) \mid ds \sim sc\}^{-1} \\
&= \delta_t(\boldsymbol{\theta}, s)^{-1}.
\end{aligned}$$

This concludes the proof of Proposition 3. □

Another AB-structure over $\mathbb{H} * \{t, t^{-1}\}^*$ can be defined by choosing, in place of the map γ_t defined in (34), the map γ_+ defined in (33). Assertion (64) is now replaced by

$$\forall s \in \mathbb{H} * \{t, t^{-1}\}^* : \gamma_+(s) \neq \emptyset. \tag{65}$$

We call the resulting structure

$$\langle \mathbb{H} * \{t, t^{-1}\}^*, \iota_A, \iota_B, \mathbb{I}_t, \mu_t, \gamma_+, \delta_t \rangle \tag{66}$$

the *positive* AB-algebra over $\mathbb{H} * \{t, t^{-1}\}^*$. This variant will be used in Section 10 where we deal with *positive* rational constraints.

One can check that the monoid-congruence $\sim$ on $\mathbb{H} * \{t, t^{-1}\}^*$ is compatible (see Definition 6) w.r.t. to the AB-algebra $\langle \mathbb{H} * \{t, t^{-1}\}^*, \iota_A, \iota_B, \mathbb{I}_t, \mu_t, \gamma_t, \delta_t \rangle$. Here, for $\gamma_t(s) = \gamma_t(s')$ and $\mu_t(\boldsymbol{\theta}, s) = \mu_t(\boldsymbol{\theta}, s')$ (if $s \sim s'$) it is important that the ftas $\mathcal{R}_6$ and $\mathcal{A}$ are $\sim$-saturated, see Definition 3. Hence, on the quotient monoid $\mathbb{H}_t = \mathbb{H} * \{t, t^{-1}\}^*/_\sim$, we obtain an AB-algebra $\langle \mathbb{H}_t, \iota_A, \iota_B, \mathbb{I}_t, \mu_t, \gamma_t, \delta_t \rangle$ that we will denote just with $\mathbb{H}_t$ in the following. Since $s \sim s'$ implies $\|s\| = \|s'\|$, the notion of norm remains well-defined in the quotient $\mathbb{H}_t$.

Similarly, we can define an AB-algebra

$$\mathbb{H}_{t,+} = \langle \mathbb{H}_t, \iota_A, \iota_B, \mathbb{I}_t, \mu_t, \gamma_+, \delta_t \rangle, \tag{67}$$

where γ_+ is defined via the fta $\mathcal{G}_6$ instead of $\mathcal{R}_6$, see (33).

3.5 Algebraic properties of $\mathbb{H}_t$

The monoid $\mathbb{H}_t$ has some properties which resemble equidivisibility. We detail here these properties.

Lemma 27. *Let $P, P', S, S' \in \mathbb{H}_t$, $\boldsymbol{\theta} \in \gamma_+(P) \cap \gamma_+(P')$, $\boldsymbol{\rho} \in \gamma_+(S) \cap \gamma_+(S')$ such that $\boldsymbol{\theta}\boldsymbol{\rho}$ is defined, $\boldsymbol{\theta}$ is an H-type and $PS = P'S'$ in $\mathbb{H}_t$. Then, there exists $c \in \mathrm{Ge}(\boldsymbol{\theta})$ such that $P = P'c$ and $cS = S'$ in $\mathbb{H}_t$.*

Proof. Let $p, p', s, s' \in \mathbb{H} * \{t, t^{-1}\}^*$ such that $P = [p]_\sim$, $P' = [p']_\sim$, $S = [s]_\sim$, and $S' = [s']_\sim$. Since $\boldsymbol{\theta}$ is an H-type, we must have $p, p' \in \mathbb{H}$ and since the product $\boldsymbol{\theta}\boldsymbol{\rho}$ is defined, $\mathrm{Ge}(\boldsymbol{\theta}) = \mathrm{Gi}(\boldsymbol{\rho})$. An inspection of the H-types in (21) and (22) shows that the vertex type $\tau\mathrm{e}(\boldsymbol{\theta}) = \tau\mathrm{i}(\boldsymbol{\rho})$ must be either (A, T), (B, T), or $(1, 1)$.

Case 1. $\tau\mathrm{e}(\boldsymbol{\theta}) = \tau\mathrm{i}(\boldsymbol{\rho}) = (1, 1)$. The structure of $\mathcal{G}_6$ implies $\boldsymbol{\rho} = (1, 1, 0, 1, 1)$. Since $\boldsymbol{\rho} = (1, 1, 0, 1, 1) \in \gamma_+(s) \cap \gamma_+(s')$, we have $s = s' = 1$, i.e., $S = S' = 1$. Hence, $P = P'$. Choosing $c = 1$, we obtain $c \in \{1\} = \mathrm{Ge}(\boldsymbol{\theta})$, $P = P'c$ and $cS = S'$.

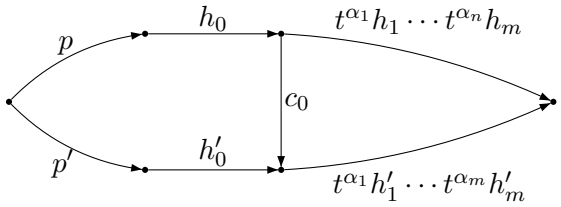
Case 2. $\tau\mathrm{e}(\boldsymbol{\theta}) = \tau\mathrm{i}(\boldsymbol{\rho}) = (C, T)$ for $C \in \{A, B\}$. Thus, $\mathrm{Gi}(\boldsymbol{\rho}) = \mathrm{Ge}(\boldsymbol{\theta}) = C$. Suppose that

$$s = h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_n} h_n \text{ and } s' = h'_0 t^{\alpha'_1} h'_1 \cdots t^{\alpha'_m} h'_m.$$

where $h_i, h'_j \in \mathbb{H}, \alpha_i, \alpha'_j \in \{-1, +1\}$. Since $ps \sim p's'$ and $p, p' \in \mathbb{H}$, we have $m = n$ and $\alpha_i = \alpha'_i$ for $1 \leq i \leq m$, i.e.,

$$s = h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_m} h_m \text{ and } s' = h'_0 t^{\alpha_1} h'_1 \cdots t^{\alpha_m} h'_m.$$

Since these sequences can be read by the fta $\mathcal{G}_6$ starting from (C, T), we must have $h_0, h'_0 \in C$. Moreover, if $m \geq 1$, then $C = A(\alpha_1)$. Since $ps \sim p's'$ there exists a van Kampen diagram of the form



with $c_0 \in C$ (if $m = 0$, then $c_0 = 1$). Let us choose $c = h'_0 c_0^{-1} h_0^{-1} \in C = \mathrm{Ge}(\boldsymbol{\theta})$. We obtain $P = P'c$ and $cS = S'$. □

Lemma 28. *Let $P, P', S, S' \in \mathbb{H}_t$, $\boldsymbol{\theta} \in \gamma_+(P)$, $\boldsymbol{\theta}' \in \gamma_+(P')$, $\boldsymbol{\rho} \in \gamma_+(S)$, $\boldsymbol{\rho}' \in \gamma_+(S')$ such that $\boldsymbol{\theta}\boldsymbol{\rho} = \boldsymbol{\theta}'\boldsymbol{\rho}'$ is defined, $\boldsymbol{\theta}, \boldsymbol{\theta}'$ are T-types (see (24)) and $PS = P'S'$ in $\mathbb{H}_t$. Then, one of the following cases must occur:*

(1) $\|P\| = \|P'\|$, $\boldsymbol{\theta} = \boldsymbol{\theta}'$, and there exists $c \in \mathrm{Ge}(\boldsymbol{\theta})$ such that $Pc = P'$ and $S = cS'$.

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

$$Pc = P'_1, \quad P' = P'_1P'_2P'_3, \quad S = cP'_2P'_3S', \quad \boldsymbol{\theta}' = \boldsymbol{\theta}\boldsymbol{\theta}'_2\boldsymbol{\theta}'_3, \quad \boldsymbol{\rho} = \boldsymbol{\theta}'_2\boldsymbol{\theta}'_3\boldsymbol{\rho}'.$$

(3) $\|P\| > \|P'\|$ and there exist $c \in \mathrm{Ge}(\boldsymbol{\theta}')$, $P_1, P_2, P_3 \in \mathbb{H}_t$ such that P_1 has the T-type $\boldsymbol{\theta}'$, P_3 has a T-type $\boldsymbol{\theta}_3$, P_2 has an H-type $\boldsymbol{\theta}_2$ and

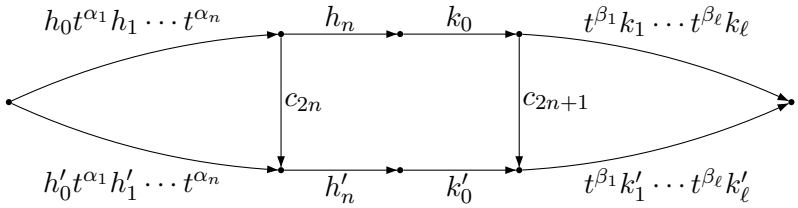
$$P = P_1P_2P_3, \quad P_1 = P'c, \quad cP_2P_3S = S', \quad \boldsymbol{\theta} = \boldsymbol{\theta}'\boldsymbol{\theta}_2\boldsymbol{\theta}_3, \quad \boldsymbol{\rho}' = \boldsymbol{\theta}_2\boldsymbol{\theta}_3\boldsymbol{\rho}.$$

Proof. Let $p, p', s, s' \in \mathbb{H} * \{t, t^{-1}\}^*$ such that $P = [p]_\sim$, $P' = [p']_\sim$, $S = [s]_\sim$, and $S' = [s']_\sim$. Since the products $\boldsymbol{\theta}\boldsymbol{\rho}, \boldsymbol{\theta}'\boldsymbol{\rho}'$ are defined, $\mathrm{Ge}(\boldsymbol{\theta}) = \mathrm{Gi}(\boldsymbol{\rho})$ and $\mathrm{Ge}(\boldsymbol{\theta}') = \mathrm{Gi}(\boldsymbol{\rho}')$. Suppose that

$$p = h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_n} h_n \qquad s = k_0 t^{\beta_1} k_1 \cdots t^{\beta_\ell} k_\ell$$
$$p' = h'_0 t^{\alpha'_1} h'_1 \cdots t^{\alpha'_\nu} h'_\nu \qquad s' = k'_0 t^{\beta'_1} k'_1 \cdots t^{\beta'_\lambda} k'_\lambda$$

where $h_i, k_j, h'_\iota, k'_\kappa \in \mathbb{H}$, $\alpha_i, \beta_j, \alpha'_\iota, \beta'_\kappa \in \{-1, +1\}$. Since $\boldsymbol{\theta}$ and $\boldsymbol{\theta}'$ are T-types, the structure of $\mathcal{G}_6$ implies that $n, \nu \geq 1$, $h_n \in \mathrm{Ge}(\boldsymbol{\theta})$, and $h'_\nu \in \mathrm{Ge}(\boldsymbol{\theta}')$ (note that the only arrow entering (A, H) (resp. (B, H)) in $\mathcal{G}_6$ that is labeled with a subset of $\mathbb{H}$ is the A-loop (resp. B-loop)). Since $ps \sim p's'$, we get $n + \ell = \nu + \lambda$ and $(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_\ell) = (\alpha'_1, \ldots, \alpha'_\nu, \beta'_1, \ldots, \beta'_\lambda)$. Moreover, $\tau\mathrm{i}(\boldsymbol{\theta}) = \tau\mathrm{i}(\boldsymbol{\theta}')$ and the boolean component of both $\boldsymbol{\theta}$ and $\boldsymbol{\theta}'$ is 1, since they are both T-types.

Case 1. $\|p\| = \|p'\|$: Thus, $n = \nu$, $\ell = \lambda$, $\tau\mathrm{e}(\boldsymbol{\theta}) = \tau\mathrm{e}(\boldsymbol{\theta}')$ (and hence $\boldsymbol{\theta} = \boldsymbol{\theta}'$), and there exists a van Kampen diagram of the form

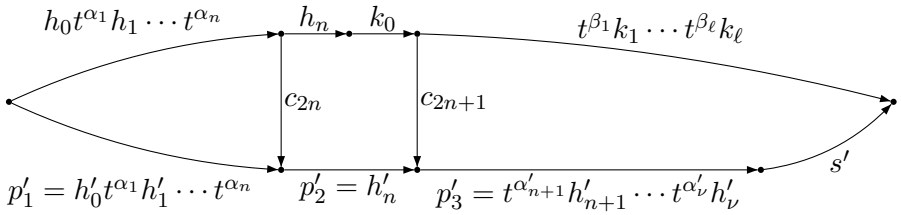


with $c_{2n} \in B(\alpha_n) = \mathrm{Ge}(\boldsymbol{\theta}) = \mathrm{Ge}(\boldsymbol{\theta}')$. Hence, we can set $c = h_n^{-1} c_{2n} h'_n \in \mathrm{Ge}(\boldsymbol{\theta})$.

Case 2. $\|p\| < \|p'\|$: Hence $n < \nu$. Let us set

$$p'_1 = h'_0 t^{\alpha_1} h'_1 \cdots h'_{n-1} t^{\alpha_n}, \quad p'_2 = h'_n, \quad p'_3 = t^{\alpha'_{n+1}} h'_{n+1} \cdots t^{\alpha'_\nu} h'_\nu.$$

Thus, $p' = p'_1 p'_2 p'_3$ and there exists a van Kampen diagram of the following form:



Since $h_n \in \mathrm{Ge}(\boldsymbol{\theta})$ and $c_{2n} \in B(\alpha_n) = \mathrm{Ge}(\boldsymbol{\theta})$, we have $c = h_n^{-1} c_{2n} \in \mathrm{Ge}(\boldsymbol{\theta})$. We obtain $p'_1 \sim pc$ and $s \sim c p'_2 p'_3 s'$.

For the T-types $\boldsymbol{\theta}$ and $\boldsymbol{\theta}'$ we get

$$\boldsymbol{\theta} = (A(\alpha_1), T, 1, B(\alpha_n), H) \quad \text{and} \quad \boldsymbol{\theta}' = (A(\alpha_1), T, 1, B(\alpha'_\nu), H).$$

A possible type for p'_1 is $\boldsymbol{\theta} = (A(\alpha_1), T, 1, B(\alpha_n), H)$, a possible type for p'_2 is

$$\boldsymbol{\theta}'_2 = (B(\alpha_n), H, 0, A(\alpha'_{n+1}), T),$$

and a possible type for p'_3 is

$$\boldsymbol{\theta}'_3 = (A(\alpha'_{n+1}), T, 1, B(\alpha'_\nu), H).$$

Thus $\boldsymbol{\theta}'_3$ is a T-type and $\boldsymbol{\theta}'_2$ is an H-type such that $\boldsymbol{\theta}' = \boldsymbol{\theta}\boldsymbol{\theta}'_2\boldsymbol{\theta}'_3$. It remains to show $\boldsymbol{\rho} = \boldsymbol{\theta}'_2\boldsymbol{\theta}'_3\boldsymbol{\rho}'$, i.e., $\boldsymbol{\rho} = (B(\alpha_n), H, 1, B(\alpha'_\nu), H)\boldsymbol{\rho}'$. Since $\|s\| = \ell > \lambda \geq 0$, the Boolean component of $\boldsymbol{\rho} \in \gamma_+(s)$ must be 1, which is the Boolean component of $(B(\alpha_n), H, 1, B(\alpha'_\nu), H)\boldsymbol{\rho}'$. Moreover, $\tau\mathrm{e}(\boldsymbol{\rho}) = \tau\mathrm{e}(\boldsymbol{\rho}') = \tau\mathrm{e}((B(\alpha_n), H, 1, B(\alpha'_\nu), H)\boldsymbol{\rho}')$. Finally, $\tau\mathrm{i}(\boldsymbol{\rho}) = \tau\mathrm{e}(\boldsymbol{\theta}) = (B(\alpha_n), H) = \tau\mathrm{i}((B(\alpha_n), H, 1, B(\alpha'_\nu), H)\boldsymbol{\rho}')$.

Case 3. $\|p\| > \|p'\|$: This case is similar to Case 2. □

3.6 The AB-algebra $\mathcal{W}^* * A * B$

Let $\mathcal{S}$ be a system of equations over $\mathbb{H}_t$ with involution and rational constraints. The rational constraints are expressed via the map μ_t defined by (62) in Section 3.4. This map comes from a normal partitioned fta $\mathcal{A} = \langle \mathcal{L}, \mathsf{Q}, \tau, \delta, \mathsf{I}, \mathsf{T} \rangle$. 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 $\mathbb{H}_t$) of that variable that leads to a solution of the system of equations.

Let $\mathcal{V}_0$ be some starting set that will be made precise later. Let us denote by $\mathcal{T}_{HT} \subseteq \mathcal{T}$ the set of all types which are either H-types or T-types [5]. The set $\mathcal{W}$ of generic symbols is the set of all 5-tuples

$$(V, \epsilon, \boldsymbol{\theta}, r, \varphi) \in \mathcal{V}_0 \times \{-1, 0, 1\} \times \mathcal{T}_{HT} \times \mathsf{B}^2(\mathsf{Q}) \times \mathrm{PGI}\{A, B\} \tag{68}$$

such that:

$$r \subseteq \left(\tau^{-1}(\tau\mathrm{i}(\boldsymbol{\theta})) \times \tau^{-1}(\tau\mathrm{e}(\boldsymbol{\theta}))\right) \times \left(\tau^{-1}(\mathbb{I}_{\mathcal{R}}(\tau\mathrm{i}(\boldsymbol{\theta}))) \times \tau^{-1}(\mathbb{I}_{\mathcal{R}}(\tau\mathrm{e}(\boldsymbol{\theta})))\right), \tag{69}$$

$$\varphi \subseteq \mathrm{Gi}(\boldsymbol{\theta}) \times \mathrm{Ge}(\boldsymbol{\theta}), \tag{70}$$

$$\forall (c, d) \in \varphi : \mu_t((\tau\mathrm{i}(\boldsymbol{\theta}), 0, \tau\mathrm{i}(\boldsymbol{\theta})), c) \circ r = r \circ \mu_t((\tau\mathrm{e}(\boldsymbol{\theta}), 0, \tau\mathrm{e}(\boldsymbol{\theta})), d) \tag{71}$$

We will need the following lemma:

[5] It turns out useful to include in the generic symbols also the *non-atomic* types of $\mathcal{T}_{HT}$ for sake of finding *short* decompositions in Lemma 45, see figure 7.

Lemma 29. *Let $W = (V, \epsilon, \boldsymbol{\theta}, r, \varphi) \in \mathcal{V}_0 \times \{-1, 0, 1\} \times \mathcal{T}_{HT} \times \mathsf{B}^2(\mathsf{Q}) \times \mathrm{PGI}\{A, B\}$ and $s \in \mathbb{H}_t$ such that $\boldsymbol{\theta} \in \gamma_t(s)$, $r = \mu_t(\boldsymbol{\theta}, s)$, and $\varphi = \delta_t(\boldsymbol{\theta}, s)$. Then, $W \in \mathcal{W}$.*

Proof. We have to verify the three conditions (69), (70), and (71). Condition (69) follows directly from (62), whereas condition (70) follows directly from (63). For (71) let $(c, d) \in \varphi = \delta_t(\boldsymbol{\theta}, s)$. Hence, we have $cs \sim sd$. Since the fta $\mathcal{A}$ is $\sim$-saturated and (AB8) holds for μ_t, we get

$$\begin{aligned}
\mu_t((\tau\mathrm{i}(\boldsymbol{\theta}), 0, \tau\mathrm{i}(\boldsymbol{\theta})), c) \circ r &= \mu_t((\tau\mathrm{i}(\boldsymbol{\theta}), 0, \tau\mathrm{i}(\boldsymbol{\theta})), c) \circ \mu_t(\boldsymbol{\theta}, s) \\
&= \mu_t(\boldsymbol{\theta}, cs) \\
&= \mu_t(\boldsymbol{\theta}, sd) \\
&= \mu_t(\boldsymbol{\theta}, s) \circ \mu_t((\tau\mathrm{e}(\boldsymbol{\theta}), 0, \tau\mathrm{e}(\boldsymbol{\theta})), d) \\
&= r \circ \mu_t((\tau\mathrm{e}(\boldsymbol{\theta}), 0, \tau\mathrm{e}(\boldsymbol{\theta})), d).
\end{aligned}$$

Hence, also (71) holds. □

Let

$$\widehat{\mathcal{W}} = \{(V, \epsilon, \boldsymbol{\theta}, r, \varphi) \in \mathcal{W} \mid \epsilon \neq 0\}. \tag{72}$$

Let us consider the free product $\mathcal{W}^* * A * B$. We denote by $\iota_A : A \to \mathcal{W}^* * A * B$ (resp. $\iota_B : B \to \mathcal{W}^* * A * B$ the natural embedding of A (resp. B) into $\mathcal{W}^* * A * B$. Note that

$$\iota_A(A) \cap \iota_B(B) = \{1\}.$$

Most of the time, we will identify $\iota_A(a)$ with a and $\iota_B(b)$ with b. For every $s \in \mathcal{W}^* * A * B$ let $\|s\|$ be the number of occurrences of symbols from $\mathcal{W}$ in s. Clearly

$$\|uv\| = \|u\| + \|v\| \qquad \text{and} \qquad \|s\| = 0 \iff s \in A * B.$$

In this section, we will define an AB-algebra

$$\langle \mathcal{W}^* * A * B, \iota_A, \iota_B, \mathbb{I}_w, \gamma_w, \mu_w, \delta_w \rangle \tag{73}$$

with underlying monoid $\mathcal{W}^* * A * B$ and set of states Q. Let $\mathbb{I}_w$ be the unique monoid anti-homomorphism on $\mathrm{dom}(\mathbb{I}_w) = \widehat{\mathcal{W}}^* * A * B$ (the submonoid generated by $\widehat{\mathcal{W}} \cup \iota_A(A) \cup \iota_B(B)$) such that

$$\mathbb{I}_w(a) = a^{-1} \text{ for } a \in A \tag{74}$$

$$\mathbb{I}_w(b) = b^{-1} \text{ for } b \in B \tag{75}$$

$$\mathbb{I}_w(V, \epsilon, \boldsymbol{\theta}, r, \varphi) = (V, -\epsilon, \mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}), \mathbb{I}_{\mathsf{Q}}(r), \varphi^{-1}). \tag{76}$$

One can easily check that the alphabet $\mathcal{W}$ is closed under the involution $\mathbb{I}_w$. The mapping $\gamma_w : \mathcal{W}^* * A * B \to 2^{\mathcal{T}}$ is defined on the generators of $\mathcal{W}^* * A * B$ as follows:

$$\gamma_w(a) = \{(A, T, 0, A, T), (A, H, 0, A, H)\} \text{ for every } a \in A \setminus \{1\} \tag{77}$$

$$\gamma_w(b) = \{(B, T, 0, B, T), (B, H, 0, B, H)\} \text{ for every } b \in B \setminus \{1\} \tag{78}$$

$$\gamma_w(V, \epsilon, \boldsymbol{\theta}, r, \varphi) = \{\boldsymbol{\theta}\} \tag{79}$$

Now let $s \in \mathcal{W}^* * A * B$. Then s can be uniquely written as

$$s = g_1 \cdots g_n$$

with $n \geq 0$ and $g_1, \ldots, g_n \in \mathcal{W} \cup (A \setminus 1) \cup (B \setminus 1)$ such that for all $1 \leq i < n$ we have neither $g_i, g_{i+1} \in A \setminus 1$ nor $g_i, g_{i+1} \in B \setminus 1$. Such a string $g_1 \cdots g_n$ is called (A, B)-*reduced* in the following. Then, let

$$\gamma_w(g_1 g_2 \cdots g_n) = \begin{cases} \{(\theta, 0, \theta) \mid \theta \in \mathcal{T}_6\} \text{ if } n = 0 \\ \gamma_w(g_1)\gamma_w(g_2)\cdots\gamma_w(g_n) \text{ if } n > 0. \end{cases} \tag{80}$$

Note that $\gamma_w(1)$ is the identity of the monoid $2^{\mathcal{T}}$. Before we continue with the definition of the mappings μ_w and δ_w from (73), let us first state some properties of γ_w:

Lemma 30. *The following holds:*

(a) For all $s \in \mathcal{W}^* * A * B$ we have $|\gamma_w(s)| \in \{0, 1, 2, 6\}$.
(b) If $\|s\| \geq 1$, then $|\gamma_w(s)| \in \{0, 1\}$.
(c) If $g_1 g_2 \cdots g_n$ is (A, B)-reduced and $\boldsymbol{\theta} \in \gamma_w(g_1 g_2 \cdots g_n)$ then there exist unique path types $\boldsymbol{\theta}_1 \in \gamma_w(g_1), \ldots, \boldsymbol{\theta}_n \in \gamma_w(g_n)$ with $\boldsymbol{\theta} = \boldsymbol{\theta}_1 \boldsymbol{\theta}_2 \cdots \boldsymbol{\theta}_n$.
(d) If the (A, B)-reduced string s contains a factor from $(A \setminus 1)(B \setminus 1) \cup (B \setminus 1)(A \setminus 1)$, then $\gamma_w(s) = \emptyset$.
(e) For all $u, v \in \mathcal{W}^* * A * B$: $\gamma_w(u)\gamma_w(v) \subseteq \gamma_w(uv)$.
(f) For all $u, v \in \mathcal{W}^* * A * B$, $W \in \mathcal{W}$, and $c \in A \cup B$: if $\gamma_w(Wc) \neq \emptyset$, then $\gamma_w(uWc)\gamma_w(v) = \gamma_w(uWcv)$.
(g) For all $u, v, \in \mathcal{W}^* * A * B$, $W \in \mathcal{W}$, and $c \in A \cup B$: if $\gamma_w(cW) \neq \emptyset$, then $\gamma_w(u)\gamma_w(cWv) = \gamma_w(uWcv)$.
(h) For all $u, v, v' \in \mathcal{W}^* * A * B$, if $\|u\| \geq 1$ and $\gamma_w(u) \neq \emptyset$ then $\gamma_w(v)\gamma_w(u)\gamma_w(v') = \gamma_w(vuv')$.

Proof. We show only statements (e)–(h), the other statements are easy to prove.

Statement (e): If $\gamma_w(u) = \emptyset$ or $\gamma_w(v) = \emptyset$ then we have $\gamma_w(u)\gamma_w(v) = \emptyset \subseteq \gamma_w(uv)$. So assume that $\gamma_w(u) \neq \emptyset \neq \gamma_w(v)$. Let $u = g_1 \cdots g_n$ and $v = h_1 \cdots h_m$ be (A, B)-reduced strings. If $g_1 \cdots g_n h_1 \cdots h_m$ is again (A, B)-reduced then we have $\gamma_w(u)\gamma_w(v) = \gamma_w(uv)$ by (80). Hence, assume that $g_1 \cdots g_n h_1 \cdots h_m$ is not (A, B)-reduced, e.g. $g_n, h_1 \in A \setminus \{1\}$. Since $\gamma_w(u) \neq \emptyset \neq \gamma_w(v)$, the letters g_{n-1} and h_2 (if they exist) cannot be from $B \setminus \{1\}$, and they cannot be from $A \setminus \{1\}$ since $g_1 \cdots g_n$ and $h_1 \cdots h_m$ are (A, B)-reduced. Hence, either $uv = g_1 \cdots g_{n-1} h_2 \cdots h_m$ is reduced (if $g_n h_1 = 1$ in A), or $uv = g_1 \cdots g_{n-1}(g_n h_1) h_2 \cdots h_m$ is reduced. In the first case, we get $\gamma_w(u)\gamma_w(v) \subseteq \gamma_w(uv)$, in the second case we even have $\gamma_w(u)\gamma_w(v) = \gamma_w(uv)$.

Statement (f): Assume w.l.o.g. that u and v are (A, B)-reduced. If $c = 1$, then uWv is the (A, B)-reduced sequence equivalent to $uWcv$. Then, (80) implies $\gamma_w(uWc)\gamma_w(v) = \gamma_w(uW)\gamma_w(v) = \gamma_w(uWv) = \gamma_w(uWcv)$. Now, assume that w.l.o.g. $c \in A \setminus 1$. If the sequence v does not start with an element from $A \setminus 1$, then $uWcv$ is again (A, B)-reduced and we get $\gamma_w(uWc)\gamma_w(v) = \gamma_w(uWcv)$ from (80). So, assume that $v = av'$ with $a \in A \setminus 1$.

Since $\gamma_w(Wc) \neq \emptyset$, we must have $\gamma_w(W) = \boldsymbol{\theta}$ for a path type $\boldsymbol{\theta}$ with $\tau\mathrm{e}(\boldsymbol{\theta}) \in \{(A, T), (A, H)\}$. But this implies $\gamma_w(W) = \gamma_w(W)\gamma_w(c) = \gamma_w(Wc)$. There are two cases:

Case 1. $ca \neq 1$ in A. Then $uWcv = uW(ca)v'$, and the latter sequence is (A, B)-reduced. By (80) we have $\gamma_w(uWcv) = \gamma_w(uW(ca)v') = \gamma_w(u)\gamma_w(W)\gamma_w((ca)v') = \gamma_w(u)\gamma_w(Wc)\gamma_w(av') = \gamma_w(uWc)\gamma_w(v)$.

Case 2. $ca = 1$. In this case $uWcv = uWv'$, and the latter sequence is (A, B)-reduced. Since $\gamma_w(c) = \gamma_w(a)$ is idempotent, we have $\gamma_w(uWcv) = \gamma_w(uWv') = \gamma_w(u)\gamma_w(W)\gamma_w(v') = \gamma_w(u)\gamma_w(W)\gamma_w(c)\gamma_w(a)\gamma_w(v') = \gamma_w(uWc)\gamma_w(v)$. This concludes the proof of (f).

Statement (g): symetrical with (f).

Statement (h): Since $\|u\| \geq 1$ and $\gamma_w(u) \neq \emptyset$, we can write u as $u = c_1 u' c_2$, where $c_1, c_2 \in A \cup B$ and u' starts and ends with a symbol from $\mathcal{W}$. Then $\gamma_w(v)\gamma_w(u)\gamma_w(v') = \gamma_w(vuv')$ follows by an application of statement (f) followed by an application of statement (g). □

Definition 7. *Let $\equiv_\gamma$ be the equivalence relation over $\mathcal{W}^* * A * B$ defined by: for every $u, u' \in \mathcal{W}^* * A * B$,*

$$u \equiv_\gamma u' \iff (\forall v, v' \in \mathcal{W}^* * A * B : \gamma_w(vuv') = \gamma_w(vu'v')). \tag{81}$$

It is clear from the definition that $\equiv_\gamma$ is a monoid congruence.

Lemma 31. *Let $u, u' \in \mathcal{W}^* * A * B$. If $\|u\| \geq 1, \|u'\| \geq 1$ and $\gamma_w(u) = \gamma_w(u') \neq \emptyset$ then $u \equiv_\gamma u'$.*

Proof. Let $u, u' \in \mathcal{W}^* * A * B$ fulfilling $\|u\| \geq 1, \|u'\| \geq 1, \gamma_w(u) = \gamma_w(u') \neq \emptyset$. Let $v, v' \in \mathcal{W}^* * A * B$. Using (h) from Lemma 30 together with the hypothesis that $\gamma_w(u) = \gamma_w(u')$ we obtain:

$$\begin{aligned}\gamma_w(vuv') &= \gamma_w(v)\gamma_w(u)\gamma_w(v') \\ &= \gamma_w(v)\gamma_w(u')\gamma_w(v') \\ &= \gamma_w(vu'v')\end{aligned}$$

□

Let us now continue with the definition of the partial mappings $\mu_w : \mathcal{T} \times \mathcal{W}^* * A * B \to \mathsf{B}^2(\mathsf{Q})$ and $\delta_w : \mathcal{T} \times \mathcal{W}^* * A * B \to \mathrm{PGI}\{A, B\}$. Also these mappings are first defined only for generators, where $c \in (A \setminus 1) \cup (B \setminus 1)$:

$$\begin{aligned}\mu_w(\boldsymbol{\theta}, c) &= \mu_t(\boldsymbol{\theta}, c) \text{ for } \boldsymbol{\theta} \in \gamma_w(c) \\ \delta_w(\boldsymbol{\theta}, c) &= \delta_t(\boldsymbol{\theta}, c) \text{ for } \boldsymbol{\theta} \in \gamma_w(c) \\ \mu_w(\boldsymbol{\theta}, (V, \epsilon, \boldsymbol{\theta}, r, \varphi)) &= r \\ \delta_w(\boldsymbol{\theta}, (V, \epsilon, \boldsymbol{\theta}, r, \varphi)) &= \varphi\end{aligned} \tag{82}$$

Finally, let $s = g_1 \cdots g_n$ $(g_1, \ldots, g_n \in \mathcal{W} \cup (A \setminus 1) \cup (B \setminus 1))$ be an (A, B)-reduced string and $\boldsymbol{\theta} \in \gamma_w(s)$. If $n = 0$, i.e. $s = 1$, then $\boldsymbol{\theta} = (\theta, 0, \theta)$ for some vertex type θ, and we set

$$\begin{aligned}\mu_w(\boldsymbol{\theta}, 1) = \mu_t(\boldsymbol{\theta}, 1) &= \langle \{(q, q) \mid \tau(q) = \theta\},\ \{(p, p) \mid \tau(p) = \mathbb{I}_{\mathcal{R}}(\theta)\}\rangle \\ \delta_w(\boldsymbol{\theta}, 1) = \delta_t(\boldsymbol{\theta}, 1) &= \mathrm{Id}_{p_1(\theta)}.\end{aligned} \tag{83}$$

If $n \geq 1$ then by Lemma 30(c), there exist unique path types $\boldsymbol{\theta}_1 \in \gamma_w(g_1), \ldots, \boldsymbol{\theta}_n \in \gamma_w(g_n)$ with $\boldsymbol{\theta} = \boldsymbol{\theta}_1 \cdots \boldsymbol{\theta}_n$. Then,

$$\mu_w(\boldsymbol{\theta}, g_1 g_2 \cdots g_n) = \mu_w(\boldsymbol{\theta}_1, g_1) \circ \mu_w(\boldsymbol{\theta}_2, g_2) \circ \cdots \circ \mu_w(\boldsymbol{\theta}_n, g_n) \tag{84}$$

$$\delta_w(\boldsymbol{\theta}, g_1 g_2 \cdots g_n) = \delta_w(\boldsymbol{\theta}_1, g_1) \circ \delta_w(\boldsymbol{\theta}_2, g_2) \circ \cdots \circ \delta_w(\boldsymbol{\theta}_n, g_n). \tag{85}$$

Proposition 4. *$\langle \mathcal{W}^* * A * B, \iota_A, \iota_B, \mathbb{I}_w, \mu_w, \gamma_w, \delta_w \rangle$ is an AB-algebra.*

Proof. Properties (AB1)–(AB4) are obvious.

(AB5): For $s \in \mathcal{W}^* * A * B$, we have $s \in \mathrm{dom}(\mathbb{I}_w) = \widehat{\mathcal{W}}^* * A * B$ if and only if all $\mathcal{W}$-symbols in s belong to $\widehat{\mathcal{W}}$. Since $\mathcal{W}$-symbols cannot cancel in a product $s_1 s_2$ it follows that $s_1 s_2 \in \mathrm{dom}(\mathbb{I}_w)$ if and only if $s_1, s_2 \in \mathrm{dom}(\mathbb{I}_w)$.

(AB6): This is stated in Lemma 30, point (e).

(AB7): Follows immediately from the definition of δ_w.

(AB8): Assume that $\boldsymbol{\theta}_1 \in \gamma_w(s_1)$ and $\boldsymbol{\theta}_2 \in \gamma_w(s_2)$ such that $\boldsymbol{\theta}_1\boldsymbol{\theta}_2$ is defined. We prove by induction over $|s_1| + |s_2|$ that $\mu_w(\boldsymbol{\theta}_1\boldsymbol{\theta}_2, s_1 s_2) = \mu_w(\boldsymbol{\theta}_1, s_1) \circ \mu_w(\boldsymbol{\theta}_2, s_2)$.

Case 1. $s_1 = 1$. Then $\boldsymbol{\theta}_1 = (\theta, 0, \theta)$ for some vertex type θ and

$$\mu_w(\boldsymbol{\theta}_1, s_1) = \mu_w(\boldsymbol{\theta}_1, 1) = \langle \{(q,q) \mid \tau(q) = \theta\},\ \{(p,p) \mid \tau(p) = \mathbb{I}_{\mathcal{R}}(\theta)\} \rangle.$$

Since $\boldsymbol{\theta}_1\boldsymbol{\theta}_2$ is defined, we must have $\mathrm{Gi}(\boldsymbol{\theta}_2) = \theta$. Hence,

$$\mu_w(\boldsymbol{\theta}_1, s_1) \circ \mu_w(\boldsymbol{\theta}_2, s_2) = \mu_w(\boldsymbol{\theta}_2, s_2) = \mu_w(\boldsymbol{\theta}_1\boldsymbol{\theta}_2, s_1 s_2).$$

Case 2. $s_2 = 1$. Can be dealt analogously.

Case 3. $s_1 \neq 1 \neq s_2$ and $s_1 s_2$ is (A,B)-reduced. This case can be dealt directly, using the definition of μ_w in (84).

Case 4. $s_1 \neq 1 \neq s_2$ and $s_1 s_2$ is not (A,B)-reduced. W.l.o.g. assume that $s_1 = u_1 a_1$ and $s_2 = a_2 u_2$ for $a_1, a_2 \in A \setminus 1$. By (77) there must exist $\theta \in \{(A,T), (A,H)\}$ such that

$$\tau\mathrm{e}(\boldsymbol{\theta}_1) = \theta, \quad \tau\mathrm{i}(\boldsymbol{\theta}_2) = \theta. \tag{86}$$

Moreover, we must have $\boldsymbol{\theta}_1 \in \gamma_w(u_1)$ and $\boldsymbol{\theta}_2 \in \gamma_w(u_2)$ (this is clear if $u_1 = 1$, resp., $u_2 = 1$, and follows from Lemma 30(c) in case $u_1 \neq 1$, resp., $u_2 \neq 1$). By induction, we obtain:

$$\mu_w(\boldsymbol{\theta}_1, s_1) = \mu_w(\boldsymbol{\theta}_1(\theta,0,\theta), u_1 a_1) = \mu_w(\boldsymbol{\theta}_1, u_1) \circ \mu_w((\theta,0,\theta), a_1), \tag{87}$$

$$\mu_w(\boldsymbol{\theta}_2, s_2) = \mu_w((\theta,0,\theta)\boldsymbol{\theta}_2, a_2 u_2) = \mu_w((\theta,0,\theta), a_2) \circ \mu_w(\boldsymbol{\theta}_2, u_2) \tag{88}$$

If $a_2 \neq a_1^{-1}$, then $u_1(a_1 a_2)u_2$ is (A,B)-reduced. Since μ_t satisfies property (AB8), we obtain:

$$\begin{aligned}
\mu_w(\boldsymbol{\theta}_1, s_1) \circ \mu_w(\boldsymbol{\theta}_2, s_2) &\overset{(87),(88)}{=} \mu_w(\boldsymbol{\theta}_1, u_1) \circ \mu_w((\theta,0,\theta), a_1) \circ \mu_w((\theta,0,\theta), a_2) \circ \mu_w(\boldsymbol{\theta}_2, u_2) \\
&\overset{(82)}{=} \mu_w(\boldsymbol{\theta}_1, u_1) \circ \mu_t((\theta,0,\theta), a_1) \circ \mu_t((\theta,0,\theta), a_2) \circ \mu_w(\boldsymbol{\theta}_2, u_2) \\
&\overset{(AB8)}{=} \mu_w(\boldsymbol{\theta}_1, u_1) \circ \mu_t((\theta,0,\theta), a_1 a_2) \circ \mu_w(\boldsymbol{\theta}_2, u_2) \\
&\overset{(82)}{=} \mu_w(\boldsymbol{\theta}_1, u_1) \circ \mu_w((\theta,0,\theta), a_1 a_2) \circ \mu_w(\boldsymbol{\theta}_2, u_2) \\
&\overset{(Ind.)}{=} \mu_w(\boldsymbol{\theta}_1(\theta,0,\theta)\boldsymbol{\theta}_2, u_1(a_1 a_2)u_2) \\
&\overset{(86)}{=} \mu_w(\boldsymbol{\theta}_1\boldsymbol{\theta}_2, s_1 s_2)
\end{aligned}$$

Finally, if $a_2 = a_1^{-1}$, then we get:

$$\begin{aligned}
\mu_w(\boldsymbol{\theta}_1, s_1) \circ \mu_w(\boldsymbol{\theta}_2, s_2) &\overset{(87),(88)}{=} \mu_w(\boldsymbol{\theta}_1, u_1) \circ \mu_w((\theta,0,\theta), a_1) \circ \mu_w((\theta,0,\theta), a_1^{-1}) \circ \mu_w(\boldsymbol{\theta}_2, u_2) \\
&\overset{(82)}{=} \mu_w(\boldsymbol{\theta}_1, u_1) \circ \mu_t((\theta,0,\theta), a_1) \circ \mu_t((\theta,0,\theta), a_1^{-1}) \circ \mu_w(\boldsymbol{\theta}_2, u_2) \\
&\overset{(\mathrm{AB8})}{=} \mu_w(\boldsymbol{\theta}_1, u_1) \circ \mu_t((\theta,0,\theta), 1) \circ \mu_w(\boldsymbol{\theta}_2, u_2) \\
&\overset{(83)}{=} \mu_w(\boldsymbol{\theta}_1, u_1) \circ \mu_w((\theta,0,\theta), 1) \circ \mu_w(\boldsymbol{\theta}_2, u_2) \\
&\overset{(\mathrm{Ind.})}{=} \mu_w(\boldsymbol{\theta}_1(\theta,0,\theta)\boldsymbol{\theta}_2, u_1 u_2) \\
&\overset{(86)}{=} \mu_w(\boldsymbol{\theta}_1\boldsymbol{\theta}_2, s_1 s_2)
\end{aligned}$$

(AB9): Can be shown with a similar calculation as (AB8).

(AB10): Assume that $s = g_1 g_2 \cdots g_n$ is (A,B)-reduced with $g_1, \ldots, g_n \in \widehat{\mathcal{W}} \cup (A \setminus 1) \cup (B \setminus 1)$. Then, also $\mathbb{I}_w(g_n) \cdots \mathbb{I}_w(g_1)$ is (A,B)-reduced. We have to show that $\gamma_w(\mathbb{I}_w(s)) = \mathbb{I}_{\mathcal{T}}(\gamma_w(s))$. If $n = 0$, then

$$\gamma_w(\mathbb{I}_w(1)) = \gamma_w(1) \overset{(80)}{=} \{(\theta,0,\theta) \mid \theta \in \mathcal{T}_6\} = \mathbb{I}_{\mathcal{T}}(\{(\theta,0,\theta) \mid \theta \in \mathcal{T}_6\}) = \mathbb{I}_{\mathcal{T}}(\gamma_w(1)).$$

The case $n = 1$, i.e., s is a single generator, is clear by (74)–(79). Finally, for $n > 1$, we have

$$\begin{aligned}
\gamma_w(\mathbb{I}_w(g_1 \cdots g_n)) &= \gamma_w(\mathbb{I}_w(g_n) \cdots \mathbb{I}_w(g_1)) \\
&\overset{(80)}{=} \gamma_w(\mathbb{I}_w(g_n)) \cdots \gamma_w(\mathbb{I}_w(g_1)) \\
&= \mathbb{I}_{\mathcal{T}}(\gamma_w(g_n)) \cdots \mathbb{I}_{\mathcal{T}}(\gamma_w(g_1)) \\
&= \mathbb{I}_{\mathcal{T}}(\gamma_w(g_1) \cdots \gamma_w(g_n)) \\
&\overset{(80)}{=} \mathbb{I}_{\mathcal{T}}(\gamma_w(g_1 \cdots g_n))
\end{aligned}$$

(AB11): Let us first consider the case of a generator of $\widehat{\mathcal{W}}^* * A * B$. For $W = (V, \epsilon, \boldsymbol{\theta}, r, \varphi)$ we have indeed

$$\mathbb{I}_{\mathsf{Q}}(\mu_w(\boldsymbol{\theta}, W)) = \mathbb{I}_{\mathsf{Q}}(r) = \mu_w(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}), \mathbb{I}_w(W)).$$

For elements from $A \cup B$, we obtain (AB11) directly from (AB11) for the AB-algebra $\mathbb{H}_t$. This settles the case of generators. Now assume that $s = g_1 g_2 \cdots g_n$ is (A,B)-reduced with $g_1, \ldots, g_n \in \widehat{\mathcal{W}} \cup (A \setminus 1) \cup (B \setminus 1)$, $n \geq 2$, and $\gamma_w(s) \neq \emptyset$. If $\boldsymbol{\theta} \in \gamma_w(s)$ then there exist unique path types $\boldsymbol{\theta}_1 \in \gamma_w(g_1), \ldots, \boldsymbol{\theta}_n \in \gamma_w(g_n)$ with $\boldsymbol{\theta} = \boldsymbol{\theta}_1 \cdots \boldsymbol{\theta}_n$. We obtain

$$\begin{aligned}
\mu_w(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}),\ \mathbb{I}_w(s)) &= \mu_w(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}_1 \cdots \boldsymbol{\theta}_n),\ \mathbb{I}_w(g_1 \cdots g_n)) \\
&= \mu_w(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}_n) \cdots \mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}_1),\ \mathbb{I}_w(g_n) \cdots \mathbb{I}_w(g_1)) \\
&\overset{(\mathrm{AB8})}{=} \mu_w(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}_n), \mathbb{I}_w(g_n)) \circ \cdots \circ \mu_w(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}_1), \mathbb{I}_w(g_1)) \\
&= \mathbb{I}_{\mathsf{Q}}(\mu_w(\boldsymbol{\theta}_n, g_n)) \circ \cdots \circ \mathbb{I}_{\mathsf{Q}}(\mu_w(\boldsymbol{\theta}_1, g_1)) \\
&= \mathbb{I}_{\mathsf{Q}}(\mu_w(\boldsymbol{\theta}_1, g_1) \circ \cdots \circ \mu_w(\boldsymbol{\theta}_n, g_n)) \\
&\overset{(\mathrm{AB8})}{=} \mathbb{I}_{\mathsf{Q}}(\mu_w(\boldsymbol{\theta}_1 \cdots \boldsymbol{\theta}_n,\ g_1 \cdots g_n)) \\
&= \mathbb{I}_{\mathsf{Q}}(\mu_w(\boldsymbol{\theta}, g)).
\end{aligned}$$

(AB12): can be shown with a similar calculation. □

Recall that $\|s\| \geq 1$ implies that $\gamma_w(s)$ is either empty or a singleton set $\{\boldsymbol{\theta}\}$, see (b) in Lemma 30. In the latter case, we also use the (abusive) notations $\tau\mathrm{i}(s)$, $\tau\mathrm{e}(s)$, $\mathrm{Gi}(s)$, $\mathrm{Ge}(s)$, $\mu_w(s)$, and $\delta_w(s)$ for what should be denoted, in full rigor, by $\tau\mathrm{i}(\boldsymbol{\theta})$, $\tau\mathrm{e}(\boldsymbol{\theta})$, $\mathrm{Gi}(\boldsymbol{\theta})$, $\mathrm{Ge}(\boldsymbol{\theta})$, $\mu_w(\boldsymbol{\theta}, s)$, and $\delta_w(\boldsymbol{\theta}, s)$. Similarly, we write $\delta_w(a)$ for $\delta_w(\boldsymbol{\theta}, a)$, where $\boldsymbol{\theta} \in \gamma_w(a)$. Recall that the mapping $\delta_w(\boldsymbol{\theta}, a)$ is $c \mapsto a^{-1}ca$ $(c \in A)$ independently of which of the two path types $\boldsymbol{\theta} \in \gamma_w(a)$ we choose.

3.7 The AB-algebra $\mathbb{W}$

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

$$\{(cW, Wd) \mid W \in \mathcal{W}, (c, d) \in \delta_w(W)\} \tag{89}$$

We define the quotient monoid $\mathbb{W} = (\mathcal{W}^* * A * B)/_{\equiv}$.

Lemma 32. *For all $s \in \mathcal{W}^* * A * B$, all $\boldsymbol{\theta} \in \gamma_w(s)$, and all $(c, d) \in \delta_w(\boldsymbol{\theta}, s)$ we have $cs \equiv sd$.*

Proof. Assume that $s = g_1 g_2 \cdots g_n$ is (A, B)-reduced. We prove the lemma by induction on n. The cases $n = 0$ and $n = 1$ follow easily from the definition of δ_w and $\equiv$. Now assume that $n \geq 2$ and let $\boldsymbol{\theta} \in \gamma_w(s)$. Since $\gamma_w(s) \neq \emptyset$, s has to contain a symbol from $\mathcal{W}$. Hence, Lemma 30 implies that $\gamma_w(s) = \{\boldsymbol{\theta}\}$. Let $\boldsymbol{\theta} = (\theta, b, \theta')$.

Case 1. $g_1 = a \in A \setminus 1$, i.e. $s = as'$. We have $\delta_w(s) = \delta_w((\theta, 0, \theta), a) \circ \delta_w(s')$ and $\mathrm{Gi}(\boldsymbol{\theta}) = p_1(\theta) = A$. With $(c, d) \in \delta_w(s)$ we obtain $c \in \mathrm{Gi}(\boldsymbol{\theta}) = A$ and $(c, a') \in \delta_w((\theta, 0, \theta), a)$, $(a', d) \in \delta_w(s')$ for some $a' \in A$. Thus, $aa' = ca$ in A and $s'd \equiv a's'$ by induction. We get $sd = as'd \equiv aa's' = cas' = cs$. The case $g_1 \in B \setminus 1$ can be dealt analogously.

Case 2. $g_1 = W \in \mathcal{W}$, i.e. $s = Ws'$. We have $\delta_w(s) = \delta_w(W) \circ \delta_w(\boldsymbol{\theta}_2, s')$ and $\boldsymbol{\theta} = \boldsymbol{\theta}_1\boldsymbol{\theta}_2$ for some path types $\boldsymbol{\theta}_1$ and $\boldsymbol{\theta}_2$ with $\gamma_w(W) = \boldsymbol{\theta}_1$ and $\boldsymbol{\theta}_2 \in \gamma_w(s')$. Moreover, there exists some $c' \in \mathrm{Ge}(\boldsymbol{\theta}_1)$ such that $(c, c') \in \delta_w(W)$ and $(c', d) \in \delta_w(\boldsymbol{\theta}_2, s')$. Hence $cW \equiv Wc'$ and $c's' \equiv s'd$ by induction. We obtain $cs = cWs' = Wc's' \equiv Ws'd = sd$. □

Lemma 32 will provide the key-argument for proving Lemma 41 on the factorization of AB-homomorphisms.

Lemma 33. *The congurence $\equiv$ on $\mathcal{W}^* * A * B$ is compatible (see Definition 6) with the AB-algebra $\langle \mathcal{W}^* * A * B, \iota_A, \iota_B, \mathbb{I}_w, \gamma_w, \mu_w, \delta_w \rangle$.*

Proof. Let $u, u' \in \mathcal{W}^* * A * B$ with $u \equiv u'$, $a \in A$, and $b \in B$. According to Definition 6 we have to check the following statements:

(a) $u \in \mathrm{dom}(\mathbb{I}_w) \Leftrightarrow u' \in \mathrm{dom}(\mathbb{I}_w)$ and if $u, u' \in \mathrm{dom}(\mathbb{I}_w)$ then $\mathbb{I}_w(u) \equiv \mathbb{I}_w(u')$,
(b) For all $a, a' \in A$ and $b, b' \in B$: $a \equiv a' \Rightarrow a = a'$ and $b \equiv b' \Rightarrow b = b'$
(c) $\gamma_w(u) = \gamma_w(u')$
(d) For all $\boldsymbol{\theta} \in \gamma_w(u)$: $\mu_w(\boldsymbol{\theta}, u) = \mu_w(\boldsymbol{\theta}, u')$ and $\delta_w(\boldsymbol{\theta}, u) = \delta_w(\boldsymbol{\theta}, u')$.

Point (b) is obvious. For (a), (c), and (d), it suffices to consider only the case that $u = cW$ and $u' = Wd$, where $W \in \mathcal{W}$ and $(c, d) \in \delta_w(W)$. Let $W = (V, \epsilon, \boldsymbol{\theta}, r, \varphi)$. Thus, $(c, d) \in \varphi$.

(a) We have $cW \in \mathrm{dom}(\mathbb{I}_w) \iff W \in \mathrm{dom}(\mathbb{I}_w) \iff Wd \in \mathrm{dom}(\mathbb{I}_w)$. Moreover, if $W \in \mathrm{dom}(\mathbb{I}_w)$ then, since $(c, d) \in \delta_w(W) = \varphi$ we have $(d, c) \in \delta_w(\mathbb{I}_w(W)) = \varphi^{-1}$. Thus, $d\,\mathbb{I}_w(W) \equiv \mathbb{I}_w(W)c$, i.e., $\mathbb{I}_w(cW) = \mathbb{I}_w(W)c^{-1} \equiv d^{-1}\mathbb{I}_w(W) = \mathbb{I}_w(Wd)$.

(c) Since $c \in \mathrm{Gi}(\boldsymbol{\theta})$ and $d \in \mathrm{Ge}(\boldsymbol{\theta})$ we have

$$\gamma_w(cW) = \gamma_w(c)\gamma_w(W) = \{\boldsymbol{\theta}\} = \gamma_w(W)\gamma_w(d) = \gamma_w(Wd).$$

(d) The type $\boldsymbol{\theta}$ splits as $\boldsymbol{\theta} = (\theta, 0, \theta)\boldsymbol{\theta} = \boldsymbol{\theta}(\theta', 0, \theta')$, where $\theta = \tau\mathrm{i}(\boldsymbol{\theta})$ and $\theta' = \tau\mathrm{e}(\boldsymbol{\theta})$. We get:

$$\begin{aligned}
\mu_w(\boldsymbol{\theta}, cW) &\overset{(\mathrm{AB8})}{=} \mu_w((\theta,0,\theta), c) \circ \mu_w(\boldsymbol{\theta}, W) \\
&= \mu_t((\theta,0,\theta), c) \circ r \\
&\overset{(71)}{=} r \circ \mu_t((\theta',0,\theta'), d) \\
&= \mu_w(\boldsymbol{\theta}, W) \circ \mu_w((\theta',0,\theta'), d) \\
&\overset{(\mathrm{AB8})}{=} \mu_w(\boldsymbol{\theta}, Wd)
\end{aligned}$$

For the mapping δ_w, we have

$$\delta_w(\boldsymbol{\theta}, cW) = \delta_w((\theta,0,\theta), c) \circ \delta_w(W) = \delta_w((\theta,0,\theta), c) \circ \varphi$$

and similarly $\delta_w(\boldsymbol{\theta}, Wd) = \varphi \circ \delta_w((\theta',0,\theta'), d)$. Hence, we have to show that

$$\delta_w((\theta,0,\theta), c) \circ \varphi = \varphi \circ \delta_w((\theta',0,\theta'), d),$$

where $(c, d) \in \varphi$. Let us first check that the domains of the left and right hand side are equal. Since $c \in \mathrm{dom}(\varphi)$ and $\mathrm{dom}(\varphi)$ is a subgroup of $\mathrm{Gi}(\boldsymbol{\theta})$, we have

$$\begin{aligned}
x \in \mathrm{dom}(\delta_w((\theta,0,\theta), c) \circ \varphi) &\iff c^{-1}xc \in \mathrm{dom}(\varphi) \\
&\iff x \in \mathrm{dom}(\varphi) \\
&\iff x \in \mathrm{dom}(\varphi \circ \delta_w((\theta',0,\theta'), d)).
\end{aligned}$$

Now let $x \in \mathrm{dom}(\delta_w((\theta,0,\theta), c) \circ \varphi) = \mathrm{dom}(\varphi)$. Then, we have:

$$\begin{aligned}
(\delta_w((\theta,0,\theta), c) \circ \varphi)(x) &= \varphi(c^{-1}xc) \\
&= d^{-1}\varphi(x)d \\
&= (\varphi \circ \delta_w((\theta',0,\theta'), d))(x)
\end{aligned}$$

This proves the lemma. □

By the previous lemma, we can endow the monoid $\mathbb{W} = (\mathcal{W}^* * A * B)/_{\equiv}$ with the structure of an AB-algebra:

$$\langle \mathbb{W}, \iota_A, \iota_B, \mathbb{I}_w, \mu_w, \gamma_w, \delta_w \rangle \tag{90}$$

In addition $u \equiv v$ implies $\|u\| = \|v\|$ for all $u, v \in \mathcal{W}^* * A * B$, so that the notion of norm remains well-defined in the quotient $\mathbb{W}$.

3.8 The AB-algebras $\mathbb{W}_t$, $\mathbb{W}_{\mathbb{H}}$, and $\widehat{\mathbb{W}}$

Recall the definition of the subset $\widehat{\mathcal{W}} \subseteq \mathcal{W}$ from (72). Let us consider the set $\mathcal{W}_t$ consisting of all the letters $W \in \mathcal{W}$ fulfilling

$$\exists s \in \mathbb{H}_t \begin{cases} W \in \mathrm{dom}(\mathbb{I}_w) \iff s \in \mathrm{dom}(\mathbb{I}_t),\ \gamma_w(W) \subseteq \gamma_t(s) \\ \forall \boldsymbol{\theta} \in \gamma_w(W) : \mu_w(W) = \mu_t(\boldsymbol{\theta}, s),\ \delta_w(W) = \delta_t(\boldsymbol{\theta}, s). \end{cases} \tag{91}$$

Intuitively, it is the set of all symbols from $\mathcal{W}$ that can be realized by some concrete t-sequence. We also define the subset

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

Note that the sets $\mathcal{W}_t$, $\mathcal{W}_{\mathbb{H}}$, and $\widehat{\mathcal{W}}$ are closed under the involution $\mathbb{I}_w$. Hence, $\mathcal{W}_t^* * A * B$, $\mathcal{W}_{\mathbb{H}}^* * A * B$, and $\widehat{\mathcal{W}}^* * A * B$ are AB-subalgebras of $\mathcal{W}^* * A * B$ in the sense of Section 3.3. Clearly, $\equiv$ is also compatible with these AB-subalgebras and we can define the quotient AB-algebras

$$\mathbb{W}_t = (\mathcal{W}_t^* * A * B)/_{\equiv}, \quad \mathbb{W}_{\mathbb{H}} = (\mathcal{W}_{\mathbb{H}}^* * A * B)/_{\equiv}, \quad \widehat{\mathbb{W}} = (\widehat{\mathcal{W}}^* * A * B)/_{\equiv}.$$

Moreover, for all $s \in \mathcal{W}_t^* * A * B$ and $s' \in \mathcal{W}^* * A * B$, if $s \equiv s'$ then also $s' \in \mathcal{W}_t^* * A * B$, and similarly for $\mathcal{W}_{\mathbb{H}}^* * A * B$ and $\widehat{\mathcal{W}}^* * A * B$. Hence, $\mathbb{W}_t$, $\mathbb{W}_{\mathbb{H}}$, and $\widehat{\mathbb{W}}$ are AB-subalgebras of $\mathbb{W}$.

The AB-subalgebra $\mathbb{W}_t$ is important, when we consider AB-homomorphisms to $\mathbb{H}_t$: In general, there does not exist an AB-homomorphism from $\mathbb{W}$ to $\mathbb{H}_t$, but there exist AB-homomorphisms from $\mathbb{W}_t$ to $\mathbb{H}_t$.

3.9 Involutive automorphisms

We consider here special AB-automorphisms of $\mathbb{W}$ that occur naturally in the process of reducing equations in the HNN-extension $\mathbb{G}$ to equations in $\mathbb{W}$. Consider a partition

$$\widehat{\mathcal{W}} = \widehat{\mathcal{W}_0} \uplus \{W_1, \ldots, W_p\} \uplus \{\overline{W}_1, \ldots, \overline{W}_p\}, \tag{92}$$

where $\overline{W}_k = \mathbb{I}_w(W_k)$ for $1 \leq k \leq p$ and $\widehat{\mathcal{W}_0}$ is closed under the involution $\mathbb{I}_w$. Assume that

$$\mathrm{Gi}(W_k) = \mathrm{Ge}(W_k) = A_k \tag{93}$$

for $1 \leq k \leq p$. Moreover, let $a_k, b_k \in A_k$ for $1 \leq k \leq p$.

Lemma 34. *Let us consider a partition of $\widehat{\mathcal{W}}$ and a tuple of group elements $(a_1, b_1, \ldots, a_p, b_p)$ as above. Then, the following holds:*

(1) There exists some AB-homomorphism $\Phi : \mathbb{W} \to \mathbb{W}$ satisfying

$$\Phi(c) = c \text{ for } c \in A \cup B \quad \Phi(W) = W \quad \text{for all } W \in (\mathcal{W} \setminus \widehat{\mathcal{W}}) \cup \widehat{\mathcal{W}_0} \tag{94}$$

$$\Phi(\overline{W}_k) = a_k W_k b_k \quad \Phi(W_k) = a_k^{-1} \overline{W}_k b_k^{-1} \text{ for } 1 \leq k \leq p \tag{95}$$

if and only if, for every $1 \leq k \leq p$ we have

$$\delta_w(\overline{W}_k) = \delta_w(W_k)^{-1} = \delta_w(a_k) \circ \delta_w(W_k) \circ \delta_w(b_k) = \delta_w(a_k W_k b_k). \tag{96}$$

$$(b_k^{-1} a_k, a_k b_k^{-1}) \in \delta_w(W_k) \tag{97}$$

$$\gamma_w(W_k) = \mathbb{I}_{\mathcal{T}}(\gamma_w(W_k)) = \gamma_w(\overline{W}_k) \tag{98}$$

$$\mu_w(a_k W_k b_k) = \mathbb{I}_{\mathsf{Q}}(\mu_w(W_k)) = \mu_w(\overline{W}_k). \tag{99}$$

(2) Every AB-homomorphism $\Phi : \mathbb{W} \to \mathbb{W}$ satisfying (94) and (95) is an involutive AB-automorphism.

Proof. Let us first prove statement (2). Let $\Phi : \mathbb{W} \to \mathbb{W}$ be an AB-homomorphism satisfying (94) and (95). For every $1 \leq k \leq p$ we have

$$\Phi(\Phi(W_k)) = \Phi(a_k^{-1}\overline{W}_k b_k^{-1}) = a_k^{-1} a_k W_k b_k b_k^{-1} = W_k$$

and, similarly $\Phi(\Phi(\overline{W}_k)) = \overline{W}_k$. For all other generators $g \in \mathcal{W} \cup A \cup B$, we have $\Phi(g) = g$ and thus $\Phi(\Phi(g)) = g$. Hence, the map Φ is involutive i.e. $\Phi \circ \Phi = \mathrm{I}_{\mathbb{W}}$. This shows that Φ has an inverse (namely Φ), which is itself an AB-homomorphism. Thus Φ is an AB-automorphism.

Let us now prove statement (1). First, suppose that $\Phi : \mathbb{W} \to \mathbb{W}$ is an AB-homomorphism satisfying (94) and (95). By (2), we know that Φ is an involutive AB-automorphism. We prove (96)–(99) for all $1 \leq k \leq p$. Fix $1 \leq k \leq p$.
(96)**:** Let $(c, d) \in A_k \times A_k$. Recall that $\delta_w(a_k)$ is the mapping $x \mapsto a_k^{-1} x a_k$ (for $x \in A_k$) and $\delta_w(b_k)$ is the mapping $x \mapsto b_k^{-1} x b_k$ (for $x \in A_k$). The following calculation shows (96):

$$\begin{aligned}
(c, d) \in \delta_w(a_k) \circ \delta_w(W_k) \circ \delta_w(b_k) &\iff (a_k^{-1} c a_k, d) \in \delta_w(W_k) \circ \delta_w(b_k) \\
&\iff (a_k^{-1} c a_k, b_k d b_k^{-1}) \in \delta_w(W_k) \\
&\iff a_k^{-1} c a_k W_k \equiv W_k b_k d b_k^{-1} \\
&\iff c a_k W_k b_k \equiv a_k W_k b_k d \\
&\iff \Phi(c\overline{W}_k) = \Phi(\overline{W}_k d) \text{ in } \mathbb{W} \\
&\iff c\overline{W}_k = \overline{W}_k d \text{ in } \mathbb{W} \\
&\iff c\overline{W}_k \equiv \overline{W}_k d \\
&\iff (c, d) \in \delta_w(\overline{W}_k).
\end{aligned}$$

(97)**:** Since Φ preserves the involution $\mathbb{I}_w$ (axiom (Hom4)) we get

$$a_k W_k b_k = \Phi(\overline{W}_k) = \Phi(\mathbb{I}_w(W_k)) = \mathbb{I}_w(\Phi(W_k)) = \mathbb{I}_w(a_k^{-1}\overline{W}_k b_k^{-1}) = b_k W_k a_k$$

in $\mathbb{W}$, i.e., $a_k W_k b_k \equiv b_k W_k a_k$. This implies $b_k^{-1} a_k W_k \equiv W_k a_k b_k^{-1}$, i.e., $(b_k^{-1} a_k, a_k b_k^{-1}) \in \delta_w(W_k)$, which establishes (97).
(98)**:** Since $\Phi(W_k) = a_k^{-1}\overline{W}_k b_k^{-1}$ and Φ preserves γ_w (axiom (Hom5)), we get

$$\begin{aligned}
\gamma_w(W_k) &\overset{\text{(Hom5)}}{\subseteq} \gamma_w(a_k^{-1}\overline{W}_k b_k^{-1}) \\
&\overset{(80)}{=} \gamma_w(a_k^{-1})\gamma_w(\overline{W}_k)\gamma_w(b_k^{-1}) \\
&= \gamma_w(\overline{W}_k) \\
&\overset{\text{(AB10)}}{=} \mathbb{I}_{\mathcal{T}}(\gamma_w(W_k)).
\end{aligned}$$

Since the two extreme terms of this sequence of inclusions are singletons, they must be equal, which establishes (98).
(99)**:** Since $a_k W_k b_k = \Phi(\overline{W}_k)$ and Φ preserves μ_w (axiom (Hom6)) we get

$$\begin{aligned}
\mu_w(a_k W_k b_k) &\overset{\text{(Hom6)}}{=} \mu_w(\overline{W}_k) \\
&\overset{\text{(AB11)}}{=} \mathbb{I}_{\mathsf{Q}}(\mu_w(W_k)),
\end{aligned}$$

which establishes (99).

For the other direction, suppose that the letters W_k and the tuple $(a_1, b_1, \ldots, a_k, b_k)$ are fulfilling conditions (96)–(99). By the universal property of the free-product, there exists a unique monoid homorphism $\tilde{\Phi} : \mathcal{W}^* * A * B \to \mathcal{W}^* * A * B$ such that

$$\tilde{\Phi}(c) = c \text{ for } c \in A \cup B \quad \tilde{\Phi}(W) = W \quad \text{for all } W \in (\mathcal{W} \setminus \widehat{\mathcal{W}}) \cup \widehat{\mathcal{W}_0} \tag{100}$$

$$\tilde{\Phi}(\overline{W}_k) = a_k W_k b_k \quad \tilde{\Phi}(W_k) = a_k^{-1}\overline{W}_k b_k^{-1} \text{ for } 1 \le k \le p. \tag{101}$$

Let $1 \le k \le p$ and $(c, d) \in \delta_w(W_k)$. We first show that

$$\tilde{\Phi}(cW_k) \equiv \tilde{\Phi}(W_k d) \quad \text{and} \quad \tilde{\Phi}(d\overline{W}_k) \equiv \tilde{\Phi}(\overline{W}_k c). \tag{102}$$

This implies that $\tilde{\Phi}$ induces a monoid homomorphism on the quotient $\mathbb{W}$. We will only prove the equivalence $\tilde{\Phi}(cW_k) \equiv \tilde{\Phi}(W_k d)$, the other equivalence can be shown similarly. We have

$$\tilde{\Phi}(cW_k) = ca_k^{-1}\overline{W}_k b_k^{-1}, \quad \tilde{\Phi}(W_k d) = a_k^{-1}\overline{W}_k b_k^{-1} d.$$

Hence, we have to show that

$$a_k c a_k^{-1}\overline{W}_k \equiv \overline{W}_k b_k^{-1} d b_k. \tag{103}$$

Condition (96) implies

$$\delta_w(W_k) = \delta_w(b_k^{-1}\overline{W}_k a_k^{-1}).$$

Hence, with $(c, d) \in \delta_w(W_k)$ we get

$$cb_k^{-1}\overline{W}_k a_k^{-1} \equiv b_k^{-1}\overline{W}_k a_k^{-1} d. \tag{104}$$

Condition (97) implies $b_k^{-1} a_k W_k \equiv W_k a_k b_k^{-1}$. Thus, we have $\overline{W}_k a_k^{-1} b_k \equiv b_k a_k^{-1}\overline{W}_k$, i.e.,

$$b_k^{-1}\overline{W}_k a_k^{-1} \equiv a_k^{-1}\overline{W}_k b_k^{-1}. \tag{105}$$

From (104) and (105) we get $ca_k^{-1}\overline{W}_k b_k^{-1} \equiv a_k^{-1}\overline{W}_k b_k^{-1} d$, i.e., (103).

As remarked above, by (102) the monoid homomorphism $\tilde{\Phi} : \mathcal{W}^* * A * B \to \mathcal{W}^* * A * B$ induces a monoid homomorphism $\Phi : \mathbb{W} \to \mathbb{W}$. This monoid homomorphism satisfies (94) and (95).

The AB-algebra $\mathcal{W}^* * A * B$ fulfills hypotheses (A), (B), and (C) from Lemma 23 for the set of generators $\Gamma = \mathcal{W} \cup A \cup B$: (B) clearly holds and the decomposition for $s \in \mathbb{W}$ that has to exist according to (C) is obtained by writting s as an (A, B)-reduced product, see (80). By Lemma 25, also the quotient $\mathbb{W}$ satisfies (A), (B), and (C) from Lemma 23 for the set of generators Γ. Thus, in order to show that Φ is an AB-homomorphism, we just have to check that it meets conditions (a)–(f) from Lemma 23. Conditions (a) and (b) are clear.

Condition (c) amounts to

$$\forall 1 \le k \le p : b_k W_k a_k \equiv a_k W_k b_k \quad \text{and} \quad b_k^{-1}\overline{W}_k a_k^{-1} \equiv a_k^{-1}\overline{W}_k b_k^{-1}.$$

These properties follow from (97).

Condition (d) asserts that $\forall g \in \Gamma : \gamma_w(g) \subseteq \gamma_w(\Phi(g))$. This is clear if g is none of the generators W_k or $\overline{W}_k$ for $1 \le k \le p$. For $g = W_k$ we have to check that $\gamma_w(W_k) \subseteq \gamma_w(a_k^{-1}\overline{W}_k b_k^{-1})$. By (98) we have $\gamma_w(W_k) = \gamma_w(\overline{W}_k)$. Moreover, $a_k^{-1}, b_k^{-1} \in A_k = \mathrm{Gi}(\overline{W}_k) = \mathrm{Ge}(\overline{W}_k)$ implies $\gamma_w(a_k^{-1}\overline{W}_k b_k^{-1}) = \gamma_w(\overline{W}_k) = \gamma_w(W_k)$. For $g = \overline{W}_k$ we have to check that $\gamma_w(\overline{W}_k) \subseteq \gamma_w(a_k W_k b_k)$ which also follows also from (98).

Condition (e) is ensured by (99) and condition (f) is ensured by (96). □

Assume that we have a partition of $\widehat{\mathcal{W}}$ satisfying (92) and (93). Hence, by Lemma 34 every tuple $(a_1, b_1, \ldots, a_k, b_k, \ldots, a_p, b_p)$ with $a_k, b_k \in A_k$ fulfilling the four conditions (96)–(99) defines an AB-automorphism Φ through the $2k$ equations (95). In the next lemma we give some simple transformations of such tuples that preserve the defined automorphism Φ. These are the transformation

$$(a_k, b_k) \mapsto (b_k, a_k)$$

for some $k \in [1, p]$ as well as the transformation

$$(a_k, b_k) \mapsto (1, \varphi_k(a_k)b_k)$$

for some $k \in [1, p]$, where φ_k is a functional notation for the partial automorphism $\delta_w(W_k) : A_k \to A_k$. For the second transformation, we assume that $a_k \in \mathrm{dom}(\varphi_k)$.

Lemma 35. *Let us fix a partition partition of $\widehat{\mathcal{W}}$ satisfying* (92) *and* (93) *and a tuple $(a_1, b_1, \ldots, a_k, b_k, \ldots, a_p, b_p)$ with $a_k, b_k \in A_k$ fulfilling the four conditions* (96)–(99)*; thus defining an AB-automorphism Φ through equations* (95)*. Then,*

(1) the tuple $(a_1, b_1, \ldots, b_k, a_k, \ldots, a_p, b_p)$ also defines the AB-automorphism Φ and
(2) the tuple $(a_1, b_1, \ldots, 1, \varphi_k(a_k)b_k, \ldots, a_p, b_p)$ also defines the AB-automorphism Φ, provided that $a_k \in \mathrm{dom}(\varphi_k)$.

Proof. For point (1), we get $(b_k^{-1}a_k, a_k b_k^{-1}) \in \delta_w(W_k)$ by (97). Hence, $a_k W_k b_k = b_k W_k a_k$ and we have

$$\Phi(\overline{W_k}) \overset{(95)}{=} a_k W_k b_k = b_k W_k a_k.$$

Since Φ is compatible with $\mathbb{I}_w$ and $\Phi(\overline{W_k}) = a_k W_k b_k$ we also have

$$\Phi(W_k) = b_k^{-1}\overline{W_k}a_k^{-1}.$$

For point (2), assume that $a_k \in \mathrm{dom}(\varphi_k)$. Hence,

$$a_k W_k = W_k \varphi_k(a_k) \tag{106}$$

in $\mathbb{W}$. Moreover, $a_k \in \mathrm{dom}(\varphi_k)$ implies that

$$a_k \in \mathrm{dom}(\delta_w(a_k) \circ \varphi_k \circ \delta_w(b_k)) \overset{(96)}{=} \mathrm{dom}(\delta_w(\overline{W}_k)) = \mathrm{dom}(\varphi_k^{-1}).$$

Hence, also $a_k^{-1} \in \mathrm{dom}(\varphi_k^{-1})$ and we have

$$a_k^{-1}\overline{W}_k = \overline{W}_k \varphi_k^{-1}(a_k^{-1}). \tag{107}$$

We have to show that $\Phi(\overline{W_k}) = W_k\varphi_k(a_k)b_k$ and $\Phi(W_k) = \overline{W_k}(\varphi_k(a_k)b_k)^{-1}$. The first identity can be deduced as follows:

$$\Phi(\overline{W_k}) \overset{(95)}{=} a_k W_k b_k \overset{(106)}{=} W_k \varphi_k(a_k) b_k.$$

For the second identity, i.e., $\Phi(W_k) = \overline{W_k}(\varphi_k(a_k)b_k)^{-1}$, note that

$$\Phi(W_k) \overset{(95)}{=} a_k^{-1}\overline{W_k}b_k^{-1} \overset{(107)}{=} \overline{W_k}\varphi_k^{-1}(a_k^{-1})b_k^{-1} = \overline{W_k}(\varphi_k^{-1}(a_k))^{-1}b_k^{-1} = \overline{W_k}(b_k\varphi_k^{-1}(a_k))^{-1}$$

Hence, it suffices to show that $\varphi_k(a_k)b_k = b_k\varphi_k^{-1}(a_k)$. By (96), we know that $\varphi_k^{-1} = \delta_w(W_k)^{-1} = \delta_w(a_kW_kb_k) = \delta_w(a_k) \circ \delta_w(W_k) \circ \delta_w(b_k)$. Recall that $(\delta_w(a_k))(a) = a_k^{-1}aa_k$ for all $a \in A_k$ and similarly for b_k. Hence, we get

$$\begin{aligned} b_k\varphi_k^{-1}(a_k) &= b_k\ (\delta_w(a_kW_kb_k))(a_k) \\ &= b_k\ (\delta_w(W_kb_k))(a_k) \\ &= b_k\ (\delta_w(b_k))(\varphi_k(a_k)) \\ &= b_kb_k^{-1}\varphi_k(a_k)b_k \\ &= \varphi_k(a_k)b_k, \end{aligned}$$

as required. □

Note that condition (98) implies for all $1 \leq k \leq p$

$$\gamma_w(W_k) \in \{(A,T,1,A,H),(B,T,1,B,H),(A,H,0,A,T),(B,H,0,B,T),(1,H,0,1,1)\}, \tag{108}$$

since these are the only T-types and H-types with $\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}) = \boldsymbol{\theta}$.

Definition 8. *We denote by* HInv *(for $\mathbb{H}$-involutive automorphisms) the set of all AB-automorphisms Φ of the form* (94) *and* (95) *such that,*

$$\forall 1 \leq k \leq p : \gamma_w(W_k) \text{ is an H-type .} \tag{109}$$

Note that Lemma 34 ensures that the automorphisms from HInv are involutive.

For $\Phi \in$ HInv we denote with $\mathbb{W}/\Phi$ the AB-algebra obtained as the quotient $\mathbb{W}/\simeq_\Phi$ where $\simeq_\Phi$ is the monoid congruence over $\mathbb{W}$ generated by the set $\{(W,\Phi(W) \mid W \in \mathcal{W}\}$ (one can easily check that this monoid congruence is compatible with the AB-algebra $\mathbb{W}$). Alternatively, we can define $\mathbb{W}/\Phi$ as the quotient $(\mathcal{W}^* * A * B)/\equiv_\Phi$, where $\equiv_\Phi$ is the monoid congruence over $\mathcal{W}^* * A * B$ generated by the set $\{(cW,Wd) \mid W \in \mathcal{W}, (c,d) \in \delta_w(W)\} \cup \{(W,\Phi(W) \mid W \in \mathcal{W}\}$ (this monoid-congruence is compatible with the AB-algebra $\mathcal{W}^* * A * B$). In the same way, one can also define the quotient AB-algebra $\mathbb{W}_{\mathbb{H}}/\Phi$.

As noticed in the course of the above proof, the AB-algebra $\mathcal{W}^* * A * B$ fulfills hypotheses (A),(B) and (C) from Lemma 23 for the set of generators $\Gamma = \mathcal{W} \cup A \cup B$. By Lemma 25 the AB-algebras $\mathbb{W}$ and $\mathbb{W}/\Phi$ also satisfy these conditions (A),(B), and (C).

3.10 AB-homomorphisms on $\mathcal{W}^* * A * B$ and $\mathbb{W}$

Let us show here some properties of AB-homomorphisms on $\mathcal{W}^* * A * B$ or $\mathbb{W}$. Let $\mathcal{W}_0 \subseteq \mathcal{W}$ be some subset which is closed under $\mathbb{I}_w$, let $\mathbb{W}_0$ be the submonoid of $\mathbb{W}$ generated by $\mathcal{W}_0 \cup A \cup B$. This submonoid induces an AB-subalgebra of $\mathbb{W}$ (as defined in Section 3.2), which we denote again by $\mathbb{W}_0$.

Lemma 36. *Let $\psi : \mathbb{W} \to \mathbb{W}$ be an AB-homomorphism and let $s \in \mathbb{W}$ with $\|s\| \geq 1$. Then also $\|\psi(s)\| \geq 1$.*

Proof. It suffices to show that $\|\psi(W)\| \geq 1$ for all $W \in \mathcal{W}$. Assume that $\psi(W) \in A * B$. By (Hom5) we have $\emptyset \neq \gamma_w(W) \subseteq \gamma_w(\psi(W))$. Hence, $\gamma_w(\psi(W))$ contains an H-type (see (21) and (22)) or a T-type (see (24)). By point (d) from Lemma 30, $\psi(W)$ cannot contain a factor from $(A \setminus 1)(B \setminus 1)$ or $(B \setminus 1)(A \setminus 1)$. Hence, we have $\psi(W) \in A \cup B$. But then $\psi(W)$ does not posess an H-type or a T-type, see (77), (78), and (80). □

Lemma 37. *Let $\psi : \mathbb{W}_{\mathbb{H}} \to \mathbb{W}_t$ or $\psi : \mathbb{W}_{\mathbb{H}} \to \mathbb{W}_t/\Phi$ be an AB-homomorphism and let $W \in \mathcal{W}_{\mathbb{H}}$. Then $\|\psi(W)\| = 1$. Moreover, we must have $\psi : \mathbb{W}_{\mathbb{H}} \to \mathbb{W}_{\mathbb{H}}$ (resp., $\psi : \mathbb{W}_{\mathbb{H}} \to \mathbb{W}_{\mathbb{H}}/\Phi$).*

Proof. We only prove the statement for $\psi : \mathbb{W}_{\mathbb{H}} \to \mathbb{W}_t$; for $\psi : \mathbb{W}_{\mathbb{H}} \to \mathbb{W}_t/\Phi$ we can argue in the same way. Let $W \in \mathcal{W}_{\mathbb{H}}$. We must have $\|\psi(W)\| \geq 1$ by the argument from the previous proof. Moreover, $\gamma_w(W)$ is an H-type and $\gamma_w(\psi(W))$ must contain an H-type. If $\psi(W)$ contains a $\mathcal{W}$-symbol with a T-type, then $\gamma_w(\psi(W))$ cannot contain an H-type. If $\psi(W)$ contains two $\mathcal{W}$-symbols with an H-type, then $\gamma_w(\psi(W)) = \emptyset$. □

Lemma 38. *Let $\psi : \mathbb{W} \to \mathbb{W}$ be an AB-homomorphism. Then $\gamma_w(W) = \gamma_w(\psi(W))$.*

Proof. By Lemma 36, we have $\|\psi(W)\| \geq 1$, and hence $|\gamma_w(\psi(W))| \leq 1$ by Lemma 30(b). Since $\gamma_w(W) \subseteq \gamma_w(\psi(W))$ by (Hom5), we must have $\gamma_w(W) = \gamma_w(\psi(W))$. □

Lemma 39. *Let $\psi : \mathbb{W}_t \to \mathbb{H}_t$ be some AB-homomorphism. Let $P, S, P', S' \in \mathbb{W}_t$ such that the following holds:*

- $\gamma_w(P) = \gamma_w(P') \neq \emptyset$,
- $\gamma_w(S) \neq \emptyset \neq \gamma_w(S')$,
- $\gamma_w(PS) = \gamma_w(P'S') \neq \emptyset$
- $\psi(P) = \psi(P')$ *and* $\psi(PS) = \psi(P'S')$.

Then $\psi(S) = \psi(S')$ and $\gamma_w(S) = \gamma_w(S')$.

Proof. Let P, S, P', S' fulfill the hypothesis of the lemma. Since $\mathbb{H}_t$ is cancellative by Lemma 6, $\psi(PS) = \psi(P'S')$ and $\psi(P) = \psi(P')$ imply $\psi(S) = \psi(S')$.

We distinguish several cases according to whether the norm of P, P', S, S' is zero. Let us notice that, since $\gamma_w(P) = \gamma_w(P') \neq \emptyset$, either $\|P\| = \|P'\| = 0$ or $\|P\|, \|P'\| \geq 1$. We also notice that (P, S) and (P', S') play the same role in the above lemma. Therefore we only have to treat the following six cases.

Case 1: $\|P\| \geq 1, \|P'\| \geq 1, \|S\| \geq 1, \|S'\| \geq 1$.
Hence, by Lemma 30, $\gamma_w(P)$, $\gamma_w(P')$, $\gamma_w(S)$, and $\gamma_w(S')$ are all singleton sets. Since $\gamma_w(PS) = \gamma_w(P'S') \neq \emptyset$ and $\gamma_w(P) = \gamma_w(P')$, we must have

$$\tau\mathrm{i}(S) = \tau\mathrm{e}(P) = \tau\mathrm{e}(P') = \tau\mathrm{i}(S') \text{ and } \tau\mathrm{e}(S) = \tau\mathrm{e}(S').$$

Moreover, since $\psi(S) = \psi(S')$, we have $\gamma_w(S) \in \gamma_t(\psi(S)) = \gamma_t(\psi(S')) \ni \gamma_w(S')$. But all path types in $\gamma_t(\psi(S))$ have the same boolean component. Hence, the boolean components of $\gamma_w(S)$ and $\gamma_w(S')$ are equal as well, and $\gamma_w(S) = \gamma_w(S')$.

Case 2: $\|P\| \geq 1, \|P'\| \geq 1, \|S\| = \|S'\| = 0$.
Since $\gamma_w(S) \neq \emptyset \neq \gamma_w(S')$, we must have $S, S' \in A \cup B$. Moreover, the type $\gamma_w(P) = \gamma_w(P')$ is a singleton. Since $\gamma_w(PS) \neq \emptyset \neq \gamma_w(P'S')$, we must have $S \in \mathrm{Ge}(P) = \mathrm{Ge}(P') \ni S'$. Thus, $S, S' \in A$ or $S, S' \in B$. Since ψ must be injective on A and B (by (Hom2)) we have either $S, S' \in A \setminus 1$ or $S, S' \in B \setminus 1$, or $S = S' = 1$. Thus, we get $\gamma_w(S) = \gamma_w(S')$.

Case 3: $\|P\| \geq 1, \|P'\| \geq 1, \|S\| \geq 1, \|S'\| = 0$.
Thus, $\gamma_w(P)$, $\gamma_w(P')$, and $\gamma_w(S)$ are singeltons and $S' \in A \cup B$. Since $\psi(S) = \psi(S') \in A \cup B$, the boolean component of $\gamma_w(S) \in \gamma_t(\psi(S)) = \gamma_t(\psi(S'))$ is 0. Now, an inspection of the graph $\mathcal{B}_6$ from Figure 1 shows that there does not exist a non-empty product of H-types that starts

and ends in the same vertex type. Thus, $\|S\| \geq 1$ and the fact that the boolean component of $\gamma_w(S)$ is 0 imply $\tau\mathrm{e}(S) \neq \tau\mathrm{i}(S) = \tau\mathrm{e}(P)$. Thus,

$$\tau\mathrm{e}(S) \neq \tau\mathrm{e}(P). \tag{110}$$

Since $S' \in A \cup B$, we have $\tau\mathrm{i}(\boldsymbol{\theta}) = \tau\mathrm{e}(\boldsymbol{\theta})$ for every $\boldsymbol{\theta} \in \gamma_w(S')$. Hence,

$$\tau\mathrm{e}(P'S') = \tau\mathrm{e}(P'). \tag{111}$$

We also have $\gamma_w(PS) = \gamma_w(P'S') \neq \emptyset$ which implies that $\tau\mathrm{e}(S) = \tau\mathrm{e}(PS) = \tau\mathrm{e}(P'S')$. Hence, taking into account (111), we get

$$\tau\mathrm{e}(S) = \tau\mathrm{e}(P'). \tag{112}$$

But equations (110) and (112) entail that $\tau\mathrm{e}(P) \neq \tau\mathrm{e}(P')$ contradicting the hypothesis that $\gamma_w(P) = \gamma_w(P') \neq \emptyset$. 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 $\gamma_w(P) = \gamma_w(P')$ implies that

$$P, P' \in A \setminus \{1\} \text{ or } P, P' \in B \setminus \{1\} \text{ or } P = P' = 1.$$

Hence, $\gamma_w(S) = \gamma_w(PS) = \gamma_w(P'S') = \gamma_w(S')$, i.e. the conclusion of the lemma holds.

Case 5: $\|P\| = \|P'\| = 0, \|S\| \geq 1, \|S'\| = 0$.
Then $|\gamma_w(PS)| = 1$ while $|\gamma_w(P'S')| \in \{2, 6\}$. This contradicts the hypothesis $\gamma_w(PS) = \gamma_w(P'S')$. This case is thus impossible.

Case 6: $\|P\| = \|P'\| = 0, \|S\| = \|S'\| = 0$.
Then $P, P', S, S' \in A \cup B$. Since $\gamma_w(P) = \gamma_w(P')$, we have

$$P, P' \in A \setminus \{1\} \text{ or } P, P' \in B \setminus \{1\} \text{ or } P = P' = 1. \tag{113}$$

Case 6.1: $S \in A \setminus 1$ and $S' \in B \setminus 1$. With (113) this implies either $\gamma_w(P'S') = \emptyset$ or $\gamma_w(PS) = \emptyset$ or $\gamma_w(PS) \neq \gamma_w(P'S')$, which is a contradiction.

Case 6.2: $S, S' \in A$. Since $\psi(S) = \psi(S')$, we have $S = 1 \Leftrightarrow S' = 1$. We get $\gamma_w(S) = \gamma_w(S')$. All other subcases can be dealt analogously to Case 6.1 or 6.2. □

Lemma 40. *Let $\psi : \mathbb{W}_t \to \mathbb{H}_t$ be some AB-homomorphism. Let $Q \in \mathbb{W}_t, P', S' \in \mathbb{H}_t, \boldsymbol{\theta} \in \gamma_t(P'), \boldsymbol{\rho} \in \gamma_t(S')$ such that $\boldsymbol{\theta}$ is an H-type, $\boldsymbol{\theta\rho}$ is defined, $\gamma_w(Q) = \{\boldsymbol{\theta\rho}\}$ and $\psi(Q) = P'S'$. Then, there exist $P, S \in \mathbb{W}_t$ such that:*

$$Q = PS, \;\; \psi(P) = P', \;\; \gamma_w(P) = \{\boldsymbol{\theta}\}, \;\; \psi(S) = S', \;\; \boldsymbol{\rho} \in \gamma_w(S).$$

Proof. Let us consider $\psi, Q, P', S', \boldsymbol{\theta}, \boldsymbol{\rho}$ fulfilling the hypothesis of the lemma. Since $\gamma_w(Q) = \{\boldsymbol{\theta\rho}\}$ is a singleton set, $Q \in \mathbb{W}_t$ must contain a letter from $\mathcal{W}_t$, i.e. we can factorize Q as

$$Q = e_0 W_0 Q_1 \tag{114}$$

where $W_0 \in \mathcal{W}_t$ and $e_0 \in \mathrm{Gi}(W_0)$. We also have $Q_1 \in \mathbb{W}_t$. Since $\gamma_w(Q) \neq \emptyset$, (Hom5) implies that $\gamma_t(\psi(Q)) \neq \emptyset$. Recall that a t-sequence s is reduced if and only if $\gamma_t(s) \neq \emptyset$, see (64). It follows that $\psi(Q) = P'S'$ viewed as a $\sim$-equivalence class of t-sequences contains

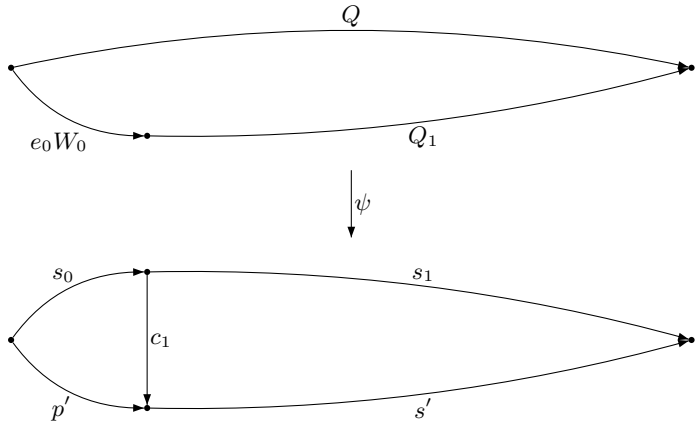


Fig. 4. Proof of Lemma 40

only reduced t-sequences. Since $P'S' = \psi(e_0W_0)\psi(Q_1)$, we can choose reduced t-sequences $s_0, s_1, p', s' \in \mathbb{H} * \{t, t^{-1}\}^*$ such that

$$\psi(e_0W_0) = [s_0]_\sim, \;\; \psi(Q_1) = [s_1]_\sim, \;\; P' = [p']_\sim, \;\; S' = [s']_\sim, \tag{115}$$

and s_0s_1 as well as $p's'$ are reduced, see Figure 4. Let $\gamma_w(W_0) = \{\boldsymbol{\theta_1}\}$. Thus, $\boldsymbol{\theta_1}$ is either an H-type or a T-type. We have

$$\{\boldsymbol{\theta\rho}\} = \gamma_w(Q) = \gamma_w(e_0W_0Q_1) = \gamma_w(W_0Q_1) = \{\boldsymbol{\theta_1}\}\gamma_w(Q_1). \tag{116}$$

Hence, we have $\tau\mathrm{i}(\boldsymbol{\theta}_1) = \tau\mathrm{i}(\boldsymbol{\theta})$. But since $\boldsymbol{\theta}$ is an H-type, also $\boldsymbol{\theta_1}$ must be an H-type. Moreover, $\boldsymbol{\theta} \in \gamma_t(P')$ and $\boldsymbol{\theta_1} \in \gamma_w(W_0) = \gamma_w(e_0W_0) \subseteq \gamma_t(\psi(e_0W_0)) = \gamma_t([s_0]_\sim)$ imply

$$p', s_0 \in \mathbb{H}. \tag{117}$$

Since $\boldsymbol{\theta}$ is an H-type and $\boldsymbol{\theta\rho}$ is defined, we can distinguish the following four cases for $\boldsymbol{\rho}$:

Case 1: $\boldsymbol{\rho}$ has the form $(*, T, 1, *, *)$.
Hence, (116) implies that the boolean component of the unique type in $\{\boldsymbol{\theta}_1\}\gamma_w(Q_1)$ must be 1. Since $\boldsymbol{\theta}_1$ is an H-type, i.e. its boolean component is 0, it follows that $\gamma_w(Q_1)$ contains a type with boolean component 1. But this is only possible if Q_1 contains a symbol from $\mathcal{W}_t$. Hence, by Lemma 30(b), $\gamma_w(Q_1)$ is a singleton set, i.e., $\gamma_w(Q_1) = \{\boldsymbol{\rho_1}\}$. It follows

$$\boldsymbol{\theta}_1\boldsymbol{\rho}_1 = \boldsymbol{\theta\rho}. \tag{118}$$

Since $\boldsymbol{\theta}_1$ is an H-type, $\boldsymbol{\rho}_1$ must be of the form $(*, T, 1, *, *)$.

Since $\boldsymbol{\rho} \in \gamma_t(s')$ and $\boldsymbol{\rho}_1 \in \gamma_w(Q_1) \subseteq \gamma_t(s_1)$ (by (Hom5)) and both types are of the form $(*, T, 1, *, *)$, we can choose the representatives s_1 and s' in such a way that they begin with the letter t or t^{-1}. This choice ensures that no $\mathbb{H}$-product takes place in the products s_0s_1 and $p's'$ in $\mathbb{H} * \{t, t^{-1}\}^*$. We know that $P'S' = \psi(Q) = \psi(e_0W_0Q_1)$, i.e. $p's' \sim s_0s_1$. Since all t-sequences are reduced and $s_0, p' \in \mathbb{H}$ by (117), there exists a connecting element c_1 such that a van Kampen diagram as in Figure 4 holds. In particular,

$$c_1 \in \mathrm{Ge}(\boldsymbol{\theta}), \;\; s_0c_1 \sim p', \;\; c_1s' \sim s_1. \tag{119}$$

Let us define

$$P = e_0 W_0 c_1 \quad \text{and} \quad S = c_1^{-1} Q_1. \tag{120}$$

We obtain from (114) and (120) that $Q = PS$. From (115), (119), and (120) we get $\psi(P) = \psi(e_0 W_0 c_1) = [s_0]_\sim c_1 = [p']_\sim = P'$ and $\psi(S) = \psi(c_1^{-1} Q_1) = c_1^{-1}[s_1]_\sim = [s']_\sim = S'$.

It remains to determine the types of P and S. Since $\boldsymbol{\rho} \in \gamma_t(s')$ and $\boldsymbol{\rho}_1 \in \gamma_t(s_1)$ and s' and s_1 both start with either t or t^{-1}, we must have $\tau\mathrm{i}(\boldsymbol{\rho}) = \tau(\boldsymbol{\rho}_1)$ (which is either (A,T) or (B,T)). Moreover, the boolean component of $\boldsymbol{\rho}$ and $\boldsymbol{\rho}_1$ is 1. Finally, by (118), $\tau\mathrm{e}(\boldsymbol{\rho}) = \tau\mathrm{e}(\boldsymbol{\theta}\boldsymbol{\rho}) = \tau\mathrm{e}(\boldsymbol{\rho}_1)$. This establishes that $\boldsymbol{\rho}_1 = \boldsymbol{\rho}$. Using (118) we know that $\boldsymbol{\theta}_1$ and $\boldsymbol{\theta}$ have same initial vertex type. Moreover, $\boldsymbol{\rho}_1 = \boldsymbol{\rho}$ implies that also the ending vertex types of $\boldsymbol{\theta}_1$ and $\boldsymbol{\theta}$ coincide. Finally, since they are H-types, they also have the same boolean component, namely 0. Hence $\boldsymbol{\theta}_1 = \boldsymbol{\theta}$. We get $\gamma_w(P) = \gamma_w(e_0 W_0 c_1) = \gamma_w(W_0) = \{\boldsymbol{\theta}_1\} = \{\boldsymbol{\theta}\}$ and $\gamma_w(S) = \gamma_w(c_1^{-1} Q_1) = \gamma_w(Q_1) = \{\boldsymbol{\rho_1}\} = \{\boldsymbol{\rho}\}$.

Case 2: $\boldsymbol{\rho} = (A, T, 0, A, T)$.
Since $\boldsymbol{\rho} = (A, T, 0, A, T) \in \gamma_t(S')$, we have $S' = a \in A$. Hence, we can set $S = a$ and $P = Qa^{-1}$. Thus, $\psi(S) = a = S'$ and $\psi(P)a = \psi(P)\psi(S) = \psi(PS) = \psi(Q) = P'S' = P'a$ implies $\psi(P) = P'$. Since $\boldsymbol{\theta}\boldsymbol{\rho}$ is defined, the H-type $\boldsymbol{\theta}$ must have the form $(*, *, 0, A, T)$. Hence $\gamma_w(P) = \gamma_w(Qa^{-1}) = \gamma(Q) = \{\boldsymbol{\theta}\boldsymbol{\rho}\} = \{\boldsymbol{\theta}\}$ and $\boldsymbol{\rho} = (A, T, 0, A, T) \in \gamma_w(a) = \gamma_w(S)$.

Case 3: $\boldsymbol{\rho} = (B, T, 0, B, T)$.
This case can be treated in the same way as Case 2.

Case 4: $\boldsymbol{\rho} = (1, 1, 0, 1, 1)$.
Hence $S' = 1$. The choice $S = 1$ and $P = Q$ fulfills the conclusion of the lemma. □

In the following, $\pi_\equiv : \mathcal{W}^* * A * B \to \mathbb{W}$ denotes the canonical homomorphism that maps $s \in \mathcal{W}^* * A * B$ to its equivalence class w.r.t. $\equiv$. The statements of the following four lemmas are visualized in Figure 5.

Lemma 41 (factorization). *Let $\psi' : \mathcal{W}^* * A * B \to \mathbb{W}$ be some AB-homomorphism. Then, there exists a unique AB-homomorphism $\psi : \mathbb{W} \to \mathbb{W}$ such that $\pi_\equiv \circ \psi = \psi'$.*

Proof. Since ψ' is an AB-homomorphism, for every $W \in \mathcal{W}$ we have $\delta_w(W) = \delta_w(\psi'(W))$. We claim that the congruence $\equiv$ is contained in the kernel of the homomorphism ψ': Consider a pair $(c, d) \in \delta_w(W)$ (i.e, $cW \equiv Wd$). Thus $(c, d) \in \delta_w(\psi'(W))$, i.e., $\psi'(cW) = c\psi'(W) = \psi'(W)d = \psi'(Wd)$ by Lemma 32. Therefore (cW, Wd) belongs to the kernel of ψ'. It follows that there exists a monoid homomorphism $\psi : \mathbb{W} \to \mathbb{W}$ with $\pi_\equiv \circ \psi = \psi'$. By Lemma 24, ψ is in fact an AB-homomorphism. Unicity of ψ follows directly from the requirement that $\psi([s]_\equiv) = \psi'(s)$ for all $s \in \mathcal{W}^* * A * B$. □

Lemma 42 (quotient). *Let $\sigma' : \mathcal{W}^* * A * B \to \mathcal{W}^* * A * B$ be some AB-homomorphism. Then, there exists a unique AB-homomorphism $\sigma : \mathbb{W} \to \mathbb{W}$ such that $\pi_\equiv \circ \sigma = \sigma' \circ \pi_\equiv$.*

Proof. Applying Lemma 41 to the AB-homomorphism $\psi' = \sigma' \circ \pi_\equiv$ we obtain this lemma. □

Lemma 43 (lifting). *Let $\psi' : \mathcal{W}^* * A * B \to \mathbb{W}$ be some AB-homomorphism. Then, there exists an AB-homomorphism $\psi : \mathcal{W}^* * A * B \to \mathcal{W}^* * A * B$ such that $\psi' = \psi \circ \pi_\equiv$.*

Proof. Choose a partition $\widehat{\mathcal{W}} = \widehat{\mathcal{W}}_1 \cup \widehat{\mathcal{W}}_2$ such that $\widehat{\mathcal{W}}_1 \cap \widehat{\mathcal{W}}_2 = \emptyset$ and $\{\mathbb{I}_w(W) \mid W \in \widehat{\mathcal{W}}_1\} = \widehat{\mathcal{W}}_2$. Since $\mathbb{I}_w(W) \neq W$ for all $W \in \widehat{\mathcal{W}}$, such a partition exists. Let us consider some map $\psi : (\mathcal{W} \cup A \cup B) \to \mathcal{W}^* * A * B$ such that for all $a \in A$, $b \in B$, and $W \in \mathcal{W} \setminus \widehat{\mathcal{W}}_2$:

$$\psi(a) = a, \quad \psi(b) = b, \quad \psi(W) \in \pi_{\equiv}^{-1}(\psi'(W)). \tag{121}$$

Moreover, for $W \in \widehat{\mathcal{W}}_2$ we set

$$\psi(W) = \mathbb{I}_w(\psi(\mathbb{I}_w(W))). \tag{122}$$

Since $\pi_{\equiv}$ and ψ' are AB-homomorphisms, this implies

$$\pi_{\equiv}(\psi(W)) = \pi_{\equiv}(\mathbb{I}_w(\psi(\mathbb{I}_w(W)))) = \mathbb{I}_w(\pi_{\equiv}(\psi(\mathbb{I}_w(W)))) = \mathbb{I}_w(\psi'(\mathbb{I}_w(W))) = \psi'(W)$$

for all $W \in \widehat{\mathcal{W}}_2$. Hence, together with (121), we get

$$\pi_{\equiv}(\psi(W)) = \psi'(W) \text{ for all } W \in \mathcal{W}. \tag{123}$$

Also notice that (122) implies

$$\mathbb{I}_w(\psi(W)) = \psi(\mathbb{I}_w(W)) \text{ for all } W \in \widehat{\mathcal{W}}. \tag{124}$$

By the universal property of the free product, ψ can be extended to a monoid homomorphism $\psi : \mathcal{W}^* * A * B \to \mathcal{W}^* * A * B$. Since $\pi_{\equiv}(\psi(g)) = \psi'(g)$ for all $g \in \mathcal{W} \cup A \cup B$, we have $\psi' = \psi \circ \pi_{\equiv}$.

It remains to show that ψ is in fact an AB-homomorphism. For this, we check conditions (a)–(f) from Lemma 23. Property (a) is obvious. For (b)–(f), assume that $g \in \mathcal{W} \cup A \cup B$. For $g \in A \cup B$, we have $\psi(g) = g$ and (b)–(f) are obvious. Thus, assume that $g = W \in \mathcal{W}$. For (b), we get:

$$\begin{aligned} W \in \mathrm{dom}(\mathbb{I}_w) &\overset{(\mathrm{Hom3})}{\iff} \psi'(W) \in \mathrm{dom}(\mathbb{I}_w) \\ &\iff \pi_{\equiv}(\psi(W)) \in \mathrm{dom}(\mathbb{I}_w) \\ &\overset{(\mathrm{Hom3})}{\iff} \psi(W) \in \mathrm{dom}(\mathbb{I}_w). \end{aligned}$$

Property (c) is stated in (124). Property (d) follows from

$$\begin{aligned} \gamma_w(W) &\overset{(\mathrm{Hom5})}{\subseteq} \gamma_w(\psi'(W)) \\ &= \gamma_w(\pi_{\equiv}(\psi(W))) \\ &\overset{(60)}{=} \gamma_w(\psi(W)). \end{aligned}$$

Finally, (e) and (f) follow directly from the preservation of the μ- and δ-mappings by ψ' and $\pi_{\equiv}$. Hence, ψ is indeed an AB-homomorphism. □

Lemma 44 (inverse image). *Let $\sigma : \mathbb{W} \to \mathbb{W}$ be some AB-homomorphism. Then, there exists an AB-homomorphism $\sigma' : \mathcal{W}^* * A * B \to \mathcal{W}^* * A * B$ such that $\pi_{\equiv} \circ \sigma = \sigma' \circ \pi_{\equiv}$.*

Proof. Applying Lemma 43 to the AB-homomorphism $\psi' = \pi_{\equiv} \circ \sigma$, we obtain this lemma. □

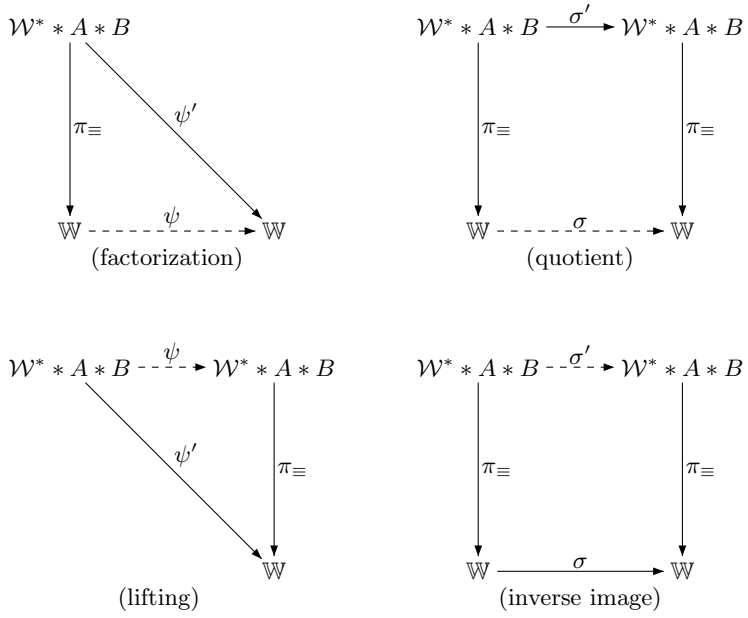


Fig. 5. AB-homomorphisms

4 Systems over $\mathbb{G}$: normalisation

Let us consider a system $(\mathcal{S}, \mathsf{C})$ of equations and disequations over the HNN-extension $\mathbb{G}$ with variables from $\mathcal{U}$ and rational constraints, see Section 2.6. By Proposition 2 we can assume that $\mathcal{S}$ is quadratic. Recall that $\mathsf{C} : \mathcal{U} \to \mathsf{bool}(\mathsf{Rat}(\mathbb{G}))$. By Proposition 1, for every variable $U \in \mathcal{U}$ one can construct a strict normal partitioned fta $\mathcal{A}_U$ over the labelling set $\mathsf{bool}(\mathsf{Rat}(\mathbb{H}))$ such that

$$\mathsf{C}(U) = \pi_{\mathbb{G}}(\mathrm{L}(\mathcal{A}_U)).$$

Let $\mathcal{A}$ be the direct product of all the fta $\mathcal{A}_U$ for $U \in \mathcal{U}$ and let Q be the set of states of $\mathcal{A}$. This fta $\mathcal{A}$ is partitioned, strict (this is straightforward from the definitions) and normal (by Lemma 17). Moreover, for every $U \in \mathcal{U}$, there exist $\mathsf{I}_U \subseteq \mathsf{Q}$ and $\mathsf{T}_U \subseteq \mathsf{Q}$ such that

$$\mathsf{C}(U) = \{g \in \mathbb{G} \mid (\mathsf{I}_U \times \mathsf{T}_U) \cap \mu_{\mathcal{A},\mathbb{G}}(g) \neq \emptyset\}$$

(recall the definition of the mapping $\mu_{\mathcal{A},\mathbb{G}}$ from (47)). Let us define, for every $U \in \mathcal{U}$, the set of binary relations $\mathsf{B}(U) \subseteq \mathsf{B}(\mathsf{Q})$ by:

$$\mathsf{B}(U) = \{\rho \in \mathsf{B}(\mathsf{Q}) \mid (\mathsf{I}_U \times \mathsf{T}_U) \cap \rho \neq \emptyset\}.$$

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

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

Let us define

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

Since $\mathsf{B}(U)$ is upwards-closed, we have:

$$(\mu \in M(\mathsf{C}) \text{ and } \forall U \in \mathcal{U} : \mu(U) \subseteq \mu'(U)) \quad \Longrightarrow \quad \mu' \in M(\mathsf{C}). \tag{125}$$

We can now express the initial system $(\mathcal{S}, \mathsf{C})$ of equations and disequations with rational constraints as a finite disjunction

$$\bigvee_{\mu \in M(\mathsf{C})} (\mathcal{S}, \mu_{\mathcal{A},\mathbb{G}}, \mu). \tag{126}$$

A solution of the system $(\mathcal{S}, \mu_{\mathcal{A},\mathbb{G}}, \mu)$ is now any monoid homomorphism $\sigma : \mathcal{U}^* \to \mathbb{G}$ such that the following holds:

$$\forall (u = u') \in \mathcal{S} : \ \sigma(u) = \sigma(u') \tag{127}$$
$$\forall (u \neq u') \in \mathcal{S} : \ \sigma(u) \neq \sigma(u') \tag{128}$$
$$\forall U \in \mathcal{U} : \ \mu_{\mathcal{A},\mathbb{G}}(\sigma(U)) = \mu(U). \tag{129}$$

Any solution of a system $(\mathcal{S}, \mu_{\mathcal{A},\mathbb{G}}, \mu)$ for some $\mu \in M(\mathsf{C})$ is a solution of the disjunction (126). An *over*-solution of the system $(\mathcal{S}, \mu_{\mathcal{A},\mathbb{G}}, \mu)$ is any monoid homomorphism $\sigma : \mathcal{U}^* \to \mathbb{G}$ fulfilling the above conditions (127) and (128) together with the condition

$$\forall U \in \mathcal{U} : \mu_{\mathcal{A},\mathbb{G}}(\sigma(U)) \supseteq \mu(U). \tag{130}$$

By condition (125), any over-solution of a system $(\mathcal{S}, \mu_{\mathcal{A},\mathbb{G}}, \mu)$ for some $\mu \in M(\mathsf{C})$ is a solution of the disjunction (126). We have thus proved the following proposition.

Proposition 5. *Given a system $(\mathcal{S}, \mathsf{C})$ of equations and disequations over $\mathbb{G}$ with variables $\mathcal{U}$ and rational constraints, one can compute a finite family of systems $(\mathcal{S}', \mu_{\mathcal{A},\mathbb{G}}, \mu_j)$ $(j \in J)$ such that the following holds:*

(a) $\mathcal{S}'$ is a quadratic system of equations and disequations with variables $\mathcal{V} \supseteq \mathcal{U}$.
(b) $\mu_{\mathcal{A},\mathbb{G}}$ is the map associated with a strict normal partitioned fta $\mathcal{A}$ over the labelling set $\mathsf{bool}(\mathsf{Rat}(\mathbb{H}))$ (see (47)).
(c) μ_j is a map $\mu_j : \mathcal{V} \to \mathsf{B}(\mathsf{Q}_{\mathcal{A}})$
(d) Every solution $\sigma : \mathcal{U}^* \to \mathbb{G}$ of $(\mathcal{S}, \mathsf{C})$ extends to a solution $\sigma' : \mathcal{V}^* \to \mathbb{G}$ of $\bigvee_{j \in J}(\mathcal{S}', \mu_{\mathcal{A},\mathbb{G}}, \mu_j)$.
(e) For every solution $\sigma' : \mathcal{V}^* \to \mathbb{G}$ of $\bigvee_{j \in J}(\mathcal{S}', \mu_{\mathcal{A},\mathbb{G}}, \mu_j)$, the restriction of σ' to $\mathcal{U}^*$ is a solution of $\mathcal{S}$.
(f) Every over-solution of $\bigvee_{j \in J}(\mathcal{S}', \mu_{\mathcal{A},\mathbb{G}}, \mu_j)$ is again a solution of $\bigvee_{j \in J}(\mathcal{S}', \mu_{\mathcal{A},\mathbb{G}}, \mu_j)$.

Moreover, if $\mathcal{S}$ is a system of equations (without disequations), then $\mathcal{S}'$ is a system of equations (without disequations).

A disjunction of systems $\bigvee_{j \in J}(\mathcal{S}', \mu_{\mathcal{A},\mathbb{G}}, \mu_j)$ that satisfies (a), (b), and (c) from Proposition 5 is said to be in *quadratic normal form*. If the disjunction moreover satisfies (f), then it 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 set

$$\mathcal{S} \subseteq \mathbb{W} \times \mathbb{W} \tag{131}$$

such that for all $(w, w') \in \mathcal{S}$ we have $\gamma_w(w) = \gamma_w(w') \neq \emptyset$. A *solution* of $\mathcal{S}$ is any AB-homomorphism $\psi : \mathbb{W}_t \to \mathbb{H}_t$ such that:

$$\forall (w, w') \in \mathcal{S} : \psi(w) = \psi(w'). \tag{132}$$

Note, that $\mathcal{S}$ can be only *solvable* if $\mathcal{S} \subseteq \mathbb{W}_t \times \mathbb{W}_t$. Moreover, notice that here the rational constraints are replaced by the even more restrictive conditions that define the notion of AB-homomorphism: besides preservation of the μ-map, the homomorphism ψ must also preserve $\mathbb{I}$, γ and δ.

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

Let us start with a system

$$\mathcal{S} = (\{(u_i = u'_i) \mid 1 \leq i \leq n\},\ \mu_{\mathcal{A},\mathbb{G}},\ \mu_{\mathcal{U}}) \tag{133}$$

of equations over $\mathbb{G}$ with variables $\mathcal{U}$ and rational constraints, which is in quadratic normal form (see Proposition 5). Assume that $u_i = U_{i,1}$ and $u'_i = U_{i,2}U_{i,3}$ with $U_{i,1}, U_{i,2}, U_{i,3} \in \mathcal{U}$ for $1 \leq i \leq n$. In the following we denote the interval $\{1, \ldots, m\}$ with $[1, m]$.

We define 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 $\pi_{\mathbb{G}} : \mathrm{Red}(\mathbb{H}, t)/_{\sim} \to \mathbb{G}$ 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 $\mathrm{Red}(\mathbb{H}, t)/_{\sim}$ that we must deal with.

Let us consider the alphabets

$$\mathcal{V}_0 = [1, n] \times [1, 3] \times [1, 5] \times [0, N_0] \tag{134}$$

and the alphabet $\mathcal{W}$ constructed from this set $\mathcal{V}_0$ in Section 3.6. We choose the integer N_0 in (134) in such a way that

$$\mathrm{Card}(\{W \in \mathcal{W} \mid \exists i, j, k : p_1(W) = (i, j, k, 0)\}) < \frac{1}{2}\mathrm{Card}(\mathcal{V}_0). \tag{135}$$

One can take, for example, $N_0 = 2 \cdot \mathrm{Card}(\{-1, 0, 1\} \times \mathcal{T}_{HT} \times \mathsf{B}^2(\mathsf{Q}) \times \mathrm{PGI}\{A, B\})$ in order to achieve this inequality. We consider all $15n$-tuples $\boldsymbol{W} = (W_{i,j,k})_{(i,j,k,0)\in\mathcal{V}_0}$ with $W_{i,j,k} \in \mathcal{W} \cup \{1\}$ and all $3n$-tuples $\boldsymbol{e} = (e_{i,1,2}, e_{i,2,3}, e_{i,3,1})_{1\leq i\leq n}$ with $e_{i,j,k} \in A \cup B$ such that the conditions in Figure 6 hold. A vector $(\boldsymbol{W}, \boldsymbol{e})$ fulfilling all the properties (136)-(147) is called an *admissible* vector. For every admissible vector $(\boldsymbol{W}, \boldsymbol{e})$ we define for all $1 \leq i, i' \leq n, 1 \leq j, j' \leq 3$ the

$$W_{i,j,3} \in \mathcal{W} \wedge \gamma_w(W_{i,j,3}) \text{ is an H-type} \tag{136}$$

$$p_1(W_{i,j,k}) = (i,j,k,0) \in \mathcal{V}_0 \text{ if } W_{i,j,k} \in \mathcal{W} \tag{137}$$

$$\gamma_w(\prod_{k=1}^{5} W_{i,j,k}) \in \{(1,H,b,1,1) \mid b \in \{0,1\}\} \tag{138}$$

$$\gamma_w(\prod_{k=1}^{5} W_{i,j,k}) = \gamma_w(\prod_{k=1}^{5} W_{i',j',k}) \text{ if } U_{i,j} = U_{i',j'} \tag{139}$$

$$\gamma_w(W_{i,1,1}W_{i,1,2}) = \gamma_w(W_{i,2,1}W_{i,2,2}) \tag{140}$$

$$\gamma_w(W_{i,1,4}W_{i,1,5}) = \gamma_w(W_{i,3,4}W_{i,3,5}) \tag{141}$$

$$\gamma_w(W_{i,2,4}W_{i,2,5}) = \gamma_w(\mathbb{I}_w(W_{i,3,2})\mathbb{I}_w(W_{i,3,1})) \tag{142}$$

$$e_{i,1,2} \in \mathrm{Gi}(W_{i,1,3}) = \mathrm{Gi}(W_{i,2,3}) \tag{143}$$

$$e_{i,2,3} \in \mathrm{Ge}(W_{i,2,3}) = \mathrm{Gi}(W_{i,3,3}) \tag{144}$$

$$e_{i,3,1} \in \mathrm{Ge}(W_{i,3,3}) = \mathrm{Ge}(W_{i,1,3}) \tag{145}$$

$$p_1(\mu_w(\prod_{k=1}^{5} W_{i,j,k})) = \mu_{\mathcal{U}}(U_{i,j}) \tag{146}$$

$$W_{i,2,k} \in \widehat{\mathcal{W}} \cup \{1\} \ni W_{i,3,6-k} \text{ for } 4 \leq k \leq 5 \tag{147}$$

Fig. 6. Conditions for an admissible vector

following equations:

$$\prod_{k=1}^{5} W_{i,j,k} = \prod_{k=1}^{5} W_{i',j',k} \text{ if } U_{i,j} = U_{i',j'} \tag{148}$$

$$W_{i,1,1}W_{i,1,2}e_{i,1,2} = W_{i,2,1}W_{i,2,2} \tag{149}$$

$$W_{i,2,4}W_{i,2,5} = e_{i,2,3}\mathbb{I}_w(W_{i,3,2})\mathbb{I}_w(W_{i,3,1}) \tag{150}$$

$$e_{i,3,1}W_{i,1,4}W_{i,1,5} = W_{i,3,4}W_{i,3,5} \tag{151}$$

$$W_{i,1,3} = e_{i,1,2}W_{i,2,3}e_{i,2,3}W_{i,3,3}e_{i,3,1} \tag{152}$$

Equations (149)–(152) correspond to a decomposition of the planar diagram associated with the $\mathbb{G}$-relation $U_{i,1} = U_{i,2}U_{i,3}$ into four pieces, as indicated in Figure 7. Equation (148) expresses the fact that some variables from $\mathcal{U}$ are common to several equations of $\mathcal{S}$.

We denote by $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ the set of equations (148)-(151) and by $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ the set of equations (152). For every $(i,j) \in [1,n] \times [1,3]$ we denote by $\overline{i,j}$ the lexicographically smallest

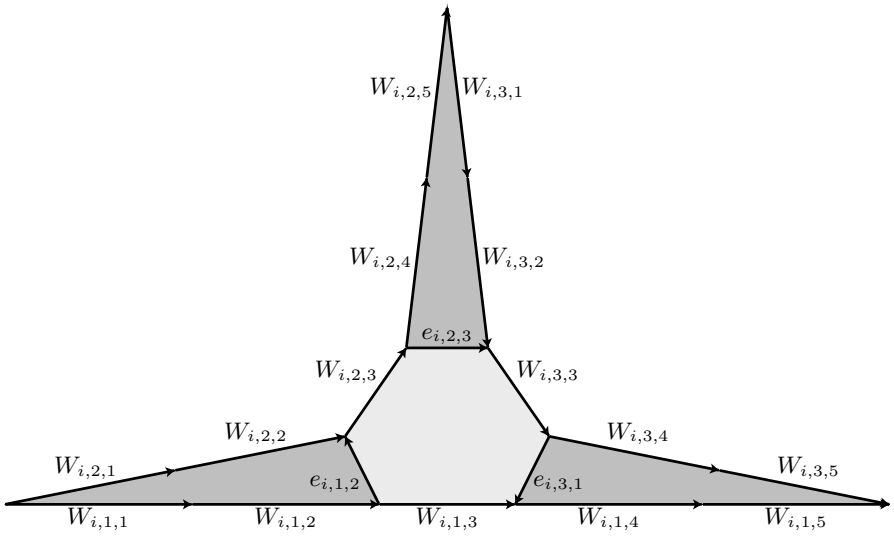


Fig. 7. Equation cut into 4 pieces

pair such that $U_{i,j} = U_{\overline{i,j}}$. By $\sigma_{\boldsymbol{W},\boldsymbol{e}} : \mathcal{U}^* \to \mathbb{W}$ we denote the unique monoid homomorphism such that

$$\sigma_{\boldsymbol{W},\boldsymbol{e}}(U_{i,j}) = \prod_{k=1}^{5} W_{\overline{i,j},k}. \tag{153}$$

Notice that, by the conditions imposed through the notion of an admissible vector, the system of equations $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ is really a system of t-equations, while some of the right-hand sides of the equations from $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ might have an empty image by γ_w.

Lemma 45. *A monoid homomorphism*

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

is a solution of the system (133) if and only if there exists an admissible vector $(\boldsymbol{W}, \boldsymbol{e})$ *and an AB-homomorphism* $\sigma_t : \mathbb{W}_t \to \mathbb{H}_t$ *such that:*

- *All components of* $(\boldsymbol{W}, \boldsymbol{e})$ *belong to* $\mathcal{W}_t \cup A \cup B$.
- σ_t *solves both systems* $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ *and* $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$.
- $\sigma = \sigma_{\boldsymbol{W},\boldsymbol{e}} \circ \sigma_t \circ \pi_{\mathbb{G}}$

Here, we denote by $\pi_{\mathbb{G}} : \mathbb{H}_t \to \mathbb{G}$ the canonical projection, see Figure 8. We prove this lemma in the following two subsections.

From $\mathbb{G}$-solutions to t-solutions. Let $\sigma : \mathcal{U}^* \to \mathbb{G}$ be a monoid homomorphism solving the system $(\{(U_{i,1} = U_{i,2}U_{i,3}) \mid 1 \le i \le n\},\ \mu_{\mathcal{A},\mathbb{G}},\ \mu_{\mathcal{U}})$ of equations over $\mathbb{G}$ with variables $\mathcal{U}$ and rational constraints ($U_{i,1}, U_{i,2}, U_{i,3} \in \mathcal{U}$ for $1 \le i \le n$). Let us fix some integer $1 \le i \le n$ and the corresponding equation $U_{i,1} = U_{i,2}U_{i,3}$. We construct the vectors $(W_{i,*,*}), (e_{i,*,*})$ corresponding to this equation. Let us choose for every $j \in [1,3]$ some $s_{i,j} \in \mathrm{Red}(\mathbb{H}, t)$ such that $\sigma(U_{i,j}) = \pi_{\mathbb{G}}(s_{i,j})$. This ensures that (where $\approx$ is the congruence defined in (2)–(4))

$$s_{i,1} \approx s_{i,2}s_{i,3} \text{ for all } 1 \le i \le n, \text{ and}$$
$$p_1(\mu_t((1, H, \|s_{i,j}\|_b, 1, 1), s_{i,j})) \overset{(62)}{=} \mu_{\mathcal{A},1}((1, H, \|s_{i,j}\|_b, 1, 1), s_{i,j}) \overset{(47)}{=} \mu_{\mathcal{A},\mathbb{G}}(\sigma(U_{i,j})) \overset{(129)}{=} \mu_{\mathcal{U}}(U_{i,j}).$$

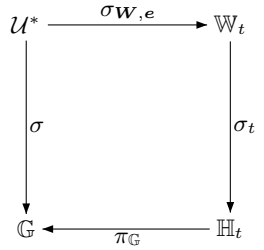


Fig. 8. Lemma 45

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

$$s_{i,2} = h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_\lambda} h_\lambda \cdots t^{\alpha_\ell} h_\ell, \tag{154}$$

$$s_{i,3} = k_0 t^{\beta_1} k_1 \cdots t^{\beta_\rho} k_\rho \cdots t^{\beta_m} k_m. \tag{155}$$

There exist integers $\lambda \in [1, \ell+1]$ and $\rho \in [0, m]$ such that $\rho = \ell - \lambda + 1$,

$$\alpha_\lambda + \beta_\rho = 0, \tag{156}$$

$$t^{\alpha_\lambda} h_\lambda \cdots t^{\alpha_\ell} h_\ell k_0 t^{\beta_1} \cdots k_{\rho-1} t^{\beta_\rho} \approx e_{i,2,3} \in A(\alpha_\lambda) = B(\beta_\rho), \tag{157}$$

$$h_0 t^{\alpha_1} \cdots h_{\lambda-2} t^{\alpha_{\lambda-1}} (h_{\lambda-1} e_{i,2,3} k_\rho) t^{\beta_{\rho+1}} k_{\rho+1} \cdots t^{\beta_m} k_m \in \mathrm{Red}(\mathbb{H}, t). \tag{158}$$

Note that by (157) and Lemma 4, $h_\lambda, \ldots, h_\ell, k_0, \ldots, k_{\rho-1}$ are invertible in the monoid $\mathbb{H}$ (for every $0 \le i \le \rho - 1$ there exist $a, a' \in A \cup B$ such that $h_{\ell-i} a' k_i = a$). We include in the above notation the following "degenerated" cases:

Left-degenerated case $\lambda = 1$: Then $h_0 t^{\alpha_1} \cdots h_{\lambda-2} t^{\alpha_{\lambda-1}}$ must be understood as 1.
Right-degenerated case $\rho = m$: Then $t^{\beta_{\rho+1}} k_{\rho+1} \cdots t^{\beta_m} k_m$ must be understood as 1.
Middle-degenerated case $\alpha_\ell + \beta_1 \neq 0$ or ($\alpha_\ell + \beta_1 = 0$ and $h_\ell k_0 \notin A(\beta_1)$): In this case we set $\lambda = \ell + 1$, $\rho = 0$, and $e_{i,2,3} = 1$. Equality (156) disappears, (157) becomes the trivial equation $1 = 1$, while (158) remains valid.
LM-degenerated case $\ell = 0$, i.e., $s_{i,2} = h_0$: We set $\lambda = 1$, $\rho = 0$ and $e_{i,2,3} = 1$. Equality (156) disappears, (157) becomes the trivial equation $1 = 1$. The left-hand side of assertion (158) consists just of $h_0 s_{i,3}$.
MR-degenerated case $m = 0$: Analogous to the previous case. The left-hand side of (158) consists just of $s_{i,2} k_0$.

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 visuallized in Figure 9 as one or two of the three triangular pieces consisting of a trivial relation. For instance, in the LM-degenerated case the left and middle triangular regions are trivial relations.

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

$$L_{i,2} = h_0 t^{\alpha_1} \cdots h_{\lambda-2} t^{\alpha_{\lambda-1}} \quad M_{i,2} = h_{\lambda-1} \quad R_{i,2} = t^{\alpha_\lambda} h_\lambda \cdots t^{\alpha_\ell} h_\ell$$
$$L_{i,3} = k_0 t^{\beta_1} \cdots k_{\rho-1} t^{\beta_\rho} \quad M_{i,3} = k_\rho \quad R_{i,3} = t^{\beta_{\rho+1}} k_{\rho+1} \cdots t^{\beta_m} k_m$$

Note that $R_{i,2}, L_{i,3} \in \mathrm{dom}(\mathbb{I}_t)$ since $h_\lambda, \ldots, h_\ell, k_0, \ldots, k_{\rho-1}$ are invertible in the monoid $\mathbb{H}$. Moreover, since $s_{i,1} \approx s_{i,2} s_{i,3} \approx L_{i,2}(M_{i,2} e_{i,2,3} M_{i,3}) R_{i,3}$ and $L_{i,2}(M_{i,2} e_{i,2,3} M_{i,3}) R_{i,3}$ as well as $s_{i,1}$ are reduced sequences, by Lemma 5 we get

$$s_{i,1} \sim L_{i,2}(M_{i,2} e_{i,2,3} M_{i,3}) R_{i,3}. \tag{159}$$

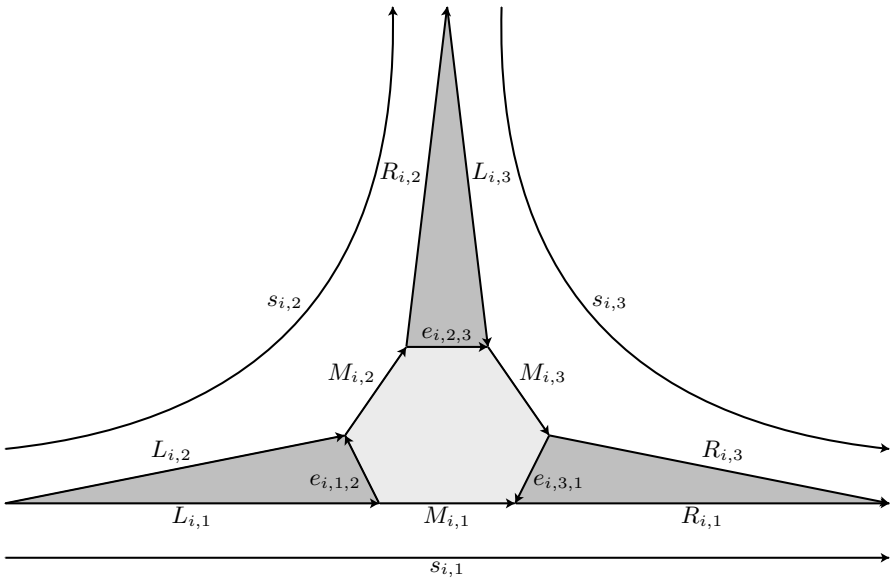


Fig. 9. Cutting the solution into three factors

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

Then $L_{i,2}$ (resp. $R_{i,3}$) ends (resp. starts) with $t^{\alpha_{\lambda-1}}$ (resp. $t^{\beta_{\rho+1}}$). By (159), there must exist a factorization

$$s_{i,1} = L_{i,1} M_{i,1} R_{i,1}$$

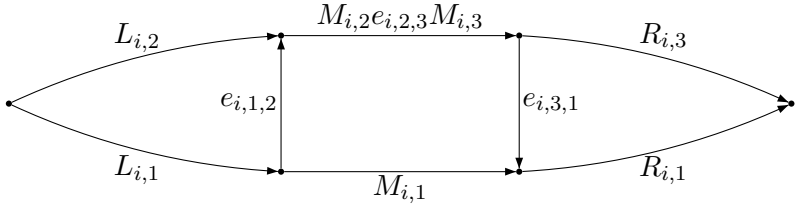
with $L_{i,1}, R_{i,1} \in \mathrm{Red}(\mathbb{H}, t)$, $M_{i,1} \in \mathbb{H}$, and connecting elements $e_{i,1,2} \in B(\alpha_{\lambda-1})$, $e_{i,3,1} \in A(\beta_{\rho+1})$ such that:

$$L_{i,1} e_{i,1,2} \sim L_{i,2}, \tag{160}$$

$$e_{i,1,2} M_{i,2} e_{i,2,3} M_{i,3} e_{i,3,1} = M_{i,1} \text{ in } \mathbb{H} \tag{161}$$

$$e_{i,3,1} R_{i,1} \sim R_{i,3}, \tag{162}$$

see also the following diagram:



The relation (157) can be rewritten as $R_{i,2} L_{i,3} \approx e_{i,2,3}$, or, since $R_{i,2}$ and $L_{i,3}$ are reduced and $L_{i,3}$ is invertible, as

$$R_{i,2} \sim e_{i,2,3} \mathbb{I}_t(L_{i,3}), \tag{163}$$

see Figure 9. Let $\pi_t : \mathbb{H} * \{t, t^{-1}\}^* \to \{t, t^{-1}\}^*$ be the natural projection. By (160), (162), and (163) we know that

$$\pi_t(L_{i,1}) = \pi_t(L_{i,2}) \neq \varepsilon, \quad \pi_t(R_{i,1}) = \pi_t(R_{i,3}) \neq \varepsilon, \quad \pi_t(R_{i,2}) = \pi_t(\mathbb{I}_t(L_{i,3})) \neq \varepsilon.$$

Hence the fta $\mathcal{R}_6$ (see Figure 3) has computations of the following forms:

$$(1,H) \xrightarrow{L_{i,1}} q_{i,1} \xrightarrow{M_{i,1}} r_{i,1} \xrightarrow{R_{i,1}} (1,1)$$

$$(1,H) \xrightarrow{L_{i,2}} q_{i,1} \xrightarrow{M_{i,2}} r_{i,2} \xrightarrow{R_{i,2}} (1,1)$$

$$(1,H) \xrightarrow{L_{i,3}} \mathbb{I}_{\mathcal{R}}(r_{i,2}) \xrightarrow{M_{i,3}} r_{i,1} \xrightarrow{R_{i,3}} (1,1).$$

Note that $(q_{i,1},0,r_{i,1})$, $(q_{i,1},0,r_{i,2})$, and $(\mathbb{I}_{\mathcal{R}}(r_{i,2}),0,r_{i,1})$ are H-types.

Since $L_{i,2}$ ends with t or t^{-1}, the same holds for $L_{i,1}$. An inspection of the fta $\mathcal{R}_6$ shows that the computation $(1,H) \xrightarrow{L_{i,1}} q_{i,1}$ can be factored into two subcomputations

$$(1,H) = q_{i,1,0} \xrightarrow{v_{i,1,1}} q_{i,1,1} \xrightarrow{v_{i,1,2}} q_{i,1,2} = q_{i,1} \text{ with } L_{i,1} = v_{i,1,1}v_{i,1,2} \tag{164}$$

such that the triple $(q_{i,1,0},\ \|v_{i,1,1}\|_b,\ q_{i,1,1})$ is an H-type and $(q_{i,1,1},\ \|v_{i,1,2}\|_b,\ q_{i,1,2})$ is a T-type. More generally, every decomposition of a computation into subcomputations $p_{k-1} \xrightarrow{w_k} p_k$ such that every triple $(p_{k-1},\ \|w_k\|_b,\ p_k)$ is either an H-type or a T-type will be called $\mathcal{R}_6$-*compatible* [6]. Similarly the computations $r_{i,1} \xrightarrow{R_{i,1}} (1,1)$ and $r_{i,2} \xrightarrow{R_{i,2}} (1,1)$ have $\mathcal{R}_6$-compatible decompositions:

$$r_{i,1} = q_{i,1,3} \xrightarrow{v_{i,1,4}} q_{i,1,4} \xrightarrow{v_{i,1,5}} q_{i,1,5} = (1,1) \text{ with } R_{i,1} = v_{i,1,4}v_{i,1,5} \tag{165}$$

$$r_{i,2} = q_{i,2,3} \xrightarrow{v_{i,2,4}} q_{i,2,4} \xrightarrow{v_{i,2,5}} q_{i,2,5} = (1,1) \text{ with } R_{i,2} = v_{i,2,4}v_{i,2,5}. \tag{166}$$

Combining decomposition (164) with equation (160), (165) with (162), and (166) with (163), we define

$$\begin{aligned} q_{i,2,k} &:= q_{i,1,k} \text{ for } 0 \le k \le 2, \\ q_{i,3,k} &:= q_{i,1,k} \text{ for } 3 \le k \le 5, \\ q_{i,3,k} &:= \mathbb{I}_{\mathcal{R}}(q_{i,2,5-k}) \text{ for } 0 \le k \le 2, \end{aligned}$$

and get the following three $\mathcal{R}_6$-compatible decompositions:

$$(1,H) = q_{i,2,0} \xrightarrow{v_{i,2,1}} q_{i,2,1} \xrightarrow{v_{i,2,2}} q_{i,2,2} = q_{i,1} \text{ with } L_{i,2} = v_{i,2,1}v_{i,2,2} \tag{167}$$

$$r_{i,1} = q_{i,3,3} \xrightarrow{v_{i,3,4}} q_{i,3,4} \xrightarrow{v_{i,3,5}} q_{i,3,5} = (1,1) \text{ with } R_{i,3} = v_{i,3,4}v_{i,3,5} \tag{168}$$

$$(1,H) = \mathbb{I}_{\mathcal{R}}(q_{i,2,5}) = q_{i,3,0} \xrightarrow{v_{i,3,1}} q_{i,3,1} \xrightarrow{v_{i,3,2}} q_{i,3,2} = \mathbb{I}_{\mathcal{R}}(r_{i,2}) \text{ with } L_{i,3} = v_{i,3,1}v_{i,3,2} \tag{169}$$

Finally, we define $v_{i,j,3} := M_{i,j} \in \mathbb{H}$ $(1 \le j \le 3)$. Note that $v_{i,2,4}, v_{i,2,5}, v_{i,3,1}, v_{i,3,2} \in \mathrm{dom}(\mathbb{I}_t)$, since $R_{i,2}, L_{i,3} \in \mathrm{dom}(\mathbb{I}_t)$. We summarize in Figure 10 the above decompositions and relations.

Let us extract from these the vector $(\boldsymbol{W}, \boldsymbol{e})$ and the AB-homomorphism σ_t. Let

$$\boldsymbol{\theta}_{i,j,k} := (q_{i,j,k-1}, \|v_{i,j,k}\|_b, q_{i,j,k}).$$

Note that $\boldsymbol{\theta}_{i,j,k} \in \gamma_t(v_{i,j,k})$ and that $\boldsymbol{\theta}_{i,j,3}$ is an H-type. We choose for $W_{i,j,k}$ a letter from $\mathcal{W}$ with the following properties:

[6] H-types are really edges of the fta $\mathcal{R}_6$ while T-types are either edges or paths of length 3 of the fta $\mathcal{R}_6$.

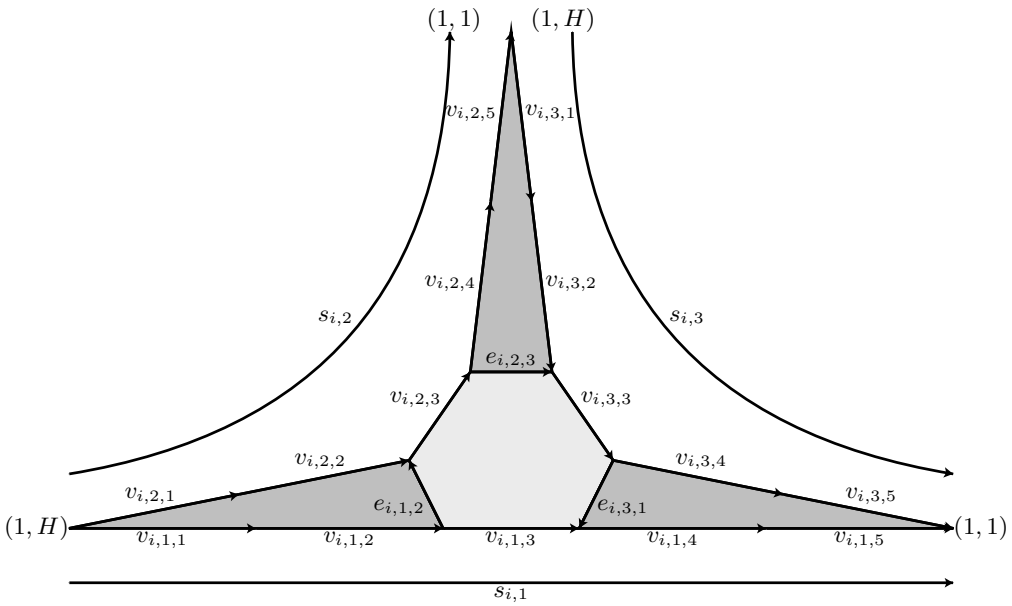


Fig. 10. Cutting the solution into five factors

- $p_1(W_{i,j,k}) = (i, j, k, 0)$, this ensures property (137).
- $\gamma_w(W_{i,j,k}) = \boldsymbol{\theta}_{i,j,k}$, this ensures properties (138)–(145).
- $\mu_w(W_{i,j,k}) = \mu_t(\boldsymbol{\theta}_{i,j,k}, v_{i,j,k})$, this ensures property (146).
- $\delta_w(W_{i,j,k}) = \delta_t(\boldsymbol{\theta}_{i,j,k}, v_{i,j,k})$
- $W_{i,j,k} \in \widehat{\mathcal{W}} \Longleftrightarrow v_{i,j,k} \in \mathrm{dom}(\mathbb{I}_t)$, this ensures property (147).

By Lemma 29, $W_{i,j,k}$ indeed belongs to $\mathcal{W}$. Moreover, $(\boldsymbol{W}, \boldsymbol{e})$ is an admissible vector. Note that $W_{i,j,k} \in \mathcal{W}_t$: one can choose $s := v_{i,j,k}$ in (91). Moreover, if $W_{i,j,k} \in \widehat{\mathcal{W}}$, then $\mathbb{I}_w(W_{i,j,k})$ does not occur among the letters $W_{i',j',k'}$ (because $(i, j, k, 0) = p_1(W_{i,j,k}) = p_1(\mathbb{I}_w(W_{i,j,k}))$ and $\mathbb{I}_w(W_{i,j,k}) \neq W_{i,j,k}$). This allows us to define a mapping σ_t by $\sigma_t(W_{i,j,k}) = [v_{i,j,k}]_\sim$ and $\sigma_t(\mathbb{I}_w(W_{i,j,k})) = [\mathbb{I}_t(v_{i,j,k})]_\sim$ in case $W_{i,j,k} \in \widehat{\mathcal{W}}$ (i.e. $v_{i,j,k} \in \mathrm{dom}(\mathbb{I}_t)$). By Lemma 23, this mapping σ_t induces an AB-homomorphism $\sigma_t : \mathbb{W}_t \to \mathbb{H}_t$. One can check that σ_t solves the systems of equations $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ and $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ and that

$$\sigma = \sigma_{\boldsymbol{W},\boldsymbol{e}} \circ \sigma_t \circ \pi_{\mathbb{G}}.$$

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

Case 2 (left-degenerated case): We have $\lambda = 1$. Let us set $L_{i,2} = L_{i,1} = e_{i,1,2} = 1$ and, accordingly, for all $1 \leq k \leq 2$:

$$v_{i,2,k} = v_{i,1,k} = 1, \;\; W_{i,2,k} = W_{i,1,k} = 1.$$

Case 3 (right-degenerated case): We have $\rho = m$. Let us set $R_{i,3} = R_{i,1} = e_{i,3,1} = 1$ and, accordingly, for all $4 \leq k \leq 5$:

$$v_{i,3,k} = v_{i,1,k} = 1, \;\; W_{i,3,k} = W_{i,1,k} = 1.$$

Case 4 (middle-degenerated case): We have $\alpha_\ell + \beta_1 \neq 0$ or ($\alpha_\ell + \beta_1 = 0$ and $h_\ell k_0 \notin A(\beta_1)$). Let us set $R_{i,2} = L_{i,3} = e_{i,2,3} = 1$ and, accordingly, for all $4 \leq k \leq 5$:

$$v_{i,2,k} = v_{i,3,6-k} = 1, \;\; W_{i,2,k} = W_{i,3,6-k} = 1.$$

Case 5 (LM-degenerated case): We have $\ell = 0$. We choose all the special values chosen in Case 2 and Case 4, i.e. $L_{i,2} = L_{i,1} = R_{i,2} = L_{i,3} = e_{i,1,2} = e_{i,2,3} = 1$ and the resulting choices for $W_{i,*,*}$.

Case 6 (MR-degenerated case): We have $m = 0$. We choose all the special values chosen in Case 3 and Case 4.

From t-solutions to $\mathbb{G}$-solutions. Let $\sigma_t : \mathbb{W}_t \to \mathbb{H}_t$ be an AB-homomorphism solving both systems $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ and $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$, where $(\boldsymbol{W}, \boldsymbol{e})$ is some admissible vector with all components in $\mathcal{W}_t \cup A \cup B$. We have to show that $\sigma_{\boldsymbol{W},\boldsymbol{e}} \circ \sigma_t \circ \pi_{\mathbb{G}}$ solves the system (133).

First, we show that for every $i \in [1, n]$,

$$\sigma_t(\sigma_{\boldsymbol{W},\boldsymbol{e}}(U_{i,1})) \approx \sigma_t(\sigma_{\boldsymbol{W},\boldsymbol{e}}(U_{i,2}U_{i,3})). \tag{170}$$

Let us fix such an integer $i \in [1, n]$. Since σ_t solves (149)–(152), we have

$$\sigma_t(\prod_{k=1}^{5} W_{i,1,k}) \approx \sigma_t(\prod_{k=1}^{5} W_{i,2,k} \prod_{k=1}^{5} W_{i,3,k}). \tag{171}$$

Figure 7 gives a decomposition of the Van-Kampen diagram corresponding to the above equivalence into four diagrams corresponding to (149)–(152). We also have

$$\sigma_t(\sigma_{\boldsymbol{W},\boldsymbol{e}}(U_{i,j})) \overset{(153)}{=} \sigma_t(\prod_{k=1}^{5} W_{\overline{i,j},k}) \overset{(148)}{=} \sigma_t(\prod_{k=1}^{5} W_{i,j,k}). \tag{172}$$

Hence, we get

$$\begin{aligned}
\sigma_t(\sigma_{\boldsymbol{W},\boldsymbol{e}}(U_{i,1})) &\overset{(172)}{=} \sigma_t(\prod_{k=1}^{5} W_{i,1,k}) \\
&\overset{(171)}{\approx} \sigma_t(\prod_{k=1}^{5} W_{i,2,k} \prod_{k=1}^{5} W_{i,3,k}) \\
&\overset{(172)}{=} \sigma_t(\sigma_{\boldsymbol{W},\boldsymbol{e}}(U_{i,2}U_{i,3})),
\end{aligned}$$

which is (170). It remains to show that for every $i \in [1, n]$,

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

By definition (47), this is equivalent to

$$\mu_{\mathcal{A},1}((1, H, b, 1, 1), \sigma_t(\sigma_{\boldsymbol{W},\boldsymbol{e}}(U_{i,j}))) = \mu_{\mathcal{U}}(U_{i,j}), \text{ where} \tag{173}$$

$$b = \|\sigma_t(\sigma_{\boldsymbol{W},\boldsymbol{e}}(U_{i,j}))\|_b \tag{174}$$

(note that $\sigma_t(\sigma_{\boldsymbol{W},\boldsymbol{e}}(U_{i,j}))$ is reduced since $\gamma_w(\sigma_{\boldsymbol{W},\boldsymbol{e}}(U_{i,j})) \neq \emptyset$). By (138), $\gamma_w(\prod_{k=1}^{5} W_{i,j,k}) = \{(1, H, b', 1, 1)\}$ for some $b' \in \{0, 1\}$. Since σ_t is an AB-homomorphism, we get

$$(1, H, b', 1, 1) \in \gamma_t(\sigma_t(\prod_{k=1}^{5} W_{i,j,k})) \overset{(172)}{=} \gamma_t(\sigma_t(\sigma_{\boldsymbol{W},\boldsymbol{e}}(U_{i,j}))).$$

By (174) this implies that $b' = b$. Thus

$$\gamma_w(\prod_{k=1}^{5} W_{i,j,k}) = \{(1, H, b, 1, 1)\}. \tag{175}$$

As σ_t is an AB-homomorphism, (Hom6) implies

$$\mu_t((1, H, b, 1, 1), \sigma_t(\prod_{k=1}^{5} W_{i,j,k})) = \mu_w((1, H, b, 1, 1), \prod_{k=1}^{5} W_{i,j,k}). \tag{176}$$

Now, the following calculation yields (173):

$$\begin{aligned}
\mu_{\mathcal{A},1}((1, H, b, 1, 1), \sigma_t(\sigma_{\boldsymbol{W},\boldsymbol{e}}(U_{i,j}))) &\overset{(172)}{=} \mu_{\mathcal{A},1}((1, H, b, 1, 1), \sigma_t(\prod_{k=1}^{5} W_{i,j,k})) \\
&\overset{(62)}{=} p_1(\mu_t((1, H, b, 1, 1), \sigma_t(\prod_{k=1}^{5} W_{i,j,k}))) \\
&\overset{(176)}{=} p_1(\mu_w((1, H, b, 1, 1), \prod_{k=1}^{5} W_{i,j,k})) \\
&\overset{(175)}{=} p_1(\mu_w(\gamma_w(\prod_{k=1}^{5} W_{i,j,k}), \prod_{k=1}^{5} W_{i,j,k})) \\
&= p_1(\mu_w(\prod_{k=1}^{5} W_{i,j,k})) \\
&\overset{(146)}{=} \mu_{\mathcal{U}}(U_{i,j})
\end{aligned}$$

Lemma 45 is thus proved. □

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 fta expressing the constraints). Given an $\mathbb{H}$-involutive automorphism Φ (see Definition 8) we abbreviate with $\mathbb{W}/\Phi$ the quotient of the AB-algebra $\mathbb{W}$ by the congruence $\simeq_\Phi$ generated by the relation $\{(W, \Phi(W)) \mid W \in \mathcal{W}\}$; see the paragraph after Definition 8. Recall that HInv denotes the set of all $\mathbb{H}$-involutive automorphisms of $\mathbb{W}$.

6.1 $\mathbb{W}$-equations

A system of $\mathbb{W}$-equations is a pair

$$(\mathcal{S}, \Phi) \tag{177}$$

such that $\mathcal{S} \subseteq \mathbb{W} \times \mathbb{W}$ is finite, $\gamma_w(s) = \gamma_w(s') \neq \emptyset$ for all $(s, s') \in \mathbb{W}$ and $\Phi \in \mathsf{HInv}$. If $\mathcal{S}$ is not a subset of $\mathbb{W}_t \times \mathbb{W}_t$, then $(\mathcal{S}, \Phi)$ has no solution. On the other hand, if $\mathcal{S} \subseteq \mathbb{W}_t \times \mathbb{W}_t$, then a *solution* of $(\mathcal{S}, \Phi)$ is any AB-homomorphism $\sigma_{\mathbb{W}} : \mathbb{W}_t \to \mathbb{W}_t/\Phi$ such that for every $(s, s') \in \mathcal{S}$:

$$\sigma_{\mathbb{W}}(s) = \sigma_{\mathbb{W}}(s'). \tag{178}$$

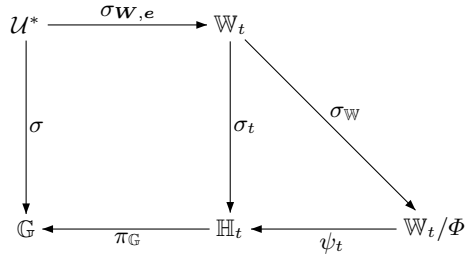


Fig. 11. Lemma 46

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

From t-solutions to $\mathbb{W}$-solutions. For every $w \in \mathbb{W}$ we use the following notation, where $\overline{W}$ denotes $\mathbb{I}_w(W)$:

$$\mathrm{Alph}(w) = \{W \in \mathcal{W} \setminus \widehat{\mathcal{W}} \mid W \text{ occurs in } w\} \cup \{W \in \widehat{\mathcal{W}} \mid W \text{ or } \overline{W} \text{ occurs in } w\}$$

$$\mathrm{A}(w) = \mathrm{Card}\{W \in \mathcal{W} \setminus \widehat{\mathcal{W}} \mid W \text{ occurs in } w\} + \frac{1}{2}\mathrm{Card}\{W \in \widehat{\mathcal{W}} \mid W \text{ or } \overline{W} \text{ occurs in } w\}.$$

Note that $\mathrm{A}(w)$ is an upper bound on the number of different first components (which are in $\mathcal{V}_0$) of symbols in $\mathrm{Alph}(w)$, i.e., $\mathrm{Card}(p_1(\mathrm{Alph}(w))) \leq \mathrm{A}(w)$. For this, note that W and $\overline{W}$ have the same first component.

Given a system of t-equations $\mathcal{S} = \{(w_i, w_i') \mid 1 \leq i \leq n\} \subseteq \mathbb{W} \times \mathbb{W}$ (see (131)), let:

$$\mathrm{Alph}(\mathcal{S}) = \mathrm{Alph}(\prod_{i=1}^{n} w_i w_i').$$

Lemma 46 (factorization of t-solutions). *Let $\mathcal{S} \subseteq \mathbb{W} \times \mathbb{W}$ be a system of t-equations. Let us suppose that $\sigma_t : \mathbb{W}_t \to \mathbb{H}_t$ is an AB-homomorphism such that:*

- *σ_t solves the system $\mathcal{S}$, and*
- *$\mathrm{Card}(\mathrm{Alph}(\mathcal{S})) \leq \frac{1}{2}\mathrm{Card}(\mathcal{V}_0)$.*

Then there exist $\Phi \in \mathsf{HInv}$ and AB-homomorphisms

$$\sigma_{\mathbb{W}} : \mathbb{W}_t \to \mathbb{W}_t/\Phi \quad \textit{and} \quad \psi_t : \mathbb{W}_t/\Phi \to \mathbb{H}_t$$

such that $\sigma_t(W) = \psi_t(\sigma_{\mathbb{W}}(W))$ for every $W \in \mathrm{Alph}(\mathcal{S})$, and $\sigma_{\mathbb{W}}(s) = \sigma_{\mathbb{W}}(s')$ for every $(s, s') \in \mathcal{S}$.

In other words: Every solution in $\mathbb{H}_t$ of a system of t-equations, over a sufficiently large alphabet, *factorizes*, over the variables of the equation, through a solution in $\mathbb{W}_t/\Phi$ of the same system of equations, where Φ is an involution which belongs to HInv.

Remark 1. In the case where the system $\mathcal{S}$ is one of the systems $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ introduced by Lemma 45:
- every variable W occurring in the system $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ occurs in the system $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ too (it must occur at least in one trivial equation (148)).
- the inequality (2) is ensured by the construction of the alphabet $\mathcal{W}$ that involves an integer N_0, choosen in such a way that inequality (135) is fulfilled.

Thus the factorization property asserted by Lemma 46 will hold for every common solution of $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ and $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$. This will be important later.

This factorization lemma is obtained via the more technical Lemma 47 below. For this lemma, we need the following definitions.

For $s \in \mathcal{W}^* * A * B$ let ($*$ denotes a placeholder)

$$\chi_{AB}(s) = \begin{cases} 1 & \text{if } s \in A \cup B \\ 0 & \text{otherwise.} \end{cases}$$

$$\chi_H(s) = \begin{cases} 0 & \text{if } |\gamma_w(s)| \neq 1 \text{ or } \gamma_w(s) \text{ has the form } \{(*, T, 1, *, H)\} \\ 1 & \text{if } \gamma_w(s) \text{ has the form } \{(*, *, 0, *, *)\} \text{ or } \{(*, T, 1, *, T)\} \\ & \qquad \text{or } \{(*, H, 1, *, H)\} \text{ or } \{(*, T, 1, 1, 1)\} \\ 2 & \text{if } \gamma_w(s) \text{ has the form } \{(*, H, 1, *, T)\} \text{ or } \{(*, H, 1, 1, 1)\} \end{cases}$$

Note that the three cases in this definition cover all possible values for $\gamma_w(s)$. The intuition behind this definition is the following: Let $s \in (\mathcal{W} \cup A \cup B)^*$ such that $|\gamma_w(s)| = 1$. Then:

- $\chi_H(s) = 0$ if s has the type of a t-sequence which begins with either t or t^{-1} and ends with either t or t^{-1}.
- $\chi_H(s) = 1$ if s has the type of a t-sequence which either belongs to $\mathbb{H}$ or begins with some $\mathbb{H}$-element or ends with some $\mathbb{H}$-element, but the other extremity is not from $\mathbb{H}$.
- $\chi_H(s) = 2$ if w has the type of a t-sequence which begins with some $\mathbb{H}$-element and ends with some $\mathbb{H}$-element and is not reduced to an $\mathbb{H}$-element.

Given $p, s, p', s' \in \mathcal{W}^* * A * B$ and $\psi_t \in \mathrm{Hom}_{AB}(\mathcal{W}^* * A * B, \mathbb{H}_t)$ we define

$$\Delta(p, s, p', s', \psi_t) = 1 - \frac{1}{2}\Big(\chi_{AB}(p) + \chi_{AB}(p')\Big) + \chi_H(s) + \chi_H(s') + 2\|\psi_t(s)\| + 2\|\psi_t(s')\|. \quad (179)$$

Note that $\Delta(p, s, p', s', \psi_t) \geq 0$. Moreover, χ_{AB}, χ_H, and Δ are invariant with respect to the congruence $\equiv$. Hence, by factorization through $\pi_{\equiv}$, the definitions apply on $\mathbb{W}$.

Lemma 47. *Let $\mathcal{S} = \{(w_i, w_i') \mid 1 \leq i \leq n + m\} \subseteq \mathbb{W}_t \times \mathbb{W}_t$ be a system of t-equations (hence, $\gamma_w(w_i) = \gamma_w(w_i') \neq \emptyset$ for all $1 \leq i \leq m + n$). Let us suppose that $\lambda_i : \mathbb{W}_t \to \mathbb{W}_t$ ($1 \leq i \leq n + m$) and $\theta_t : \mathbb{W}_t \to \mathbb{H}_t$ are AB-homomorphisms such that*

$$\theta_t(\lambda_i(w_i)) = \theta_t(\lambda_i(w_i')) \text{ for all } 1 \leq i \leq n + m, \quad (180)$$

$$\lambda_i = \lambda_j \text{ for all } 1 \leq i, j \leq n, \quad (181)$$

$$\mathrm{A}(\prod_{i=1}^{n+m} \lambda_i(w_i w_i')) < \frac{1}{2}\mathrm{Card}(\mathcal{V}_0). \quad (182)$$

Then there exist $\Phi \in \mathsf{HInv}$ and AB-homomorphisms

$$\lambda_i' : \mathbb{W}_t \to \mathbb{W}_t \ (1 \leq i \leq n + m) \quad \text{and} \quad \theta_t' : \mathbb{W}_t \to \mathbb{H}_t$$

such that

$$\theta_t(\lambda_i(W)) = \theta_t'(\lambda_i'(W)) \text{ for all } 1 \leq i \leq n + m, W \in \mathrm{Alph}(\mathcal{S}) \quad (183)$$

$$\theta_t'(W) = \theta_t'(\Phi(W)) \text{ for all } W \in \mathcal{W} \quad (184)$$

$$\lambda_i'(w_i) \simeq_\Phi \lambda_i'(w_i') \text{ for all } 1 \leq i \leq n + m, \quad (185)$$

$$\lambda_i' = \lambda_j' \text{ for all } 1 \leq i, j \leq n. \quad (186)$$

Proof. Let $\mathcal{S} = \{(w_i, w_i') \mid 1 \leq i \leq n+m\} \subseteq \mathbb{W}_t \times \mathbb{W}_t$ such that $\gamma_w(w_i) = \gamma_w(w_i') \neq \emptyset$ and let $\boldsymbol{\lambda} = (\lambda_i)_{1 \leq i \leq n+m}$ be a sequence of AB-homomorphisms $\lambda_i : \mathbb{W}_t \to \mathbb{W}_t$.

Claim 1. For every $1 \leq i \leq n+m$ we either have $w_i = w_i' \in A \cup B$ (and hence $\lambda_i(w_i) = \lambda_i(w_i') \in A \cup B$) or $\|w_i\|, \|w_i'\| \geq 1$ and $\gamma_w(\lambda_i(w_i)) = \gamma_w(\lambda_i(w_i'))$. In particular, $\gamma_w(\lambda_i(w_i)) = \gamma_w(\lambda_i(w_i'))$ for all $1 \leq i \leq n+m$.

Since $\gamma_w(w_i) = \gamma_w(w_i') \neq \emptyset$, we can distinguish the following cases:

Case 1. $w_i = 1$: By (80), we get $\gamma_w(w_i') = \gamma_w(w_i) = \{(\theta, 0, \theta) \mid \theta \in \mathcal{T}_6\}$. But this implies $w_i' = 1$.

Case 2. $w_i \in A \setminus 1$: We get $\gamma_w(w_i') = \gamma_w(w_i) \overset{(77)}{=} \{(A, T, 0, A, T), (A, H, 0, A, H)\}$, which implies $w_i' \in A \setminus 1$. Since λ_i and θ_t are AB-homomorphisms and therefore the identity on A, we get

$$w_i = \theta_t(\lambda_i(w_i)) \overset{(180)}{=} \theta_t(\lambda_i(w_i')) = w_i'.$$

The cases $w_i \in B \setminus 1$ and $w_i' \in A \cup B$ are symmetric.

Case 3. $\|w_i\|, \|w_i'\| \geq 1$: By Lemma 30(b) we have $|\gamma_w(w_i)| = 1 = |\gamma_w(w_i')|$. Moreover, $\|w_i\|, \|w_i'\| \geq 1$ implies $\|\lambda_i(w_i)\|, \|\lambda_i(w_i')\| \geq 1$ by Lemma 36. Hence, $|\gamma_w(\lambda_i(w_i))| = 1 = |\gamma_w(\lambda_i(w_i'))|$. With (Hom5) we finally get $\gamma_w(\lambda_i(w_i)) = \gamma_w(w_i) = \gamma_w(w_i') = \gamma_w(\lambda_i(w_i'))$. This concludes the proof of Claim 1.

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

$$\lambda_i(w_i) = P_i S_i \quad \text{and} \quad \lambda_i(w_i') = P_i' S_i' \tag{187}$$

such that $P_i \equiv_i P_i'$, $\gamma_w(P_i) \neq \emptyset$, $\gamma_w(S_i) \neq \emptyset$, $\gamma_w(P_i') \neq \emptyset$, $\gamma_w(S_i') \neq \emptyset$ (such decompositions always exists, since we can take $P_i = 1 = P_i'$), and this choice (187) minimizes the integer

$$\Delta(P_i, S_i, P_i', S_i', \theta_t)$$

(this value was defined in (179)). 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 $\Delta(P_i, S_i, P_i', S_i', \theta_t)$.

The *size* of the triple $(\mathcal{S}, \boldsymbol{\lambda}, \theta_t)$ is defined as the finite multiset of natural numbers

$$\|(\mathcal{S}, \boldsymbol{\lambda}, \theta_t)\| = \{\{\Delta_1(\mathcal{S}, \boldsymbol{\lambda}, \theta_t), \ldots, \Delta_{n+m}(\mathcal{S}, \boldsymbol{\lambda}, \theta_t)\}\}. \tag{188}$$

Moreover, let

$$\mathrm{Alph}(\mathcal{S}, \boldsymbol{\lambda}) = \mathrm{Alph}(\prod_{i=1}^{n+m} \lambda_i(w_i w_i')),$$

$$\mathrm{A}(\mathcal{S}, \boldsymbol{\lambda}) = \mathrm{A}(\prod_{i=1}^{n+m} \lambda_i(w_i w_i')).$$

Let us prove Lemma 47 by induction over $\|(\mathcal{S}, \boldsymbol{\lambda}, \theta_t)\|$ with respect to the partial ordering over finite multisets of naturals induced by the natural ordering over $\mathbb{N}$ (it is known that this ordering is well-founded). Let $(\mathcal{S}, \boldsymbol{\lambda}, \theta_t)$ fulfill the hypothesis of the lemma.

In the following, we write $\overline{W}$ for the symbol $\mathbb{I}_w(W)$ ($W \in \widehat{\mathcal{W}}$).

Case 1: For every $i \in [1, n+m]$, one of the following two situations occurs:

$$\lambda_i(w_i) \equiv_i \lambda_i(w_i') \tag{189}$$

$$\exists W \in \widehat{\mathcal{W}}, (e_i, f_i), (d_i, c_i) \in \mathrm{Gi}(W) \times \mathrm{Ge}(W) : \lambda_i(w_i) = e_i W f_i, \quad \lambda_i(w_i') = c_i^{-1} \overline{W} d_i^{-1} \tag{190}$$

In the following, a pair of variables $(W, \overline{W})$ occuring in some equation (190) is called a *twisted pair*. By Claim 1 we get

$$\gamma_w(W) = \gamma_w(e_i W f_i) = \gamma_w(\lambda_i(w_i)) = \gamma_w(\lambda_i(w_i')) = \gamma_w(c_i^{-1} \overline{W} d_i^{-1}) = \gamma_w(\overline{W}) \tag{191}$$

for every twisted pair $(W, \overline{W})$. Hence, $\mathrm{Gi}(W) = \mathrm{Ge}(W) = \mathrm{Gi}(\overline{W}) = \mathrm{Ge}(\overline{W})$.

Let us consider the partition

$$\widehat{\mathcal{W}} = \widehat{\mathcal{W}_0} \cup \mathcal{W}_1' \cup \overline{\mathcal{W}_1'} \cup \mathcal{W}_1'' \cup \overline{\mathcal{W}_1''},$$

where $\mathcal{W}_1' \cup \overline{\mathcal{W}_1'}$ (resp. $\mathcal{W}_1'' \cup \overline{\mathcal{W}_1''}$) is exactly the set of symbols with an H-type (resp. with a T-type) which are members of some twisted pair. Let us write

$$\mathcal{W}_1' = \{W_1, \ldots, W_p\}, \qquad \overline{\mathcal{W}_1'} = \{\overline{W} \mid W \in \mathcal{W}_1'\},$$
$$\mathcal{W}_1'' = \{W_{p+1}, \ldots, W_{p+q}\}, \qquad \overline{\mathcal{W}_1''} = \{\overline{W} \mid W \in \mathcal{W}_1''\}.$$

By multiplying with e_i^{-1} and f_i^{-1}, we can modify the system $\mathcal{S}$ in such a way that $e_i = f_i = 1$ in every equation of type (190) with preservation of the hypothesis of the lemma (with the same morphisms) and also of the size of $(\mathcal{S}, \boldsymbol{\lambda}, \theta_t)$. We can also suppose that $\mathcal{W}_1' \cup \mathcal{W}_1''$ is exactly the set of variables appearing in the righthand-sides of the first equation of (190). For every $k \in [1, p+q]$, let $(W_k, c_{\nu(k)}^{-1} \overline{W}_k d_{\nu(k)}^{-1})$ be the equation of type (190) with smallest index $\nu(k) \in [1, n+m]$ such that $\lambda_{\nu(k)}(w_{\nu(k)}) = W_k$. Since θ_t is an AB-homomorphism and

$$\theta_t(W_k) = \theta_t(\lambda_{\nu(k)}(w_{\nu(k)})) \overset{(180)}{=} \theta_t(\lambda_{\nu(k)}(w'_{\nu(k)})) = \theta_t(c_{\nu(k)}^{-1} \overline{W}_k d_{\nu(k)}^{-1})$$

we know that

$$\theta_t(\overline{W}_k) = \theta_t(c_{\nu(k)} W_k d_{\nu(k)}). \tag{192}$$

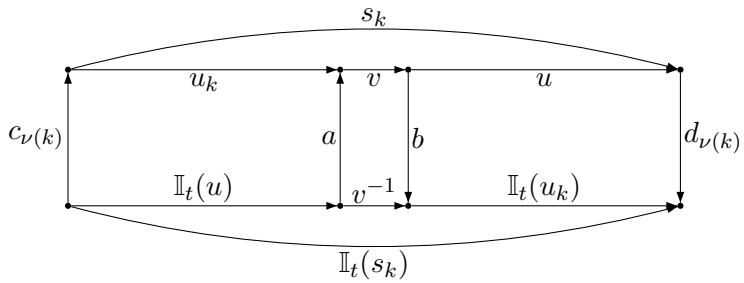
Let us "cut" the variables W_k, which have a T-type, into three parts in such a way that we transform the twisted pair $(W_k, \overline{W}_k)$ into another twisted pair but with an H-type. For every $k \in [p+1, p+q]$, let s_k be a reduced t-sequence such that

$$\theta_t(W_k) = [s_k]_\sim \in \mathrm{dom}(\mathbb{I}_t). \tag{193}$$

Since W_k has a T-type, s_k has to contain at least one occurrence of t or t^{-1}. Since $\mathbb{I}_t(s_k) \sim c_{\nu(k)} s_k d_{\nu(k)}$ by (192), the t-sequence s_k can be decomposed as

$$s_k = u_k \, v \, u \text{ where } u_k = u_k' t^\alpha, u = t^{-\alpha} u' \tag{194}$$

for some invertible $v \in \mathbb{H}$, reduced t-sequences u_k, u, and $\alpha \in \{1, -1\}$, such that $\pi_t(u) = \mathbb{I}_t(\pi_t(u_k))$. We obtain a van Kampen diagram of the following form:



We have $a, b \in B(\alpha) = A(-\alpha)$. Define $v_k = vb \in \mathbb{H}$, which is invertible in $\mathbb{H}$. We obtain

$$s_k \sim u_k v_k \mathbb{I}_t(u_k) d_{\nu(k)}^{-1} \text{ and } \mathbb{I}_t(s_k) \sim c_{\nu(k)} u_k v_k \mathbb{I}_t(u_k). \tag{195}$$

Thus $c_{\nu(k)} u_k v_k \mathbb{I}_t(u_k) \sim \mathbb{I}_t(s_k) \sim d_{\nu(k)} u_k v_k^{-1} \mathbb{I}_t(u_k)$. Since $\mathbb{H}_t$ is cancellative by Lemma 6, we get

$$d_{\nu(k)} u_k v_k^{-1} \sim c_{\nu(k)} u_k v_k. \tag{196}$$

Since $\gamma_w(W_k) = \gamma_w(\overline{W}_k)$ (see (191)) is a T-type, we must have $\gamma_w(W_k) = (C, T, 1, C, H)$ for either $C = A$ or $C = B$; see the list of T-types in (24). We have $(C, T, 1, C, H) \in \gamma(s_k) = \gamma_t(u_k v_k \mathbb{I}_t(u_k) d_{\nu(k)}^{-1})$. We can decompose the type $\gamma_w(W_k)$ as

$$\gamma_w(W_k) \;=\; (C, T, 1, B(\alpha), H)\,(B(\alpha), H, 0, B(\alpha), T)\,(B(\alpha), T, 1, C, H)$$

(here α is from (194)) with $(C, T, 1, B(\alpha), H) \in \gamma_t(u_k)$ and $(B(\alpha), H, 0, B(\alpha), T) \in \gamma_t(v_k)$. For the latter, $v_k \notin B(\alpha)$ is important (since s_k is a reduced t-sequence, we have $v \notin B(\alpha)$ and hence $v_k = vb \notin B(\alpha)$).

Let $\boldsymbol{\theta}'_k = (C, T, 1, B(\alpha), H) \in \gamma_t(u_k)$ (which is a T-type) and $\boldsymbol{\theta}_k = (B(\alpha), H, 0, B(\alpha), T) \in \gamma_t(v_k)$ (which is an H-type). We get

$$\gamma_w(\overline{W}_k) \overset{(191)}{=} \gamma_w(W_k) = \{\boldsymbol{\theta}'_k \boldsymbol{\theta}_k \mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}'_k)\} \text{ with } \boldsymbol{\theta}_k = \mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}_k). \tag{197}$$

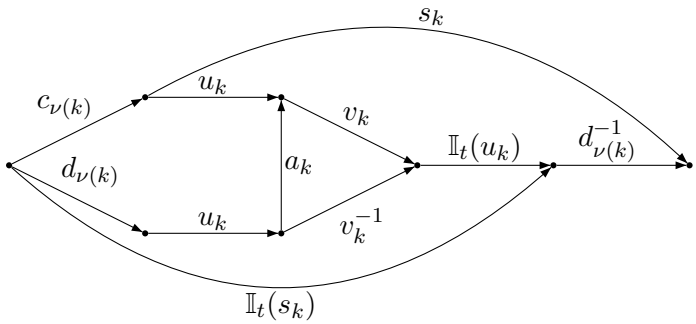
Moreover, by (196), there exists $a_k \in \mathrm{Gi}(\boldsymbol{\theta}_k) = \mathrm{Ge}(\boldsymbol{\theta}'_k) = B(\alpha)$ with

$$c_{\nu(k)} u_k a_k^{-1} \sim d_{\nu(k)} u_k \quad \text{and} \quad a_k v_k = v_k^{-1} \text{ in } \mathbb{H}. \tag{198}$$

Note that the last equation implies

$$a_k v_k = v_k a_k \text{ in } \mathbb{H}. \tag{199}$$

Omitting the elements a, b, u, v and inserting the new elements v_k, a_k in the preceding van Kampen diagram, we obtain the following van Kampen diagram:



Each of the $2q$ many letters $W_i, \overline{W}_i$ $(p+1 \leq i \leq p+q)$ occurs in $\prod_{i=1}^{n+m} \lambda_i(w_i w_i')$. Hence, we get

$$\begin{aligned} q = \frac{1}{2}2q &\leq \frac{1}{2}\mathrm{Card}\{W \in \widehat{\mathcal{W}} \mid W \text{ or } \overline{W} \text{ occurs in } \prod_{i=1}^{n+m} \lambda_i(w_i w_i')\} \\ &\leq \mathrm{A}(\prod_{i=1}^{n+m} \lambda_i(w_i w_i')) \\ &\overset{(182)}{<} \frac{1}{2}\mathrm{Card}(\mathcal{V}_0). \end{aligned}$$

Thus, $q + \mathrm{A}(\prod_{i=1}^{n+m} \lambda_i(w_i w_i')) < \mathrm{Card}(\mathcal{V}_0)$. Hence, there are at least q symbols $\alpha_{p+1}, \ldots, \alpha_{p+q} \in \mathcal{V}_0$ that do not occur as a first component of a symbol in $\mathrm{Alph}(\prod_{i=1}^{n+m} \lambda_i(w_i w_i')) = \mathrm{Alph}(\mathcal{S}, \boldsymbol{\lambda})$. Let us define for every $p+1 \leq k \leq p+q$ variables $U_k, V_k, \overline{U}_k, \overline{V}_k \in \mathcal{W}_t \cap \widehat{\mathcal{W}}$ with first component α_k and such that

$$\gamma_w(U_k) = \{\boldsymbol{\theta}_k'\}, \qquad \gamma_w(V_k) = \{\boldsymbol{\theta}_k\}, \tag{200}$$

$$\delta_w(\boldsymbol{\theta}_k', U_k) = \delta_t(\boldsymbol{\theta}_k', u_k), \quad \delta_w(\boldsymbol{\theta}_k, V_k) = \delta_t(\boldsymbol{\theta}_k, v_k), \tag{201}$$

$$\mu_w(\boldsymbol{\theta}_k', U_k) = \mu_t(\boldsymbol{\theta}_k', u_k), \quad \mu_w(\boldsymbol{\theta}_k, V_k) = \mu_t(\boldsymbol{\theta}_k, v_k). \tag{202}$$

Note that (201) implies with (198) and (199):

$$c_{\nu(k)} U_k a_k^{-1} = d_{\nu(k)} U_k \qquad \text{and} \qquad a_k V_k = V_k a_k \tag{203}$$

Let $\lambda' : \mathcal{W}^* * A * B \to \mathcal{W}^* * A * B$ be the unique monoid homomorphism fulfilling:

$$\lambda'(e) = e \qquad \text{for } e \in A \cup B \tag{204}$$

$$\lambda'(W_k) = U_k V_k \overline{U}_k d_{\nu(k)}^{-1} \quad \text{for } p+1 \leq k \leq p+q \tag{205}$$

$$\lambda'(\overline{W}_k) = d_{\nu(k)} U_k \overline{V}_k \overline{U}_k \quad \text{for } p+1 \leq k \leq p+q. \tag{206}$$

$$\lambda'(W) = W \qquad \text{for all other } W \in \mathcal{W} \tag{207}$$

Claim 2. λ' induces a monoid homomorphism $\lambda' : \mathbb{W} \to \mathbb{W}$.

Let $W \in \mathcal{W}$ and $(c, d) \in \delta_w(W)$. We have to prove that

$$\lambda'(cW) = c\lambda'(W) \equiv \lambda'(W)d = \lambda'(Wd). \tag{208}$$

By Lemma 32 it suffices to show $(c, d) \in \delta_w(\lambda'(W))$, i.e.

$$\delta_w(W) = \delta_w(\lambda'(W)) \tag{209}$$

Case 1. $\lambda'(W) = W$: Then (209) trivially holds.

Case 2. $W = W_k$ for some $p+1 \leq k \leq p+q$: We have

$$\begin{aligned}
\delta_w(W_k) &\overset{(\text{Hom7})}{=} \delta_t(\gamma_w(W_k), \theta_t(W_k)) \\
&\overset{(193)}{=} \delta_t(\gamma_w(W_k), s_k) \\
&\overset{(195)}{=} \delta_t(\gamma_w(W_k), u_k v_k \mathbb{I}_t(u_k) d^{-1}_{\nu(k)}) \\
&\overset{(197)}{=} \delta_t(\boldsymbol{\theta}'_k \boldsymbol{\theta}_k \mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}'_k), u_k v_k \mathbb{I}_t(u_k) d^{-1}_{\nu(k)}) \\
&\overset{(201)}{=} \delta_w(\boldsymbol{\theta}'_k \boldsymbol{\theta}_k \mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}'_k), U_k V_k \overline{U}_k d^{-1}_{\nu(k)}) \\
&\overset{(205)}{=} \delta_w(\gamma_w(W_k), \lambda'(W_k)),
\end{aligned}$$

i.e., (209) holds.

Case 3. $W = \overline{W}_k$ for some $p+1 \leq k \leq p+q$: One can check, using the formulas (205)–(207), that $\lambda'(\mathbb{I}_w(W)) = \mathbb{I}_w(\lambda'(W))$ for all $W \in \mathcal{W}$. Thus Case 3 reduces to Case 2. Claim 2 is thus established.

Claim 3. $\lambda' : \mathbb{W} \to \mathbb{W}$ is an AB-homomorphism.

We will apply Lemma 23. Hence, we have to check properties (a)–(f) from Lemma 23. By (204), λ' preserves ι_A and ι_B, i.e., (a) is satisfied. Also (b) follows immediately from the definition of λ'.

Condition (c) from Lemma 23: We have to show that $\lambda'(\mathbb{I}_w(W)) = \mathbb{I}_w(\lambda'(W))$ for all $W \in \widehat{\mathcal{W}}$. This property can be checked directly on the equations (204)–(207) defining λ'.

Condition (d) from Lemma 23: The definition of λ' together with (197) and (200) implies in fact $\gamma_w(W) = \gamma_w(\lambda'(W))$ for all $W \in \mathcal{W}$.

Condition (f) from Lemma 23: This was shown in (209).

Conditions (e) from Lemma 23: The same arguments as for (f) work. We have thus established Claim 3.

For $1 \leq i \leq n+m$ let us define

$$\lambda'_i = \lambda_i \circ \lambda'. \tag{210}$$

As every λ'_i is the composition of two AB-homomorphisms, λ'_i is an AB-homomorphism from $\mathbb{W}_t$ to $\mathbb{W}_t$. Let $\theta'_t : \mathcal{W}_t^* * A * B \to \mathbb{H}_t$ be the unique monoid homomorphism satisfying:

$$\theta'_t(e) = e \qquad \text{for all } e \in A \cup B \tag{211}$$
$$\theta'_t(U_k) = u_k \qquad \text{for all } p+1 \leq k \leq p+q \tag{212}$$
$$\theta'_t(\overline{U}_k) = \mathbb{I}_t(u_k) \quad \text{for all } p+1 \leq k \leq p+q \tag{213}$$
$$\theta'_t(V_k) = v_k \qquad \text{for all } p+1 \leq k \leq p+q \tag{214}$$
$$\theta'_t(\overline{V}_k) = v_k^{-1} \quad \text{for all } p+1 \leq k \leq p+q \tag{215}$$
$$\theta'_t(W) = \theta_t(W) \quad \text{for all other } W \in \mathcal{W}_t \tag{216}$$

Claim 4. θ'_t induces a monoid homomorphism $\theta'_t : \mathbb{W}_t \to \mathbb{H}_t$.

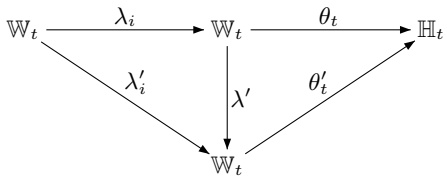


Fig. 12. Lemma 47, Case 1, Claim 6

It suffices to prove that $c\theta_t'(W) = \theta_t'(W)d$ in $\mathbb{H}_t$ for every $W \in \mathcal{W}_t$ and $(c,d) \in \delta_w(W)$. For this, it suffices to show that

$$\delta_w(W) = \delta_t(\gamma_w(W), \theta_t'(W)). \tag{217}$$

If $\theta_t'(W) = \theta_t(W)$ then (217) follows from the fact that θ_t is an AB-homomorphism. In all other cases, i.e., (212)–(215), we get (217) from (200) and (201).

Claim 5. $\theta_t' : \mathbb{W}_t \to \mathbb{H}_t$ is an AB-homomorphism.

We will apply Lemma 23. Hence, we have to check properties (a)-(f) from Lemma 23. By (211), θ_t' preserves ι_A and ι_B, i.e., (a) is satisfied. Condition (b) for the variables U_k, V_k, $\overline{U}_k$, and $\overline{V}_k$ (which all belong to $\mathrm{dom}(\mathbb{I}_w)$) follows from the fact that $u_k, v_k \in \mathrm{dom}(\mathbb{I}_t)$. Condition (b) for other variables $W \in \mathcal{W}_t$ follows from (216) and the fact that $\theta_t : \mathbb{W}_t \to \mathbb{H}_t$ is an AB-homomorphism.

Condition (c) from Lemma 23: We have to show that $\theta_t'(\mathbb{I}_w(W)) = \mathbb{I}_t(\theta_t'(W))$ for all $W \in \widehat{\mathcal{W}_t}$.

Let us first consider a variable $W \in \mathcal{W}_t$ with $\theta_t'(W) = \theta_t(W)$. Then, since $\theta_t : \mathbb{W}_t \to \mathbb{H}_t$ is an AB-homomorphism, we have

$$\mathbb{I}_t(\theta_t'(W)) = \mathbb{I}_t(\theta_t(W)) = \theta_t(\mathbb{I}_w(W)) = \theta_t'(\mathbb{I}_w(W)).$$

For a variable U_k we have

$$\mathbb{I}_t(\theta_t'(U_k)) \overset{(212)}{=} \mathbb{I}_t(u_k) \overset{(213)}{=} \theta_t'(\mathbb{I}_w(U_k))$$

and similarly for a variable $\overline{U}_k$. Finally, for a variable V_k we have

$$\mathbb{I}_t(\theta_t'(V_k)) \overset{(214)}{=} \mathbb{I}_t(v_k) = v_k^{-1} \overset{(215)}{=} \theta_t'(\mathbb{I}_w(V_k))$$

and similarly for a variable $\overline{V}_k$.

Conditions (d)–(f) from Lemma 23: For variables $W \in \mathcal{W}_t$ with $\theta_t'(W) = \theta_t(W)$ we get these conditions directly from the fact that θ_t is an AB-homomorphism. For variables from $\{U_k, \overline{U}_k, V_k, \overline{V}_k \mid p+1 \leq k \leq p+q\}$ we get (d)–(f) from (200)–(202).

Claim 6. λ_i' and θ_t' fulfill conclusion (183) of the lemma.

We have to show $\theta_t(\lambda_i(W)) = \theta_t'(\lambda_i'(W))$ for all $1 \leq i \leq n+m$ and all $W \in \mathrm{Alph}(\mathcal{S})$. Recall that $\lambda_i' = \lambda_i \circ \lambda'$ by (210). Hence, it suffices to show that $\theta_t = \lambda' \circ \theta_t'$ over $\mathrm{Alph}(\mathcal{S}, \boldsymbol{\lambda})$, i.e., that

$$\theta_t(W) = \theta_t'(\lambda'(W)) \tag{218}$$

for every $W \in \mathrm{Alph}(\mathcal{S}, \boldsymbol{\lambda})$. Note that $\mathrm{Alph}(\mathcal{S}, \boldsymbol{\lambda})$ does not contain the symbols $U_k, \overline{U}_k, V_k, \overline{V}_k$ for $p+1 \leq k \leq p+q$.

Case 1. $W \in \mathrm{Alph}(\mathcal{S}, \boldsymbol{\lambda})$ is such that $\lambda'(W) = W$:

$$\theta'_t(\lambda'(W)) = \theta'_t(W) \overset{(216)}{=} \theta_t(W),$$

which establishes (218).

Case 2. $W = W_k$ for some $p+1 \leq k \leq p+q$: We have in $\mathbb{H}_t$:

$$\begin{aligned}
\theta'_t(\lambda'(W_k)) &\overset{(205)}{=} \theta'_t(U_k V_k \overline{U}_k d_{\nu(k)}^{-1}) \\
&\overset{(212)\text{–}(214)}{=} u_k v_k \mathbb{I}_t(u_k) d_{\nu(k)}^{-1} \\
&\overset{(195)}{=} s_k \\
&\overset{(193)}{=} \theta_t(W_k).
\end{aligned}$$

Case 3. $W = \overline{W}_k$ for some $p+1 \leq k \leq p+q$: We have in $\mathbb{H}_t$:

$$\begin{aligned}
\theta'_t(\lambda'(\overline{W}_k)) &\overset{(206)}{=} \theta'_t(d_{\nu(k)} U_k \overline{V}_k \overline{U}_k) \\
&\overset{(212)\text{–}(215)}{=} d_{\nu(k)} u_k \mathbb{I}_t(v_k) \mathbb{I}_t(u_k) \\
&\overset{(195)}{=} \mathbb{I}_t(s_k) \\
&\overset{(193)}{=} \theta_t(\overline{W}_k).
\end{aligned}$$

This concludes the proof of Claim 6.

We next define a mapping $\Phi : \widehat{\mathcal{W}}^* * A * B \to \widehat{\mathcal{W}}^* * A * B$ as follows:

$$\Phi(e) = e \qquad \text{for } e \in A \cup B \tag{219}$$

$$\Phi(\overline{W}_k) = c_{\nu(k)} W_k d_{\nu(k)} \quad \text{for } 1 \leq k \leq p \tag{220}$$

$$\Phi(W_k) = c_{\nu(k)}^{-1} \overline{W}_k d_{\nu(k)}^{-1} \quad \text{for } 1 \leq k \leq p \tag{221}$$

$$\Phi(\overline{V}_k) = a_k V_k \qquad \text{for } p+1 \leq k \leq p+q \tag{222}$$

$$\Phi(V_k) = a_k^{-1} \overline{V}_k \qquad \text{for } p+1 \leq k \leq p+q \tag{223}$$

$$\Phi(W) = W \qquad \text{for all other } W \in \widehat{\mathcal{W}} \tag{224}$$

Claim 7. Φ induces an involutive AB-automorphism $\Phi : \widehat{\mathbb{W}} \to \widehat{\mathbb{W}}$ that belongs to HInv.

We have to check that Φ fulfills conditions (96)–(99) from Lemma 34 and also the H-type condition (109).

Condition (96): For $1 \leq k \leq p$ we have to show that $\delta_w(\overline{W}_k) = \delta_w(c_{\nu(k)} W_k d_{\nu(k)})$.

$$\begin{aligned}
\delta_w(\overline{W}_k) &\overset{(\mathrm{Hom7})}{=} \delta_t(\gamma_w(\overline{W}_k), \theta_t(\overline{W}_k)) \\
&\overset{(192)}{=} \delta_t(\gamma_w(\overline{W}_k), \theta_t(c_{\nu(k)} W_k d_{\nu(k)})) \\
&= \delta_t(\gamma_w(c_{\nu(k)} W_k d_{\nu(k)}), \theta_t(c_{\nu(k)} W_k d_{\nu(k)})) \\
&\overset{(\mathrm{Hom7})}{=} \delta_w(c_{\nu(k)} W_k d_{\nu(k)})
\end{aligned}$$

For $p+1 \leq k \leq q$ we have to show that $\delta_w(\overline{V}_k) = \delta_w(a_k V_k)$:

$$\begin{aligned}
\delta_w(\overline{V}_k) &\overset{(200)}{=} \delta_w(\boldsymbol{\theta}_k, \overline{V}_k) \\
&\overset{(\mathrm{AB12})}{=} \delta_w(\boldsymbol{\theta}_k, V_k)^{-1} \\
&\overset{(201)}{=} \delta_t(\boldsymbol{\theta}_k, v_k)^{-1} \\
&\overset{(\mathrm{AB12})}{=} \delta_t(\boldsymbol{\theta}_k, v_k^{-1}) \\
&\overset{(198)}{=} \delta_t(\boldsymbol{\theta}_k, a_k v_k) \\
&\overset{(201)}{=} \delta_w(a_k V_k)
\end{aligned}$$

Condition (97): For $1 \leq k \leq p$ we have to show that $(d_{\nu(k)}^{-1} c_{\nu(k)}, c_{\nu(k)} d_{\nu(k)}^{-1}) \in \delta_w(W_k)$. We have

$$\theta_t(W_k) \overset{(192)}{=} \theta_t(d_{\nu(k)}^{-1} \overline{W}_k c_{\nu(k)}^{-1}) \overset{(192)}{=} \theta_t(d_{\nu(k)}^{-1} c_{\nu(k)} W_k d_{\nu(k)} c_{\nu(k)}^{-1}),$$

i.e., $d_{\nu(k)}^{-1} c_{\nu(k)} \theta_t(W_k) = \theta_t(W_k) c_{\nu(k)} d_{\nu(k)}^{-1}$. This implies that

$$(d_{\nu(k)}^{-1} c_{\nu(k)}, c_{\nu(k)} d_{\nu(k)}^{-1}) \in \delta_t(\gamma_w(W_k), \theta_t(W_k)) = \delta_w(W_k).$$

For $p+1 \leq k \leq p+q$, condition (97) is equivalent to $(a_k, a_k) \in \delta_w(V_k)$, which is true, by (203).

Condition (98): This follows from (191), (197), and (200).

Condition (99): First assume that $1 \leq k \leq p$. Since θ_t is an AB-homomorphism, we get:

$$\begin{aligned}
\mu_w(\overline{W}_k) &\overset{(\mathrm{Hom6})}{=} \mu_t(\gamma_w(W_k), \theta_t(\overline{W}_k)) \\
&\overset{(192)}{=} \mu_t(\gamma_w(W_k), \theta_t(c_{\nu(k)} W_k d_{\nu(k)})) \\
&\overset{(\mathrm{Hom6})}{=} \mu_w(c_{\nu(k)} W_k d_{\nu(k)})
\end{aligned}$$

For $p+1 \leq k \leq p+q$ we get:

$$\begin{aligned}
\mu_w(\overline{V}_k) &\overset{(202)}{=} \mu_t(\boldsymbol{\theta}_k, v_k^{-1})) \\
&\overset{(198)}{=} \mu_t(\boldsymbol{\theta}_k, a_k v_k) \\
&\overset{(202)}{=} \mu_w(a_k V_k)
\end{aligned}$$

Condition (109): Recall that $\gamma_w(W_k)$ is an H-type for $1 \leq k \leq p$, and that $\boldsymbol{\theta}_k$ (see the assertion before (197)) is an H-type for $p+1 \leq k \leq p+q$. Hence Φ meets also the requirement (109). This concludes the proof of Claim 7.

Claim 8. θ'_t and Φ fulfill conclusion (184) of the lemma, i.e. $\theta'_t(W) = \theta'_t(\Phi(W))$ for all $W \in \mathcal{W}_t$.

Let us fix $W \in \mathcal{W}_t$.

Case 1. $W = W_k$ where $1 \leq k \leq p$. We have

$$\theta'_t(\Phi(W_k)) \overset{(221)}{=} \theta'_t(c^{-1}_{\nu(k)}\overline{W}_k d^{-1}_{\nu(k)}) \overset{(216)}{=} \theta_t(c^{-1}_{\nu(k)}\overline{W}_k d^{-1}_{\nu(k)}) \overset{(192)}{=} \theta_t(W_k) \overset{(216)}{=} \theta'_t(W_k).$$

Case 2. $W = \overline{W}_k$ where $1 \leq k \leq p$. This case reduces to Case 1, since θ'_t and Φ are AB-homomorphisms and therefore commute with the suitable involutions $\mathbb{I}_w$ and $\mathbb{I}_t$.

Case 3. $W = V_k$ where $p+1 \leq k \leq p+q$. We have

$$\theta'_t(\Phi(V_k)) \overset{(223)}{=} \theta'_t(a^{-1}_k\overline{V}_k) \overset{(215)}{=} a^{-1}_k v^{-1}_k \overset{(198)}{=} v_k \overset{(214)}{=} \theta'_t(V_k).$$

Case 4. $W = \overline{V}_k$ where $p+1 \leq k \leq p+q$. This case reduces to Case 2 with the same argument as for Case 2.

Case 5. $W \in \mathcal{W}$ and W does not fulfill any of the above cases. Then, (224) implies $\theta'_t(\Phi(W)) = \theta'_t(W)$. Claim 8 has been established in all cases.

Claim 9. λ'_i and Φ fulfill conclusion (185) of the lemma i.e. $\lambda'_i(w_i) \simeq_\Phi \lambda'_i(w'_i)$ for all $1 \leq i \leq n+m$.

Let $1 \leq i \leq n+m$. Suppose first that (w_i, w'_i) is one of the pairs of the form (190) (recall that we reduced to the case where $e_i = f_i = 1$). There exists some $k \in [1, p+q]$ such that

$$\lambda_i(w_i) = W_k \text{ and } \lambda_i(w'_i) = c_i^{-1}\overline{W}_k d_i^{-1}. \tag{225}$$

The equality

$$\theta_t(c_i^{-1}\overline{W}_k d_i^{-1}) \overset{(180)}{=} \theta_t(W_k) \overset{(180)}{=} \theta_t(c^{-1}_{\nu(k)}\overline{W}_k d^{-1}_{\nu(k)})$$

shows that $(c_{\nu(k)}c_i^{-1}, d^{-1}_{\nu(k)}d_i) \in \delta_t(\gamma_w(\overline{W}_k), \theta_t(\overline{W}_k))$. Since θ_t is an AB-homomorphism, this implies that

$$(c_{\nu(k)}c_i^{-1}, d^{-1}_{\nu(k)}d_i) \in \delta_w(\overline{W}_k) \tag{226}$$

and thus

$$c_{\nu(k)}c_i^{-1}\overline{W}_k = \overline{W}_k d^{-1}_{\nu(k)}d_i. \tag{227}$$

Let us first suppose that $k \in [1, p]$. Then

$$\lambda'_i(w_i) \overset{(210)}{=} \lambda'(\lambda_i(w_i)) \overset{(207)}{=} W_k \text{ and } \lambda'_i(w'_i) \overset{(210)}{=} \lambda'(\lambda_i(w'_i)) \overset{(207)}{=} c_i^{-1}\overline{W}_k d_i^{-1}. \tag{228}$$

Applying the automorphism Φ on W_k we obtain

$$\Phi(W_k) \overset{(221)}{=} c^{-1}_{\nu(k)}\overline{W}_k d^{-1}_{\nu(k)}. \tag{229}$$

We get

$$\lambda'_i(w_i) \overset{(228)}{=} W_k \overset{(229)}{\simeq_\Phi} c^{-1}_{\nu(k)}\overline{W}_k d^{-1}_{\nu(k)} \overset{(227)}{=} c_i^{-1}\overline{W}_k d_i^{-1} \overset{(228)}{=} \lambda'_i(w'_i).$$

Let us now suppose that $k \in [p+1, p+q]$. Then

$$\lambda'_i(w_i) \overset{(210)}{=} \lambda'(\lambda_i(w_i)) \overset{(205)}{=} U_k V_k \overline{U}_k d^{-1}_{\nu(k)} \text{ and} \tag{230}$$

$$\lambda'_i(w'_i) \overset{(210)}{=} \lambda'(\lambda_i(w'_i)) \overset{(206)}{=} c_i^{-1} d_{\nu(k)} U_k \overline{V}_k \overline{U}_k d_i^{-1}. \tag{231}$$

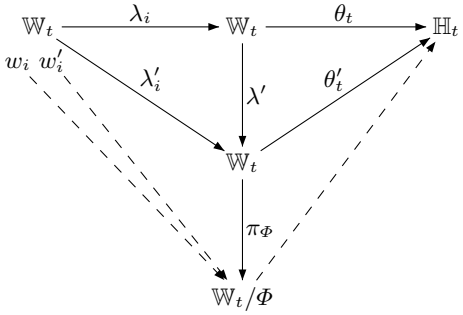


Fig. 13. Lemma 47, Case 1, Claim 8 and 9

Using the definition of Φ, we get

$$\Phi(U_k V_k \overline{U}_k d_{\nu(k)}^{-1}) \overset{(223)}{=} U_k a_k^{-1} \overline{V}_k \overline{U}_k d_{\nu(k)}^{-1}. \tag{232}$$

The commutation (203) can be equivalently formulated as

$$U_k a_k^{-1} = c_{\nu(k)}^{-1} d_{\nu(k)} U_k. \tag{233}$$

We get

$$\lambda_i'(w_i) \overset{(230),(232)}{\simeq_\Phi} U_k a_k^{-1} \overline{V}_k \overline{U}_k d_{\nu(k)}^{-1} \overset{(233)}{=} c_{\nu(k)}^{-1} (d_{\nu(k)} U_k \overline{V}_k \overline{U}_k) d_{\nu(k)}^{-1}. \tag{234}$$

Moreover, (226) and the fact that λ' is an AB-homomorphism implies

$$(c_{\nu(k)} c_i^{-1}, d_{\nu(k)}^{-1} d_i) \in \delta_w(\overline{W}_k) \overset{(\mathrm{Hom7})}{=} \delta_w(\gamma(\overline{W}_k), \lambda'(\overline{W}_k)) \overset{(206)}{=} \delta_w(\gamma(\overline{W}_k), d_{\nu(k)} U_k \overline{V}_k \overline{U}_k)$$

and hence

$$c_{\nu(k)}^{-1} (d_{\nu(k)} U_k \overline{V}_k \overline{U}_k) d_{\nu(k)}^{-1} = c_i^{-1} (d_{\nu(k)} U_k \overline{V}_k \overline{U}_k) d_i^{-1}. \tag{235}$$

Finally, chaining (234), (235), and (231), we obtain $\lambda_i'(w_i) \simeq_\Phi \lambda_i'(w_i')$.

We treat now the pairs (w_i, w_i') of the form (189) by descending induction over i. So, assume that $\lambda_i(w_i) \equiv_i \lambda_i(w_i')$ and $\lambda_j'(w_j) \simeq_\Phi \lambda_j'(w_j')$ for all $j \in [i+1, n+m]$. Hence, $\lambda'(\lambda_j(w_j)) \simeq_\Phi \lambda'(\lambda_j(w_j'))$ for all $j \in [i+1, n+m]$. Recall that the congruence $\equiv_i$ is generated by the set of pairs $P = \{(\lambda_j(w_j), \lambda_j(w_j')) \mid j \in [i+1, n+m]\}$, i.e., $\equiv_i = \equiv_P$. Hence, $\lambda'(P)$ is included in the congruence $\simeq_\Phi$ on $\mathbb{W}$. Therefore, $\lambda_i(w_i) \equiv_P \lambda_i(w_i')$ together with Lemma 3 implies $\lambda_i'(w_i) = \lambda'(\lambda_i(w_i)) \simeq_\Phi \lambda'(\lambda_i(w_i')) = \lambda_i'(w_i')$. We have thus established (185) in all cases.

Claim 10. λ_i' fulfills conclusion (186) of the lemma.

For all $1 \leq i, j \leq n$ we get

$$\lambda_i' \overset{(210)}{=} \lambda_i \circ \lambda' \overset{(181)}{=} \lambda_j \circ \lambda' \overset{(210)}{=} \lambda_j'.$$

Case 2: There exists some $i \in [1, n+m]$, such that neither condition (189) nor (190) holds.

Let $i \in [1, n+m]$ be the minimal integer for which neither (189) nor (190) holds. Let (P_i, P_i') be a distinguishing pair for $(\lambda_i(w_i), \lambda_i(w_i'))$. The generators of the congruence $\equiv_i$ are, by

definition, all pairs $(\lambda_j(w_j), \lambda_j(w'_j))$ for $j \in [i+1, n+m]$. Hence, by Claim 1 and Lemma 36, $\equiv_i$ is also generated by the subset

$$\mathcal{P}_i = \{(\lambda_j(w_j), \lambda_j(w'_j)) \mid j \in [i+1, n+m], \|\lambda_j(w_j)\| \geq 1, \|\lambda_j(w'_j)\| \geq 1\}.$$

Moreover, $\gamma_w(\lambda_j(w_j)) = \gamma_w(\lambda_j(w_j))$ for all pairs $(\lambda_j(w_j), \lambda_j(w'_j)) \in \mathcal{P}_i$ by Claim 1. By Lemma 31, every pair from $\mathcal{P}_i$ belongs to the congruence $\equiv_\gamma$ from (81). Hence $\equiv_i \subseteq \equiv_\gamma$, which implies

$$\gamma_w(P_i) = \gamma_w(P'_i). \tag{236}$$

Moreover, by (180) every element of $\mathcal{P}_i$ belongs to the kernel of θ_t, hence

$$\theta_t(P_i) = \theta_t(P'_i). \tag{237}$$

Lemma 30 and (236) imply

$$P_i \in A \iff P'_i \in A \quad \text{and} \quad P_i \in B \iff P'_i \in B. \tag{238}$$

Lemma 39 applied to $P_i, S_i, P'_i, S'_i \in \mathbb{W}$ asserts that $\gamma_w(S_i) = \gamma_w(S'_i)$ and

$$\theta_t(S_i) = \theta_t(S'_i). \tag{239}$$

As θ_t restricted to A and B is injective by (Hom2), the value $\|S_i\| = 0$ or $\|S'_i\| = 0$ would lead to $S_i = S'_i$ and hence to $\lambda_i(w_i) = P_i S_i \equiv_i P'_i S'_i = \lambda_i(w'_i)$, i.e., to (189), which contradicts the choice of i. Hence, we have

$$\|S_i\| \geq 1, \ \|S'_i\| \geq 1 \text{ and } \gamma_w(S_i) = \gamma_w(S'_i). \tag{240}$$

Recall the definition of $\Delta(P_i, S_i, P'_i, S'_i, \theta_t)$ from (179). Equations (238), (239), and (240) imply

$$\Delta(P_i, S_i, P'_i, S'_i, \theta_t) = 1 - \chi_{AB}(P_i) + 2\chi_H(S_i) + 4\|\theta_t(S_i)\| \tag{241}$$

Since $\|S_i\| \geq 1$ and $\|S'_i\| \geq 1$, we can write S_i and S'_i as

$$S_i = cWL_i \text{ and } S'_i = c'W'L'_i, \tag{242}$$

where $W, W' \in \mathcal{W}$ and $c, c' \in \mathrm{Gi}(W) = \mathrm{Gi}(W')$. Note that $\tau\mathrm{i}(W) = \tau\mathrm{i}(S_i) \overset{(240)}{=} \tau\mathrm{i}(S'_i) = \tau\mathrm{i}(W')$ Hence, either $\gamma_w(W)$ and $\gamma_w(W')$ are both T-types or $\gamma_w(W)$ and $\gamma_w(W')$ are both H-types.

Case 2.1: $\gamma_w(W)$ and $\gamma_w(W')$ are both H-types.

Claim 11. $\gamma_w(W) = \gamma_w(W')$

We know that $\tau\mathrm{i}(W) = \tau\mathrm{i}(W')$. Moreover, the boolean component of $\gamma_w(W)$ and $\gamma_w(W')$ is 0. Hence, it remains to show that $\tau\mathrm{e}(W) = \tau\mathrm{e}(W')$. Assume that $\tau\mathrm{e}(W) \neq \tau\mathrm{e}(W')$. There are several cases according to the possible H-types in (21) and (22), which can be all dealt in the same way. Let us consider the case $\tau\mathrm{e}(W) = (A, T)$ and $\tau\mathrm{e}(W') = (B, T)$. Since $\theta_t(cWL_i) = \theta_t(c'W'L'_i)$ by (239) and (242) and $\theta_t(cW), \theta_t(c'W') \in \mathbb{H}$ we get $\pi_t(\theta_t(L_i)) = \pi_t(\theta_t(L'_i))$. Moreover, by (240) there exists a vertex type θ such that $\gamma_t(\theta_t(L_i))$ contains a path type of the form $(A, T, *, \theta)$ and $\gamma_t(\theta_t(L'_i))$ contains a path type of the form $(B, T, *, \theta)$. But this contradicts $\pi_t(\theta_t(L_i)) = \pi_t(\theta_t(L'_i))$. This proves Claim 11.

Let $\gamma_w(W) = \gamma_w(W') = \{\boldsymbol{\theta}\}$ in the following.

Claim 12. There exists a path type $\boldsymbol{\rho} \in \gamma_w(L_i) \cap \gamma_w(L_i') \neq \emptyset$ such that $\boldsymbol{\theta\rho}$ is defined.

There exist $\boldsymbol{\rho} \in \gamma_w(L_i)$ and $\boldsymbol{\rho'} \in \gamma_w(L_i')$ such that $\{\boldsymbol{\theta\rho}\} = \gamma_w(S_i) = \gamma_w(S_i') = \{\boldsymbol{\theta\rho'}\}$. Hence, $\tau\mathrm{i}(\boldsymbol{\rho}) = \tau\mathrm{e}(\boldsymbol{\theta}) = \tau\mathrm{i}(\boldsymbol{\rho'})$ and $\tau\mathrm{e}(\boldsymbol{\rho}) = \tau\mathrm{e}(\boldsymbol{\rho'})$. Moreover, the boolean component of $\boldsymbol{\rho}$ is 1 if and only if the boolean component of $\gamma_w(S_i) = \gamma_w(S_i')$ is 1 if and only if the boolean component of $\boldsymbol{\rho'}$ is 1. Hence $\boldsymbol{\rho} = \boldsymbol{\rho'}$. This proves Claim 12.

Claim 12 implies

$$L_i \in A \iff L_i' \in A \quad \text{and} \quad L_i \in B \iff L_i' \in B. \tag{243}$$

If, e.g., $L_i \in A$ and $\|L_i'\| \geq 1$ then $\gamma_w(L_i) \cap \gamma_w(L_i') = \emptyset$ (note that no product of H-types is of the form $(\theta, 0, \theta)$ for a vertex type θ). Morevoer $\gamma_w(a) \cap \gamma_w(b) = \emptyset$ for all $a \in A \setminus \{1\}$ and $b \in B \setminus \{1\}$.

Since θ_t is an AB-homomorphism, we have $\boldsymbol{\theta} \in \gamma_t(\theta_t(cW)) \cap \gamma_t(\theta_t(c'W'))$ and $\boldsymbol{\rho} \in \gamma_t(\theta_t(L_i)) \cap \gamma_t(\theta_t(L_i'))$. Lemma 27 applied to the identity $\theta_t(cW)\theta_t(L_i) = \theta_t(S_i) = \theta_t(S_i') = \theta_t(c'W')\theta_t(L_i')$ yields $d \in \mathrm{Ge}(\boldsymbol{\theta}) = \mathrm{Gi}(\boldsymbol{\rho})$ such that

$$\theta_t(cWd) = \theta_t(c'W') \text{ and } \theta_t(L_i) = \theta_t(dL_i'). \tag{244}$$

Since $\theta_t(W), \theta_t(W') \in \mathbb{H}$, we have

$$\|\theta_t(L_i)\| = \|\theta_t(dL_i')\| = \|\theta_t(S_i)\|. \tag{245}$$

Claim 13. $\Delta(P_icWd, d^{-1}L_i, P_i'c'W', L_i', \theta_t) < \Delta(P_i, S_i, P_i', S_i', \theta_t)$

We have

$$\begin{aligned}
\Delta(P_icWd, d^{-1}L_i, P_i'c'W', L_i', \theta_t) &\overset{(179)}{=} 1 - \frac{1}{2}\Big(\chi_{AB}(P_icWd) + \chi_{AB}(P_i'c'W')\Big) + \\
&\qquad \chi_H(d^{-1}L_i) + \chi_H(L_i') + 2\|\theta_t(d^{-1}L_i)\| + 2\|\theta_t(L_i')\| \\
&\overset{(245)}{=} 1 + \chi_H(L_i) + \chi_H(L_i') + 4\|\theta_t(S_i)\| \\
\\
\Delta(P_i, S_i, P_i', S_i', \theta_t) &\overset{(241)}{=} 1 - \chi_{AB}(P_i) + 2\chi_H(S_i) + 4\|\theta_t(S_i)\| \\
&\geq 2\chi_H(S_i) + 4\|\theta_t(S_i)\|.
\end{aligned}$$

We claim that $\chi_H(L_i) = \chi_H(L_i') = \chi_H(S_i) - 1$, which implies the claim. We distinguish several cases according to the H-type $\boldsymbol{\theta}$ of W and W'.

Case A. $\boldsymbol{\theta}$ has the form $(*, H, 0, 1, 1)$: Then $\gamma_w(S_i)$ has the form $\{(*, H, *, *, *)\}$. Moreover, a path type of the form $(1, 1, *, *, *)$ belongs to both $\gamma_w(L_i)$ and $\gamma_w(L_i')$. But this already implies $L_i = L_i' = 1$. Hence, $|\gamma_w(L_i)| = |\gamma_w(L_i')| > 1$. We get $\chi_H(L_i) = \chi_H(L_i') = 0$. Moreover, $\gamma_w(S_i)$ has the form $\{(*, H, 0, 1, 1)\}$. This implies $\chi_H(S_i) = 1$.

Case B. $\boldsymbol{\theta}$ has the form $(*, H, 0, *, T)$: Again, $\gamma_w(S_i)$ has the form $\{(*, H, *, *, *)\}$. Moreover, $\gamma_w(L_i)$ and $\gamma_w(L_i')$ contain a path type of the form $(*, T, *, *, *)$. We distinguish the following three subcases:

Case B.1 $\gamma_w(S_i)$ has the form $\{(*, H, 0, *, *)\}$: We get $\chi_H(S_i) = 1$. Moreover, $\gamma_w(L_i)$ and $\gamma_w(L_i')$ contain a path type of the form $(*, T, 0, *, *)$. Note that there is no proper product of H-types and T-type of this form. Hence, $|\gamma_w(L_i)|, |\gamma_w(L_i)| > 1$ and $\chi_H(L_i) = \chi_H(L_i') = 0$.

Case B.2 $\gamma_w(S_i)$ has the form $\{(*, H, 1, *, T)\}$: We get $\chi_H(S_i) = 2$. Moreover, $\gamma_w(L_i)$ and $\gamma_w(L'_i)$ contain a path type of the form $(*, T, 1, *, T)$. But this implies $\gamma_w(L_i) = \gamma_w(L'_i) = \{(*, T, 1, *, T)\}$ and $\chi_H(L_i) = \chi_H(L'_i) = 1$.

Case B.3 $\gamma_w(S_i)$ has the form $\{(*, H, 1, *, H)\}$: We get $\chi_H(S_i) = 1$. Moreover, $\gamma_w(L_i)$ and $\gamma_w(L'_i)$ contain a path type of the form $(*, T, 1, *, H)$. But this implies $\gamma_w(L_i) = \gamma_w(L'_i) = \{(*, T, 1, *, H)\}$ and $\chi_H(L_i) = \chi_H(L'_i) = 0$.

Case B.4 $\gamma_w(S_i)$ has the form $\{(*, H, 1, 1, 1)\}$: We get $\chi_H(S_i) = 2$. Moreover, $\gamma_w(L_i)$ and $\gamma_w(L'_i)$ contain a path type of the form $(*, T, 1, 1, 1)$. But this implies $\gamma_w(L_i) = \gamma_w(L'_i) = \{(*, T, 1, 1, 1)\}$ and $\chi_H(L_i) = \chi_H(L'_i) = 1$. This concludes the proof of Claim 13.

Case 2.1.1. $W' = W$: As the AB-homomorphism θ_t is δ-preserving by (Hom7), $\theta_t(cWd) = \theta_t(c'W)$ implies $cWd = c'W$. Hence, we have $P_i cWd \equiv_i P'_i c'W$. Together with Claim 13, this violates the hypothesis of minimality in the choice of decomposition (187). This case is thus impossible.

Case 2.1.2. $W' = \overline{W}$: Hence, $\gamma_w(W) = \{\boldsymbol{\theta}\} = \gamma_w(\overline{W})$ and we get

$$\boldsymbol{\theta} \in \{(A, H, 0, A, T), (B, H, 0, B, T), (1, H, 0, 1, 1)\}. \tag{246}$$

Hence, $\gamma_w(S_i)$ has the form $\{(*, H, *, *, *)\}$ and we get

$$\chi_H(S_i) \geq 1 \tag{247}$$

Moreover, by (238) and (243) we either have $P_i, P'_i \notin A \cup B$ or $L_i, L'_i \notin A \cup B$, because otherwise the index i would satisfy (190), which we exclude in Case 2.

Let us define a new equation (w_{n+m+1}, w'_{n+m+1}) with

$$w_{n+m+1} = cWd \quad \text{and} \quad w'_{n+m+1} = c'\overline{W} \tag{248}$$

and the AB-morphisms

$$\lambda'_i = \lambda_i \text{ for all } 1 \leq i \leq n+m \quad \text{and} \quad \lambda'_{n+m+1} = \mathrm{Id}_{\mathbb{W}_t}. \tag{249}$$

Hence, $\gamma_w(w_{n+m+1}) = \gamma_w(w'_{n+m+1})$. Let

$$\mathcal{S}' = \{(w_i, w'_i) \mid 1 \leq i \leq n+m+1\} \quad \text{and} \quad \boldsymbol{\lambda'} = (\lambda_i)_{1 \leq i \leq n+m+1}. \tag{250}$$

The triple $(\mathcal{S}', \boldsymbol{\lambda'}, \theta_t)$ fulfills the hypothesis of Lemma 47 (condition (180) for the new equation (w_{n+m+1}, w'_{n+m+1}) follows from (244)). Moreover, w.r.t. this triple, we have

$$P_i cWd \equiv_i P'_i c'\overline{W}.$$

The definition of Δ_i and Claim 13 imply

$$\Delta_i(\mathcal{S}', \boldsymbol{\lambda'}, \theta_t) < \Delta_i(\mathcal{S}, \boldsymbol{\lambda}, \theta_t). \tag{251}$$

Let us now bound the size of $\Delta(P_i, S_i, P'_i, S'_i, \theta_t)$:

$$\begin{aligned} \Delta(P_i, S_i, P'_i, S'_i, \theta_t) &\overset{(241)}{=} 1 - \chi_{AB}(P_i) + 2\chi_H(S_i) + 4\|\theta_t(S_i)\| \\ &\overset{(247)}{\geq} 3 - \chi_{AB}(P_i) + 4\|\theta_t(S_i)\| \end{aligned}$$

In case $P_i, P_i' \notin A \cup B$, we have $\chi_{AB}(P_i) = 0$ and hence $\Delta(P_i, S_i, P_i', S_i', \theta_t) \geq 3$. In case $P_i, P_i' \in A \cup B$ we have $L_i, L_i' \notin A \cup B$ (as argued above) and $\chi_{AB}(P_i) = 1$. Hence, $\Delta(P_i, S_i, P_i', S_i', \theta_t) \geq 2 + 4\|\theta_t(S_i)\|$. Since $L_i \notin A \cup B$ and $\gamma_w(L_i) \neq \emptyset$, we can write L_i as $L_i = eUK_i$ for some $U \in \mathcal{W}$ and $e \in \mathrm{Gi}(U)$. Moreover, (246) and $\tau\mathrm{i}(U) = \tau\mathrm{e}(W)$ imply that $\gamma_w(U)$ has the form $\{(*, T, *, *, *)\}$ or $\{(1, 1, *, *, *)\}$. The latter is not possible (it is neither an H-type nor a T-type), hence $\gamma_w(U)$ has the form $\{(*, T, *, *, *)\}$, i.e., it is a T-type. This implies $\|\theta_t(S_i)\| = \|\theta_t(L_i)\| \geq \|\theta_t(U)\| \geq 1$. This implies $\Delta(P_i, S_i, P_i', S_i', \theta_t) \geq 2 + 4\|\theta_t(S_i)\| \geq 6$. In both cases, we have shown

$$\Delta_i(\mathcal{S}, \boldsymbol{\lambda}, \theta_t) = \Delta(P_i, S_i, P_i', S_i', \theta_t) \geq 3. \tag{252}$$

Let us choose

$$P_{n+m+1} = \varepsilon, \quad P'_{n+m+1} = \varepsilon, \quad S_{n+m+1} = cWd, \quad S'_{n+m+1} = c'\overline{W}.$$

Since $\|\theta_t(W)\| = \|\theta_t(\overline{W})\| = 0$ (we have $\theta_t(W), \theta_t(\overline{W}) \in \mathbb{H}$ since $\gamma_w(W)$ is an H-type) we have

$$\begin{aligned}\Delta(P_{n+m+1}, S_{n+m+1}, P'_{n+m+1}, S'_{n+m+1}, \theta_t) &= 1 - \chi_{AB}(\varepsilon) + \chi_H(W) + \chi_H(\overline{W}) + \\ &\qquad 2\|\theta_t(W)\| + 2\|\theta_t(\overline{W})\| \\ &= 1 - 1 + 2 + 0 \\ &= 2. \end{aligned} \tag{253}$$

Finally, using (252) and (253), we obtain:

$$\begin{aligned}\Delta_{n+m+1}(\mathcal{S}', \boldsymbol{\lambda}', \theta_t) &\leq \Delta(P_{n+m+1}, S_{n+m+1}, P'_{n+m+1}, S'_{n+m+1}, \theta_t) \\ &= 2 \\ &< 3 \\ &\leq \Delta_i(\mathcal{S}, \boldsymbol{\lambda}, \theta_t). \end{aligned} \tag{254}$$

The above inequalities (251) and (254) prove that

$$\{\{\Delta_i(\mathcal{S}', \boldsymbol{\lambda}', \theta_t), \Delta_{n+m+1}(\mathcal{S}', \boldsymbol{\lambda}', \theta_t')\}\} < \{\{\Delta_i(\mathcal{S}, \boldsymbol{\lambda}, \theta_t)\}\}$$

w.r.t. the partial ordering on finite multisets of naturals induced by the ordering on $\mathbb{N}$. Moreover, for $1 \leq j \leq n + m$ with $j \neq i$ we have $\Delta_j(\mathcal{S}', \boldsymbol{\lambda}', \theta_t) \leq \Delta_j(\mathcal{S}, \boldsymbol{\lambda}, \theta_t)$. Hence

$$\|(\mathcal{S}', \boldsymbol{\lambda}', \theta_t)\| < \|(\mathcal{S}, \boldsymbol{\lambda}, \theta_t)\|.$$

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.

Case 2.1.3. $W' \notin \{W, \overline{W}\}$: Let us consider the monoid homomorphism $\lambda' : \mathbb{W} \to \mathbb{W}$ fulfilling:

$$\lambda'(e) = e \text{ for all } e \in A \cup B \tag{255}$$
$$\lambda'(W) = c^{-1}c'W'd^{-1} \tag{256}$$
$$\lambda'(\overline{W}) = d\overline{W'}c'^{-1}c \tag{257}$$
$$\lambda'(W'') = W'' \text{ for all } W'' \in \mathcal{W} \setminus \{W, \overline{W}\} \tag{258}$$

This definition is written for the case where $W \in \widehat{\mathcal{W}}$. In the case where $W \notin \widehat{\mathcal{W}}$, line (257) of this definition must be cancelled. Such a homomorphism exists because (244) ensures that

$$\delta_w(W) = \delta_t(\boldsymbol{\theta}, \theta_t(W)) \overset{(244)}{=} \delta_t(\boldsymbol{\theta}, \theta_t(c^{-1}c'W'd^{-1})) = \delta_w(c^{-1}c'W'd^{-1}) = \delta_w(\lambda'(W))$$

(and analogously $\delta_w(\overline{W}) = \delta_w(\lambda'(\overline{W}))$ in case $W \in \widehat{\mathcal{W}}$). The same argument shows that λ' also preserves μ_w. Moreover, λ' preserves γ_w, since $\gamma_w(W) = \gamma_w(W') = \gamma_w(\lambda'(W))$ by Claim 11. The submonoid $\mathrm{dom}(\mathbb{I}_w)$ is preserved by λ' because we have

$$\begin{aligned} W \in \widehat{\mathcal{W}} &\iff cWd \in \mathrm{dom}(\mathbb{I}_w) \\ &\iff \theta_t(cWd) \in \mathrm{dom}(\mathbb{I}_t) \\ &\overset{(244)}{\iff} \theta_t(c'W') \in \mathrm{dom}(\mathbb{I}_t) \\ &\iff c'W' \in \mathrm{dom}(\mathbb{I}_w) \\ &\iff W' \in \widehat{\mathcal{W}}. \end{aligned}$$

Finally, λ' preserves the partial involution $\mathbb{I}_w$ because (in case $W \in \widehat{\mathcal{W}}$)

$$\lambda'(\overline{W}) = d\overline{W'}c'^{-1}c = \mathbb{I}_w(c^{-1}c'W'd^{-1}) = \mathbb{I}_w(\lambda'(W)).$$

Hence, Lemma 23 implies that λ' is an AB-homomorphism. Let us define $\boldsymbol{\lambda}' = (\lambda_i \circ \lambda')_{1 \leq i \leq n+m}$. Since $\mathrm{Alph}(\mathcal{S}, \boldsymbol{\lambda}') = \mathrm{Alph}(\mathcal{S}, \boldsymbol{\lambda}) \setminus \{W, \overline{W}\}$, the inequality $\mathrm{A}(\mathcal{S}, \boldsymbol{\lambda}') < \frac{1}{2}\mathrm{Card}(\mathcal{V}_0)$ still holds. Moreover, we have

$$\theta_t(\lambda'(W)) \overset{(256)}{=} \theta_t(c^{-1}c'W'd^{-1}) \overset{(244)}{=} \theta_t(W)$$

and hence (in case $W \in \widehat{\mathcal{W}}$) also $\theta_t(\lambda'(\overline{W})) = \theta_t(\overline{W})$. Since moreover $\theta_t(\lambda'(W'')) = \theta_t(W'')$ for all $W'' \in \mathcal{W} \setminus \{W, \overline{W}\}$, we get $\theta_t = \lambda' \circ \theta_t$. This implies

$$\theta_t(\lambda'(\lambda_i(w_i))) = \theta_t(\lambda_i(w_i)) \overset{(180)}{=} \theta_t(\lambda_i(w_i')) = \theta_t(\lambda'(\lambda_i(w_i'))).$$

It follows that the triple $(\mathcal{S}, \boldsymbol{\lambda}', \theta_t)$ fulfills the hypothesis of Lemma 47. W.r.t. to this triple we have $\lambda'(P_i) \equiv_i \lambda'(P_i')$ (since $P_i \equiv_i P_i'$ w.r.t. $(\mathcal{S}, \boldsymbol{\lambda}, \theta_t)$). Hence, we have

$$\lambda'(P_i cWd) \equiv_i \lambda'(P_i' c'W'). \tag{259}$$

Also note that for all $w \in \mathbb{W}$ we have $\chi_{AB}(w) = \chi_{AB}(\lambda'(w))$ and $\chi_H(w) = \chi_H(\lambda'(w))$, since w and $\lambda'(w)$ have the same type by Claim 11, which uniquely determines the value under χ_H. Furthermore, also $\|\theta_t(w)\| = \|\theta_t(\lambda'(w))\|$. This implies that

$$\begin{aligned} \Delta_i(\mathcal{S}, \boldsymbol{\lambda}', \theta_t) &\overset{(259)}{\leq} \Delta(\lambda'(P_i cWd), \lambda'(d^{-1}L_i), \lambda'(P_i' c'W'), \lambda'(L_i'), \theta_t) \\ &= \Delta(P_i cWd, d^{-1}L_i, P_i' c'W', L_i', \theta_t) \\ &\overset{\text{Claim 13}}{<} \Delta(P_i, S_i, P_i', S_i', \theta_t) \\ &= \Delta_i(\mathcal{S}, \boldsymbol{\lambda}, \theta_t). \end{aligned}$$

Hence, we have $\|(\mathcal{S}, \boldsymbol{\lambda}', \theta_t)\| < \|(\mathcal{S}, \boldsymbol{\lambda}, \theta_t)\|$, i.e., the triple $(\mathcal{S}, \boldsymbol{\lambda}', \theta_t)$ fulfills the hypothesis of Lemma 47 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.

Case 2.2: $\gamma_w(W)$ and $\gamma_w(W')$ are T-types and $W' \in \{W, \overline{W}\}$. This implies $\|\theta_t(cW)\| = \|\theta_t(c'W')\| \geq 1$. In view of this equality, and equations (239) and (242), point (1) of Lemma 28 applies. Hence, there exists $d \in \mathrm{Ge}(W)$ such that

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

Next, let us show:

Claim 14. $\Delta(P_icWd, d^{-1}L_i, P'_ic'W', L'_i, \theta_t) < \Delta(P_i, S_i, P'_i, S'_i, \theta_t)$.

First note that

$$\|\theta_t(d^{-1}L_i)\| = \|\theta_t(L_i)\| = \|\theta_t(S_i)\| - \|\theta_t(W)\| \leq \|\theta_t(S_i)\| - 1 \text{ and} \tag{260}$$

$$\|\theta_t(L'_i)\| = \|\theta_t(S'_i)\| - \|\theta_t(W')\| \leq \|\theta_t(S'_i)\| - 1 \overset{(239)}{=} \|\theta_t(S_i)\| - 1, \tag{261}$$

because W and W' have a T-type and therefore $\|\theta_t(W)\|, \|\theta_t(W')\| \geq 1$. Next, we claim that

$$\chi_H(d^{-1}L_i) = \chi_H(L_i) \leq \chi_H(S_i) + 1 \quad \text{and} \quad \chi_H(L'_i) \leq \chi_H(S_i) + 1. \tag{262}$$

The case that $\chi_H(S_i) \geq 1$ is clear. Hence, assume that $\chi_H(S_i) = 0$, i.e., $\gamma_w(S_i)$ has the form $\{(*, T, 1, *, H)\}$. Since $S_i = cWL_i$, $\gamma_w(L_i)$ cannot have the form $\{(*,*,*,*,T)\}$ or $\{(*,*,*,1,1)\}$. Thus, $\chi_H(L_i) \leq 1$, and (262) holds for L_i. For L'_i the same argument holds (note that $\gamma_w(S_i) = \gamma_w(S'_i)$ by (240)).

Since $\chi_{AB}(P_icWd) = \chi_{AB}(P'_ic'W') = 0$, we get

$$\begin{aligned}
\Delta(P_icWd, d^{-1}L_i, P'_ic'W', L'_i, \theta_t) &\overset{(179)}{=} 1 - \frac{1}{2}\Big(\chi_{AB}(P_icWd) + \chi_{AB}(P'_ic'W')\Big) + \\
&\quad \chi_H(d^{-1}L_i) + \chi_H(L'_i) + 2\|\theta_t(d^{-1}L_i)\| + 2\|\theta_t(L'_i)\| \\
&\overset{(260)\text{–}(262)}{\leq} 1 + 2\chi_H(S_i) + 2 + 4\|\theta_t(S_i)\| - 4 \\
&= 2\chi_H(S_i) + 4\|\theta_t(S_i)\| - 1 \\
&\overset{(241)}{<} \Delta(P_i, S_i, P'_i, S'_i, \theta_t).
\end{aligned}$$

This proves Claim 14.

Case 2.2.1. $W' = W$: Then, as in Case 2.1.1, $\theta_t(cWd) = \theta_t(c'W)$ implies $cWd = c'W$ and hence $P_icWd \equiv_i P'_ic'W$. With Claim 14, this contradicts the minimality of $\Delta(P_i, S_i, P'_i, S'_i, \theta_t)$.

Case 2.2.2. $W' = \overline{W}$: By (242) and (240) we have $\gamma_w(cWL_i) = \gamma_w(S_i) = \gamma_w(S'_i) = \gamma_w(c'\overline{W}L'_i)$. Hence, $\tau\mathrm{e}(\overline{W}) = \tau\mathrm{i}(W) = \tau\mathrm{i}(\overline{W}) = \tau\mathrm{e}(W)$ and we get $\gamma_w(W) = \gamma_w(\overline{W})$. Since this is a T-type, we have $\gamma_w(W) = (C, T, 1, C, H) = \gamma_w(\overline{W})$ for either $C = A$ or $C = B$. We claim that

$$L_i \in A \iff L'_i \in A \quad \text{and} \quad L_i \in B \iff L'_i \in B. \tag{263}$$

Assume that, e.g., $L_i \in A \cup B$. We must have $L_i \in C$, otherwise $\gamma_w(S_i) = \gamma_w(cWL_i) = \emptyset$. Hence, $d^{-1}L_i \in C$ and $\theta_t(L'_i) = \theta_t(d^{-1}L_i) \in C \subseteq \mathbb{H}$. This implies that $\gamma_t(\theta_t(L'_i))$ only contains path types, whose boolean component is 0. Since $\gamma_w(L'_i) \subseteq \gamma_t(\theta_t(L'_i))$ the same holds for $\gamma_w(L'_i)$. Moreover, $(C, T, 1, C, H) = \gamma_w(S_i) = \gamma_w(S'_i) = \gamma_w(c'\overline{W}L'_i)$. Since $\gamma_w(\overline{W}) = (C, T, 1, C, H)$, $(C, H, 0, C, H)$ must be a path type of L'_i. We obtain $L'_i \in C$, since no product of H-types is of the form $(C, H, 0, C, H)$.

A new system $\mathcal{S}'$ and tuple $\boldsymbol{\lambda}'$ of AB-homomorphisms can be defined as in (248)–(250) in Case 2.1.2. Note that $\gamma_w(w_{n+m+1}) = \gamma_w(cWd) = \gamma_w(c'\overline{W}) = \gamma_w(w'_{n+m+1})$ since $\gamma_w(W) = \gamma_w(\overline{W})$. The triple $(\mathcal{S}', \boldsymbol{\lambda}', \theta_t)$ satisfies all hypothesis of Lemma 47. Moreover, w.r.t. the triple $(\mathcal{S}', \boldsymbol{\lambda}', \theta_t)$ we have

$$P_i cWd \equiv_i P'_i c'\overline{W}.$$

The definition of Δ_i and Claim 14 imply

$$\Delta_i(\mathcal{S}', \boldsymbol{\lambda}', \theta_t) < \Delta_i(\mathcal{S}, \boldsymbol{\lambda}, \theta_t). \tag{264}$$

Let us define

$$P_{n+m+1} = \varepsilon, \quad P'_{n+m+1} = \varepsilon, \quad S_{n+m+1} = cWd, \quad S'_{n+m+1} = c'\overline{W}.$$

Note that $\chi_H(W) = \chi_H(\overline{W}) = 0$. Hence, we get

$$\begin{aligned}\Delta(P_{n+m+1}, S_{n+m+1}, P'_{n+m+1}, S'_{n+m+1}, \theta_t) &= 1 - \chi_{AB}(\varepsilon) + \chi_H(W) + \chi_H(\overline{W}) + \\ &\quad 2\|\theta_t(W)\| + 2\|\theta_t(\overline{W})\| \\ &= 4\|\theta_t(W)\|. \end{aligned} \tag{265}$$

Next, let us estimate the size of

$$\Delta_i(\mathcal{S}, \boldsymbol{\lambda}, \theta_t) = \Delta(P_i, S_i, P'_i, S'_i, \theta_t) \overset{(241)}{=} 1 - \chi_{AB}(P_i) + 2\chi_H(S_i) + 4\|\theta_t(S_i)\|.$$

We claim that

$$1 - \chi_{AB}(P_i) + 2\chi_H(S_i) + 4\|\theta_t(S_i)\| > 4\|\theta_t(W)\|, \tag{266}$$

which implies

$$\begin{aligned}\Delta_i(\mathcal{S}, \boldsymbol{\lambda}, \theta_t) &> 4\|\theta_t(W)\| \\ &\overset{(265)}{=} \Delta(P_{n+m+1}, S_{n+m+1}, P'_{n+m+1}, S'_{n+m+1}, \theta_t) \\ &\geq \Delta_{n+m+1}(\mathcal{S}', \boldsymbol{\lambda}', \theta_t). \end{aligned} \tag{267}$$

So, let us prove (266). We distinguish the cases $P_i \in A \cup B$ and $P_i \notin A \cup B$. If $P_i \notin A \cup B$, then $\chi_{AB}(P_i) = 0$ and hence

$$1 - \chi_{AB}(P_i) + 2\chi_H(S_i) + 4\|\theta_t(S_i)\| = 1 + 2\chi_H(S_i) + 4\|\theta_t(S_i)\| > 4\|\theta_t(S_i)\| \geq 4\|\theta_t(W)\|.$$

Now assume that $P_i \in A \cup B$. From (238) we get $P'_i \in A \cup B$. If moreover $L_i \in A \cup B$, then also $L'_i \in A \cup B$ by (263). But then the index i satisfies (190), which we exclude in Case 2. Hence, we must have $L_i \notin A \cup B$. We have

$$1 - \chi_{AB}(P_i) + 2\chi_H(S_i) + 4\|\theta_t(S_i)\| = 2\chi_H(S_i) + 4\|\theta_t(S_i)\|.$$

If moreover $\|\theta_t(L_i)\| \geq 1$ then $\|\theta_t(S_i)\| = \|\theta_t(W)\| + \|\theta_t(L_i)\| > \|\theta_t(W)\|$ and hence $2\chi_H(S_i) + 4\|\theta_t(S_i)\| > 4\|\theta_t(W)\|$. If $\|\theta_t(L_i)\| = 0$, then $\|\theta_t(S_i)\| = \|\theta_t(W)\|$ and all symbols from $\mathcal{W}$ that occur in L_i have H-types. Since $L_i \notin A \cup B$, there is at least one such symbol. It follows that $\gamma_w(S_i)$ is either of the form $\{(*, T, 1, *, T)\}$ or of the form $\{(*, T, 1, 1, 1)\}$. In both cases we

get $\chi_H(S_i) = 1$ and hence again $2\chi_H(S_i) + 4\|\theta_t(S_i)\| = 2 + 4\|\theta_t(W)\| > \|\theta_t(W)\|$. This proves (266) and hence (267). Together with (264), we get

$$\|(\mathcal{S}', \boldsymbol{\lambda}', \theta_t)\| < \|(\mathcal{S}, \boldsymbol{\lambda}, \theta_t)\|.$$

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.

Case 2.3. $W' \notin \{W, \overline{W}\}$ and $\gamma_w(W)$, $\gamma_w(W')$ are T-types: By (239), $\theta_t(cWL_i) = \theta_t(c'W'L_i')$. Using that $\gamma_w(W)$ and $\gamma_w(W')$ are T-types, we can apply Lemma 28 with $P = \theta_t(cW)$, $P' = \theta_t(cW')$, $S = \theta_t(L_i)$, and $S' = \theta_t(L_i')$. We distinguish 3 subcases according to which point of Lemma 28 occurs.

Case 2.3.1. $\|\theta_t(cW)\| = \|\theta_t(c'W')\|$ (and hence $\|\theta_t(W)\| = \|\theta_t(W')\|$): This corresponds to point (1) of Lemma 28: There exists some $d \in \mathrm{Ge}(W)$ such that

$$\theta_t(cWd) = \theta_t(c'W') \quad \text{and} \quad \theta_t(L_i) = \theta_t(dL_i'). \tag{268}$$

Claim 15. $\Delta(P_icWd, d^{-1}L_i, P_i'c'W', L_i', \theta_t) < \Delta(P_i, S_i, P_i', S_i', \theta_t)$.

The same arguments as for Claim 14 in Case 2.2 apply (the crucial hypothesis that $\|\theta_t(W)\| = \|\theta_t(W')\| \geq 1$ is still valid).

Moreover, $\gamma_w(W) = \gamma_w(W')$. We can end this case as for Case 2.1.3: Using (268) and $\gamma_w(W) = \gamma_w(W')$, we can define an AB-homomorphism λ' as in (255)–(258). Then, we define $\boldsymbol{\lambda}' = (\lambda_i \circ \lambda')_{1 \leq i \leq n+m}$. We get again (259) for the triple $(\mathcal{S}, \boldsymbol{\lambda}', \theta_t)$. The definition of λ' implies that for all $w \in \mathbb{W}$: $\chi_{AB}(w) = \chi_{AB}(\lambda'(w))$, $\chi_H(w) = \chi_H(\lambda'(w))$ (since w and $\lambda'(w)$ have the same type), and $\|\theta_t(w)\| = \|\theta_t(\lambda'(w))\|$ (since $\|\theta_t(W)\| = \|\theta_t(W')\|$). This allows to derive $\Delta_i(\mathcal{S}, \boldsymbol{\lambda}', \theta_t) < \Delta_i(\mathcal{S}, \boldsymbol{\lambda}, \theta_t)$ in the same way as in Case 2.1.3 (using Claim 15 instead of Claim 13). We can conclude as in Case 2.1.3.

Case 2.3.2. $\|\theta_t(cW)\| < \|\theta_t(c'W')\|$: This corresponds to point (2) of Lemma 28: Let $\gamma_w(W) = \{\boldsymbol{\theta}\}$, $\gamma_w(W') = \{\boldsymbol{\theta}'\}$, $\boldsymbol{\rho} \in \gamma_w(L_i)$ and $\boldsymbol{\rho}' \in \gamma_w(L_i')$ such that $\boldsymbol{\theta}\boldsymbol{\rho} = \boldsymbol{\theta}'\boldsymbol{\rho}'$. By point (2) of Lemma 28, there exist $d \in \mathrm{Ge}(W)$ and $P_1', P_2', P_3' \in \mathbb{H}_t$ such that P_1' has the T-type $\boldsymbol{\theta}$, P_3' has a T-type $\boldsymbol{\theta}_3'$, P_2' has an H-type $\boldsymbol{\theta}_2'$, and

$$\theta_t(cW) = P_1'd,\ \theta_t(c'W') = P_1'P_2'P_3',\ \theta_t(dL_i) = P_2'P_3'\theta_t(L_i'),\ \boldsymbol{\theta}' = \boldsymbol{\theta}\boldsymbol{\theta}_2'\boldsymbol{\theta}_3',\ \boldsymbol{\rho} = \boldsymbol{\theta}_2'\boldsymbol{\theta}_3'\boldsymbol{\rho}'. \tag{269}$$

Note that $\|L_i\| \geq 1$, because otherwise we have $\theta_t(L_i) \in \mathbb{H}$, which contradicts the fact that P_3' has a T-type. Hence, $\gamma_w(dL_i) = \{\boldsymbol{\rho}\} = \{\boldsymbol{\theta}_2'\boldsymbol{\theta}_3'\boldsymbol{\rho}'\}$. Let us apply Lemma 40 to the AB-homomorphism θ_t, the equality $\theta_t(dL_i) = P_2'(P_3'\theta_t(L_i'))$, the H-type $\boldsymbol{\theta}_2' \in \gamma_t(P_2')$, and the type $\boldsymbol{\theta}_3'\boldsymbol{\rho}' \in \gamma_t(P_3'\theta_t(L_i'))$ (note that $\gamma_w(dL_i) = \{\boldsymbol{\theta}_2'\boldsymbol{\theta}_3'\boldsymbol{\rho}'\}$ as required in Lemma 40). We obtain $\hat{P}_2, S \in \mathbb{W}_t$ with

$$dL_i = \hat{P}_2S, \quad \theta_t(\hat{P}_2) = P_2', \quad \gamma_w(\hat{P}_2) = \{\boldsymbol{\theta}_2'\}, \quad \theta_t(S) = P_3'\theta_t(L_i'), \quad \boldsymbol{\theta}_3'\boldsymbol{\rho}' \in \gamma_w(S). \tag{270}$$

see Figure 14.

Let us first assume that $W' \in \widehat{\mathcal{W}}$. Hence, also $c'W' \in \widehat{\mathbb{W}}$. Axiom (Hom3) on AB-homomorphisms implies that $P_1'P_2'P_3' \in \mathrm{dom}(\mathbb{I}_t)$. Axiom (AB5) implies that $P_1', P_2', P_3' \in \mathrm{dom}(\mathbb{I}_t)$ and axiom (Hom3) implies that

$$W, \hat{P}_2 \in \widehat{\mathbb{W}}. \tag{271}$$

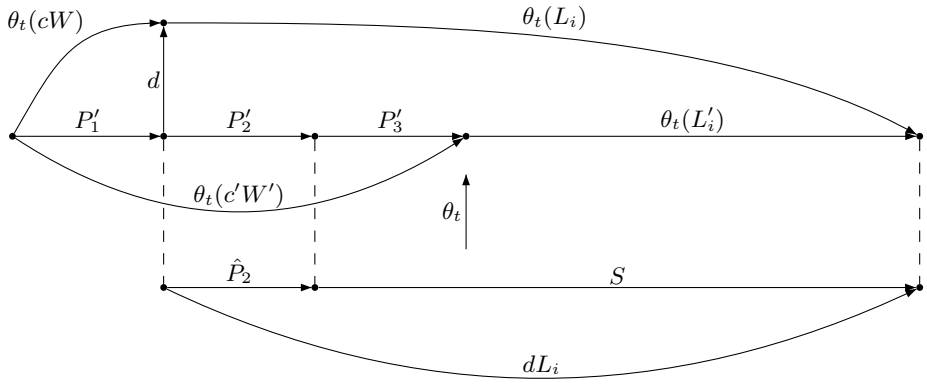


Fig. 14. Case 2.3.2

We saw above that $\gamma_t(P'_3)$ contains the T-type $\boldsymbol{\theta}'_3$. Moreover, by hypothesis, $\mathrm{A}(\mathcal{S},\boldsymbol{\lambda}) < \frac{1}{2}\mathrm{Card}(\mathcal{V}_0)$. Hence, we can choose a letter $W_3 \in \widehat{\mathcal{W}_t}$ such that

$$\begin{aligned} &W_3 \notin \mathrm{Alph}(\mathcal{S},\boldsymbol{\lambda}), \quad \gamma_w(W_3) = \boldsymbol{\theta}'_3 \in \gamma_t(P'_3),\\ &\mu_w(W_3) = \mu_t(\boldsymbol{\theta}'_3, P'_3), \quad \delta_w(W_3) = \delta_t(\boldsymbol{\theta}'_3, P'_3). \end{aligned} \tag{272}$$

Since $W_3 \notin \mathrm{Alph}(\mathcal{S},\boldsymbol{\lambda})$ and $dL_i = \hat{P}_2 S$ we have

$$W_3 \notin \mathrm{Alph}(\hat{P}_2) \tag{273}$$

We define a monoid homomorphism $\lambda' : \mathbb{W} \to \mathbb{W}$ by:

$$\lambda'(e) = e \text{ for } e \in A \cup B$$

$$\lambda'(W') = c'^{-1} c W d^{-1} \hat{P}_2 W_3 \tag{274}$$

$$\lambda'(\overline{W'}) = \mathbb{I}_w(c'^{-1} c W d^{-1} \hat{P}_2 W_3) \tag{275}$$

$$\lambda'(W'') = W'' \text{ for } W'' \in \mathcal{W} \setminus \{W', \overline{W'}\} \tag{276}$$

Note that

$$\begin{aligned} \delta_w(W') &\overset{(\mathrm{Hom7})}{=} \delta_t(\boldsymbol{\theta}', \theta_t(W'))\\ &\overset{(269)}{=} \delta_t(\boldsymbol{\theta}', c'^{-1} P'_1 P'_2 P'_3)\\ &\overset{(269),(270)}{=} \delta_t(\boldsymbol{\theta}(\boldsymbol{\theta}'_2 \boldsymbol{\theta}'_3), \theta_t(c'^{-1} c W d^{-1} \hat{P}_2) P'_3)\\ &\overset{(272)}{=} \delta_w(c'^{-1} c W d^{-1} \hat{P}_2 W_3)\\ &\overset{(274)}{=} \delta_w(\lambda'(W')) \end{aligned}$$

and similarly $\delta_w(\overline{W'}) = \delta_w(\lambda'(\overline{W'}))$. Hence, by Lemma **??**, λ' is indeed a monoid homomorphism on $\mathbb{W}$. Next, since $\delta_t(\boldsymbol{\theta}'_3, P'_3) = \delta_w(W_3)$, we can define a monoid homomorphism $\theta'_t : \mathbb{W}_t \to \mathbb{H}_t$ by

$$\theta'_t(e) = e \text{ for } c \in A \cup B,$$

$$\theta'_t(W_3) = P'_3, \tag{277}$$

$$\theta'_t(\overline{W}_3) = \mathbb{I}_t(P'_3), \tag{278}$$

$$\theta'_t(W'') = \theta_t(W'') \text{ for } W'' \in \mathcal{W}_t \setminus \{W_3, \overline{W}_3\}. \tag{279}$$

As in the above cases we can check that λ' and θ'_t are AB-homomorphisms. Moreover, we claim that

$$\forall W'' \in \mathrm{Alph}(\mathcal{S}, \boldsymbol{\lambda}) : \theta'_t(\lambda'(W'')) = \theta_t(W''). \tag{280}$$

Since $W_3, \overline{W}_3 \notin \mathrm{Alph}(\mathcal{S}, \boldsymbol{\lambda})$, we have

$$\theta'_t(\lambda'(W'')) \overset{(276)}{=} \theta'_t(W'') \overset{(279)}{=} \theta_t(W'')$$

for every $W'' \in \mathrm{Alph}(\mathcal{S}, \boldsymbol{\lambda}) \setminus \{W', \overline{W'}\}$. Moreover

$$\begin{aligned}
\theta'_t(\lambda'(W')) &\overset{(274)}{=} \theta'_t(c'^{-1} c W d^{-1} \hat{P}_2 W_3) \\
&\overset{(277),(279)}{=} c'^{-1} \theta_t(cW) d^{-1} \theta'_t(\hat{P}_2) P'_3 \\
&\overset{(273)}{=} c'^{-1} \theta_t(cW) d^{-1} \theta_t(\hat{P}_2) P'_3 \\
&\overset{(270)}{=} c'^{-1} \theta_t(cW) d^{-1} P'_2 P'_3 \\
&\overset{(269)}{=} c'^{-1} P'_1 d d^{-1} P'_2 P'_3 \\
&\overset{(269)}{=} \theta_t(W').
\end{aligned}$$

Finally, since λ' preserves $\mathbb{I}_w$ and θ'_t, θ_t preserve $\mathbb{I}_t$, we also get $\theta'_t(\lambda'(\overline{W'})) = \theta_t(\overline{W'})$. We get

$$\theta'_t(\lambda'(\lambda_i(w_i))) \overset{(280)}{=} \theta_t(\lambda_i(w_i)) \overset{(180)}{=} \theta_t(\lambda_i(w'_i)) \overset{(280)}{=} \theta'_t(\lambda'(\lambda_i(w'_i))) \tag{281}$$

for all $1 \leq i \leq n+m$. Let us define

$$\lambda'_i = \lambda_i \circ \lambda' \text{ for all } 1 \leq i \leq n+m.$$

Recall that $\hat{P}_2$ has the H-type $\boldsymbol{\theta}'_2$. Since $\gamma_w(W')$ is a T-type, this shows that

$$W', \overline{W'} \notin \mathrm{Alph}(\hat{P}_2). \tag{282}$$

Hence $\mathrm{Alph}(\mathcal{S}, \boldsymbol{\lambda}') = (\mathrm{Alph}(\mathcal{S}, \boldsymbol{\lambda}) \cup \{W_3, \overline{W}_3\}) \setminus \{W', \overline{W'}\}$. Thus, we have

$$\mathrm{A}(\mathcal{S}, \boldsymbol{\lambda}') < \frac{1}{2}\mathrm{Card}(\mathcal{V}_0). \tag{283}$$

Equality (281) and inequality (283) ensure that the new triple $(\mathcal{S}, \boldsymbol{\lambda}', \theta'_t)$ fulfills the hypothesis of Lemma 47. Let us evaluate now the size of this new triple. For the i-th equation (w_i, w'_i) we have:

$$\begin{aligned}
(\lambda'_i(w_i), \lambda'_i(w'_i)) &= (\lambda'(P_i c W L_i),\ \lambda'(P'_i c' W' L'_i)) \\
&\overset{(270),\,(274)}{=} (\lambda'(P_i) c W \lambda'(d^{-1} \hat{P}_2 S),\ \lambda'(P'_i) c' (c'^{-1} c W d^{-1} \hat{P}_2 W_3) \lambda'(L'_i)) \\
&\overset{(282)}{=} (\lambda'(P_i) c W d^{-1} \hat{P}_2 \lambda'(S),\ \lambda'(P'_i) c W d^{-1} \hat{P}_2 W_3 \lambda'(L'_i))
\end{aligned}$$

Let us set

$$Q_i = \lambda'(P_i) c W d^{-1} \hat{P}_2,\ \ T_i = \lambda'(S),\ \ Q'_i = \lambda'(P'_i) c W d^{-1} \hat{P}_2,\ \ T'_i = W_3 \lambda'(L'_i).$$

We next want to bound the size of

$$\Delta(Q_i, T_i, Q_i', T_i', \theta_t') = 1 - \frac{1}{2}(\chi_{AB}(Q_i) + \chi_{AB}(Q_i')) + \chi_H(T_i) + \chi_H(T_i') + 2\|\theta_t'(T_i)\| + 2\|\theta_t'(T_i')\|.$$

First note that $\chi_{AB}(Q_i) = \chi_{AB}(Q_i') = 0$ since Q_i and Q_i' contain the symbol $W \in \mathcal{W}$. Moreover,

$$\theta_t'(T_i) = \theta_t'(\lambda'(S)) \overset{(280)}{=} \theta_t(S) \overset{(270)}{=} P_3'\theta_t(L_i') \overset{(280)}{=} P_3'\theta_t'(\lambda'(L_i')) \overset{(277)}{=} \theta_t'(W_3\lambda'(L_i')) = \theta_t'(T_i'). \tag{284}$$

Since $T_i' = W_3\lambda'(L_i')$ and W_3 has a T-type, it follows that $\gamma_w(T_i')$ is of the form $\{(*, T, 1, *, *)\}$. Hence, $\chi_H(T_i') \leq 1$. For $T_i = \lambda'(S)$ we either have $|\gamma_w(T_i)| > 1$ and hence $\chi_H(T_i) = 0$ or $\gamma_w(T_i) = \gamma_w(S) = \{\boldsymbol{\theta}_3'\boldsymbol{\rho}'\}$. Since $\boldsymbol{\theta}_3'$ is a T-type, it follows again $\chi_H(T_i) \leq 1$. We therefore obtain:

$$\begin{aligned}
\Delta(Q_i, T_i, Q_i', T_i', \theta_t') &= 1 - \frac{1}{2}(\chi_{AB}(Q_i) + \chi_{AB}(Q_i')) + \chi_H(T_i) + \chi_H(T_i') + 2\|\theta_t'(T_i)\| + 2\|\theta_t'(T_i')\| \\
&\overset{(284)}{\leq} 3 + 4\|\theta_t'(T_i')\| \\
&\overset{(277),(280)}{=} 3 + 4\|P_3'\| + 4\|\theta_t(L_i')\| \\
&\overset{\|P_1'\|>0}{<} 4(\|P_1'\| + \|P_2'\| + \|P_3'\| + \|\theta_t(L_i')\|) \\
&\overset{(269)}{=} 4\|\theta_t(c'W'L_i')\| \\
&\overset{(242)}{=} 4\|\theta_t(S_i')\| \\
&\overset{(239)}{=} 2\|\theta_t(S_i)\| + 2\|\theta_t(S_i')\| \\
&\leq \Delta(P_i, S_i, P_i', S_i', \theta_t).
\end{aligned}$$

By Lemma 3, the hypothesis that P_i and 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 $\lambda'(P_i)$ and $\lambda'(P_i')$ (and hence Q_i and Q_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

$$\Delta_i(\mathcal{S}, \boldsymbol{\lambda}', \theta_t') \leq \Delta(Q_i, T_i, Q_i', T_i', \theta_t') < \Delta(P_i, S_i, P_i', S_i', \theta_t) = \Delta_i(\mathcal{S}, \boldsymbol{\lambda}, \theta_t).$$

Moreover, (280) implies that $\Delta_j(\mathcal{S}, \boldsymbol{\lambda}', \theta_t') \leq \Delta_j(\mathcal{S}, \boldsymbol{\lambda}, \theta_t)$ for all other j. Thus, we have $\|(\mathcal{S}, \boldsymbol{\lambda}', \theta_t')\| < \|(\mathcal{S}, \boldsymbol{\lambda}, \theta_t)\|$. By induction hypothesis, conclusions (183)–(186) are true for $(\mathcal{S}, \boldsymbol{\lambda}')$, which also implies that they hold for $(\mathcal{S}, \boldsymbol{\lambda})$. This concludes the case that $W' \in \widehat{\mathcal{W}}$. In case $W' \notin \widehat{\mathcal{W}}$ we just cancel the last line of (275) and can conclude as before.

Case 2.3.3. $\|\theta_t(cW)\| > \|\theta_t(c'W')\|$: Symmetric to Case 2.3.2.

This concludes the proof of Lemma 47. □

Let us now prove Lemma 46.

Proof of Lemma 46. Let $\sigma_t : \mathbb{W}_t \to \mathbb{H}_t$ fulfill the assumptions of Lemma 46. By assumption (1), σ_t is an AB-homomorphism solving the system of t-equations $\mathcal{S} = \{(w_i, w_i') \mid 1 \leq i \leq n\}$. Let us define $m = 0$, $\lambda_i = \mathrm{Id}_{\mathbb{W}_t}$ for $1 \leq i \leq n$, and $\theta_t = \sigma_t$. By assumption (2) of Lemma 46 it also fullfills

$$\mathrm{A}(\prod_{i=1}^{n} w_i w_i') < \frac{1}{2}\mathrm{Card}(\mathcal{V}_0).$$

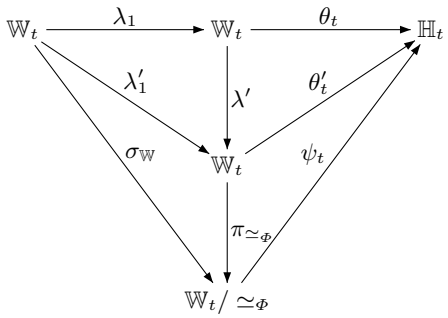


Fig. 15. Proof of Lemma 46

Hence, the system $\mathcal{S}$, the integers m, n, and the maps $(\lambda_i)_{1\leq i\leq n+m}$, θ_t are fulfiling the hypothesis of Lemma 47.

Let us consider the maps Φ, λ'_i, and θ'_t given by the conclusion of Lemma 47 and the natural projection $\pi_\Phi : \mathbb{W}_t \to \mathbb{W}_t/\Phi$, which is an AB-homomorphism. Choose

$$\sigma_{\mathbb{W}} = \lambda'_1 \circ \pi_\Phi : \mathbb{W}_t \to \mathbb{W}_t/\Phi \tag{285}$$

and let

$$\psi_t : \mathbb{W}_t/\Phi \to \mathbb{H}_t$$

be the AB-homomorphism defined by

$$\forall W \in \mathcal{W}_t : \psi_t([W]_{\simeq_\Phi}) = \theta'_t(W).$$

By point (184) of Lemma 47, the congruence $\simeq_\Phi$ is contained in the kernel of θ'_t. This implies the existence and unicity of the monoid homomorphism ψ_t. We have

$$\theta'_t = \pi_\Phi \circ \psi_t. \tag{286}$$

With Lemma 24, it follows that ψ_t is indeed an AB-homomorphism.

Finally, we show that the mappings $\sigma_{\mathbb{W}}$ and ψ_t fulfill the properties asserted in Lemma 46. For all $W \in \mathrm{Alph}(\mathcal{S})$ we have

$$\sigma_t(W) = \theta_t(W) = \theta_t(\lambda_1(W)) \overset{(183)}{=} \theta'_t(\lambda'_1(W)) \overset{(286)}{=} \psi_t(\pi_\Phi(\lambda'_1(W))) \overset{(285)}{=} \psi_t(\sigma_{\mathbb{W}}(W)).$$

Moreover, for all $1 \leq i \leq n$ we have

$$\sigma_{\mathbb{W}}(w_i) \overset{(285)}{=} \pi_\Phi(\lambda'_i(w_i)) \overset{(185)}{=} \pi_\Phi(\lambda'_i(w'_i)) \overset{(285)}{=} \sigma_{\mathbb{W}}(w'_i).$$

Figure 15 shows all morphisms involved in the proof. □

From $\mathbb{W}$-solutions to t-solutions. Conversely to Lemma 46, every $\mathbb{W}$-solution of a given system $\mathcal{S}$ of the form (131) provides a t-solution of the same system. Let us state this formally.

Lemma 48 ($\mathbb{W}$-solutions provide t-solutions). *Let $\mathcal{S}_t = \{(w_i, w_i') \mid 1 \leq i \leq n\}$ be a system of t-equations of the form (131) and let $\mathcal{S}_{\mathbb{H}} = \{(v_i, v_i') \mid 1 \leq i \leq m\} \subseteq \mathbb{W}_{\mathbb{H}} \times \mathbb{W}_{\mathbb{H}}$ be a system of equations over the monoid $\mathbb{H}$. Let us suppose that there exist $\Phi \in \mathsf{HInv}$, an AB-homomorphism $\sigma_{\mathbb{W}} : \mathbb{W}_t \to \mathbb{W}_t/\Phi$, and an AB-homomorphism $\psi_{H,t} : \mathbb{W}_{\mathbb{H}}/\Phi \to \mathbb{H}_t$ such that*

$$\sigma_{\mathbb{W}}(w_i) = \sigma_{\mathbb{W}}(w_i') \text{ for all } 1 \leq i \leq n, \tag{287}$$

$$\psi_{H,t}(\sigma_{\mathbb{W}}(v_i)) = \psi_{H,t}(\sigma_{\mathbb{W}}(v_i')) \text{ for all } 1 \leq i \leq m. \tag{288}$$

Then, there is an AB-homomorphism $\psi_t : \mathbb{W}_t/\Phi \to \mathbb{H}_t$, which extends $\psi_{H,t}$, such that $\sigma_{\mathbb{W}} \circ \psi_t$ solves the systems $\mathcal{S}_t$ and $\mathcal{S}_{\mathbb{H}}$.

Proof. Let Φ, $\sigma_{\mathbb{W}}$, and $\psi_{H,t}$ fulfill the hypothesis of the lemma. Since $\Phi \in \mathsf{HInv}$, there exists a partition $\widehat{\mathcal{W}} = \widehat{\mathcal{W}_0} \uplus \{W_1, \ldots, W_p\} \uplus \{\overline{W}_1, \ldots, \overline{W}_p\}$ (see (92)), where $\widehat{\mathcal{W}_0}$ is closed under the involution $\mathbb{I}_w$. Moreover, there exists a tuple $(a_1, b_1, \ldots, a_p, b_p)$ with $a_k, b_k \in \mathrm{Gi}(W_k) = \mathrm{Ge}(W_k)$ $(1 \leq k \leq p)$ such that (94) and (95) hold. We first define a monoid homomorphism $\psi_t : \mathcal{W}_t^* * A * B \to \mathbb{H}_t$ in the following way:

- $\psi_t(c) = c$ for $c \in A \cup B$
- $\psi_t(W) = \psi_{H,t}([W]_{\simeq_\Phi})$ for $W \in \mathcal{W}_{\mathbb{H}}$
- Let $W \in \mathcal{W}_t \setminus \mathcal{W}_{\mathbb{H}}$. By (91), we can choose $s_W \in \mathbb{H}_t$ which realizes W in the sense that

$$s_W \in \mathrm{dom}(\mathbb{I}_t) \Longleftrightarrow W \in \mathrm{dom}(\mathbb{I}_w), \quad \gamma_w(W) \subseteq \gamma_t(s_W),$$
$$\forall \boldsymbol{\theta} \in \gamma_w(W) : \mu_w(\boldsymbol{\theta}, W) = \mu_t(\boldsymbol{\theta}, s_W),\ \delta_w(\boldsymbol{\theta}, W) = \delta_t(\boldsymbol{\theta}, s_W).$$

We can make this choice such that $s_{\overline{W}} = \mathbb{I}_t(s_W)$ for all $W \in \widehat{\mathcal{W}} \setminus \mathcal{W}_{\mathbb{H}}$. We set $\psi_t(W) = s_W$.

It follows that for all $W \in \mathcal{W}_t$, $\delta_w(W) = \delta_t(\gamma_w(W), \psi_t(W))$ (for $W \in \mathcal{W}_{\mathbb{H}}$ this follows from the fact that $\pi_\Phi \circ \psi_{H,t}$ is an AB-homomorphism). Thus, for every $(c, d) \in \delta_w(W)$ we have $\psi_t(cW) = \psi_t(Wd)$. Therefore, ψ_t induces a monoid homomorphism $\psi_t : \mathbb{W}_t \to \mathbb{H}_t$. This monoid homomorphism clearly fulfills conditions (a)–(f) from Lemma 23. Thus $\psi_t : \mathbb{W}_t \to \mathbb{H}_t$ is an AB-homomorphism. By the hypothesis on $\psi_{H,t}$, for all $w, w' \in \mathbb{W}_{\mathbb{H}}$ with $w \simeq_\Phi w'$ we have $\psi_t(w) = \psi_{H,t}([w]_{\simeq_\Phi}) = \psi_{H,t}([w']_{\simeq_\Phi}) = \psi_t(w')$. Let us note that all the W_k and $\overline{W}_k$ belong to $\mathcal{W}_{\mathbb{H}}$:

- every symbol $W_k, \overline{W}_k$ has an H-type
- the existence of $\Psi_{H,t}$ shows that $W_k, \overline{W}_k$ belong to $\mathcal{W}_t$.

Since the congruence $\simeq_\Phi$ is generated by its restriction to the set $\mathbb{W}_{\mathbb{H}}$, we have

$$\forall w, w' \in \mathbb{W}_t : w \simeq_\Phi w' \Rightarrow \psi_t(w) = \psi_t(w').$$

It follows that ψ_t induces a monoid homomorphism $\mathbb{W}_t/\Phi \to \mathbb{H}_t$, which by Lemma 24 is in fact an AB-homomorphism. Moreover, ψ_t extends $\psi_{H,t}$. Since $\sigma_{\mathbb{W}}$ solves $\mathcal{S}_t$, $\sigma_{\mathbb{W}} \circ \psi_t$ solves $\mathcal{S}_t$ too. Since $\sigma_{\mathbb{W}} \circ \psi_{H,t}$ solves $\mathcal{S}_{\mathbb{H}}$, $\sigma_{\mathbb{W}} \circ \psi_t$ solves $\mathcal{S}_{\mathbb{H}}$ too. □

7 The groups $\mathbb{U}$ and $\mathbb{E}$

We define in this section a group $\mathbb{U}$, in which the partial monoid consisting of the elements of $\mathbb{W}$ with a non-empty type, is embedded. Well-typed equations over $\mathbb{W}$ thus translate into

equations with rational constraints over $\mathbb{U}$. But $\mathbb{W}$-equations involve, beside well-typed equations, an $\mathbb{H}$-involutive automorphism Φ, which induces an involutive automorphism $\Phi_{\mathbb{U}}$ of $\mathbb{U}$. We define a quotient $\mathbb{E}$ of $\mathbb{U}$ by making equal every element $u \in \mathbb{U}$ with its image $\Phi_{\mathbb{U}}(u)$. The notion of a solution $\mathbb{W}_t \to \mathbb{W}_t/\simeq_\Phi$ of a $\mathbb{W}$-equation can thus be translated into the notion of a solution $\mathcal{W}^* * A * B \to \mathbb{E}$ of an equation with rational constraints in $\mathbb{E}$.

7.1 The group $\mathbb{U}$

Let us adjoin for every non-invertible symbol $W \in \mathcal{W} \setminus \widehat{\mathcal{W}}$ a formal inverse $\overline{W}$. The extended alphabet $\mathcal{W}' = \mathcal{W} \cup \{\overline{W} \mid W \in \mathcal{W} \setminus \widehat{\mathcal{W}}\}$ is now endowed with a total involution, which extends the partial involution $\mathbb{I}_w$ by the rules $\mathbb{I}_w(W) = \overline{W}$ and $\mathbb{I}_w(\overline{W}) = W$ for $W \in \mathcal{W} \setminus \widehat{\mathcal{W}}$. The maps γ_w, μ_w, and δ_w are extended to $\mathcal{W}'$ in such a way that the axioms (AB10), (AB11), and (AB12) for AB-algebras are fulfilled by $\mathcal{W}'^* * A * B$ endowed with this involution $\mathbb{I}_w$. We denote by $\equiv'$ the monoid-congruence over $\mathcal{W}'^* * A * B$ generated by the set of pairs

$$\{(cW, Wd) \mid W \in \mathcal{W}', (c,d) \in \delta_w(W)\} \tag{289}$$

and by $\mathbb{W}'$ the AB-algebra obtained from $\mathcal{W}'^* * A * B$ by quotienting it by the equivalence $\equiv'$. We define the group $\mathbb{U}$ by the following monoid-presentation:

$$\mathbb{U} = \langle A * B, \mathcal{W}';\ \mathbb{I}_w(W)cW = d\ (W \in \mathcal{W}', (c,d) \in \delta_w(W))\rangle. \tag{290}$$

Note that the above relations include $\mathbb{I}_w(W)W = \varepsilon$ which guaranty that the monoid $\mathbb{U}$ is a group. When working in the group $\mathbb{U}$, we will also write W^{-1} instead of $\mathbb{I}_w(W)$.

The group $\mathbb{U}$ is an HNN-extension of the free product $A * B$: the elements from $\mathcal{W}'$ are the stable letters and the mappings $\delta_w(W')$ ($W \in \mathcal{W}'$) are the partial isomorphisms. We identify ι_A (resp. ι_B) with the natural embedding of A (resp. B) into $A * B$. We denote by $\equiv_{\mathbb{U}}$ the monoid congruence over $\mathcal{W}'^* * A * B$ such that $u \equiv_{\mathbb{U}} v$ if and only if u and v represent the same element of the group $\mathbb{U}$. We denote by

$$\pi_{\mathbb{U}} : \mathcal{W}'^* * A * B \to \mathbb{U} \tag{291}$$

the canonical monoid homomorphism with $\pi_{\mathbb{U}}(z) = [z]_{\equiv_{\mathbb{U}}}$. Clearly, all the pairs in (89) also belong to $\equiv_{\mathbb{U}}$, hence $\equiv \subseteq \equiv_{\mathbb{U}}$. Thus, there exists a unique monoid homomorphism $\overline{\pi}_{\mathbb{U}} : \mathbb{W} \to \mathbb{U}$ such that

$$\pi_{\mathbb{U}} \restriction_{\mathcal{W}^* * A * B} = \pi_{\equiv} \circ \overline{\pi}_{\mathbb{U}}.$$

An element $z \in \mathcal{W}'^* * A * B$ is said to be a $\mathbb{U}$-*reduced sequence* if its corresponding (A,B)-reduced string does not contain any factor of the form $\mathbb{I}_w(W)cW$ with $W \in \mathcal{W}'$ and $c \in \mathrm{dom}(\delta_w(W))$. We denote by $\mathrm{Red}_{\mathbb{U}}(A * B, \mathcal{W}')$ the subset of $\mathcal{W}'^* * A * B$ consisting of all $\mathbb{U}$-reduced sequences.

Lemma 49. *Let s, s' be some $\mathbb{U}$-reduced sequences in $\mathcal{W}'^* * A * B$. Then $s \equiv_{\mathbb{U}} s'$ if and only if $s \equiv' s'$.*

This lemma is an analogue of Lemma 5 for HNN-extensions with a set $\mathcal{W}'$ of stable letters (instead of just a single stable letter t). This analogue can be obtained from Lemma 5 by induction over the number of stable letters.

Lemma 50. *Let $s \in \mathcal{W}'^* * A * B$ with $\gamma_w(s) \neq \emptyset$. Then s is $\mathbb{U}$-reduced.*

Proof. It suffices to prove that $\gamma_w(\mathbb{I}_w(W)cW) = \emptyset$ for all $W \in \mathcal{W}'$ and $c \in \mathrm{dom}(\delta_w(W))$: If $\gamma_w(W) = \{(\theta, b, \rho)\}$ for $\theta, \rho \in \mathcal{T}_6$, $b \in \{0, 1\}$, then we obtain

$$\gamma_w(\mathbb{I}_w(W)cW) = \{(\mathbb{I}_{\mathcal{R}}(\rho), b, \mathbb{I}_{\mathcal{R}}(\theta))\}\{(\theta, b, \rho)\} = \emptyset,$$

since $\mathbb{I}_{\mathcal{R}}(\theta) \neq \theta$ (the mapping $\mathbb{I}_{\mathcal{R}}$ defined in (15)–(17) has no fixpoints). □

7.2 The group $\mathbb{E}$

Let us recall that an $\mathbb{H}$-involutive automorphism $\Phi \in \mathsf{HInv}$ is defined through p letters W_k ($1 \leq k \leq p$), their inverses $\overline{W}_k$, and a tuple $(a_1, b_1, \ldots, a_p, b_p)$, as specified in Definition 8 from Section 3.9. Let us fix such an involution and assume that (96)–(99) hold. We extend Φ to an involutive AB-automorphism of $\mathbb{W}'$ by setting $\Phi(W) = W$ for $W \in \mathcal{W}' \setminus \mathcal{W}$. We define the group $\mathbb{E}$ by the group-presentation

$$\mathbb{E} = \langle \mathbb{U}; W_k = a_k^{-1} W_k^{-1} b_k^{-1} (1 \leq k \leq p) \rangle. \tag{292}$$

where we know by (97) that

$$W_k^{-1} a_k^{-1} b_k W_k \equiv_{\mathbb{U}} b_k a_k^{-1} \text{ for } 1 \leq k \leq p \tag{293}$$

and by (96) that

$$(W_k b_k W_k a_k)^{-1} x (W_k b_k W_k a_k) \equiv_{\mathbb{U}} x \text{ for } 1 \leq k \leq p \text{ and } x \in \mathrm{dom}(\delta_w(W_k)). \tag{294}$$

We denote by $\equiv_{\mathbb{E}}$ the monoid-congruence over $\mathcal{W}'^* * A * B$ such that $u \equiv_{\mathbb{E}} v$ if and only if u and v represent the same element of the group $\mathbb{E}$. We denote by

$$\pi_{\mathbb{E}} : \mathcal{W}'^* * A * B \to \mathbb{E}$$

the canonical monoid homomorphism with $\pi_{\mathbb{E}}(z) = [z]_{\equiv_{\mathbb{E}}}$.

Definition 9. *For a given finite group A, we denote by $\mathsf{PHNN}(A)$ the set of all presentations consisting of a set of relations of the form* (290) *and* (292)*, where the letters $W_k, \overline{W}_k$ ($1 \leq k \leq p$) and the tuple $(a_1, b_1, \ldots, a_p, b_p)$ are fulfilling conditions* (93) *and* (96)–(99)*.*

Note that, in the definition of the algebra $\mathcal{W}^* * A * B$, as well as for the group $\mathbb{U}$, A, B are *trivially intersecting* copies of the initial (isomorphic) subgroups $A, B \leq \mathbb{H}$ (i.e. these copies have an intersection reduced to $\{1\}$). Thus, the resulting presentations depend, up to isomorphism, on A only; this explains the notation $\mathsf{PHNN}(A)$ in Definition 9.
Note also that, within the AB-algebra $\mathbb{H}_t$, the subgroups $\iota_A(A), \iota_B(B) \subseteq \mathbb{H}_t$ can have a non-trivial intersection (isomorphic with the intersection of the initial concrete subgroups $A, B \subseteq \mathbb{H}$).
Note that the results demonstrated in the rest of this section hold for any group $\mathbb{E}$, provided it has a presentation in the set $\mathsf{PHNN}(A)$ for some finite group A.

Lemma 51. *The monoid homorphism $\Phi : \mathbb{W}' \to \mathbb{W}'$ (from Lemma 34) induces an involutive group automorphism $\Phi_{\mathbb{U}}$ of $\mathbb{U}$.*

Proof. By point 2 from Lemma 34, adapted to the larger alphabet $\mathcal{W}'$, we know that the monoid homomorphism $\Phi : \mathbb{W}' \to \mathbb{W}'$ is an involutive AB-automorphism. Let $W \in \mathcal{W}'$. By (Hom7), we have

$$\delta_w(\Phi(W)) = \delta_w(W). \tag{295}$$

Let $e \in \mathrm{dom}(\delta_w(W)) = \mathrm{dom}(\delta_w(\Phi(W)))$. Since Φ commutes with $\mathbb{I}_w$ and $\Phi(c) = c$ for all $c \in A \cup B$, we get

$$\Phi(\mathbb{I}_w(W)eW) \equiv' \mathbb{I}_w(\Phi(W))e\Phi(W) \equiv_{\mathbb{U}} \delta_w(\Phi(W))(e) \overset{(295)}{=} \delta_w(W)(e) = \Phi(\delta_w(W)(e)).$$

Hence, Φ is compatible with the defining relations of $\mathbb{U}$. It follows that, for all $m, m' \in \mathbb{W}'$, $m \equiv_{\mathbb{U}} m'$ implies $\Phi(m) \equiv_{\mathbb{U}} \Phi(m')$. Thus $\Phi : \mathbb{W}' \to \mathbb{W}'$ induces a group homomorphism $\Phi_{\mathbb{U}} : \mathbb{U} \to \mathbb{U}$ and since $\Phi_{\mathbb{U}} \circ \Phi_{\mathbb{U}} = \mathrm{Id}_{\mathbb{U}}$, $\Phi_{\mathbb{U}}$ is an involutive group automorphism of $\mathbb{U}$. □

Note that the presentation (292) can be rewritten as

$$\mathbb{E} = \langle \mathbb{U}; w = \Phi_{\mathbb{U}}(w)(w \in \mathbb{U}) \rangle. \tag{296}$$

Let us define a finite semi-Thue system[7] $S_{\mathbb{E}}$ over the alphabet

$$\mathcal{G}_{\mathbb{E}} = \mathcal{W}' \cup (A \setminus \{1\}) \cup (B \setminus \{1\}),$$

which will provide a *confluent and Noetherian* monoid presentation for the group $\mathbb{E}$. Let us choose for every $W \in \mathcal{W}'$ a transversal R_W of the left-congruence modulo the subgroup $\mathrm{dom}(\delta_w(W))$ over the group $\mathrm{Gi}(W)$, i.e.,

$$\forall x \in \mathrm{Gi}(W) \exists! r \in R_W : x \in r \cdot \mathrm{dom}(\delta_w(W))$$

(here $\exists! r$ means that there exists a unique r). For every $W \in \mathcal{W}'$, we choose $1 \in R_W$ and for every $1 \leq k \leq p$, we choose $b_k \in R_{W_k}$. These two assumptions can be made compatible, possibly after a preliminary change of the defining tuple $(a_1, b_1, \ldots, a_k, b_k, \ldots, a_p, b_p)$ into another tuple $(a'_1, b'_1, \ldots, a'_k, b'_k, \ldots, a'_p, b'_p)$ as follows:

- If $b_k \notin \mathrm{dom}(\delta_w(W_k))$, then we can choose $1 \in R_W$.
- If $b_k \in \mathrm{dom}(\delta_w(W_k))$, then we can change the tuple $(a_1, b_1, \ldots, a_k, b_k, \ldots, a_p, b_p)$ by Lemma 35 as follows (without changing Φ):

$$\begin{aligned}
(a_1, b_1, \ldots, a_k, b_k, \ldots, a_p, b_p) &\to \\
(a_1, b_1, \ldots, b_k, a_k, \ldots, a_p, b_p) &\to \\
(a_1, b_1, \ldots, 1, \varphi_k(b_k)a_k, \ldots, a_p, b_p) &\to \\
(a_1, b_1, \ldots, \varphi_k(b_k)a_k, 1, \ldots, a_p, b_p)&
\end{aligned}$$

  Let $(a'_1, b'_1, \ldots, a'_k, b'_k, \ldots, a'_p, b'_p)$ be the last tuple, and take it as the defining tuple for Φ. We have $1 = b'_k$, hence we can satisfy both requirements $1 \in R_{W_k}$ and $b'_k \in R_{W_k}$.

For every $x, y \in A$ we denote by $\underline{xy}$ the element of $(A \setminus \{1\}) \cup \{\varepsilon\}$ that represents the result of the product xy performed in the group A. Note that in the rules below, xy denotes a word of length 2 over the alphabet $A \setminus \{1\}$ while $\underline{xy}$ denotes either an element of $A \setminus \{1\}$ or the empty word. The same notation is used for B as well.

[7] Background on semi-Thue systems can be found in [BO93].

For every $W \in \mathcal{W}'$, we also denote by φ_W the partial isomorphism $\delta_w(W)$. In the case $W = W_k$ $(1 \leq k \leq p)$ we write φ_k for φ_{W_k}. The semi-Thue system $S_{\mathbb{E}}$ consists of the following set of rules:

$$c_1c_2 \to \underline{c_1c_2} \qquad \text{for } c_1, c_2 \in A \setminus \{1\} \text{ or } c_1, c_2 \in B \setminus \{1\} \tag{297}$$

$$\underline{rx}W \to rW\varphi_W(x) \qquad \text{for } W \in \mathcal{W}', r \in R_W, x \in \mathrm{dom}(\varphi_W) \setminus \{1\} \tag{298}$$

$$\overline{W}xW \to \varphi_W(x) \qquad \text{for } W \in \mathcal{W}' \setminus \{W_k, \overline{W}_k \mid 1 \leq k \leq p\}, x \in \mathrm{dom}(\varphi_W) \tag{299}$$

$$\overline{W}_k \to a_kW_kb_k \qquad \text{for } 1 \leq k \leq p \tag{300}$$

$$W_kb_kW_k \to a_k^{-1} \qquad \text{for } 1 \leq k \leq p. \tag{301}$$

Note that (299) includes the rule $\overline{W}W \to \varepsilon$.

Lemma 52. *The following holds:*

(1) The monoid $\mathcal{G}_{\mathbb{E}}^*/\overset{*}{\longleftrightarrow}_{S_{\mathbb{E}}}$ is isomorphic to $\mathbb{E}$.
(2) The semi-Thue system $S_{\mathbb{E}}$ is confluent and Noetherian.

Proof. For point (1) we show that $\overset{*}{\longleftrightarrow}_{S_{\mathbb{E}}} = \equiv_{\mathbb{E}}$. Since for every rule $u \to v$ of $S_{\mathbb{E}}$ we have $u \equiv_{\mathbb{E}} v$, we certainly have $\overset{*}{\longleftrightarrow}_{S_{\mathbb{E}}} \subseteq \equiv_{\mathbb{E}}$. For the other inclusion, i.e., $\equiv_{\mathbb{E}} \subseteq \overset{*}{\longleftrightarrow}_{S_{\mathbb{E}}}$, let us first show $\equiv_{\mathbb{U}} \subseteq \overset{*}{\longleftrightarrow}_{S_{\mathbb{E}}}$.

The rules defining the multiplication tables for A and B are also rules of $S_{\mathbb{E}}$, see (297). These rules yield a presentation of the free product $A * B$. Let us now consider an identity of the presentation of $\mathbb{U}$ of the form

$$\overline{W}cW \equiv_{\mathbb{U}} \varphi_W(c) \text{ for } c \in \mathrm{dom}(\varphi_W).$$

If $W \notin \{W_k, \overline{W}_k \mid 1 \leq k \leq p\}$, we get $\overline{W}cW \to_{S_{\mathbb{E}}} \varphi_W(c)$ directly with rule (299). If $W = W_k$ for some $1 \leq k \leq p$, we get

$$\begin{aligned}
\overline{W}_kcW_k &\xrightarrow{(300)}_{S_{\mathbb{E}}} a_kW_kb_kcW_k && (302)\\
&\xrightarrow{(298)}_{S_{\mathbb{E}}} a_kW_kb_kW_k\varphi_k(c) && (303)\\
&\xrightarrow{(301)}_{S_{\mathbb{E}}} a_ka_k^{-1}\varphi_k(c) && (304)\\
&\xrightarrow{(297)}_{S_{\mathbb{E}}} \varphi_k(c). && (305)
\end{aligned}$$

If $W = \overline{W}_k$ for some $1 \leq k \leq p$ and $c = 1$, then, using the fact that $\varphi_k(b_k^{-1}a_k) = a_kb_k^{-1}$ by (97), we get:

$$\begin{aligned}
W_k\overline{W}_k &\xrightarrow{(300)}_{S_{\mathbb{E}}} W_ka_kW_kb_k\\
&= \quad W_k\underline{b_k(b_k^{-1}a_k)}W_kb_k\\
&\xrightarrow{(298)}_{S_{\mathbb{E}}} W_kb_kW_ka_kb_k^{-1}b_k\\
&\xrightarrow{(297)} \quad W_kb_kW_ka_k\\
&\xrightarrow{(301)}_{S_{\mathbb{E}}} a_k^{-1}a_k\\
&\xrightarrow{(297)} \quad \varepsilon.
\end{aligned}$$

Note that by the previous two derivations, W_k and $\overline{W}_k$ are inverses in the monoid presented by $S_{\mathbb{E}}$.

Finally, assume that $W = \overline{W}_k$ for some $1 \leq k \leq p$ and $c \neq 1$. Thus, $\varphi_W = \varphi_k^{-1}$. Let $d = \varphi_k^{-1}(c) \neq 1$. Hence, $\varphi_k(d) = c$. By the above calculation, we know that

$$\overline{W}_k d W_k \to_{S_{\mathbb{E}}}^* c.$$

Hence, since W_k and $\overline{W}_k$ are inverses in the monoid $\mathcal{G}_{\mathbb{E}}^* / \overset{*}{\longleftrightarrow}_{S_{\mathbb{E}}}$, we get

$$d \overset{*}{\longleftrightarrow}_{S_{\mathbb{E}}} W_k c \overline{W}_k.$$

We have checked that $\equiv_{\mathbb{U}} \subseteq \overset{*}{\longleftrightarrow}_{S_{\mathbb{E}}}$.

By (296) the group $\mathbb{E}$ is obtained by adding to $\mathbb{U}$ the additional identity $g = \Phi(g)$ for $g \in \mathcal{G}_{\mathbb{E}}$. Hence, to show that $\equiv_{\mathbb{E}} = \overset{*}{\longleftrightarrow}_{S_{\mathbb{E}}}$, it remains to show that $g \overset{*}{\longleftrightarrow}_{S_{\mathbb{E}}} \Phi(g)$ for $g \in \mathcal{G}_{\mathbb{E}}$.

If $g \in \mathcal{G}_{\mathbb{E}} \setminus \{W_k, \overline{W}_k \mid 1 \leq k \leq p\}$, then $\Phi(g) = g$, so that $g \overset{*}{\longleftrightarrow}_{S_{\mathbb{E}}} \Phi(g)$. If $g = \overline{W}_k$ for some $1 \leq k \leq p$, then

$$\overline{W}_k \xrightarrow{(300)}_{S_{\mathbb{E}}} a_k W_k b_k = \Phi(\overline{W}_k).$$

Finally, if $g = W_k$ for some $1 \leq k \leq p$, then

$$W_k b_k W_k \xrightarrow{(301)}_{S_{\mathbb{E}}} a_k^{-1}.$$

Hence, using the fact that $\overline{W}_k$ and W_k as well as b_k and b_k^{-1} are inverses in the monoid $\mathcal{G}_{\mathbb{E}}^* / \overset{*}{\longleftrightarrow}_{S_{\mathbb{E}}}$, we get

$$W_k \overset{*}{\longleftrightarrow}_{S_{\mathbb{E}}} a_k^{-1} \overline{W}_k b_k^{-1} = \Phi(W_k).$$

This concludes the proof for $\equiv_{\mathbb{E}} = \overset{*}{\longleftrightarrow}_{S_{\mathbb{E}}}$, i.e., of point (1) from the lemma.

For point (2), we first show that $S_{\mathbb{E}}$ is Noetherian. Assume that there exists an infinite derivation

$$u_0 \to_{S_{\mathbb{E}}} u_1 \to_{S_{\mathbb{E}}} u_2 \to_{S_{\mathbb{E}}} \cdots.$$

There exist only finitely many i such that $u_i \to_{S_{\mathbb{E}}} u_{i+1}$ via one of the rules (299), (300), or (301): Simply assign weight 2 to every letter $\overline{W}_k$ ($1 \leq k \leq p$), weight 1 to all letter from $\mathcal{W} \setminus \{\overline{W}_k \mid 1 \leq k \leq p\}$, and weight 0 to every letter from $(A \setminus \{1\}) \cup (B \setminus \{1\})$. Then no rule increases the weight, and rules (299), (300), and (301) strictly decrease the weight.

Hence, we can assume that in the above infinite derivation only the rules (297) and (298) are applied. Thus, the projection to the subalphabet $\mathcal{W}'$ is the same for all u_i. Let $u_i = s_i W v_i$ with $s_i \in ((A \setminus \{1\}) \cup (B \setminus \{1\}))^*$, $W \in \mathcal{W}'$, and $v_i \in \mathcal{G}_{\mathbb{E}}^*$. We can assume that for infinitely many i, the prefix $s_i W$ of u_i is rewritten (necessarily using rule (298)); otherwise, wo obtain an infinite derivation, where in each word the number of occurrences of symbols from $\mathcal{W}'$ is smaller. But this is easily seen to be impossible. We have established that $S_{\mathbb{E}}$ is Noetherian.

It remains to show that $S_{\mathbb{E}}$ is confluent. Since $S_{\mathbb{E}}$ is Noetherian, it suffices to show that every critical pair of the system $S_{\mathbb{E}}$ can be resolved. Here is a list of all critical pairs of $S_{\mathbb{E}}$,

where we assume that $x \in \mathrm{dom}(\varphi_W)$ whenever we write $\varphi_W(x)$ for the partial mapping φ_W:

$$\begin{aligned}
r\overline{W}\varphi_W^{-1}(x)yW \leftarrow \quad & \underline{rx}\overline{W}yW && \to \underline{rx}\varphi_W(y) \text{ for } r \in R_{\overline{W}} && (306)\\
\varphi_W(y) \leftarrow \quad & \overline{W}yW && \to \overline{W}W\varphi_W(y) && (307)\\
\underline{xry}W \leftarrow \quad & xr\underline{y}W && \to xrW\varphi_W(y) \text{ for } r \in R_W, x \in \mathrm{Gi}(W) && (308)\\
rW_k\varphi_k(x)b_kW_k \leftarrow \quad & \underline{rx}W_kb_kW_k && \to \underline{rx}a_k^{-1} \text{ for } r \in R_{W_k} && (309)\\
a_k^{-1}b_kW_k \leftarrow \quad & W_kb_kW_kb_kW_k && \to W_kb_ka_k^{-1} && (310)\\
r\overline{W}_k\varphi_k^{-1}(x) \leftarrow \quad & \underline{rx}\overline{W}_k && \to \underline{rx}a_kW_kb_k \text{ for } r \in R_{\overline{W}_k} && (311)
\end{aligned}$$

Let us give for each of these critical pairs a common descendant modulo $S_{\mathbb{E}}$.

Pairs of type (306):

$$r\overline{W}\varphi_W^{-1}(x)yW \to r\overline{W}\underline{\varphi_W^{-1}(x)y}W \to r\underline{x\varphi_W(y)} \to \underline{rx\varphi_W(y)} \leftarrow \underline{rx}\varphi_W(y)$$

Pairs of type (307):

$$\overline{W}W\varphi(y) \to \varphi(y)$$

Pairs of type (308): Let us choose a representative $s \in R_W$ and an element $y' \in \mathrm{dom}(\varphi_W)$ such that $xry = sy'$. We have

$$\underline{xry}W = \underline{sy'}W \to sW\varphi_W(y').$$

Moreover, since $y, y' \in \mathrm{dom}(\varphi_W)$, we have $y'y^{-1} \in \mathrm{dom}(\varphi_W)$. Hence, we also get

$$xrW\varphi_W(y) \to \underline{xr}W\varphi_W(y) = \underline{sy'y^{-1}}W\varphi_W(y) \to sW\varphi_W(y'y^{-1})\varphi_W(y) \to sW\varphi_W(y').$$

Pairs of type (309): First, note that

$$\varphi_k^{-1} \overset{(96)}{=} \delta_w(a_k) \circ \varphi_k \circ \delta_w(b_k) \overset{(97)}{=} \delta_w(b_k) \circ \varphi_k \circ \delta_w(a_k).$$

Since $\varphi_k(x) \in \mathrm{dom}(\varphi_k^{-1})$ we get

$$x = \varphi_k^{-1}(\varphi_k(x)) = a_k^{-1}\varphi_k(b_k^{-1}\varphi_k(x)b_k)a_k. \tag{312}$$

Inparticular, $b_k^{-1}\varphi_k(x)b_k \in \mathrm{dom}(\varphi_k)$. Since $b_k \in R_{W_k}$, we get:

$$\begin{aligned}
rW_k\varphi_k(x)b_kW_k \;&\to\; rW_k\underline{b_k(b_k^{-1}\varphi_k(x)b_k)}W_k\\
&\to\; rW_kb_kW_k\varphi_k(b_k^{-1}\varphi_k(x)b_k)\\
&\to\; ra_k^{-1}\varphi_k(b_k^{-1}\varphi_k(x)b_k)\\
&\to^* \underline{ra_k^{-1}\varphi_k(b_k^{-1}\varphi_k(x)b_k)} \overset{(312)}{=} \underline{rxa_k^{-1}} \leftarrow \underline{rx}a_k^{-1}.
\end{aligned}$$

Pairs of type (310): Since by (97), $\varphi_k(a_k^{-1}b_k) = b_ka_k^{-1}$ we have

$$a_k^{-1}b_kW_k \to_{S_{\mathbb{E}}} W_kb_ka_k^{-1}.$$

Pair of type (311): Since $x \in \mathrm{dom}(\varphi_k^{-1})$ and $\varphi_k^{-1} = \delta_w(a_k) \circ \varphi_k \circ \delta_w(b_k)$ by (96), we have

$$\varphi_k^{-1}(x) = b_k^{-1}\varphi_k(a_k^{-1}xa_k)b_k. \tag{313}$$

In particular, $a_k^{-1}xa_k \in \mathrm{dom}(\varphi_k)$. Let us choose a representative $s \in R_{W_k}$ and an element $x' \in \mathrm{dom}(\varphi_k)$ such that $ra_k = sx'$. With (313), we get

$$\varphi_k(x')b_k\varphi_k^{-1}(x) = \varphi_k(x'a_k^{-1}xa_k)b_k. \tag{314}$$

We get:

$$\begin{aligned} r\overline{W}_k\varphi_k^{-1}(x) &\to_{S_{\mathbb{E}}} ra_kW_kb_k\varphi_k^{-1}(x) \\ &\to_{S_{\mathbb{E}}} \underline{ra_k}W_kb_k\varphi_k^{-1}(x) \\ &= \underline{sx'}W_kb_k\varphi_k^{-1}(x) \\ &\to_{S_{\mathbb{E}}}^* sW_k\underline{\varphi_k(x')b_k\varphi_k^{-1}(x)} \\ &\overset{(314)}{=} sW_k\underline{\varphi_k(x'a_k^{-1}xa_k)b_k} \end{aligned}$$

On the other hand, we have

$$\underline{rx}a_kW_kb_k \to_{S_{\mathbb{E}}} \underline{rxa_k}W_kb_k = \underline{ra_k(a_k^{-1}xa_k)}W_kb_k = \underline{sx'(a_k^{-1}xa_k)}W_kb_k \to_{S_{\mathbb{E}}}^* sW_k\underline{\varphi_k(x'a_k^{-1}xa_k)b_k}.$$

We have shown that all critical pairs can be resolved. Hence $S_{\mathbb{E}}$ is indeed confluent. □

An element $s \in \mathcal{W}'^* * A * B$ is said to be a $\mathbb{E}$-*reduced sequence* if its corresponding (A, B)-reduced string neither contains a factor of the form $\mathbb{I}_w(W)cW$ with $W \in \mathcal{W}', c \in \mathrm{dom}(\delta_w(W))$ nor of the form $W_kb_kW_k$ for $1 \leq k \leq p$. We denote by $\mathrm{Red}_{\mathbb{E}}(A*B, \mathcal{W}')$ the subset of $\mathcal{W}'^**A*B$ consisting of all $\mathbb{E}$-reduced sequences.

Lemma 53. *Let $s \in \mathcal{W}'^* * A * B$ with $\gamma_w(s) \neq \emptyset$. Then s is $\mathbb{E}$-reduced.*

Proof. Let $s \in \mathcal{W}'^**A*B$ with $\gamma_w(s) \neq \emptyset$. We already know by Lemma 50 that s is $\mathbb{U}$-reduced. By (109), every W_k has an H-type, which implies that $\gamma(W_kb_kW_k) = \emptyset$, hence s cannot have any factor of the form $W_kb_kW_k$. □

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

$$\{(cW, Wd) \mid W \in \mathcal{W}', (c, d) \in \delta_w(W)\} \cup \{(W, \Phi(W) \mid W \in \mathcal{W}'\}. \tag{315}$$

Note that the congruence $\equiv_{\Phi}$ over $\mathcal{W}^* * A * B$, which was defined at the end of Section 3.9, is generated by the set of pairs

$$\{(cW, Wd) \mid W \in \mathcal{W}, (c, d) \in \delta_w(W)\} \cup \{(W, \Phi(W) \mid W \in \mathcal{W}\}. \tag{316}$$

The congruence $\equiv$ over $\mathcal{W}^* * A * B$ was defined by (89), the congruence $\equiv'$ over $\mathcal{W}'^* * A * B$ was defined by (289), and the congruences $\equiv_{\mathbb{U}}$ and $\equiv_{\mathbb{E}}$ over $\mathcal{W}'^**A*B$ are defined just above.

Leaning on the semi-Thue system $S_{\mathbb{E}}$ we are now able to prove the following lemma which is a key-argument for reducing equations over $\mathbb{W}/\Phi$ to equations over the group $\mathbb{E}$.

Lemma 54. *The following holds:*

(1) Let $s, s' \in \mathcal{W}'^* * A * B$ such that $\gamma(s) \neq \emptyset \neq \gamma(s')$. Then $s \equiv_{\mathbb{E}} s'$ if and only if $s \equiv'_{\Phi} s'$.
(2) Let $s, s' \in \mathcal{W}^* * A * B$ such that $\gamma(s) \neq \emptyset \neq \gamma(s')$. Then $s \equiv_{\mathbb{E}} s'$ if and only if $s \equiv_{\Phi} s'$.
(3) Let $s, s' \in \mathcal{W}'^* * A * B$ such that $\gamma(s) \neq \emptyset \neq \gamma(s')$. Then $s \equiv_{\mathbb{U}} s'$ if and only if $s \equiv' s'$.
(4) Let $s, s' \in \mathcal{W}^* * A * B$ such that $\gamma(s) \neq \emptyset \neq \gamma(s')$. Then $s \equiv_{\mathbb{U}} s'$ if and only if $s \equiv s'$.

Proof. For point (1) let us take $s, s' \in \mathcal{W}'^* * A * B$ such that $\gamma(s) \neq \emptyset \neq \gamma(s')$. First, assume that $s \equiv_{\mathbb{E}} s'$. Let us denote by z (resp. z') the unique (A,B)-reduced string representing s (resp. s'). In this proof, for every string $w \in \mathcal{G}_{\mathbb{E}}^*$, we denote by $[w]_{AB}$ its image in the free product $\mathcal{W}'^* * A * B$. Let us consider the reduction of z (resp. z') towards its normal form w.r.t. the system $S_{\mathbb{E}}$:

$$z \to_{S_{\mathbb{E}}}^* \rho_{S_{\mathbb{E}}}(z), \quad z' \to_{S_{\mathbb{E}}}^* \rho_{S_{\mathbb{E}}}(z'). \tag{317}$$

By Lemma 52(1), $z \overset{*}{\longleftrightarrow}_{S_{\mathbb{E}}} z'$ and by Lemma 52(2), $\rho_{S_{\mathbb{E}}}(z) = \rho_{S_{\mathbb{E}}}(z')$. Let us denote by $\gamma : \mathcal{G}_{\mathbb{E}}^* \to 2^{\mathcal{T}}$ the unique homomorphism such that for every $g \in \mathcal{G}_{\mathbb{E}}$, $\gamma(g) = \gamma_w([g]_{AB})$. Note that every rule of type (297), (298), or (300) increases (for the inclusion ordering) the value of γ. Note also that, if $\gamma(w) \neq \emptyset$, then by Lemma 53, the sequence $[w]_{AB}$ is $\mathbb{E}$-reduced which implies that the only rules of $S_{\mathbb{E}}$ that might have a redex in w are those of type (297), (298), or (300). Thus, for every $w, w' \in \mathcal{G}_{\mathbb{E}}^*$,

$$(\gamma(w) \neq \emptyset \text{ and } w \to_{S_{\mathbb{E}}} w') \Rightarrow \gamma(w') \neq \emptyset.$$

By induction, this implies that every reduction step in (317) uses a rule of type (297), (298), or (300). Since, every rule $(u \to v)$ of these types fulfills $[u]_{AB} \equiv'_{\Phi} [v]_{AB}$, we conclude that:

$$[z]_{AB} \equiv'_{\Phi} [\rho_{S_{\mathbb{E}}}(z)]_{AB} = [\rho_{S_{\mathbb{E}}}(z')]_{AB} \equiv'_{\Phi} [z']_{AB}.$$

Conversely, the congruence $\equiv'_{\Phi}$ is generated by all the defining relations of $\mathbb{W}'$ union the set of rules $\{(W, \Phi(W)) \mid W \in \mathcal{W}'\}$ which all belong to the presentation (296) of $\mathbb{E}$. Hence $\equiv'_{\Phi} \subseteq \equiv_{\mathbb{E}}$.

For point (2) from the lemma, let $T_{\mathbb{E}}$ be the set of all rules of type (297), (300), (301) together with those rules of type (298) where $W \in \mathcal{W}$ and those rules of type (299) where $W \in \widehat{\mathcal{W}}$. One can check that $T_{\mathbb{E}}$ is complete too (because in the above proof of Lemma 52, the resolutions for the critical pairs of $T_{\mathbb{E}}$ only use rules of $T_{\mathbb{E}}$ itself). Moreover, every rule $(u \to v)$ of $T_{\mathbb{E}}$ of type (297), (298), or (300) fulfills that $[u]_{AB} \equiv_{\Phi} [v]_{AB}$. Hence, by similar arguments, if $s, s' \in \mathcal{W}^* * A * B$ fulfill the hypothesis of point (2) then $s \equiv_{\Phi} s'$.

Point (3) of the lemma follows immediately from Lemma 49 and 50. It can also be proved by an adaptation of point (1), where instead of the semi-Thue system $S_{\mathbb{E}}$, we use the semi-Thue system $S_{\mathbb{U}}$ consisting of all rules of type (297), (298), and (299).

Finally, point (4) can be also proved by an adaptation of point (1), where instead of the semi-Thue system $S_{\mathbb{E}}$, we use the semi-Thue system $T_{\mathbb{U}}$ consisting of all rules of type (297) together with those rules of type (298) where $W \in \mathcal{W}$ and those rules of type (299) where $W \in \widehat{\mathcal{W}}$. Every rule $(u \to v)$ of $T_{\mathbb{U}}$ of type (297) or (298) with $W \in \mathcal{W}$, fulfills that $[u]_{AB} \equiv [v]_{AB}$. Hence, by similar arguments, if $s, s' \in \mathcal{W}^* * A * B$ fulfill the hypothesis of point (4) then $s \equiv s'$. □

7.3 Extensions of degree 2

The structure of $\mathbb{E}$ turns out to be based on quadratic extensions of A that are combined together by free product with amalgamation over A. We thus state some basic facts about quadratic extensions of groups. Let K be a group and E be the group presented by

$$E = \langle K, u;\ u^2 = c,\ u^{-1}xu = \psi(x)\,(x \in K)\rangle, \tag{318}$$

where u is a new letter, c is some element from K and $\psi : K \to K$ is a group automorphism fulfilling

$$\psi(c) = c \quad \text{and} \quad \forall x \in K : \psi(\psi(x)) = c^{-1}xc. \tag{319}$$

One can easily check that under hypothesis (319) on c and ψ, the group E is an extension of K with $[E : K] = 2$. Conversely, every extension E of K with $[E : K] = 2$ must have the form (318) for some $c \in K$ and some group automorphism $\psi : K \to K$ fulfilling (319).

7.4 The structure of $\mathbb{E}$

We show here by applying successive Tietze transformations that $\mathbb{E}$ can be obtained from a certain group $\mathbb{K}$ by a finite number of HNN-extensions over some strict subgroups of A. In Section 7.5, we will show that solvability of equations with rational constraints in $\mathbb{K}$ is decidable by a reduction to the main result of [DHG05], stating that solvability of equations with rational constraints over a free monoid with involution is decidable.

Remark 2. Note that $\mathbb{U}$ is by definition the fundamental group of a finite graph of groups where the vertex groups are A and B. Thus $\mathbb{U}$ is virtually free. The decomposition of $\mathbb{E}$ that we exhibit in this subsection can be seen as a finite graph of groups whose fundamental group is $\mathbb{E}$ showing that $\mathbb{E}$ is virtually-free, too.

First transformation: Let us choose some symbol from $\mathcal{W}$ such that the corresponding δ_w-value is a total isomorphism from A to B. We call this symbol t in the following, since any generic symbol from $\mathcal{W}$ that represents the stable letter t may serve. Hence $\delta_w(t) = \varphi$.

By applying the Tietze transformation

$$b \longrightarrow t^{-1}\varphi^{-1}(b)t \text{ for all } b \in B \setminus \{1\}$$

to the presentation (292), we obtain a group presentation with the set of generators $\mathcal{W}' \cup (A \setminus \{1\})$ and the following set of relations:

$$\begin{gathered}
W^{-1}aW = \delta_w(W)(a) \text{ if } \mathrm{Gi}(W) = \mathrm{Ge}(W) = A, a \in \mathrm{dom}(\delta_w(W)) \\
W^{-1}aW = t^{-1}\varphi^{-1}(\delta_w(W)(a))t \text{ if } \mathrm{Gi}(W) = A, \mathrm{Ge}(W) = B, W \neq t, a \in \mathrm{dom}(\delta_w(W)) \\
W^{-1}t^{-1}\varphi^{-1}(b)tW = t^{-1}\varphi^{-1}(\delta_w(W)(b))t \text{ if } \mathrm{Gi}(W) = \mathrm{Ge}(W) = B, b \in \mathrm{dom}(\delta_w(W)) \\
a_1a_2 = a_3 \text{ for } a_1, a_2, a_3 \in A \text{ with } a_1a_2 = a_3 \text{ in } A \\
W_k = a_k^{-1}W_k^{-1}b_k^{-1} \text{ for } 1 \leq k \leq p \text{ and } \mathrm{Gi}(W_k) = \mathrm{Ge}(W_k) = A \\
W_k = t^{-1}\varphi^{-1}(a_k^{-1})tW_k^{-1}t^{-1}\varphi^{-1}(b_k^{-1})t \text{ for } 1 \leq k \leq p \text{ and } \mathrm{Gi}(W_k) = \mathrm{Ge}(W_k) = B
\end{gathered}$$

where we know that (293) and (294) hold.

Second transformation: Let us define

$$\begin{aligned}
\mathcal{V} = \{t\} \cup \{W \in \mathcal{W}' \mid \mathrm{Gi}(W) = \mathrm{Ge}(W) = A\} \ \cup \ \{Wt^{-1} \mid \mathrm{Gi}(W) = A, \mathrm{Ge}(W) = B, W \neq t\} \\
\cup \{tWt^{-1} \mid \mathrm{Gi}(W) = \mathrm{Ge}(W) = B\}.
\end{aligned}$$

We take the new set of group generators $\mathcal{V} \cup (A \setminus \{1\})$. For every $1 \leq k \leq p$ we define:

$$\begin{aligned}
a'_k &= a_k, & b'_k &= b_k & &\text{if } \mathrm{Gi}(W_k) = \mathrm{Ge}(W_k) = A \\
a'_k &= \varphi^{-1}(a_k), & b'_k &= \varphi^{-1}(b_k) & &\text{if } \mathrm{Gi}(W_k) = \mathrm{Ge}(W_k) = B
\end{aligned}$$

Hence, we have $a'_k, b'_k \in A$ for $1 \leq k \leq p$. Moreover, for every $V \in \mathcal{V} \setminus \{t\}$ we define the partial automorphism $\delta_w(V) : A \to A$ in the natural way. E.g. if $V = tWt^{-1}$, where $W \in \mathcal{W}'$ with

$\mathrm{Gi}(W) = \mathrm{Ge}(W) = B$, then we set $\delta_w(V)(a) = \varphi \circ \delta_w(W) \circ \varphi^{-1}$. For $V = t$, since all the relations involving t and $A \cup B$ have now disappeared, $\delta_w(t)$ is defined as the trivial partial isomorphism, i.e., $\mathrm{dom}(\delta_w(t)) = \{1\}$.

We obtain the following finite set of relations:

$$V^{-1}aV = \delta_w(V)(a) \text{ for } V \in \mathcal{V}, a \in \mathrm{dom}(\delta_w(V)) \tag{320}$$

$$a_1a_2 = a_3 \text{ for } a_1, a_2, a_3 \in A \text{ with } a_1a_2 = a_3 \text{ in } A \tag{321}$$

$$V_k = (a'_k)^{-1}V_k^{-1}(b'_k)^{-1} \text{ for } 1 \leq k \leq p \tag{322}$$

In order to get (322), it is important to note that $\mathrm{Gi}(W_k) = \mathrm{Ge}(W_k)$ for $1 \leq k \leq p$. If, for instance, $\mathrm{Gi}(W_k) = \mathrm{Ge}(W_k) = B$, then we have $V_k = tW_kt^{-1}$, i.e., $W_k = t^{-1}V_kt$. Hence, the relation

$$W_k = t^{-1}\varphi^{-1}(a_k^{-1})tW_k^{-1}t^{-1}\varphi^{-1}(b_k^{-1})t$$

becomes

$$V_k = tW_kt^{-1} = \varphi^{-1}(a_k^{-1})(tW_k^{-1}t^{-1})\varphi^{-1}(b_k^{-1}) = (a'_k)^{-1}V_k^{-1}(b'_k)^{-1},$$

i.e., (322). Moreover, by translating the $\mathbb{U}$-relations (293) and (294) over W_k into relations over V_k (simply conjugate these relations with t in case $\mathrm{Gi}(W_k) = \mathrm{Ge}(W_k) = B$), we obtain:

$$V_k^{-1}(a'_k)^{-1}b'_kV_k \equiv_{\mathbb{U}} b'_k(a'_k)^{-1} \text{ for } 1 \leq k \leq p \tag{323}$$

$$(V_kb'_kV_ka'_k)^{-1}x(V_kb'_kV_ka'_k) \equiv_{\mathbb{U}} x \text{ for } 1 \leq k \leq p, x \in \mathrm{dom}(\delta_w(V_k)) \tag{324}$$

Third transformation: Let us define

$$\mathcal{U} = (\mathcal{V} \setminus \{V_1, V_1^{-1}, \ldots, V_p, V_p^{-1}\}) \cup \{U_1, U_1^{-1}, \ldots, U_p, U_p^{-1}\},$$

where $U_k = V_kb'_k$ and $U_k^{-1} = (b'_k)^{-1}V_k^{-1}$ and take as set of generators $\mathcal{U} \cup (A \setminus \{1\})$. Let us define $c_k = (a'_k)^{-1}b'_k \in A$. Moreover, let $\delta_w(U_k) = \delta_w(V_k) \circ \delta_w(b'_k)$. We obtain the following relations:

$$U^{-1}aU = \delta_w(U)(a) \text{ for } U \in \mathcal{U}, a \in \mathrm{dom}(\delta_w(U))$$

$$a_1a_2 = a_3 \text{ for } a_1, a_2, a_3 \in A \text{ with } a_1a_2 = a_3 \text{ in } A$$

$$U_k^2 = c_k \text{ for } 1 \leq k \leq p$$

Here, the last equation is obtained as follows: By (322) we have $a'_kV_kb'_kV_k = 1$, i.e., $a'_kV_kb'_kV_kb'_k = b'_k$. Hence, $a'_kU_k^2 = b'_k$, i.e., $U_k^2 = (a'_k)^{-1}b'_k = c_k$. Moreover, translating the $\mathbb{U}$-relations (323) and (324) over V_k into relations over U_k yields:

$$U_k^{-1}c_kU_k \equiv_{\mathbb{U}} c_k \text{ for } 1 \leq k \leq p \tag{325}$$

$$U_k^{-2}xU_k^2 \equiv_{\mathbb{U}} c_k^{-1}xc_k \text{ for } 1 \leq k \leq p, x \in \mathrm{dom}(\delta_w(U_k)) \tag{326}$$

Fourth transformation: Let us set $\varphi_U = \delta_w(U)$ for $U \in \mathcal{U}$. For φ_{U_k} $(1 \leq k \leq p)$ we also write φ_k. Thus, the last set of relations can be written as:

$$U^{-1}aU = \varphi_U(a) \text{ for } U \in \mathcal{U}, a \in \mathrm{dom}(\varphi_U) \tag{327}$$

$$a_1a_2 = a_3 \text{ for } a_1, a_2, a_3 \in A \text{ with } a_1a_2 = a_3 \text{ in } A \tag{328}$$

$$U_k^2 = c_k \text{ for } 1 \leq k \leq p \tag{329}$$

Moreover, by (325) and (326) we know that:

$$\varphi_k(c_k) \equiv_{\mathbb{U}} c_k \text{ for } 1 \leq k \leq p \tag{330}$$

$$\varphi_k^2(x) \equiv_{\mathbb{U}} c_k^{-1} x c_k \text{ for } x \in \mathrm{dom}(\varphi_k) \tag{331}$$

Remark 3. The group $\mathbb{U}$ is an HNN-extension of A. Hence A is embedded into $\mathbb{U}$. Thus (330) and (331) hold in A too.

Remark 4. Equation (331) shows that for every $a \in \mathrm{dom}(\varphi_k)$, $\varphi_k(a) \in \mathrm{dom}(\varphi_k)$. Hence, we have $\mathrm{im}(\varphi_k) \subseteq \mathrm{dom}(\varphi_k)$. Since φ_k is injective and $\mathrm{dom}(\varphi_k)$ is finite, we get

$$\mathrm{dom}(\varphi_k) = \mathrm{im}(\varphi_k)$$

for all $1 \leq k \leq p$. Hence, φ_k is an automorphism of the finite group $\mathrm{dom}(\varphi_k)$.

Decomposition of $\mathbb{E}$: Since φ_k is an automorphism of the finite group $\mathrm{dom}(\varphi_k)$, we can define the group

$$B_k = \langle \mathrm{dom}(\varphi_k), U_k; U_k^{-1} a U_k = \varphi_k(a) (a \in \mathrm{dom}(\varphi_k)), U_k^2 = c_k \rangle \text{ for } 1 \leq k \leq p. \tag{332}$$

By Remark 3 and Section 7.3 on quadratic extensions, each B_k is a quadratic extension of $\mathrm{dom}(\varphi_k)$. Hence, each B_k is a finite group.

Consider the iterated amalgamated free product

$$\mathbb{E}_0 = (\cdots ((A *_{\mathrm{dom}(\varphi_1)} B_1) *_{\mathrm{dom}(\varphi_2)} B_2) *_{\mathrm{dom}(\varphi_3)} \cdots *_{\mathrm{dom}(\varphi_p)} B_p).$$

Since each amalgamation is over a finite group, $\mathbb{E}_0$ is virtually-free. Let

$$\mathcal{U}_\infty = \mathcal{U} \setminus \{U_1, U_1^{-1}, \ldots, U_p, U_p^{-1}\}.$$

From the presentation (327)–(329) of $\mathbb{E}$ it follows that $\mathbb{E}$ can be obtained as a multiple HNN-extension of $\mathbb{E}_0$ over finite groups:

$$\mathbb{E} = \langle \mathbb{E}_0, \mathcal{U}_\infty; U^{-1} a U = \varphi_U(a) (U \in \mathcal{U}_\infty, a \in \mathrm{dom}(\varphi_U)) \rangle$$

Hence, $\mathbb{E}$ is virtually-free.

Let us now change the order of the operations (amalgamated free products and HNN-extensions) in which $\mathbb{E}$ is constructed. Let

$$\begin{aligned} \mathcal{U}_A &= \{U \in \mathcal{U} \mid \mathrm{dom}(\varphi_U) = A\}, \\ \mathcal{U}_{A,\infty} &= \mathcal{U}_A \cap \mathcal{U}_\infty, \\ \mathcal{U}_{A,2} &= \mathcal{U}_A \setminus \mathcal{U}_{A,\infty}. \end{aligned}$$

Up to a permutation of the indices $1, 2, \ldots, p$, we can assume that there is $0 \leq p_A \leq p$ such that

$$\mathcal{U}_{A,2} = \{U_1, U_1^{-1}, \ldots, U_{p_A}, U_{p_A}^{-1}\},$$

i.e., $\mathrm{dom}(\varphi_k) = A$ for $1 \leq k \leq p_A$, while $\mathrm{dom}(\varphi_k) \subsetneq A$ for $p_A + 1 \leq k \leq p$. Let

$$\mathbb{K}_0 = (\cdots ((A *_A B_1) *_A B_2) *_A \cdots *_A B_{p_A}) \tag{333}$$

(the factor A in the innermost amalgamated free product is only necessary if $p_A = 0$) and

$$\mathbb{K} = \langle \mathbb{K}_0, \mathcal{U}_{A,\infty}; U^{-1} a U = \varphi_U(a) (U \in \mathcal{U}_{A,\infty}, a \in \mathrm{dom}(\varphi_U)) \rangle. \tag{334}$$

Then, the group $\mathbb{E}$ can be obtained from $\mathbb{K}$ by a finite number of operations, each of which is

– either an HNN-extension with associated subgroups of cardinality $< |A|$ (relation (327) when $\mathrm{dom}(\varphi_{\mathcal{U}}) \subsetneq A$ and $\mathcal{U} \in \mathcal{U}_\infty$),
– or an amalgamated free product with a finite group B_k, where the amalgamation is over the subgroup $\mathrm{dom}(\varphi_k) \subsetneq A$ (relations (327) and (329) when $p_A + 1 \leq k \leq p$).

The following group presentation of $\mathbb{K}$ can be extracted from (333) and (334):

$$a_1 a_2 = a_3 \text{ for } a_1, a_2, a_3 \in A \text{ with } a_1 a_2 = a_3 \text{ in } A \tag{335}$$
$$U^{-1} a U = \varphi_U(a) \text{ for } a \in A, U \in \mathcal{U}_{A,\infty} \tag{336}$$
$$U_k^{-1} a U_k = \varphi_k(a) \text{ for } a \in A, 1 \leq k \leq p_A \tag{337}$$
$$U_k^2 = c_k \text{ for } 1 \leq k \leq p_A \tag{338}$$

From the above presentations, we see the following:

Lemma 55. *$\mathbb{K}$ and $\mathbb{E}$ are finitely generated virtually-free groups.*

Proof. Both groups can be constructed from finite groups using the operations of amalgamated free products over finite groups and HNN-extensions with finite associated subgroups. □

7.5 Equations over $\mathbb{K}$

In this section we show that solvability of equations with rational constraints is decidable for $\mathbb{K}$. Let us consider the alphabets

$$\mathcal{G}_U = \mathcal{U}_{A,\infty} \cup \{U_k \mid 1 \leq k \leq p_A\},$$
$$\mathcal{G}_{\mathbb{K}} = \mathcal{G}_U \cup (A \setminus \{1\}).$$

Since $U_k^{-1} = U_k c_k^{-1}$ in $\mathbb{K}$, $\mathcal{G}_{\mathbb{K}}$ is a set of monoid generators of $\mathbb{K}$. Let us define the group:

$$K_0 = \langle \mathcal{G}_U ; U_k^2 = \varepsilon \ (1 \leq k \leq p_A) \rangle \cong (\mathbb{Z}_2)^{p_A} * F(\mathcal{U}_{A,\infty}),$$

where $F(\mathcal{U}_{A,\infty})$ is the free group generated by $\mathcal{U}_{A,\infty}$.

Let us define the following sets of words over $\mathcal{G}_U$:

$$\mathsf{FORB} = \{U^{-1} U \mid U \in \mathcal{U}_{A,\infty}\} \cup \{U_k U_k \mid 1 \leq k \leq p_A\}$$
$$R = \mathcal{G}_U^* \setminus (\mathcal{G}_U^* \, \mathsf{FORB} \, \mathcal{G}_U^*).$$

Let the finite semi-Thue system S over the alphabet $\mathcal{G}_U$ contain all rules $u \to \varepsilon$ for $u \in \mathsf{FORB}$. Note that R is the set of irreducible words with respect to S. The proof for following lemma is straightforward.

Lemma 56. *The following holds:*

(1) The monoid $\mathcal{G}_U^* / \overset{*}{\longleftrightarrow}_S$ is isomorphic to K_0.
(2) The semi-Thue system S is confluent and Noetherian.
(3) The set of words $R \subseteq \mathcal{G}_U^*$ is a transversal for $\overset{*}{\longleftrightarrow}_S$.

Lemma 57. *There exists a unique group homomorphism $\psi : \mathbb{K} \to K_0$ such that*

– *for all* $g \in \mathcal{G}_U$, $\psi(g) = g$ *and*
– *for all* $a \in A$, $\psi(a) = 1$.

Proof. Let us first prove the existence of ψ. Let us consider the monoid homomorphism $\theta : \mathcal{G}_{\mathbb{K}}^* \to K_0$ defined as follows:

– For all $g \in \mathcal{G}_U$, $\theta(g) = g$, and
– for all $a \in A$, $\theta(a) = 1$.

Then, for every relation $u = v$ from (335)–(338), we have $\theta(u) = \theta(v)$. Hence, there exists a homomorphism $\psi : \mathbb{K} \to K_0$ such that $\theta(w) = \psi([w]_{\mathbb{K}})$ for all $w \in \mathcal{G}_{\mathbb{K}}^*$. This homomorphism ψ satisfies the requirements from the lemma. To show unicity, note that $\mathcal{G}_{\mathbb{K}}$ is a set of monoid generators of $\mathbb{K}$. Hence, the values of ψ on these generators completely determine ψ. □

For $z \in \mathcal{G}_U^*$, let us use the abreviated notation $[z]_0$ for $[z]_{K_0}$. Let $\mathsf{nf} : K_0 \to R$ be the mapping such that $\mathsf{nf}(g)$ is the unique word $w \in R$ such that $g = [w]_0$.

Lemma 58. *The homomorphism* ψ *introduced in Lemma 57 is such that:*

(1) $\mathrm{Ker}(\psi) = A$ *and*
(2) $[R]_{\mathbb{K}}$ *is a transversal of* $\mathbb{K}$ *for the cosets of* $A \leq \mathbb{K}$.

Proof. Let us first prove that every element of $\mathbb{K}$ has the form $[wa]_{\mathbb{K}}$ for some $w \in R, a \in A$. Let us consider the following set of rules, $S_{\mathbb{K}}$, obtained essentially by orientating the relations (335)–(338):

$$\begin{aligned} a_1a_2 &\to a_3 \text{ for } a_1, a_2 \in A \setminus \{1\}, a_3 \in A \text{ with } a_1a_2 = a_3 \text{ in } A \\ aU &\to U\varphi_U(a) \text{ for } a \in A \setminus \{1\}, U \in \mathcal{U}_{A,\infty} \\ aU_k &\to U_k\varphi_k(a) \text{ for } a \in A \setminus \{1\}, 1 \leq k \leq p_A \\ U_k^2 &\to c_k \text{ for } 1 \leq k \leq p_A \\ U^{-1}U &\to \varepsilon \text{ for } U \in \mathcal{U}_{A,\infty} \end{aligned}$$

Applying iteratively these rules to a word $v \in \mathcal{G}_{\mathbb{K}}^*$ until no rule is applicable anymore, one can find a word $v' \in R$ and some $a \in A$ such that $v \equiv_{\mathbb{K}} v'a$.

Now, we can show point (1) from the lemma. Clearly, $A \subseteq \mathrm{Ker}(\psi)$. For the other inclusion, let $w \in R$ and $a \in A$ such that $\psi([wa]_{\mathbb{K}}) = 1$. Hence, $w \equiv_{K_0} \varepsilon$. Since R is the set of irreducible words with respect to S, which presents K_0, we get $w = \varepsilon$, i.e., $[wa]_{\mathbb{K}} \in A$. This establishes that $\mathrm{Ker}(\psi) \subseteq A$.

For point (2) from the lemma, let $w, w' \in R$ and $a, a' \in A$ such that $[wa]_{\mathbb{K}} = [w'a']_{\mathbb{K}}$. Then, $\psi([wa]_{\mathbb{K}}) = \psi([w'a']_{\mathbb{K}})$. Since $A \subseteq \mathrm{Ker}(\psi)$, we have $\psi([w]_{\mathbb{K}}) = \psi([w']_{\mathbb{K}})$ i.e. $[w]_0 = [w']_0$. By Lemma 56, $w = w'$ which proves that $[w]_{\mathbb{K}} = [w']_{\mathbb{K}}$. This establishes point (2) of the lemma. □

In other words,

$$1 \to A \to \mathbb{K} \xrightarrow{\psi} K_0 \to 1$$

is an exact sequence and the restriction $\psi\restriction[R]_{\mathbb{K}} : [R]_{\mathbb{K}} \to K_0$ is bijective.

Let $\psi' : \mathbb{K} \to R$ be the mapping $\psi \circ \mathsf{nf}$.

Lemma 59. *Let L be a rational subset of $\mathbb{K}$. Then, for every $a \in A$, $\psi'(L \cap [Ra]_{\mathbb{K}})$ is a rational subset of R, and an automaton for this set can be effectively constructed from an automaton for L. Moreover, if $w \in R$ and $a \in A$, then $[wa]_{\mathbb{K}} \in L$ if and only if $w \in \psi'(L \cap [Ra]_{\mathbb{K}})$.*

Proof. First, suppose that L is a rational subset of $\mathbb{K}$. The subsets R and $\{a\}$ are rational subsets of $\mathcal{G}_{\mathbb{K}}^*$. Thus, Ra is a rational subset of $\mathcal{G}_{\mathbb{K}}^*$, which implies that its homomorphic image in $\mathbb{K}$, $[Ra]_{\mathbb{K}}$, is a rational subset of $\mathbb{K}$. It is well-known that rational subsets of a virtually-free group are effectively closed under intersection (see, e.g., [Sén96,LS08]), hence $L \cap [Ra]_{\mathbb{K}}$ is rational. Since ψ is a monoid homomorphism, we get that $\psi(L \cap [Ra]_{\mathbb{K}})$ is a rational subset of K_0. Let $M \subseteq \mathcal{G}_U^*$ be a rational subset such that $[M]_0 = \psi(L \cap [Ra]_{\mathbb{K}})$. Since S is a monadic semi-Thue system, the set of descendants

$$M' = \{v \in \mathcal{G}_U^* \mid \exists u \in M : u \to_S^* v\}$$

of M is rational too, see [BO93]. Finally, we have $\psi'(L \cap [Ra]_{\mathbb{K}}) = \mathsf{nf}([M]_0) = M' \cap R$, which is therefore rational, too.

Now, assume that $w \in R$ and $a \in A$. If $[wa]_{\mathbb{K}} \in L$, then clearly $w \in \psi'(L \cap [Ra]_{\mathbb{K}})$. On the other hand, if $w \in \psi'(L \cap [Ra]_{\mathbb{K}})$, then there exists $[w'a']_{\mathbb{K}} \in L \cap [Ra]_{\mathbb{K}}$ such that $w = \psi'([w'a']_{\mathbb{K}}) = \mathsf{nf}([w']_0) = w'$. From $[w'a']_{\mathbb{K}} \in [Ra]_{\mathbb{K}}$, we get $a = a'$ with Lemma 58(2). Hence $[wa]_{\mathbb{K}} = [w'a']_{\mathbb{K}} \in L$. □

Let us introduce now a right-action $a \mapsto a^w$ and a right-action $a \mapsto a \odot w$ of the free monoid $\mathcal{G}_U^*$ over the set A in order to express some equalities in $\mathbb{K}$ by some rational constraints in the free monoid $\mathcal{G}_U^*$. For every $a \in A$, $U \in \mathcal{U}_{A,\infty}$, and $1 \leq k \leq p_A$, we set:

$$\begin{aligned} a^U &= \varphi_U(a) \\ a^{U_k} &= \varphi_k(a) \\ a \odot U &= \varphi_U(a) \\ a \odot U_k &= c_k \cdot \varphi_k(a) \end{aligned}$$

The action $a \mapsto a^w$ does *not* induce an action of the *group* K_0 over the set A: For example, $a^{U_k U_k} = \varphi_k^2(a) = c_k^{-1} a c_k$, which might be different from $a^\varepsilon = a$, while $U_k U_k \equiv_{K_0} \varepsilon$. The same remark applies to the action $\odot$ with the counter-example $a \odot U_k U_k = c_k \varphi_k(c_k) c_k^{-1} a c_k = c_k a c_k$.

For every $w \in \mathcal{G}_U^*$, $a \mapsto a^w$ is a group isomorphism of A. But, for some $w \in \mathcal{G}_U^*$, $a \mapsto a \odot w$ might *not* be a group homomorphism: For example, $(a_1 a_2) \odot U_k = c_k \varphi_k(a_1) \varphi_k(a_2)$ while $(a_1 \odot U_k)(a_2 \odot U_k) = c_k \varphi_k(a_1) c_k \varphi_k(a_2)$, which is a different element of A as soon as $c_k \neq 1$.

Note that $w^{-1} a w \equiv_{\mathbb{K}} a^w$ for all $w \in \mathcal{G}_U^*$ and $a \in A$. Hence, we get:

Lemma 60. *For all $w \in \mathcal{G}_U^*$ and $a \in A$, we have $aw \equiv_{\mathbb{K}} wa^w$.*

Let us denote by $\mathbb{J} : \mathcal{G}_U^* \to \mathcal{G}_U^*$ the monoid involution such that $\mathbb{J}(U) = U^{-1}$ and $\mathbb{J}(U^{-1}) = U$ for $U \in \mathcal{U}_{A,\infty}$ and $\mathbb{J}(U_k) = U_k$ for $1 \leq k \leq p_A$. Note that in the group $\mathbb{K}$, we have $a \odot U_k = c_k \varphi_k(a) = U_k^2 \varphi_k(a) = U_k^2 U_k^{-1} a U_k = U_k a U_k$. Hence, we get:

Lemma 61. *For every $w \in \mathcal{G}_U^*$, $\mathbb{J}(w) a w \equiv_{\mathbb{K}} a \odot w$.*

The following lemma expresses the product in $\mathbb{K}$ in the free monoid $\mathcal{G}_U^*$ with involution $\mathbb{J}$.

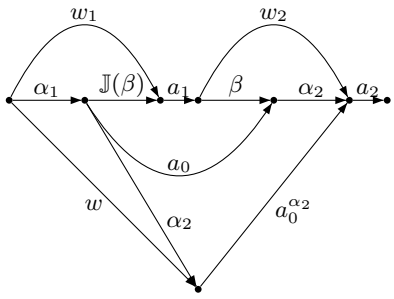


Fig. 16. Proof of Lemma 62

Lemma 62. *For every $w_1, w_2, w \in R, a_1, a_2, a \in A$,*

$$w_1 a_1 \, w_2 a_2 \equiv_{\mathbb{K}} wa$$

if and only if there exist $a_0 \in A$ and $\alpha_1, \alpha_2, \beta \in R$ such that

$$a_1 \odot \beta = a_0 \tag{339}$$
$$a_0^{\alpha_2} a_2 = a \tag{340}$$
$$w_1 = \alpha_1 \mathbb{J}(\beta) \tag{341}$$
$$w_2 = \beta \alpha_2 \tag{342}$$
$$w = \alpha_1 \alpha_2 \tag{343}$$

Proof. First, suppose that $w_1, w_2, w \in R, a_1, a_2, a \in A$ and

$$w_1 a_1 w_2 a_2 \equiv_{\mathbb{K}} wa. \tag{344}$$

Let β be the longest common prefix of w_2 and $\mathbb{J}(w_1)$ (the mirror image of w_1). There exist words $\alpha_1, \alpha_2 \in \mathcal{G}_U^*$ such that

$$w_1 = \alpha_1 \mathbb{J}(\beta) \text{ and } w_2 = \beta \alpha_2.$$

Since $\alpha_1, \alpha_2, \beta$ are factors of words from R, they belong to R as well. Moreover, by maximality of β, we have $\alpha_1 \alpha_2 \in R$.

By Lemma 61,

$$\mathbb{J}(\beta) a_1 \beta \equiv_{\mathbb{K}} a_1 \odot \beta$$

Let us define

$$a_0 = a_1 \odot \beta.$$

The initial equality (344) can be now rephrased as

$$\alpha_1 a_0 \alpha_2 a_2 \equiv_{\mathbb{K}} wa.$$

By Lemma 60,

$$a_0 \alpha_2 \equiv_{\mathbb{K}} \alpha_2 a_0^{\alpha_2}.$$

Hence, we get

$$(\alpha_1\alpha_2)(a_0^{\alpha_2}a_2) \equiv_{\mathbb{K}} wa.$$

Since $w, \alpha_1\alpha_2 \in R$, we get

$$w = \alpha_1\alpha_2 \text{ and } a_0^{\alpha_2}a_2 = a.$$

For the other direction, suppose now that there exist $a_0 \in A$ and $\alpha_1, \alpha_2, \beta \in R$ fulfilling conditions (339)–(343). Translating the right-actions by appropriate products (by means of Lemma 60 and Lemma 61) one can recover the equality (344). □

Proposition 6. *The satisfiability problem for systems of equations with rational constraints in $\mathbb{K}$ is decidable.*

Proof. We reduce the satisfiability problem for systems of equations with rational constraints in $\mathbb{K}$ to the satisfiability problem for systems of equations with rational constraints in the free monoid $\mathcal{G}_U^*$ with involution $\mathbb{J}$. The latter problem is decidable by [DHG05].

By Lemma 62, the product in $\mathbb{K}$ can be expressed by a finite boolean combination of equalities in the free monoid $\mathcal{G}_U^*$ with involution $\mathbb{J}$, together with some rational constraints and the additional conditions (339) and (340) using the operations $\odot$ and $a \mapsto a^u$. All variables will be restricted to the rational subset $R \subseteq \mathcal{G}_U^*$. Condition (339) can be expressed by the rational constraint

$$\beta \in \{w \in R \mid a_1 \odot w = a_0\}.$$

Similarly, condition (340) can be expressed by the rational constraint $a_0^{\alpha_2} = aa_2^{-1}$.

Every equation over $\mathbb{K}$ can thus be translated into a finite disjunction of systems of equations with rational constraints over the free monoid $\mathcal{G}_U^*$ with involution $\mathbb{J}$. The disjunction enumerates the finite list of all the possible values of $a_0, a_1, a_2, a \in A$. Moreover, by Lemma 59, every rational constraint over $\mathbb{K}$ can be translated into a rational constraint over $\mathcal{G}_U^*$. □

8 Equations over $\mathbb{E}$

8.1 From $\mathbb{W}$-equations to $\mathbb{E}$-equations

We use here the notion of system of equations with rational constraints over $\mathbb{E}$, as defined in Section 2.6 for any monoid. Recall from Section 3.8 that $\mathbb{W}_{\mathbb{H}}$ is the AB-subalgebra of $\mathbb{W}_t$ generated by those $W \in \mathcal{W}_t$ which have an H-type. Let us consider a system of $\mathbb{W}$-equations $(\mathcal{S}_{\mathbb{W}}, \Phi)$, where

$$\mathcal{S}_{\mathbb{W}} = \{(w_i, w_i') \mid 1 \leq i \leq n\}$$

(hence, $\Phi \in \mathsf{HInv}$) together with an AB-homomorphism

$$\sigma_{\mathbb{H}} \in \mathrm{Hom}_{AB}(\mathbb{W}_{\mathbb{H}}, \mathbb{W}_{\mathbb{H}}/\Phi).$$

The AB-homomorphism $\Phi : \mathbb{W} \to \mathbb{W}$ is given by formulas of the form (92)–(95) with the additional conditions (96)–(99). For every $1 \leq k \leq p$, $\gamma_w(W_k)$ must be an H-type and $\mathrm{Gi}(W_k) = \mathrm{Ge}(W_k)$ (see (93)).

Let $z_i, z_i' \in \mathcal{W}_t^* * A * B$ be some representatives, modulo $\equiv$, of w_i and w_i', respectively. Recall that

- $\gamma_w(z_i) = \gamma_w(z_i') \neq \emptyset$ for all $1 \leq i \leq n$ (see Section 6), and
- $\pi_{\equiv} : \mathcal{W}^* * A * B \to \mathbb{W}$ and $\pi_{\equiv_\Phi} : \mathcal{W}^* * A * B \to \mathbb{W}/\phi$ are the canonical morphisms.

We can also choose a monoid-homomorphism $\widetilde{\sigma}_{\mathbb{H}} : \mathcal{W}_{\mathbb{H}}^* * A * B \to \mathcal{W}_{\mathbb{H}}^* * A * B$ such that $\pi_{\equiv} \circ \sigma_{\mathbb{H}} = \widetilde{\sigma}_{\mathbb{H}} \circ \pi_{\equiv_\Phi}$. For every $W \in \mathcal{W}_t$ we consider the following rational subsets of $\mathcal{W}_t^* * A * B$:

$$\begin{aligned}
R_{\mathbb{I},W} &= \{z \in \mathcal{W}_t^* * A * B \mid \gamma_w(z) = \gamma_w(W) \ \wedge \ z \in \widehat{\mathcal{W}}_t^* * A * B \Leftrightarrow W \in \widehat{\mathcal{W}}_t\} \\
R_{\mu,W} &= \{z \in \mathcal{W}_t^* * A * B \mid \gamma_w(z) = \gamma_w(W) \ \wedge \ \mu_w(z) = \mu_w(W)\} \\
R_{\delta,W} &= \{z \in \mathcal{W}_t^* * A * B \mid \gamma_w(z) = \gamma_w(W) \ \wedge \ \delta_w(z) = \delta_w(W)\} \\
R_{\mathbb{H},W} &= \begin{cases} \{\widetilde{\sigma}_{\mathbb{H}}(W)\} & \text{if } W \in \mathcal{W}_{\mathbb{H}} \\ \mathcal{W}_t^* * A * B & \text{if } W \in \mathcal{W}_t \setminus \mathcal{W}_{\mathbb{H}} \end{cases}
\end{aligned}$$

We next want to define a system of equations over $\mathbb{E}$ (in the sense of Section 2.6), whose equations comprise the pairs (z_i, z_i') together with equations expressing the compatibility with $\mathbb{I}_w$, i.e., the fact that images of inverses for $\mathbb{I}_w$ must be inverses in the group $\mathbb{E}$. In order to be in accordance with Section 2.6, we have to identify z_i, z_i' with their (A, B)-reduced representatives in $(\mathcal{W} \cup A \cup B)^*$ and to consider elements from $(A \cup B) \setminus \{1\}$ (which may occur in these representatives) as variables, since the z_i and z_i' are only allowed to contain variables. With these conventions, we introduce the following constraint $\mathsf{C} : \mathcal{W}_t \cup (A \cup B) \setminus \{1\} \to \mathsf{bool}(\mathsf{Rat}(\mathbb{E}))$:

$$\begin{gathered}
\forall W \in \mathcal{W}_t : \mathsf{C}(W) = \pi_{\mathbb{E}}(R_{\mathbb{I},W}) \cap \pi_{\mathbb{E}}(R_{\mu,W}) \cap \pi_{\mathbb{E}}(R_{\delta,W}) \cap \pi_{\mathbb{E}}(R_{\mathbb{H},W}) \\
\forall c \in (A \cup B) \setminus \{1\} : \mathsf{C}(c) = \{\pi_{\mathbb{E}}(c)\}
\end{gathered}$$

Here, $\pi_{\mathbb{E}} : \mathcal{W}_t^* * A * B \to \mathbb{E}$ is the natural projection onto $\mathbb{E}$. Let us now define the system $(\mathcal{S}_{\mathbb{E}}, \mathsf{C})$ of equations over $\mathbb{E}$ with rational constraints, where

$$\mathcal{S}_{\mathbb{E}} = \{(z_i, z_i') \mid 1 \leq i \leq n\} \cup \{(W\mathbb{I}_w(W), \varepsilon) \mid W \in \widehat{\mathcal{W}}_t \setminus \mathcal{W}_{\mathbb{H}}\}.$$

Note that the constraint mapping C depends on $\sigma_{\mathbb{H}}$, but not on the choice of $\widetilde{\sigma}_{\mathbb{H}}$. Let us denote by $\overline{\pi}_{\mathbb{E}} : \mathbb{W}_t/\Phi \to \mathbb{E}$ the map induced by $\pi_{\mathbb{E}}$, i.e., $\overline{\pi}_{\mathbb{E}}([w]_{\equiv_\Phi}) = \pi_{\mathbb{E}}(w)$).

Lemma 63. *The map* $\Psi : \mathrm{Hom}_{AB}(\mathbb{W}_t, \mathbb{W}_t/\Phi) \to \mathrm{Hom}(\mathcal{W}_t^* * A * B, \mathbb{E})$ *defined by:*

$$\Psi(\sigma_{\mathbb{W}}) = \pi_{\equiv} \circ \sigma_{\mathbb{W}} \circ \overline{\pi}_{\mathbb{E}}$$

induces a bijection from the set of solutions of $(\mathcal{S}_{\mathbb{W}}, \Phi)$*, which extend* $\sigma_{\mathbb{H}}$*, into the set of solutions of* $(\mathcal{S}_{\mathbb{E}}, \mathsf{C})$*.*

We prove this lemma in the subsequent three subsections, see Figure 17 for the general context and Figure 18 for the details of the proof. Note that the diagram in Figure 17 contains the diagram from Figure 11.

8.2 From $\mathbb{W}$-solutions to $\mathbb{E}$-solutions

Let $\sigma_{\mathbb{W}} : \mathbb{W}_t \to \mathbb{W}_t/\Phi$ be a solution of $(\mathcal{S}_{\mathbb{W}}, \Phi)$, extending $\sigma_{\mathbb{H}}$. Let $\sigma_{\mathbb{E}} = \Psi(\sigma_{\mathbb{W}}) = \pi_{\equiv} \circ \sigma_{\mathbb{W}} \circ \overline{\pi}_{\mathbb{E}}$. From the definitions of z_i and z_i' we get

$$\sigma_{\mathbb{E}}(z_i) = \overline{\pi}_{\mathbb{E}}(\sigma_{\mathbb{W}}(w_i)) = \overline{\pi}_{\mathbb{E}}(\sigma_{\mathbb{W}}(w_i')) = \sigma_{\mathbb{E}}(z_i'). \tag{345}$$

By hypothesis, $\sigma_{\mathbb{W}}$ is an AB-homomorphism. Hence, it commutes with the involutions given by the AB-structures, i.e.,

$$\forall W \in \widehat{\mathcal{W}}_t : \sigma_{\mathbb{W}}(\mathbb{I}_w(W)) = \mathbb{I}_w(\sigma_{\mathbb{W}}(W)). \tag{346}$$

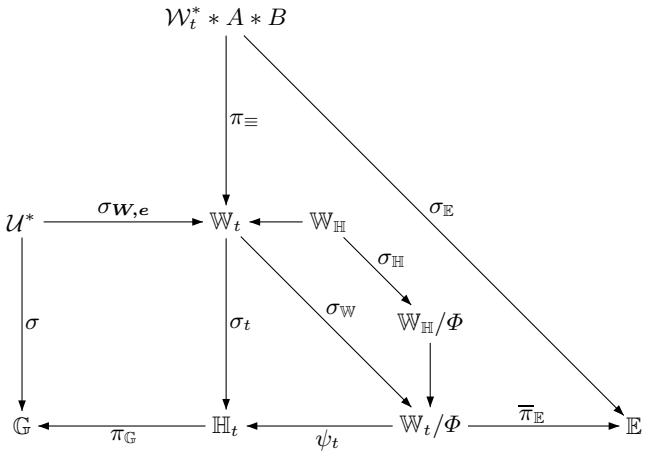


Fig. 17. Lemma 63: the context

The defining relations of $\mathbb{E}$ ensure that for every $w \in \mathbb{W}_t$,

$$\overline{\pi}_{\mathbb{E}}\big(\sigma_{\mathbb{W}}(w)\mathbb{I}_w(\sigma_{\mathbb{W}}(w))\big) = 1.$$

Hence, the relations (346) imply

$$\forall W \in \widehat{\mathcal{W}_t} : \sigma_{\mathbb{E}}(W\mathbb{I}_w(W)) = \overline{\pi}_{\mathbb{E}}(\sigma_{\mathbb{W}}(W)\sigma_{\mathbb{W}}(\mathbb{I}_w(W))) = 1. \tag{347}$$

The map $\pi_{\equiv} \circ \sigma_{\mathbb{W}} : \mathcal{W}_t^* * A * B \to \mathbb{W}_t/\Phi$ is an AB-homomorphism. Hence, it preserves γ_w, μ_w, and δ_w (by Lemma 38 the type is exactly preserved). It follows that for every $W \in \mathcal{W}_t$.

$$\sigma_{\mathbb{W}}(\pi_{\equiv}(W)) \in \pi_{\equiv_\Phi}(R_{\mathbb{I},W}) \cap \pi_{\equiv_\Phi}(R_{\mu,W}) \cap \pi_{\equiv_\Phi}(R_{\delta,W}).$$

As $\sigma_{\mathbb{W}}$ extends $\sigma_{\mathbb{H}}$, we get

$$\sigma_{\mathbb{W}}(\pi_{\equiv}(W)) \in \pi_{\equiv_\Phi}(R_{\mathbb{H},W})$$

for every $W \in \mathcal{W}_t$. Applying $\overline{\pi}_{\mathbb{E}}$ on both sides of these membership relations, we obtain

$$\forall W \in \mathcal{W}_t : \sigma_{\mathbb{E}}(W) \in \mathsf{C}(W). \tag{348}$$

Moreover the three maps $\pi_{\equiv}$, $\sigma_{\mathbb{W}}$, and $\overline{\pi}_{\mathbb{E}}$ fix every element of $A \cup B$. Thus, we have

$$\forall c \in (A \cup B) \setminus \{1\} : \sigma_{\mathbb{E}}(c) \in \mathsf{C}(c). \tag{349}$$

By (345), (347), (348) and (349), $\sigma_{\mathbb{E}}$ is a solution of $(\mathcal{S}_{\mathbb{E}}, \mathsf{C})$.

8.3 From $\mathbb{E}$-solutions to $\mathbb{W}$-solutions

Let $\sigma_{\mathbb{E}}$ be a solution of $(\mathcal{S}_{\mathbb{E}}, \mathsf{C})$. Since, for every $W \in \mathcal{W}_t$, $\sigma_{\mathbb{E}}(W) \in \mathsf{C}(W) \subseteq \pi_{\mathbb{E}}(R_{\mu,W})$, there is a choice map $\widetilde{\sigma}_{\mathbb{E}} : \mathcal{W}_t \to \mathcal{W}_t^* * A * B$ fulfilling

$$\forall W \in \mathcal{W}_t : \widetilde{\sigma}_{\mathbb{E}}(W) \in R_{\mu,W} \text{ and } \pi_{\mathbb{E}}(\widetilde{\sigma}_{\mathbb{E}}(W)) = \sigma_{\mathbb{E}}(W). \tag{350}$$

From $\widetilde{\sigma}_{\mathbb{E}}(W) \in R_{\mu,W}$ we get

$$\gamma_w(\widetilde{\sigma}_{\mathbb{E}}(W)) = \gamma_w(W) \text{ and } \mu_w(\widetilde{\sigma}_{\mathbb{E}}(W)) = \mu_w(W). \tag{351}$$

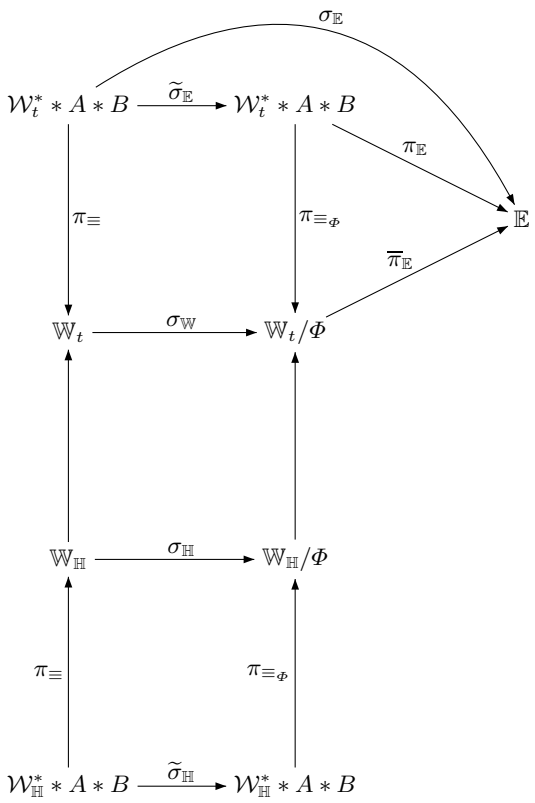


Fig. 18. Lemma 63: the proof

Let us denote by $\widetilde{\sigma}_{\mathbb{E}} : \mathcal{W}_t^* * A * B \to \mathcal{W}_t^* * A * B$ the unique monoid homomorphism fixing every element of $A \cup B$ and extending the above choice map. Since $\sigma_{\mathbb{E}}(W) \in \mathsf{C}(W)$, there exist $z_{\mathbb{I},W} \in R_{\mathbb{I},W}$, $z_{\delta,W} \in R_{\delta,W}$, and $z_{\mathbb{H},W} \in R_{\mathbb{H},W}$ fulfilling

$$\sigma_{\mathbb{E}}(W) = \pi_{\mathbb{E}}(\widetilde{\sigma}_{\mathbb{E}}(W)) = \pi_{\mathbb{E}}(z_{\mathbb{I},W}) = \pi_{\mathbb{E}}(z_{\delta,W}) = \pi_{\mathbb{E}}(z_{\mathbb{H},W}).$$

All these $z_{\mathbb{I},W}$, $z_{\delta,W}$, $z_{\mathbb{H},W}$ have a non-empty image under γ_w (namely $\gamma_w(W)$) and are equivalent with $\widetilde{\sigma}_{\mathbb{E}}(W)$ modulo $\equiv_{\mathbb{E}}$. By Lemma 54(2) we have

$$\widetilde{\sigma}_{\mathbb{E}}(W) \equiv_\Phi z_{\mathbb{I},W} \equiv_\Phi z_{\delta,W} \equiv_\Phi z_{\mathbb{H},W}.$$

The equivalence $\equiv_\Phi$ is compatible with the AB-algebra $\mathcal{W}^* * A * B$ (see the end of section 3.9). Hence, for every $W \in \mathcal{W}_t$, we have

$$\widetilde{\sigma}_{\mathbb{E}}(W) \in \widehat{\mathcal{W}_t} * A * B \iff z_{\mathbb{I},W} \in \widehat{\mathcal{W}_t} * A * B \iff W \in \widehat{\mathcal{W}_t}$$

$$\delta_w(\widetilde{\sigma}_{\mathbb{E}}(W)) = \delta_w(z_{\delta,W}) = \delta_w(W) \tag{352}$$

$$\widetilde{\sigma}_{\mathbb{E}}(W) \equiv_\Phi z_{\mathbb{H},W} = \widetilde{\sigma}_{\mathbb{H}}(W) \text{ if } W \in \mathcal{W}_{\mathbb{H}}. \tag{353}$$

By (352), the map $\widetilde{\sigma}_{\mathbb{E}}$ induces a monoid-homomorphism $\sigma_{\mathbb{W}} : \mathbb{W}_t \to \mathbb{W}_t/\Phi$ fulfilling

$$\pi_{\equiv} \circ \sigma_{\mathbb{W}} = \widetilde{\sigma}_{\mathbb{E}} \circ \pi_{\equiv_\Phi}. \tag{354}$$

Since $\sigma_{\mathbb{E}}$ solves every equation $(W\mathbb{I}_w(W), \varepsilon) \in \mathcal{S}_{\mathbb{E}}$ for $W \in \widehat{\mathcal{W}_t} \setminus \mathcal{W}_{\mathbb{H}}$, we are sure that

$$\forall W \in \widehat{\mathcal{W}_t} \setminus \mathcal{W}_{\mathbb{H}} : \pi_{\mathbb{E}}(\widetilde{\sigma}_{\mathbb{E}}(\mathbb{I}_w(W))) = \sigma_{\mathbb{E}}(\mathbb{I}_w(W)) = \sigma_{\mathbb{E}}(W)^{-1} = \pi_{\mathbb{E}}(\mathbb{I}_w(\widetilde{\sigma}_{\mathbb{E}}(W))).$$

Hence, by Lemma 54(2), we have

$$\forall W \in \widehat{\mathcal{W}_t} \setminus \mathcal{W}_{\mathbb{H}} : \widetilde{\sigma}_{\mathbb{E}}(\mathbb{I}_w(W)) \equiv_{\Phi} \mathbb{I}_w(\widetilde{\sigma}_{\mathbb{E}}(W)). \tag{355}$$

Since $\pi_{\equiv_\Phi}$ is an AB-homomorphism, we get

$$\forall W \in \widehat{\mathcal{W}_t} \setminus \mathcal{W}_{\mathbb{H}} : \sigma_{\mathbb{W}}(\mathbb{I}_w(W)) \overset{(354)}{=} \pi_{\equiv_\Phi}(\widetilde{\sigma}_{\mathbb{E}}(\mathbb{I}_w(W))) \overset{(355)}{=} \pi_{\equiv_\Phi}(\mathbb{I}_w(\widetilde{\sigma}_{\mathbb{E}}(W))) = \mathbb{I}_w(\pi_{\equiv_\Phi}(\widetilde{\sigma}_{\mathbb{E}}(W))) \overset{(354)}{=} \mathbb{I}_w(\sigma_{\mathbb{W}}(W)). \tag{356}$$

By (353) and (354),

$$\sigma_{\mathbb{W}} \text{ extends } \sigma_{\mathbb{H}}. \tag{357}$$

This in particular ensures that

$$\forall W \in \widehat{\mathcal{W}_t} \cap \mathcal{W}_{\mathbb{H}} : \sigma_{\mathbb{W}}(\mathbb{I}_w(W)) = \mathbb{I}_w(\sigma_{\mathbb{W}}(W)). \tag{358}$$

By the properties (351), (352), (356), and (358), $\sigma_{\mathbb{W}}$ preserves γ, μ, δ and the involutions $\mathbb{I}_w$, i.e., $\sigma_{\mathbb{W}} \in \mathrm{Hom}_{AB}(\mathbb{W}_t, \mathbb{W}_t/\Phi)$.

By hypothesis, $\widetilde{\sigma}_{\mathbb{E}} \circ \pi_{\mathbb{E}}$ is a solution of the equations of $\mathcal{S}_{\mathbb{E}}$ that are written over $\mathcal{W}_t^* * A * B$. Hence, for all $1 \leq i \leq n$ we have

$$\pi_{\mathbb{E}}(\widetilde{\sigma}_{\mathbb{E}}(z_i)) = \pi_{\mathbb{E}}(\widetilde{\sigma}_{\mathbb{E}}(z_i')),$$

i.e. $\widetilde{\sigma}_{\mathbb{E}}(z_i) \equiv_{\mathbb{E}} \widetilde{\sigma}_{\mathbb{E}}(z_i')$. We know that $\gamma_w(z_i) = \gamma_w(z_i') \neq \emptyset$ (this is required for a system of $\mathbb{W}$-equations) and that $\widetilde{\sigma}_{\mathbb{E}}$ preserves γ_w (see (351)). Using Lemma 54(2), we conclude that $\widetilde{\sigma}_{\mathbb{E}}(z_i) \equiv_{\Phi} \widetilde{\sigma}_{\mathbb{E}}(z_i')$, i.e.,

$$\sigma_{\mathbb{W}}(w_i) = \sigma_{\mathbb{W}}(w_i').$$

Thus, $\sigma_{\mathbb{W}}$ is a solution of $(\mathcal{S}_{\mathbb{W}}, \Phi)$, which by (357) extends $\sigma_{\mathbb{H}}$. Using (354), we finally get

$$\Psi(\sigma_{\mathbb{W}}) = \pi_{\equiv} \circ \sigma_{\mathbb{W}} \circ \overline{\pi}_{\mathbb{E}} = \widetilde{\sigma}_{\mathbb{E}} \circ \pi_{\equiv_\Phi} \circ \overline{\pi}_{\mathbb{E}} = \widetilde{\sigma}_{\mathbb{E}} \circ \pi_{\mathbb{E}} = \sigma_{\mathbb{E}}.$$

8.4 Ψ is bijective

The previous considerations established that Ψ is surjective. Let us check that it is injective. Suppose that $\sigma_{\mathbb{W}}, \sigma'_{\mathbb{W}} \in \mathrm{Hom}_{AB}(\mathbb{W}_t, \mathbb{W}_t/\Phi)$ fulfill $\Psi(\sigma_{\mathbb{W}}) = \Psi(\sigma'_{\mathbb{W}})$. This means that:

$$\pi_{\equiv} \circ \sigma_{\mathbb{W}} \circ \overline{\pi}_{\mathbb{E}} = \pi_{\equiv} \circ \sigma'_{\mathbb{W}} \circ \overline{\pi}_{\mathbb{E}}$$

As $\pi_{\equiv}$ is surjective we get

$$\sigma_{\mathbb{W}} \circ \overline{\pi}_{\mathbb{E}} = \sigma'_{\mathbb{W}} \circ \overline{\pi}_{\mathbb{E}}.$$

By Lemma 54, point 2, $\overline{\pi}_{\mathbb{E}}$ is injective over $\{z \in \mathbb{W}_t \mid \gamma_w(z) \neq \emptyset\}$. Hence, $\sigma_{\mathbb{W}}(g) = \sigma'_{\mathbb{W}}(g)$ for every $g \in \mathcal{W}_t \cup A \cup B$. This implies $\sigma_{\mathbb{W}} = \sigma'_{\mathbb{W}}$. By the above three paragraphs, Lemma 63 is proved. □

9 Transfer of solvability

We prove a general transfer theorem for systems of equations with rational constraints. We first treat the case of groups since it is technically simpler.

1 compute the subalphabet $\mathcal{W}_t \subseteq \mathcal{W}$ that generates $\mathbb{W}_t$
2 **for all** admissible vectors $(\boldsymbol{W}, \boldsymbol{e})$ over $\mathcal{W}_t \cup A \cup B$, **all** $\Phi \in \mathsf{HInv}$, and
all $\sigma_{\mathbb{H}} \in \mathrm{Hom}_{AB}(\mathbb{W}_{\mathbb{H}}, \mathbb{W}_{\mathbb{H}}/\Phi)$ **do**
3 construct the systems $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ and $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ defined on page 53
4 from $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$, Φ, and $\sigma_{\mathbb{H}}$ construct the system $(\mathcal{S}_{\mathbb{E}}, \mathsf{C})$ according to Section 8.1
5 check, whether $(\mathcal{S}_{\mathbb{E}}, \mathsf{C})$ is solvable over $\mathbb{E}$
6 check, whether there is $\psi_{H,t} \in \mathrm{Hom}_{AB}(\mathbb{W}_{\mathbb{H}}/\Phi, \mathbb{H}_t)$ such that $\sigma_{\mathbb{H}} \circ \psi_{H,t}$ solves $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$
7 **endfor**
8 **if** solutions in 6 and 7 are found **then** $(\mathcal{S}, \mu_{\mathcal{A},\mathbb{G}}, \mu_{\mathcal{U}})$ is satisfiable
else $(\mathcal{S}, \mu_{\mathcal{A},\mathbb{G}}, \mu_{\mathcal{U}})$ is unsatisfiable

Fig. 19. The algorithm for checking satisfiability of a system of equations with rational constraints in a group $\mathbb{G}$.

9.1 Transfer for groups

Proposition 7. *Let $\mathbb{H}$ be a group and $\mathbb{G}$ an HNN-extension of $\mathbb{H}$ with finite associated subgroups A and 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*

- *Q_1 is the satisfiability problem for systems of equations with rational constraints in a group $\mathbb{E}$ defined by a presentation in $\mathsf{PHNN}(A)$ (see Definition 9), and*
- *Q_2 is the satisfiability 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 5, solvability of $\mathcal{S}_0$ reduces to solvability of a disjunction $\mathcal{DS} = \bigvee_{j \in J} \mathcal{S}_j$ in closed quadratic normal form, where $\mathcal{S}_j = (\mathcal{S}, \mu_{\mathcal{A},\mathbb{G}}, \mu_{\mathcal{U},j})$ (i.e. the different systems are differing by their maps $\mu_{\mathcal{U},j}$ only). Here $\mathcal{A}$ is a strict normal partitioned fta over the labelling set $\mathsf{bool}(\mathsf{Rat}(\mathbb{H}))$. We have to check, whether one of the systems $\mathcal{S}_j = (\mathcal{S}, \mu_{\mathcal{A},\mathbb{G}}, \mu_{\mathcal{U},j})$ is satisfiable. Let us fix one such system, and write $\mu_{\mathcal{U}}$ for $\mu_{\mathcal{U},j}$. Satisfiability of the system $(\mathcal{S}, \mu_{\mathcal{A},\mathbb{G}}, \mu_{\mathcal{U}})$ can be checked by the high-level algorithm from Figure 19.

Let us first show that this algorithm is correct. Then, we argue that every line of the algorithm can be made effective. Recall the notion of an admissible vector from page 52. By Lemma 45, $(\mathcal{S}, \mu_{\mathcal{A},\mathbb{G}}, \mu_{\mathcal{U}})$ is satisfiable, if and only if there exists an admissible vector $(\boldsymbol{W}, \boldsymbol{e})$ and an AB-homomorphism $\sigma_t : \mathbb{W}_t \to \mathbb{H}_t$ such that:

- All components of $(\boldsymbol{W}, \boldsymbol{e})$ belong to $\mathcal{W}_t \cup A \cup B$.
- σ_t solves both systems $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ and $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ defined on page 53.

Let us fix an admissible vector $(\boldsymbol{W}, \boldsymbol{e})$. By Lemma 46, $\sigma_t : \mathbb{W}_t \to \mathbb{H}_t$ solves the system $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ if and only if there exist $\Phi \in \mathsf{HInv}$ and AB-homomorphisms $\sigma_{\mathbb{W}} : \mathbb{W}_t \to \mathbb{W}_t/\Phi$ and $\psi_t : \mathbb{W}_t/\Phi \to \mathbb{H}_t$ such that, for every $W \in \mathrm{Alph}(\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e}))$, $\sigma_t(W) = \psi_t(\sigma_{\mathbb{W}}(W))$ and $\sigma_{\mathbb{W}}$ solves $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$. Let us fix $\Phi \in \mathsf{HInv}$. Hence, we have to check whether there exist AB-homomorphisms $\sigma_{\mathbb{W}} : \mathbb{W}_t \to \mathbb{W}_t/\Phi$ and $\psi_t : \mathbb{W}_t/\Phi \to \mathbb{H}_t$ such that $\sigma_{\mathbb{W}}$ solves $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ and $\sigma_{\mathbb{W}} \circ \psi_{H,t}$ solves $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$. Let us fix $\sigma_{\mathbb{H}} \in \mathrm{Hom}_{AB}(\mathbb{W}_{\mathbb{H}}, \mathbb{W}_t/\Phi)$. By Lemma 37 we must have $\sigma_{\mathbb{H}} \in \mathrm{Hom}_{AB}(\mathbb{W}_{\mathbb{H}}, \mathbb{W}_{\mathbb{H}}/\Phi)$ and there are only finitely many such AB-homomorphisms. We have to check, whether

(a) there exists an AB-homomorphisms $\sigma_{\mathbb{W}} : \mathbb{W}_t \to \mathbb{W}_t/\Phi$ that extends $\sigma_{\mathbb{H}}$ and solves $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ and

(b) there exists an AB-homomorphism $\psi_t : \mathbb{W}_t/\Phi \to \mathbb{H}_t$ such that $\sigma_{\mathbb{H}} \circ \psi_{H,t}$ solves $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$.

Since all $\mathcal{W}$-symbols occuring in $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ have an H-type and $\sigma_{\mathbb{H}} \in \mathrm{Hom}_{AB}(\mathbb{W}_{\mathbb{H}}, \mathbb{W}_{\mathbb{H}}/\Phi)$, we can restrict ψ_t to an AB-homomorphism $\psi_{H,t} : \mathbb{W}_{\mathbb{H}}/\Phi \to \mathbb{H}_t$. Moreover, $\psi_{H,t}(W)$ for $W \in \mathcal{W}_{\mathbb{H}}$ must belong to $\mathbb{H}$. By Lemma 63, point (a) is equivalent to the solvability of the system $(\mathcal{S}_{\mathbb{E}}, \mathsf{C})$ constructed in line 4, which is checked in line 5. Point (b) is checked in line 6.

Let now argue that every line of the algorithm can be made effective. First, recall that the set $\mathcal{W}_t$ is defined in (91). Since $\mathbb{H}$ is a group, we have $\mathrm{dom}(\mathbb{I}_t) = \mathbb{H}_t$. Thus, $\mathcal{W}_t \subseteq \widehat{\mathcal{W}}$.

Line 1 of the algorithm: We have to check for every letter $W \in \widehat{\mathcal{W}}$ whether (91) holds. Let $\gamma_w(W) = \{\boldsymbol{\theta}\}$. First, assume that $\boldsymbol{\theta}$ is an H-type. We define the following constraint sets:

$$\begin{aligned}
\mathsf{C}_\gamma(W) &= \{h \in \mathbb{H} \mid \boldsymbol{\theta} \in \gamma_t(h)\} \\
\mathsf{C}_\mu(W) &= \{h \in \mathbb{H} \mid \mu_w(W) = \mu_t(\boldsymbol{\theta}, h)\} \\
\mathsf{C}_\delta(W) &= \{h \in \mathbb{H} \mid \delta_w(W) = \delta_t(\boldsymbol{\theta}, h)\} \\
\mathsf{C}(W) &= \mathsf{C}_\gamma(W) \cap \mathsf{C}_\mu(W) \cap \mathsf{C}_\delta(W)
\end{aligned} \tag{359}$$

Thus, $W \in \mathcal{W}_t$ if and only if $\mathsf{C}(W) \neq \emptyset$. Recall from Section 2.6 the notions of equational and positively definable subsets of a monoid. We observe that C_γ takes values in $\mathsf{bool}(\{\{1\}, A, B, \mathbb{H}\})$ and C_μ takes values in $\mathsf{bool}(\mathsf{Rat}(\mathbb{H}))$. The map C_δ takes values which are intersections of sets of the form

$$\mathrm{C}_\delta(c, d) = \{h \in \mathbb{H} \mid ch = hd \text{ in } \mathbb{H}\} \tag{360}$$

and $\mathbb{H} \setminus \mathrm{C}_\delta(c, d)$ for $c, d \in A \cup B$. It is clear that $\mathrm{C}_\delta(c, d) \in \mathrm{EQ}(\mathbb{H}, \mathsf{bool}(\mathsf{Rat}(\mathbb{H})))$. By Lemma 19, $\mathbb{H} \setminus \mathrm{C}_\delta(c, d)$ belongs to $\mathrm{Def}_{\exists+}(\mathbb{H}, \mathsf{bool}(\mathsf{Rat}(\mathbb{H})))$. Therefore, the sets $\mathsf{C}_\gamma(W)$, $\mathsf{C}_\mu(W)$, and $\mathsf{C}_\delta(W)$ all belong to $\mathrm{Def}_{\exists+}(\mathbb{H}, \mathsf{bool}(\mathsf{Rat}(\mathbb{H})))$. Hence, $\mathsf{C}(W)$ belongs to $\mathrm{Def}_{\exists+}(\mathbb{H}, \mathsf{bool}(\mathsf{Rat}(\mathbb{H})))$ as well. Deciding whether $\mathsf{C}(W) \neq \emptyset$ is thus an instance of the problem Q_2.

Now, assume that $\boldsymbol{\theta}$ is a T-type. Let $\boldsymbol{\theta} = (\theta, 1, \theta')$. Hence, $\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}) = (\mathbb{I}_{\mathcal{R}}(\theta'), 1, \mathbb{I}_{\mathcal{R}}(\theta))$. We set

$$\begin{aligned}
\mathsf{C}_\gamma(W) &= \{s \in \mathrm{Red}(\mathbb{H}, t) \mid \boldsymbol{\theta} \in \gamma_t(s)\}, \\
\mathsf{C}_\mu(W) &= \{s \in \mathrm{Red}(\mathbb{H}, t) \mid \mu_w(W) = \mu_t(\boldsymbol{\theta}, s)\}, \\
\mathsf{C}_\delta(W) &= \{s \in \mathrm{Red}(\mathbb{H}, t) \mid \delta_w(W) = \delta_t(\boldsymbol{\theta}, s)\}, \\
\mathsf{C}(W) &= \mathsf{C}_\gamma(W) \cap \mathsf{C}_\mu(W) \cap \mathsf{C}_\delta(W).
\end{aligned}$$

Claim 16. $\mathsf{C}_\gamma(W)$ is recognized by a fta with labels in $\mathsf{bool}(\mathsf{Rat}(\mathbb{H}))$.

The set $\{s \in \mathrm{Red}(\mathbb{H}, t) \mid \boldsymbol{\theta} \in \gamma_t(s)\}$ is recognized by the variant of the fta $\mathcal{R}_6$, where we choose θ as the initial state and θ' as the terminal state.

Claim 17. $\mathsf{C}_\mu(W)$ is recognized by an fta with labels in the set $\mathsf{bool}(\mathsf{Rat}(\mathbb{H}))$.

Recall the definition of μ_t from (62) and recall that $\mathbb{H}$ is a group. For states $q, r \in \mathsf{Q}$ with $\tau(q) = \theta$ and $\tau(r) = \theta'$, let $\mathcal{A}_{q,r}$ be the fta obtained from $\mathcal{A}$ by taking q as the initial state and r as the terminal state. Then, the set

$$\mathsf{C}_\mu(q, r) = \{s \in \mathrm{Red}(\mathbb{H}, t) \mid (q, r) \in \mu_{\mathcal{A},1}(\boldsymbol{\theta}, s)\}$$

is recognized by the direct product $\mathcal{R}_6 \times \mathcal{A}_{q,r}$ This fta is partitioned (by Lemma 12), $\sim$-saturated, and strict (by Lemma 11).

Similarly, for states $q, r \in \mathsf{Q}$ with $\tau(q) = \mathbb{I}_{\mathcal{R}}(\theta)$ and $\tau(r) = \mathbb{I}_{\mathcal{R}}(\theta')$, let $\mathcal{A}'_{q,r}$ be the fta obtained from $\mathcal{A}$ by replacing every label L by L^{-1} (note that $\mathsf{bool}(\mathsf{Rat}(\mathbb{H}))$ is closed under taking the inverse of a set), taking q as the initial state and r as the terminal state. Then, the set

$$\begin{aligned}\overline{\mathsf{C}}_\mu(q,r) &= \{s \in \mathrm{Red}(\mathbb{H},t) \mid (q,r) \in \mu_{\mathcal{A},1}(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}), \mathbb{I}_t(s))^{-1}\} \\ &= \{s \in \mathrm{Red}(\mathbb{H},t) \mid (r,q) \in \mu_{\mathcal{A},1}(\mathbb{I}_{\mathcal{T}}(\boldsymbol{\theta}), \mathbb{I}_t(s))\}\end{aligned}$$

is recognized by $\mathcal{R}_6 \times \mathcal{A}'_{q,r}$. Moreover, this fta is partitioned, $\sim$-saturated, and strict.

Now assume that $\mu_w(W) = \langle \mu_1, \mu_2 \rangle$. Hence, by (69) we have $\mu_1 \subseteq \tau^{-1}(\theta) \times \tau^{-1}(\theta')$ and $\mu_2 \subseteq \tau^{-1}(\mathbb{I}_{\mathcal{R}}(\theta)) \times \tau^{-1}(\mathbb{I}_{\mathcal{R}}(\theta'))$. The subset $\mathsf{C}_\mu(W)$ can be described as the intersection of the following sets:

- $\mathsf{C}_\mu(q,r)$ for $(q,r) \in \mu_1$
- $\mathrm{Red}(\mathbb{H},t) \setminus \mathsf{C}_\mu(q,r)$ for $(q,r) \notin \mu_1$
- $\overline{\mathsf{C}}_\mu(q,r)$ for $(q,r) \in \mu_2$
- $\mathrm{Red}(\mathbb{H},t) \setminus \overline{\mathsf{C}}_\mu(q,r)$ for $(q,r) \notin \mu_2$

By [LS08, Prop. 28], all sets $\mathsf{C}_\mu(q,r)$ and $\overline{\mathsf{C}}_\mu(q,r)$ are recognized by partitioned, $\sim$-saturated, deterministic and complete fta with labelling sets from $\mathsf{bool}(\mathsf{Rat}(\mathbb{H}))$. By [LS08, Lemma 20], all sets $\mathrm{Red}(\mathbb{H},t) \setminus \mathsf{C}_\mu(q,r)$ and $\mathrm{Red}(\mathbb{H},t) \setminus \overline{\mathsf{C}}_\mu(q,r)$ are also recognized by partitioned, $\sim$-saturated, deterministic and complete fta with labelling sets from $\mathsf{bool}(\mathsf{Rat}(\mathbb{H}))$. By Lemma 11, we conclude that $\mathsf{C}_\mu(W)$ is recognized by an fta with labels from $\mathsf{bool}(\mathsf{Rat}(\mathbb{H}))$.

Claim 18. $\mathsf{C}_\delta(W)$ is recognized by an fta with labels from the set $\mathrm{Def}_{\exists+}(\mathbb{H}, \mathsf{bool}(\mathsf{Rat}(\mathbb{H})))$.

The subset $\mathsf{C}_\delta(W)$ is a boolean combination of subsets of the form

$$\mathsf{C}_\delta(c,d) = \{s \in \mathrm{Red}(\mathbb{H},t) \mid cs \sim sd\}, \tag{361}$$

where $c, d \in A \cup B$. For $c, d \in A \cup B$ let $\mathcal{A}_{c,d}$ be the fta with state set $A \cup B$, c as the initial state, d as the terminal state, and the following transitions:

- There is a t-labelled transition from $a \in A$ to $\varphi(a) \in B$.
- There is a t^{-1}-labelled transition from $b \in B$ to $\varphi^{-1}(b)$.
- There is a transition from $c \in A \cup B$ to $d \in A \cup B$ that is labelled with the set $\{h \in \mathbb{H} \mid ch = hd\} \in \mathrm{EQ}(\mathbb{H}, \mathsf{bool}(\mathsf{Rat}(\mathbb{H})))$.

This fta has labels in $\mathrm{EQ}(\mathbb{H}, \mathsf{bool}(\mathsf{Rat}(\mathbb{H})))$ and is $\sim$-saturated. Then, the set $\mathsf{C}_\delta(c,d)$ is recognized by the partitioned fta $\mathcal{R}_6 \times \mathcal{A}_{c,d}$. Moreover, this fta is strict and $\sim$-saturated. The claim follows by the same arguments as for Claim 17.

Due to the Claims 16, 17, 18 and Lemma 11, the set $\mathsf{C}(W)$ is recognized by some fta $\mathcal{D}$ with labels in $\mathrm{Def}_{\exists+}(\mathbb{H}, \mathsf{bool}(\mathsf{Rat}(\mathbb{H})))$. The emptiness problem for $\mathsf{C}(W) = \mathrm{L}(\mathcal{D})$ reduces to the emptiness problem for elements of $\mathrm{Def}_{\exists+}(\mathbb{H}, \mathsf{bool}(\mathsf{Rat}(\mathbb{H})))$ (given by a system of equations with rational constraints). This leads to an instance of Q_2.

Line 2 of the algorithm: Enumerating all admissible tuples is easy (see Figure 6). In order to enumerate all $\Phi \in \mathsf{HInv}$, we enumerate all possible partitions of $\mathcal{W}_{\mathbb{H}}$ and check for each of them

conditions (96)–(99). In order to enumerate $\mathrm{Hom}_{AB}(\mathbb{W}_{\mathbb{H}}, \mathbb{W}_{\mathbb{H}}/\Phi)$, it suffices by Lemma 37 to enumerate all maps $\sigma_{\mathbb{H}} : \mathcal{W}_{\mathbb{H}} \to (A \cup B)\,\mathcal{W}_{\mathbb{H}}\,(A \cup B)$ that preserve γ_w, μ_w, and δ_w.

Line 3 and 4 of the algorithm: These steps are clearly effective.

Line 5 of the algorithm: This is an instance of the problem Q_1.

Line 6 of the algorithm: The involution Φ (choosen in line 2) is given by the formulas (94) and (95) of Section 3.9. By Lemma 23, line 6 amounts to find some tuple $(\psi_{H,t}(W))_{W \in \mathcal{W}_{\mathbb{H}}}$ over $\mathbb{H}$ such that conditions (b)–(f) of Lemma 23 are fulfilled and $(\psi_{H,t}(W))_{W \in \mathcal{W}_{\mathbb{H}}}$ is a solution of

$$\sigma_{\mathbb{H}}(\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})) \cup \{(W_k, a_k^{-1}\overline{W}_k b_k^{-1}) \mid 1 \leq k \leq p\} \cup \{(\overline{W}_k, a_k W_k b_k) \mid 1 \leq k \leq p\}$$

in the group $\mathbb{H}$. Condition (b) is automatically satisfied since all involutions are total (we assume that $\mathbb{H}$ is a group). Also (c) is automatically satisfied by the definition of a solution of a system over the group $\mathbb{H}$. Conditions (d)–(f) can be expressed by the constraints $\mathsf{C}(W)$ defined in (359). Hence, line 6 reduces to an instance of the problem Q_2. □

Theorem 2. *Let $\mathbb{H}$ be a group with decidable satisfiability problem for systems of equations with rational constraints and let $\mathbb{G}$ be 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 $\mathbb{G}$.

Induction base: $|A| = 1$.
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 satisfiability problem for systems of equations with rational constraints (see, for example, [ES69]). By Theorem 1, a free product of two groups with decidable satisfiability problems for systems of equations with rational constraints has a decidable satisfiability problem for systems of equations with rational constraints as well. Hence $\mathbb{G}$ has decidable satisfiability problem for systems of equations with rational constraints.

Induction step: $|A| > 1$.
By Proposition 7, the satisfiability problem for systems of equations with rational constraints reduces to the decision problems Q_1 and Q_2. By hypothesis, problem Q_2 is decidable. Q_1 is the satisfiability problem for systems of equations with rational constraints in the group $\mathbb{E}$, which has a presentation in $\mathsf{PHNN}(A)$. By Section 7.4, $\mathbb{E}$ is obtained from the group $\mathbb{K}$ by a finite number of HNN-extension and amalgamated product operations with associated subgroups (resp., amalgamated subgroups) of cardinality $< |A|$. By Proposition 6, $\mathbb{K}$ has a decidable satisfiability problem for equations with rational constraints. By induction hypothesis, each of the HNN-extensions preserves this decidability property. Moreover, by a combination of this induction hypothesis with Lemmas 8 and 20 and Theorem 1, each of the free products with amalgamation preserves this decidability property as well. Hence $\mathbb{E}$ has a decidable satisfiability problem for equations with rational constraints. Thus problem Q_1 is decidable too. Hence, by Proposition 7, $\mathbb{G}$ has a decidable satisfiability problem for equations with rational constraints. □

Theorem 3. *If $\mathbb{G}$ is a finitely generated virtually-free group, then the satisfiability problem for systems of equations with rational constraints in $\mathbb{G}$ is decidable.*

Proof. Recall that the finitely generated virtually-free groups are exactly the groups obtained from finite groups by a finite number of operations which are either HNN-extensions with finite associated subgroups or free products with amalgamation with finite amalgamated subgroups [DD90]. In a finite group, systems of equations with rational constraints are algorithmically solvable. By Proposition 2, every HNN-extension with finite associated subgroups preserves this decidability property. The combination of Lemmas 8 and 20 with Proposition 2 and Theorem 1 shows that a free product with amalgamation over finite subgroups also preserves this decidability property. Hence every finitely generated virtually-free group has the asserted decidability property. □

Another proof of Theorem 3 was given in [DG07,DG10].

Theorem 4. *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 satisfiability problem for systems of equations with rational constraints in $\mathbb{H}$.*

Proof. By Proposition 7 the satisfiability problem for systems of equations with rational constraints in $\mathbb{G}$ is Turing-reducible to the problems Q_1 and Q_2 defined in the proposition. But Q_1 is the satisfiability problem for systems of equations with rational constraints in $\mathbb{E}$, where, by Lemma 55, $\mathbb{E}$ is a finitely generated virtually-free group. Since, by Theorem 3, problem Q_1 is decidable, 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 satisfiability problem for systems of equations with rational constraints in $\mathbb{H}$. □

9.2 Transfer for cancellative monoids

In this section, we will prove the extension of Proposition 7 to cancellative monoids:

Proposition 8. *Let $\mathbb{H}$ be a cancellative monoid and $\mathbb{G}$ an HNN-extension of $\mathbb{H}$ with finite associated subgroups A and 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*

- *Q_1 is the satisfiability problem for systems of equations with rational constraints in a group $\mathbb{E}$ defined by a presentation in $\mathsf{PHNN}(A)$, and*
- *Q_2 is the satisfiability problem for systems of equations with rational constraints in $\mathbb{H}$.*

A new difficulty arises here for 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 $\gamma_w(W)$ is a H-type), s is not invertible (if $W \notin \widehat{\mathcal{W}}$), 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 a universally quantified formula $(\forall x : hx \neq 1 \vee xh \neq 1)$, 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 $\mathcal{W}_t$. The same kind of difficulty arises in the computation of an AB-homomorphism $\psi_t : \mathbb{W}' \to \mathbb{H}_t$ (whatever variant $\mathbb{W}'$ of the AB-algebra $\mathbb{W}_t$ we use). 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 19 is no more ensured when $\mathbb{H}$ is not assumed to be a group.

We overcome the above difficulties by introducing the notion of a *weak* AB-homomorphism. For two AB-algebras $\mathcal{M}_i = \langle \mathbb{M}_i, \iota_{A,i}, \iota_{B,i}, \mathbb{I}_i, \gamma_i, \mu_i, \delta_i \rangle$ $(i \in \{1, 2\})$ a weak-AB-homomorphism from $\mathcal{M}_1$ to $\mathcal{M}_2$ is a map $\psi : \mathbb{M}_1 \to \mathbb{M}_2$ fulfilling the following properties:

(Hom1) $\psi : \mathbb{M}_1 \to \mathbb{M}_2$ is a monoid homomorphism.

(Hom2) $\forall a \in A : \psi(\iota_{A,1}(a)) = \iota_{A,2}(a)$ and $\forall b \in B : \psi(\iota_{B,1}(b)) = \iota_{B,2}(b)$

(wHom3) $\forall m \in \mathbb{M}_1 : m \in \mathrm{dom}(\mathbb{I}_1) \Rightarrow \psi(m) \in \mathrm{dom}(\mathbb{I}_2)$

(Hom4) $\forall m \in \mathrm{dom}(\mathbb{I}_1) : \mathbb{I}_2(\psi(m)) = \psi(\mathbb{I}_1(m))$

(Hom5) $\forall m \in \mathbb{M}_1 : \gamma_1(m) \subseteq \gamma_2(\psi(m))$

(wHom6) $\forall m \in \mathbb{M}_1 : \forall \boldsymbol{\theta} \in \gamma_1(m) : \mu_1(\boldsymbol{\theta}, m) \subseteq \mu_2(\boldsymbol{\theta}, \psi(m))$

(wHom7) $\forall m \in \mathbb{M}_1 : \forall \boldsymbol{\theta} \in \gamma_1(m) : \delta_1(\boldsymbol{\theta}, m) \subseteq \delta_2(\boldsymbol{\theta}, \psi(m))$

In axiom (wHom6), the ordering $\subseteq$ refers to the product ordering over $\mathsf{B}^2(\mathsf{Q})$, which is defined by $(r_1, r_2) \subseteq (r_1', r_2')$ if and only if $r_1 \subseteq r_1'$ and $r_2 \subseteq r_2'$.

We have thus replaced the axioms (Hom3), (Hom6), and (Hom7) by the weaker axioms (wHom3), (wHom6), and (wHom7), respectively. It remains true that the above list of axioms can be checked on the generators only, i.e., the following analogue of Lemma 23 is true.

Lemma 64. *Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be two AB-algebra as above and assume that $\mathcal{M}_1$ satisfies the following:*

(A) The monoid $\mathbb{M}_1$ is generated by the set Γ and $A \cup B \subseteq \Gamma$
(B) $\gamma_1(g) \neq \emptyset$ for all $g \in \Gamma$
(C) For every $m \in \mathbb{M}_1$ there exists a decomposition $m = g_1 \cdots g_n$ with $g_1, \ldots, g_n \in \Gamma$ such that: $\gamma_1(m) = \gamma_1(g_1) \cdots \gamma_1(g_n)$ [8]

Let $\psi : \mathbb{M}_1 \to \mathbb{M}_2$ be a monoid homomorphism. This map ψ is a weak AB-homomorphism if and only if for all $g \in \Gamma$ and $\boldsymbol{\theta} \in \gamma_1(g)$ we have:

(a) $\forall a \in A : \psi(\iota_{A,1}(a)) = \iota_{A,2}(a)$ and $\forall b \in B : \psi(\iota_{B,1}(b)) = \iota_{B,2}(b)$
(b) $g \in \mathrm{dom}(\mathbb{I}_1) \Rightarrow \psi(g) \in \mathrm{dom}(\mathbb{I}_2)$
(c) If $g \in \mathrm{dom}(\mathbb{I}_1)$ then $\mathbb{I}_2(\psi(g)) = \psi(\mathbb{I}_1(g))$
(d) $\gamma_1(g) \subseteq \gamma_2(\psi(g))$
(e) $\mu_1(\boldsymbol{\theta}, g) \subseteq \mu_2(\boldsymbol{\theta}, \psi(g))$
(f) $\delta_1(\boldsymbol{\theta}, g) \subseteq \delta_2(\boldsymbol{\theta}, \psi(g))$.

Given two AB-algebras $\mathcal{M}_1, \mathcal{M}_2$, we denote by $\mathrm{wHom}_{AB}(\mathcal{M}_1, \mathcal{M}_2)$ the set of all weak AB-homomorphisms from $\mathcal{M}_1$ to $\mathcal{M}_2$.

Let us notice that the subalphabet $\mathcal{W}_t$ was equal to $\{W \in \mathcal{W} \mid \mathrm{Hom}_{AB}(\langle W \rangle, \mathbb{H}_t) \neq \emptyset\}$, where $\langle W \rangle$ is the smallest sub-AB-algebra containing $\{W\}$. We are thus naturally led to define

$$\mathcal{W}_t' = \{W \in \mathcal{W} \mid \mathrm{wHom}_{AB}(\langle W \rangle, \mathbb{H}_t) \neq \emptyset\}.$$

We then define

$$\mathbb{W}_t' = (\mathcal{W}_t'^* * A * B)/_{\equiv}.$$

Moreover, we define $\mathcal{W}_{\mathbb{H}}' = \{W \in \mathcal{W}_t' \mid \gamma_w(W) \text{ is an H-type}\}$ and $\mathbb{W}_{\mathbb{H}}' = (\mathcal{W}_{\mathbb{H}}'^* * A * B)/_{\equiv}$. We can then express the solutions of the original equation over $\mathbb{G}$ via some AB-homomorphisms, resp., weak AB-homomorphisms:

[8] If $n = 0$, i.e., $m = 1$, then $\gamma_1(g_1) \cdots \gamma_1(g_n)$ is the neutral element $\{(\theta, 0, \theta) \mid \theta \in \mathcal{T}_6\}$ of the monoid $2^{\mathcal{T}}$.

Lemma 65. *Let $\mathcal{DS} = \bigvee_{j\in J} \mathcal{S}_j$ be a finite disjunction of systems of equations over $\mathbb{G}$, with rational constraints, where $\mathcal{S}_j = (\mathcal{S}, \mu_{\mathcal{A},\mathbb{G}}, \mu_j)$. Let us suppose that $\mathcal{DS}$ is in closed quadratic normal form (defined at the end of Section 4). A monoid homomorphism*

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

is a solution of $\mathcal{DS}$ if and only if there exist an index $j \in J$, an admissible vector $(\boldsymbol{W}, \boldsymbol{e})$ with all components from $\mathcal{W}'_t \cup A \cup B$, an involution $\Phi \in \mathsf{HInv}$, an AB-homomorphism $\sigma_{\mathbb{W}} : \mathbb{W}'_t \to \mathbb{W}'_t/\Phi$ and a weak AB-homomorphism $\psi_t : \mathbb{W}'_t/\Phi \to \mathbb{H}_t$ such that:

(S1) *$\sigma_{\mathbb{W}}$ is a solution of $\mathcal{S}_t(\mathcal{S}_j, \boldsymbol{W}, \boldsymbol{e})$*
(S2) *$\sigma_{\mathbb{W}} \circ \psi_t$ is a solution of $\mathcal{S}_{\mathbb{H}}(\mathcal{S}_j, \boldsymbol{W}, \boldsymbol{e})$*
(S3) *$\sigma = \sigma_{\boldsymbol{W},\boldsymbol{e}} \circ \sigma_{\mathbb{W}} \circ \psi_t \circ \pi_{\mathbb{G}}$*

Remark 5. Discarding the adjective "weak" in the above statement and replacing $\mathbb{W}'_t$ by $\mathbb{W}_t$ results in a straightforward synthesis of Lemma 45 with Lemma 46. The introduction of "weak" and $\mathbb{W}'_t$ makes the statement usable for an *effective* characterisation of satisfiable systems of equations. These maps were summarized in Figure 11 and form the left-lower part of Figure 21.

Proof. First suppose that a monoid homomorphism

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

is a solution of $\mathcal{DS}$. By Lemma 45, there exists an admissible vector $(\boldsymbol{W}, \boldsymbol{e})$ over $\mathcal{W}_t \cup A \cup B$ and an AB-homomorphism $\tilde{\sigma}_t : \mathbb{W}_t \to \mathbb{H}_t$ such that

$$\tilde{\sigma}_t \text{ solves } \mathcal{S}_t(\mathcal{S}_j, \boldsymbol{W}, \boldsymbol{e}) \text{ and } \mathcal{S}_{\mathbb{H}}(\mathcal{S}_j, \boldsymbol{W}, \boldsymbol{e}), \text{and} \tag{362}$$

$$\sigma = \sigma_{\boldsymbol{W},\boldsymbol{e}} \circ \tilde{\sigma}_t \circ \pi_{\mathbb{G}}. \tag{363}$$

By Lemma 46, $\tilde{\sigma}_t$ can be decomposed over the image of $\sigma_{\boldsymbol{W},\boldsymbol{e}}$ as

$$\tilde{\sigma}_t = \tilde{\sigma}_{\mathbb{W}} \circ \tilde{\psi}_t \tag{364}$$

where $\tilde{\sigma}_{\mathbb{W}} \in \mathrm{Hom}_{AB}(\mathbb{W}_t, \mathbb{W}_t/\Phi)$, $\tilde{\psi}_t \in \mathrm{Hom}_{AB}(\mathbb{W}_t/\Phi, \mathbb{H}_t)$, and $\Phi \in \mathsf{HInv}$ such that

$$\tilde{\sigma}_{\mathbb{W}} \text{ solves } \mathcal{S}_t(\mathcal{S}_j, \boldsymbol{W}, \boldsymbol{e}). \tag{365}$$

The automorphism Φ can be chosen in such a way that

$$\forall W \in \mathcal{W}'_t \setminus \mathcal{W}_t : \Phi(W) = W. \tag{366}$$

For this, it suffices, if necessary, to modify the original Φ over the symbols W_k and $\overline{W}_k$, which do not belong to $\mathcal{W}_t$; this can be done without violating the properties (96)–(99) that define HInv. Let us extend the maps $\tilde{\sigma}_{\mathbb{W}}$ and $\tilde{\psi}_t$ to maps $\sigma_{\mathbb{W}} \in \mathrm{Hom}_{AB}(\mathbb{W}'_t, \mathbb{W}'_t/\Phi)$ and $\psi_t \in \mathrm{wHom}_{AB}(\mathbb{W}'_t/\Phi, \mathbb{H}_t)$, respectively, by setting

$$\forall W \in \mathcal{W}'_t \setminus \mathcal{W}_t : \sigma_{\mathbb{W}}(W) = [W]_{\equiv_\Phi} \text{ and } \psi_t([W]_{\equiv_\Phi}) = h_W(W),$$

where $h_W \in \mathrm{wHom}_{AB}(\langle W \rangle, \mathbb{H}_t)$. Lemma 64 and (366) ensure that such extensions exist. We then define

$$\sigma_t = \sigma_{\mathbb{W}} \circ \psi_t. \tag{367}$$

1 compute the subalphabet $\mathcal{W}'_t \subseteq \mathcal{W}$ that generates $\mathbb{W}'_t$
2 **for all** admissible vectors $(\boldsymbol{W}, \boldsymbol{e})$ over $\mathcal{W}'_t \cup A \cup B$, **all** $\Phi \in \mathsf{HInv}$, and
all $\sigma_{\mathbb{H}} \in \mathrm{Hom}_{AB}(\mathbb{W}'_{\mathbb{H}}, \mathbb{W}'_{\mathbb{H}}/\Phi)$ **do**
3 construct the systems $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ and $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ defined on page 53
4 from $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$, Φ, and $\sigma_{\mathbb{H}}$ construct the system $(\mathcal{S}_{\mathbb{E}}, \mathsf{C})$ according to Section 8.1
5 check, whether $(\mathcal{S}_{\mathbb{E}}, \mathsf{C})$ is solvable over $\mathbb{E}$
6 check, whether there is $\psi_{H,t} \in \mathrm{wHom}_{AB}(\mathbb{W}'_{\mathbb{H}}/\Phi, \mathbb{H}_t)$ such that $\sigma_{\mathbb{H}} \circ \psi_{H,t}$ solves $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$
7 **endfor**
8 **if** solutions in 6 and 7 are found **then** $(\mathcal{S}, \mu_{\mathcal{A},\mathbb{G}}, \mu_{\mathcal{U}})$ is satisfiable
else $(\mathcal{S}, \mu_{\mathcal{A},\mathbb{G}}, \mu_{\mathcal{U}})$ is unsatisfiable

Fig. 20. The algorithm for checking satisfiability of a system of equations with rational constraints in a monoid $\mathbb{G}$.

By (365), the restriction of $\sigma_{\mathbb{W}}$ to $\mathbb{W}_t$ solves the system $\mathcal{S}_t(\mathcal{S}_j, \boldsymbol{W}, \boldsymbol{e})$. Since all symbols in $\mathcal{S}_t(\mathcal{S}_j, \boldsymbol{W}, \boldsymbol{e})$ are from $\mathcal{W}_t \cup A \cup B$, also $\sigma_{\mathbb{W}}$ solves this system. Hence (S1) is true.

By the same argument, (362) and (364) imply that (S2) is true. Finally, by (363) and (364) we have $\sigma = \sigma_{\boldsymbol{W},\boldsymbol{e}} \circ \tilde{\sigma}_{\mathbb{W}} \circ \tilde{\psi}_t \circ \pi_{\mathbb{G}}$. But the image of $\sigma_{\boldsymbol{W},\boldsymbol{e}}$ is included in $\mathbb{W}_t$, and the image of $\tilde{\sigma}_{\mathbb{W}}$ is included in $\mathbb{W}_t/\Phi$. Thus, the above identity is still true after replacing the maps $\tilde{\sigma}_{\mathbb{W}}$ and $\tilde{\psi}_t$ by $\sigma_{\mathbb{W}}$ and ψ_t, respectively, i.e., (S3) is true.

Conversely, suppose that $(\boldsymbol{W}, \boldsymbol{e})$ (with all components from $\mathcal{W}'_t \cup A \cup B$), $\Phi \in \mathsf{HInv}$, $\sigma_{\mathbb{W}} \in \mathrm{Hom}_{AB}(\mathbb{W}'_t, \mathbb{W}'_t/\Phi)$, and $\psi_t \in \mathrm{wHom}_{AB}(\mathbb{W}'_t/\Phi, \mathbb{H}_t)$ are fulfilling (S1), (S2), and (S3). Let us define $\sigma_t = \sigma_{\mathbb{W}} \circ \psi_t$ and $\sigma = \sigma_{\boldsymbol{W},\boldsymbol{e}} \circ \sigma_t \circ \pi_{\mathbb{G}}$. By (S1) and (S2), the map σ_t is a weak-AB-homomorphism solving $\mathcal{S}_t(\mathcal{S}_j, \boldsymbol{W}, \boldsymbol{e}) \wedge \mathcal{S}_{\mathbb{H}}(\mathcal{S}_j, \boldsymbol{W}, \boldsymbol{e})$. The arguments given in Section 5.2 (page 59), adapted to a *weak* AB-homomorphism ψ_t from the AB-algebra $\mathbb{W}'_t/\Phi$ into $\mathbb{H}_t$ show that σ is an *over*-solution of $\mathcal{DS}$ (see Section 4). Since $\mathcal{DS}$ is assumed to be in closed quadratic normal form, σ is a solution of $\mathcal{DS}$. □

Proof of Proposition 8. By Proposition 5, every system $\mathcal{S}_0$ of equations with rational constraints over $\mathbb{G}$ can be reduced to a disjunction $\mathcal{DS} = \bigvee_{j \in J} \mathcal{S}_j$ in closed quadratic normal form where $\mathcal{S}_j = (\mathcal{S}, \mu_{\mathcal{A}}, \mu_{\mathcal{U},j})$. Note that the different systems $\mathcal{S}_j$ only differ by their maps $\mu_{\mathcal{U},j}$. Fix a $j \in J$ and let $\mu_{\mathcal{U}} = \mu_{\mathcal{U},j}$. Solvability of the system $(\mathcal{S}, \mu_{\mathcal{A}}, \mu_{\mathcal{U}})$ is checked by the algorithm from Figure 20, which is a variant of the algorithm from Figure 19.

We summarize in Figure 21 the different maps to be found, where *dashed* arrows correspond to *weak* AB-homomorphisms. Correctness of the algorithm can be shown, using Lemma 65, in the same way as correctness of the algorithm for the group case (Figure 19). Let us now argue that every line of the algorithm can be made effective.

In line 1, we have to check for every letter $W \in \mathcal{W}$, whether there exists a weak AB-homomorphism from the induced AB-subalgebra $\langle W \rangle$ to $\mathbb{H}_t$. By Lemma 64, this amounts to test that conditions (a)–(f) of this lemma are fulfilled. Let us define constraints on the variable W that express these conditions. Assume that $\gamma_w(W) = \{\boldsymbol{\theta}\}$. If $\boldsymbol{\theta}$ is an H-type, then

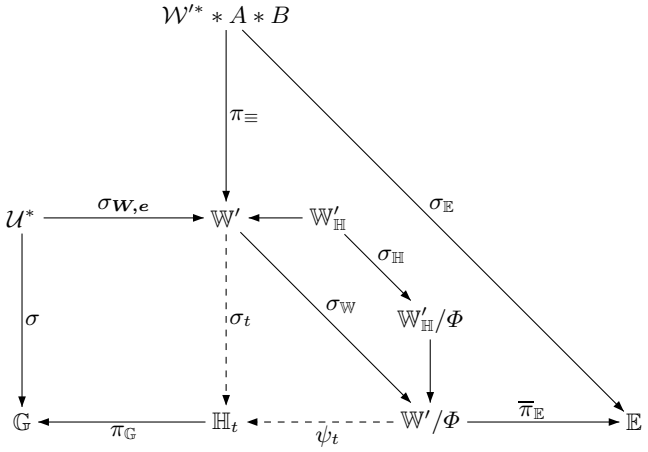


Fig. 21. The algorithm: monoid case

we set:

$$\mathsf{C}_I(W) = \begin{cases} \mathbb{H} & \text{if } W \in \mathcal{W}' \setminus \widehat{\mathcal{W}}, \\ \mathsf{I}(\mathbb{H}) & \text{if } W \in \widehat{\mathcal{W}}, \end{cases} \tag{368}$$

$$\mathsf{C}_\gamma(W) = \{h \in \mathbb{H} \mid \boldsymbol{\theta} \in \gamma_t(h)\}, \tag{369}$$

$$\mathsf{C}_\mu(W) = \{h \in \mathbb{H} \mid \mu_w(W) \subseteq \mu_t(\boldsymbol{\theta}, h)\}, \tag{370}$$

$$\mathsf{C}_\delta(W) = \{h \in \mathbb{H} \mid \delta_w(W) \subseteq \delta_t(\boldsymbol{\theta}, h)\}. \tag{371}$$

$$\mathsf{C}(W) = \mathsf{C}_I(W) \cap \mathsf{C}_\gamma(W) \cap \mathsf{C}_\mu(W) \cap \mathsf{C}_\delta(W). \tag{372}$$

If $\boldsymbol{\theta}$ is a T-type, then we set:

$$\mathsf{C}_I(W) = \begin{cases} \mathbb{H} * \{t, t^{-1}\}^* & \text{if } W \in \mathcal{W}' \setminus \widehat{\mathcal{W}}, \\ \mathrm{dom}(\mathbb{I}_t) & \text{if } W \in \widehat{\mathcal{W}}, \end{cases} \tag{373}$$

$$\mathsf{C}_\gamma(W) = \{s \in \mathbb{H} * \{t, t^{-1}\}^* \mid \boldsymbol{\theta} \in \gamma_t(s)\}, \tag{374}$$

$$\mathsf{C}_\mu(W) = \{s \in \mathbb{H} * \{t, t^{-1}\}^* \mid \mu_w(W) \subseteq \mu_t(\boldsymbol{\theta}, s)\}, \tag{375}$$

$$\mathsf{C}_\delta(W) = \{s \in \mathbb{H} * \{t, t^{-1}\}^* \mid \delta_w(W) \subseteq \delta_t(\boldsymbol{\theta}, s)\}, \tag{376}$$

$$\mathsf{C}(W) = \mathsf{C}_I(W) \cap \mathsf{C}_\gamma(W) \cap \mathsf{C}_\mu(W) \cap \mathsf{C}_\delta(W). \tag{377}$$

The values of the $\mathsf{C}(W)$ are defined in such a way that now, every set $\mathsf{C}(W)$ with $\gamma_w(W)$ an H-type belongs to $\mathrm{EQ}(\mathbb{H}, \mathsf{bool}(\mathsf{Rat}(\mathbb{H})))$, while every set $\mathsf{C}(W)$ with $\gamma_w(W)$ a T-type is recognized by some fta with labels in $\mathrm{EQ}(\mathbb{H}, \mathsf{bool}(\mathsf{Rat}(\mathbb{H})))$. Line 1 thus reduces to instances of Q_2. Moreover, line 5 is an instance of Q_1. Let us finally show that line 6 can be achieved by a Turing-reduction to Q_2. By Lemma 64 again, line 4 amounts to find some tuple $(\psi_{H,t}(W))_{W \in \mathcal{W}'_{\mathbb{H}}}$ over $\mathbb{H}$ solving the system of equations

$$\sigma_{\mathbb{W}}(\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})) \cup \{(W_k, a_k^{-1}\overline{W}_k b_k^{-1}) \mid 1 \leq k \leq p\} \cup \{(\overline{W}_k, a_k W_k b_k) \mid 1 \leq k \leq p\},$$

together with the constraint C defined for line 1. Line 4 is thus an instance of Q_2. We have thus proved Proposition 8. □

Theorem 5. *Let $\mathbb{H}$ be a cancellative monoid and $\mathbb{G}$ an HNN-extension of $\mathbb{H}$ with finite associated subgroups A and B. The satisfiability problem for systems of equations with rational*

constraints in $\mathbb{G}$ is Turing-reducible to the satisfiability 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 A and B. By Proposition 8 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 Q_1 is the satisfiability problem for systems of equations with rational constraints in a group $\mathbb{E}$ having a presentation in $\mathsf{PHNN}(A)$. But, due to the structure of $\mathbb{E}$ (see Section 7.4) and Theorem 4, this problem 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., the satisfiability problem for systems of equations with rational constraints in $\mathbb{H}$. □

The two following sections are stating some variants of the main Theorem 5. 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 analogues of Theorem 5.

10 Equations with positive rational constraints over $\mathbb{G}$

10.1 Positive rational constraints

We consider here constraints for the variables consisting of rational subsets of the monoid (while in Theorem 5 the constraint sets are *boolean combinations* of rational subsets). More formally, a system of equations with *positive* rational constraints in the monoid $\mathbb{M}$ is a system $(\mathcal{S}, \mathsf{C})$ with constraints in $\mathcal{C} = \mathsf{Rat}(\mathbb{M})$.

Theorem 6. *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 satisfiability problem for systems of equations with positive rational constraints in $\mathbb{H}$.*

Proof. It suffices to adapt the reduction given in the proof of Theorem 5:

- The *strict normal* partitioned fta $\mathcal{A}$ with labeling set $\mathsf{bool}(\mathsf{Rat}(\mathbb{H}))$ is merely replaced by a *normal* partitioned fta $\mathcal{A}$ with labeling set $\mathsf{Rat}(\mathbb{H})$. The existence of such an fta recognizing the given positive constraints is ensured by point (1) from Proposition 2.
- The AB-algebra $\mathbb{H}_t$ is replaced by the AB-algebra $\mathbb{H}_{t,+}$(defined in (67)).
- For every $W \in \mathcal{W}'_{\mathbb{H}}$: $\mathsf{C}_\gamma(W) = \{h \in \mathbb{H} \mid \gamma_w(W) \subseteq \gamma_+(h)\}$.
- For $W \in \mathcal{W}'_t \setminus \mathcal{W}'_{\mathbb{H}}$: $\mathsf{C}_\gamma(W) = \{s \in \mathbb{H} * \{t, t^{-1}\}^* \mid \gamma_w(W) \subseteq \gamma_+(s)\}$.
- For $W \in \mathcal{W}'_t \setminus \mathcal{W}'_{\mathbb{H}}$, each of the sets $\mathsf{C}_I(W)$, $\mathsf{C}_\gamma(W)$, $\mathsf{C}_\mu(W)$, and $\mathsf{C}_\delta(W)$ is recognized by an fta with labels in $\mathrm{EQ}(\mathbb{H}, \mathsf{Rat}(\mathbb{H}))$. □

10.2 Positive subgroup constraints

We consider here the case where $\mathbb{G}$ is the HNN-extension of a group $\mathbb{H}$ by an isomorphism $\varphi : A \to A$ 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

$$\mathcal{C}_{\mathbb{H}} = \{C_1, \dots, C_n\} \text{ and } \mathcal{C}_{\mathbb{G}} = \{C_1, \dots, C_n, \langle C_1, t\rangle, \dots, \langle C_n, t\rangle\}.$$

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 7. *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 satisfiability problem for systems of equations over $\mathbb{H}$ with constraints in $\mathcal{C}_{\mathbb{H}}$.*

Proof sketch. It suffices to adapt the reduction given in the proof of Theorem 5:

- The *strict normal* partitioned fta $\mathcal{A}$ with labeling set $\mathsf{bool}(\mathsf{Rat}(\mathbb{H}))$ is replaced by a *normal* partitioned fta $\mathcal{A}$ 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 $\mathbb{H}_{t,+}$ (defined by (67)).

Let us describe more precisely the necessary adaptations. Given a finitely generated subgroup C_i, we consider the fta $\mathcal{A}_i$ that posesses 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 occurence 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 θ, there exists only one state mapped to the type θ by τ) 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 [LS08, Lemma 5]) and unitary (because unitarity is also preserved by direct products). Given a finite set of constraints $\mu : \mathcal{U}^* \to \mathcal{C}_{\mathbb{G}}$, there exist $I_U \subseteq Q_{\mathcal{A}}, T_U \subseteq Q_{\mathcal{A}}$ such that

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

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 (126), fulfiling points (a), (c), (d), and (e) of Proposition 5 and point (b), with the modification that the fta $\mathcal{A}$ is a normal partitioned fta (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 the following:

- Find a solution in $\mathbb{H}$ to the system

$$\sigma_{\mathbb{W}}(\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})) \cup \{(W_k, a_k^{-1}\overline{W}_k b_k^{-1}) \mid 1 \leq k \leq p\} \cup \{(\overline{W}_k, a_k W_k b_k) \mid 1 \leq k \leq p\}$$

  with the additional constraints $\mathsf{C}(W)$ for $W \in \mathcal{W}'_{\mathbb{H}}$; this is an instance of the satisfiability problem for systems of equations with constraints in $\mathcal{C}_{\mathbb{H}}$.
- Find an element in the set $\mathsf{C}(W)$ for $W \in \mathcal{W}'_t - \mathcal{W}'_{\mathbb{H}}$; the set $\mathsf{C}(W)$ is recognized by an fta 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 satisfiability problem for systems of equations with constraints in $\mathcal{C}_{\mathbb{H}}$. □

10.3 Constants

The sets of constraints corresponding to so called equations *with constants* are

$$\mathcal{C}_{\mathbb{H}} = \{\{h\} \mid h \in \mathbb{H}\} \cup \{\mathbb{H}\} \text{ and } \mathcal{C}_{\mathbb{G}} = \{\{g\} \mid g \in \mathbb{G}\} \cup \{\mathbb{G}\}.$$

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 with constants in $\mathbb{G}$ is Turing-reducible to the satisfiability problem for systems of equations with constants in $\mathbb{H}$.*

Proof sketch. It suffices to adapt the reduction given in the proof of Theorem 5:

- The *strict normal* partitioned fta $\mathcal{A}$ with labeling set $\mathsf{bool}(\mathsf{Rat}(\mathbb{H}))$ is replaced by a *normal* partitioned fta $\mathcal{A}$ with labeling set $\mathcal{C}_{\mathbb{H}}$.
- The AB-algebra $\mathbb{H}_t$ is replaced by the AB-algebra $\mathbb{H}_{t,+}$ (defined in (67)). □

11 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 Section 2.6.

11.1 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 (dis)equations (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 5):

$$((E_i)_{1\leq i\leq n}, (\overline{E}_i)_{n+1\leq i\leq 2n}, \mu_{\mathcal{A},\mathbb{G}}, \mu_{\mathcal{U}}) \tag{378}$$

The equations E_i have the form

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

while the disequations $\overline{E}_i$ have the form

$$\overline{E}_i : (U_{i,1}, U_{i,2}) \text{ for all } n+1 \leq i \leq 2n$$

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 $\mathcal{V}_0 = [1, 2n] \times [1, 3] \times [1, 5] \times [0, N_0]$ and the alphabet $\mathcal{W}$ constructed from this $\mathcal{V}_0$ in Section 3.6. We choose the integer N_0 in such a way that

$$\text{Card}(\{W \in \mathcal{W} \mid \exists i, j, k, p_1(W) = (i, j, k, 0)\}) < \frac{1}{2}\text{Card}(\mathcal{V}_0) \tag{379}$$

(one can still take, as in the case of equations, $N_0 := 2\text{Card}(\{-1, 0, 1\} \times \mathcal{T}_{HT} \times \mathsf{B}^2(\mathsf{Q}) \times \text{PGI}\{A, B\}) + 1$ in order to achieve this inequality).

We consider all the vectors $(W_{i,j,k})$ where $1 \leq i \leq 2n, 1 \leq j \leq 3, 1 \leq k \leq 5$ 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

$$(W_{i,j,k})_{1\leq i\leq n, 1\leq j\leq 3, 1\leq k\leq 5}, \quad (e_{i,1,2}, e_{i,2,3}, e_{i,3,1})_{1\leq i\leq n}$$

fulfill conditions (137)-(145) and their counterpart for disequations

$$(W_{i,j,k})_{n+1\leq i\leq 2n,1\leq j\leq 2,1\leq k\leq 5},\quad (e_{i,1,2})_{n+1\leq i\leq 2n}$$

fulfill the analogous conditions:

$$p_1(W_{i,j,k}) = (i,j,k,0) \in \mathcal{V}_0 \text{ for } W_{i,j,k} \neq 1 \tag{380}$$

$$\gamma(\prod_{k=1}^{5} W_{i,j,k}) = (1,H,b,1,1) \text{ for some } b \in \{0,1\} \tag{381}$$

$$\mu(\prod_{k=1}^{5} W_{i,j,k}) = \mu_{\mathcal{U}}(U_{i,j}) \tag{382}$$

$$\gamma(\prod_{k=1}^{2} W_{i,1,k}) = \gamma(\prod_{k=1}^{2} W_{i,2,k}) \tag{383}$$

$$W_{i,j,3} \in \mathcal{W} \ \wedge\ \gamma_w(W_{i,j,3}) \text{ is an H-type} \tag{384}$$

$$e_{i,1,2} \in \mathrm{Gi}(W_{i,1,3}) = \mathrm{Gi}(W_{i,2,3}) \tag{385}$$

A vector $(\boldsymbol{W},\boldsymbol{e})$ fulfilling (137)-(145) for the indices $i \in [1,n]$ and (380)–(385) for the indices $i \in [n+1,2n]$ is called an *admissible* vector. For every admissible vector $(\boldsymbol{W},\boldsymbol{e})$ we define the following equations and disequations:

– For all $1 \leq i \leq 2n$:

$$\prod_{k=1}^{5} W_{i,j,k} = \prod_{k=1}^{5} W_{i',j',k} \text{ if } U_{i,j} = U_{i',j'} \tag{386}$$

$$W_{i,1,1}W_{i,1,2}e_{i,1,2} = W_{i,2,1}W_{i,2,2} \tag{387}$$

– For all $1 \leq i \leq n$:

$$W_{i,2,4}W_{i,2,5} = e_{i,2,3}\mathbb{I}_w(W_{i,3,2})\mathbb{I}_w(W_{i,3,1}) \tag{388}$$

$$e_{i,3,1}W_{i,1,4}W_{i,1,5} = W_{i,3,4}W_{i,3,5} \tag{389}$$

$$W_{i,1,3} = e_{i,1,2}W_{i,2,3}e_{i,2,3}W_{i,3,3}e_{i,3,1} \tag{390}$$

– For all $n+1 \leq i \leq 2n$ such that $\tau\mathrm{e}(W_{i,1,3}) = \tau\mathrm{e}(W_{i,2,3})$ and all $d \in \mathrm{Ge}(W_{i,1,3})$:

$$W_{i,1,3}d \neq e_{i,1,2}W_{i,2,3} \tag{391}$$

We denote by $\mathcal{S}_t(\mathcal{S},\boldsymbol{W},\boldsymbol{e})$ the system of equations (386)–(389), and by $\mathcal{S}_{\mathbb{H}}(\mathcal{S},\boldsymbol{W},\boldsymbol{e})$ the system of equations and disequations (390)–(391). 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 $\sigma_{\boldsymbol{W},\boldsymbol{e}} : \mathcal{U}^* \to \mathbb{W}$ we denote the unique monoid homomorphism such that

$$\sigma_{\boldsymbol{W},\boldsymbol{e}}(U_{i,j}) = \prod_{k=1}^{5} W_{\overline{i,j},k}.$$

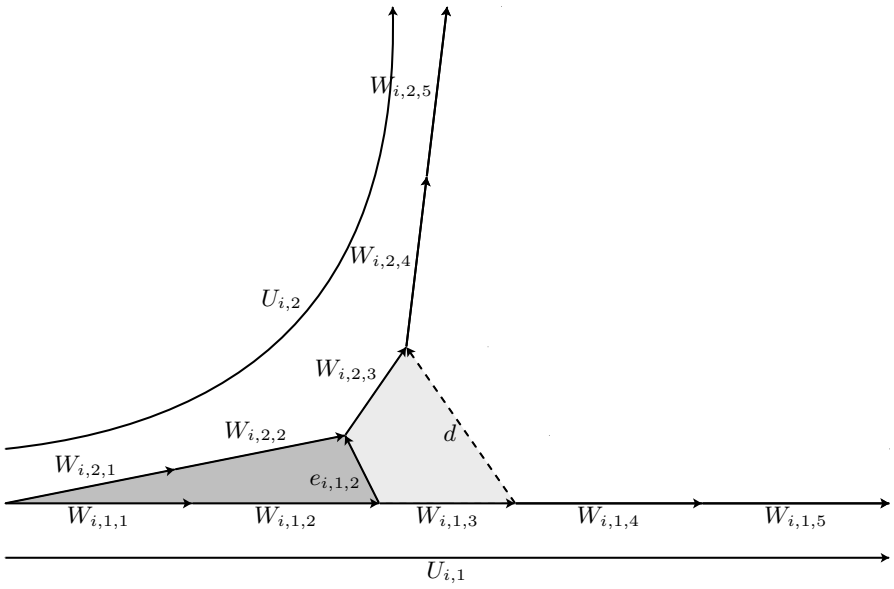


Fig. 22. A disequation cut into parts

Lemma 66. *Let $\mathcal{S} = ((E_i)_{1\leq i\leq n}, (\overline{E_i})_{n+1\leq i\leq 2n}, \mu_{\mathcal{A},\mathbb{G}}, \mu_{\mathcal{U}})$ 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*

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

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

$$\sigma_t : \mathbb{W}_t \to \mathbb{H}_t$$

solving simultaneously the system $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ of equations over $\mathbb{H}_t$ and the system $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ of equations and disequations over $\mathbb{H}$, and such that

$$\sigma = \sigma_{\boldsymbol{W},\boldsymbol{e}} \circ \sigma_t \circ \pi_{\mathbb{G}}.$$

From $\mathbb{G}$-solutions to t-solutions. Let $\sigma : \mathcal{U}^* \to \mathbb{G}$ 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 Section 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 $s_{i,j} \in \mathrm{Red}(\mathbb{H}, t)$ such that

$$\sigma(U_{i,j}) = \pi_{\mathbb{G}}(s_{i,j}).$$

Let us consider some decomposition of the form (5) for $s_{i,1}$ and $s_{i,2}$:

$$s_{i,1} = h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_\lambda} h_\lambda \cdots t^{\alpha_\ell} h_\ell, \tag{392}$$

$$s_{i,2} = h'_0 t^{\alpha'_1} h'_1 \cdots t^{\alpha'_\lambda} h'_\lambda \cdots t^{\alpha'_{\ell'}} h'_{\ell'}. \tag{393}$$

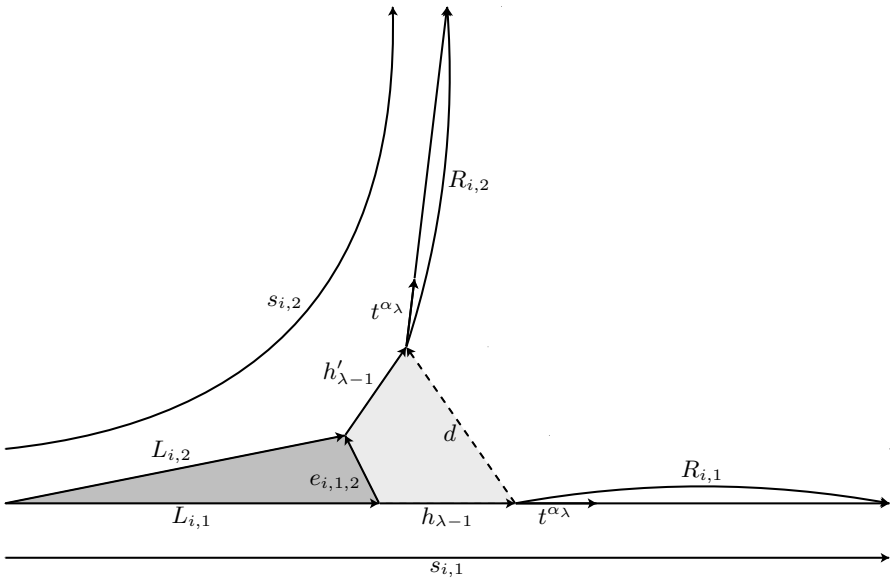


Fig. 23. Disequations, case 1

We know that $s_{i,1} \not\approx s_{i,2}$. Let us distinguish the possible forms for $s_{i,1}$, as represented in Figures 23-25.

Case 1. There exists $2 \leq \lambda \leq \min\{\ell, \ell'\}$ and $e_{i,1,2} \in B(\alpha_{\lambda-1})$ such that $\alpha_s = \alpha'_s$ for $1 \leq s \leq \lambda$ and

$$h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_{\lambda-1}} e_{i,1,2} = h'_0 t^{\alpha_1} h'_1 \cdots t^{\alpha_{\lambda-1}}, \quad h_{\lambda-1} d \neq e_{i,1,2} h'_{\lambda-1} \text{ for all } d \in A(\alpha_\lambda).$$

We consider the following factors of $s_{i,1}$ and $s_{i,2}$:

$$L_{i,1} = h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_{\lambda-1}}, \;\; M_{i,1} = h_{\lambda-1}, \;\; R_{i,1} = t^{\alpha_\lambda} h_\lambda t^{\alpha_{\lambda+1}} \cdots t^{\alpha_\ell} h_\ell,$$

$$L_{i,2} = h'_0 t^{\alpha_1} h'_1 \cdots t^{\alpha_{\lambda-1}}, \;\; M_{i,2} = h'_{\lambda-1}, \;\; R_{i,2} = t^{\alpha_\lambda} h'_\lambda t^{\alpha'_{\lambda+1}} \cdots t^{\alpha'_{\ell'}} h'_{\ell'}.$$

Following the lines of Section 5.2, the reduced sequences $s_{i,j}$ $(1 \leq j \leq 2)$ can be cut into five factors $v_{i,j,k}$ $(1 \leq k \leq 5)$ and subsequently lifted to five letters $(W_{i,j,k})$ $(1 \leq k \leq 5)$ such that the vector $(W_{i,*,*}, e_{i,1,2})$ fulfills conditions (380)-(385) and the classes $([v_{i,*,*}]_\sim)$ fulfill equation (387) and disequations (391). We can define $\sigma_t(W_{i,j,k}) = [v_{i,j,k}]_\sim$. Then, σ_t can be extended to an AB-homomorphism solving both systems $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$, $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ and such that

$$\sigma = \sigma_{\boldsymbol{W},\boldsymbol{e}} \circ \sigma_t \circ \pi_{\mathbb{G}}.$$

Case 2. There exist $2 \leq \lambda \leq \min\{\ell, \ell'\}$ and $e_{i,1,2} \in B(\alpha_{\lambda-1})$ such that $\alpha_s = \alpha'_s$ for $1 \leq s \leq \lambda - 1$, $\alpha_\lambda = -\alpha'_\lambda$ and

$$h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_{\lambda-1}} e_{i,1,2} = h'_0 t^{\alpha_1} h'_1 \cdots t^{\alpha_{\lambda-1}}.$$

We consider the factors $L_{i,1}, M_{i,1}, R_{i,1}, L_{i,2}, M_{i,2}$ defined by the same formulas as in case 1, and define

$$R_{i,2} = t^{-\alpha_\lambda} h'_\lambda t^{\alpha'_{\lambda+1}} \cdots t^{\alpha'_{\ell'}} h'_{\ell'}.$$

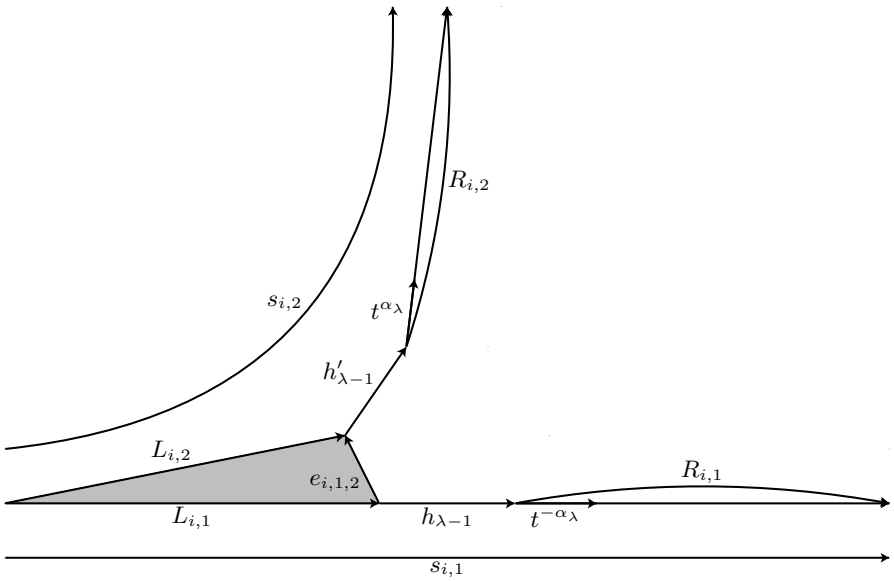


Fig. 24. Disequations, case 2

This time we obtain a vector $(W_{i,*,*})$ such that $\tau\mathrm{e}(W_{i,1,3}) \neq \tau\mathrm{e}(W_{i,2,3})$. Hence, there is no disequation (391) associated to this index i. The vector $(W_{i,*,*}, e_{i,1,2})$ fulfills conditions (380)-(385) and the classes $[v_{i,*,*}]_\sim$ fulfill equation (387).

Case 3. $1 \leq \ell \leq \ell'$, $\alpha_s = \alpha'_s$ for $1 \leq s \leq \ell$ and there exists $e_{i,1,2} \in B(\alpha_\ell)$ such that

$$h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_\ell} e_{i,1,2} = h'_0 t^{\alpha_1} h'_1 \cdots t^{\alpha_\ell}.$$

This case can be treated similarly as case 2. We just define $R_{i,1} = 1$ and, correspondingly $W_{i,1,k} = 1$, for $4 \leq k \leq 5$.

Case 4. $1 \leq \ell' \leq \ell$, $\alpha_s = \alpha'_s$ for $1 \leq s \leq \ell'$ and there exists $e_{i,1,2} \in B(\alpha_{\ell'})$ such that

$$h_0 t^{\alpha_1} h_1 \cdots t^{\alpha_{\ell'}} e_{i,1,2} = h'_0 t^{\alpha_1} h'_1 \cdots t^{\alpha_{\ell'}}.$$

This case is obtained from Case 3 by exchanging $s_{i,1}$ and $s_{i,2}$.

It remains to treat some degenerated cases.

Case 5. $\alpha_1 = -\alpha'_1$ or $(\alpha_1 = \alpha'_1$ and $h_0 d \neq h'_0$ for all $d \in A(\alpha_1))$. We set $L_{i,1} = L_{i,2} = 1$, $e_{i,1,2} = 1$, $M_{i,1} = h_0$, $M_{i,2} = h'_0$, $R_{i,1} = t^{\alpha_1} h_1 \cdots t^{\alpha_\ell} h_\ell$, and $R_{i,2} = t^{\alpha'_1} h'_1 \cdots t^{\alpha'_{\ell'}} h'_{\ell'}$. The construction is ended as in the degenerated cases from Section 5.2.

Case 6. $\ell = 0 < \ell'$. We set $L_{i,1} = L_{i,2} = R_{i,1} = 1$, $e_{i,1,2} = 1$, $M_{i,1} = h_0$, $M_{i,2} = h'_0$, and $R_{i,2} = t^{\alpha'_1} h'_1 \cdots t^{\alpha'_{\ell'}} h'_{\ell'}$. The construction is ended as in the degenerated cases of Section 5.2.

Case 7. $\ell' = 0 < \ell$. This case is treated analogously to the previous case.

Case 8. $\ell = \ell' = 0$. We set $L_{i,1} = L_{i,2} = R_{i,1} = R_{i,2} = 1$, $e_{i,1,2} = 1$, $M_{i,1} = h_0$, and $M_{i,2} = h'_0$.

From t-solutions to $\mathbb{G}$-solutions Let $\sigma_t : \mathbb{W}_t \to \mathbb{H}_t$ be an AB-homomorphism solving both systems $\mathcal{S}_t(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ and $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$. Owing to the proofs of Section 5.2, we just have to prove that for every $i \in [n+1, 2n]$,

$$\sigma_t(\sigma_{\boldsymbol{W},\boldsymbol{e}}(U_{i,1})) \not\approx \sigma_t(\sigma_{\boldsymbol{W},\boldsymbol{e}}(U_{i,2})).$$

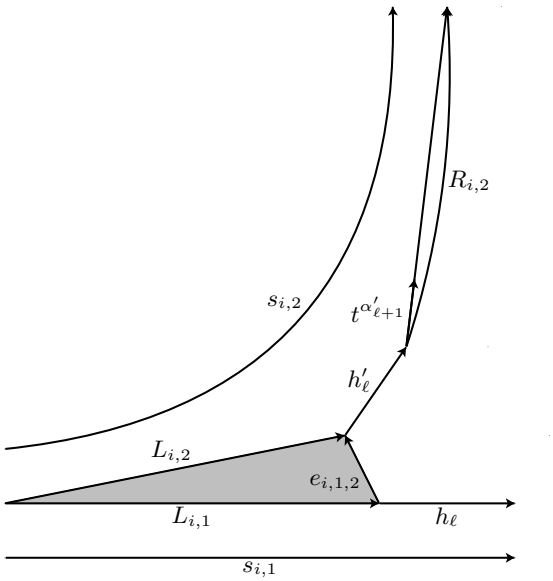


Fig. 25. Disequations, case 3

Using equation (386) and the definition of $\sigma_{\boldsymbol{W},\boldsymbol{e}}$, the above inequalities are equivalent with

$$\sigma_t(\prod_{k=1}^{5} W_{i,1,k}) \not\approx \sigma_t(\prod_{k=1}^{5} W_{i,2,k}). \tag{394}$$

Equation (387) states that

$$\sigma_t(W_{i,1,1}W_{i,1,2})e_{i,1,2} = \sigma_t(W_{i,2,1}W_{i,2,2}). \tag{395}$$

Since $\mathbb{G}$ is cancellative, we must show

$$\sigma_t(\prod_{k=3}^{5} W_{i,1,k}) \not\approx e_{i,1,2}\sigma_t(\prod_{k=3}^{5} W_{i,2,k}). \tag{396}$$

Let us distinguish several cases according to the values of $\tau\mathrm{e}(W_{i,j,3})$. Since by (384), the $\gamma_w(W_{i,j,3})$ are H-types, one of the following cases must occur.

Case 1. $\tau\mathrm{e}(W_{i,1,3}) = \tau\mathrm{e}(W_{i,2,3}) = (1,1)$. With (381), we get $\gamma(W_{i,j,4}W_{i,j,5}) = (1,1,0,1,1)$, i.e., $\sigma_t(W_{i,j,4}W_{i,j,5}) = 1$ for $j \in [1,2]$. Hence, the negation of (396) and cancellativity of $\mathbb{G}$ imply $\sigma_t(W_{i,1,3}) \approx e_{i,1,2}\sigma_t(W_{i,2,3})$, i.e., $\sigma_t(W_{i,1,3}) \neq e_{i,1,2}\sigma_t(W_{i,2,3})$ But this contradicts disequation (391) for $d = 1$.

Case 2. $\tau\mathrm{e}(W_{i,1,3}) = \tau\mathrm{e}(W_{i,2,3}) = (A,T)$. Then we would get an identity of the form $\sigma_t(W_{i,1,3})d \neq e_{i,1,2}\sigma_t(W_{i,2,3})$ for some $d \in A$ from the negation of (396). But this contradicts disequation (391).

Case 3. $\tau\mathrm{e}(W_{i,1,3}) = \tau\mathrm{e}(W_{i,2,3}) = (B,T)$. The same argument as for Case 2 works.

Case 4. $\tau\mathrm{e}(W_{i,1,3}) \neq \tau\mathrm{e}(W_{i,2,3})$. This implies that the projections of $\sigma_t(\prod_{k=3}^{5} W_{i,1,k})$ and $\sigma_t(\prod_{k=1}^{5} W_{i,2,3})$ on $\{t, t^{-1}\}^*$ are not equal. Hence, inequality (396) holds.

This concludes the proof of Lemma 66. □

Theorem 9. *Let $\mathbb{H}$ be a cancellative monoid and $\mathbb{G}$ an HNN-extension of $\mathbb{H}$ with finite associated subgroups A and B. The satisfiability problem for systems of equations and disequations with rational constraints in $\mathbb{G}$ is Turing-reducible to the satisfiability problem for systems of equations and disequations with rational constraints in $\mathbb{H}$.*

In order to prove this theorem we must, as for the proof of Theorem 5, cope with the fact that we do not know an algorithm for testing the satisfiability over $\mathbb{H}$ of an equation with the constraint $\mathbb{H} \setminus \mathsf{I}(\mathbb{H})$ (the set of non-units of the monoid $\mathbb{H}$). Therefore we use again the notion of a *weak* AB-homomorphism. [9] We first adapt Lemma 65 to:

Lemma 67. *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 where $\mathcal{S}_j = ((E_i)_{1\leq i\leq n}, (\overline{E}_i)_{n+1\leq i\leq 2n}, \mu_{\mathcal{A}}, \mu_{\mathcal{U},j})$. Let us suppose that $\mathcal{DS}$ is in closed quadratic normal form. A monoid homomorphism*

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

is a solution of $\mathcal{DS}$ if and only if, there exists and index $j \in J$, an admissible vector $(\boldsymbol{W}, \boldsymbol{e})$ of variables of $\mathcal{W}$ and elements of $A \cup B$, an involution $\Phi \in \mathsf{HInv}$, an AB-homomorphism $\sigma_{\mathbb{W}} : \mathbb{W}'_t \to \mathbb{W}'_t/\Phi$ and a weak AB-homomorphism $\psi_t : \mathbb{W}'_t/\Phi \to \mathbb{H}_t$ such that:

(S1) *$\sigma_{\mathbb{W}}$ is a solution of the system of equations $\mathcal{S}_t(\mathcal{S}_j, \boldsymbol{W}, \boldsymbol{e})$,*
(S2) *$\sigma_{\mathbb{W}} \circ \psi_t$ is a solution of the system of equations and disequations $\mathcal{S}_{\mathbb{H}}(\mathcal{S}_j, \boldsymbol{W}, \boldsymbol{e})$,*
(S3) *$\sigma = \sigma_{\boldsymbol{W},\boldsymbol{e}} \circ \sigma_{\mathbb{W}} \circ \psi_t \circ \pi_{\mathbb{G}}$.*

This lemma can be proved in the same way as Lemma 65.

Sketch of the proof of Theorem 9. It suffices to adapt the reductions given in the proof of Theorem 5 as follows:

- Lemma 65 is replaced by Lemma 67.
- Instead of a system of equations with rational constraints in $\mathbb{H}$ we use the system $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ of equations and disequations with rational contraints in $\mathbb{H}$ supplied by Lemma 66. □

11.2 Positive rational constraints

Here we consider $\mathcal{C}_{\mathbb{G}} = \mathsf{Rat}(\mathbb{G})$ and $\mathcal{C}_{\mathbb{H}} = \mathsf{Rat}(\mathbb{H})$.

Theorem 10. *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 satisfiability problem for systems of equations and disequations with positive rational constraints in $\mathbb{H}$.*

In order to prove this theorem we must, as for Theorem 5, cope with the fact that we do not know an algorithm for testing emptiness of a set of the form $\{s \in \mathbb{H}*\{t, t^{-1}\}^* \mid \mu_t(s) = \mu(W)\}$: such a set is not known to be recognized by an fta with labels which are defined by equations, disequations and *positive* rational constraints over $\mathbb{H}$. Therefore we use the notion of *weak*-AB-homomorphism.

Sketch of the proof of Theorem 10. It suffices to adapt the reduction given in the proof of Theorem 5 as follows:

[9] Though we might also use a notion weaker than AB-homomorphisms and stronger than weak AB-homomorphisms, since we are able to translate the conditions over γ, μ, δ by equations and disequations with rational constraints.

– Lemma 65 is replaced by Lemma 67.
– The initial positive constraints given by the system of equations and disequations are defined by normal (possibly non-strict) ftas with labelling set $\mathsf{Rat}(\mathbb{H})$.
– Instead of a system of equations with rational constraints in $\mathbb{H}$ we use the system $\mathcal{S}_{\mathbb{H}}(\mathcal{S}, \boldsymbol{W}, \boldsymbol{e})$ of equations and disequations with positive rational contraints in $\mathbb{H}$ supplied by Lemma 66.
– For every $W \in \mathcal{W}'_{\mathbb{H}}$, $\mathsf{C}(W)$ belongs to $\mathrm{DEQ}(\mathbb{H}, \mathsf{Rat}(\mathbb{H}))$.
– For every $W \in \mathcal{W}'_t \setminus \mathcal{W}'_{\mathbb{H}}$, $\mathsf{C}(W)$ is recognized by an fta with labels in $\mathrm{DEQ}(\mathbb{H}, \mathsf{Rat}(\mathbb{H}))$: this is clear for $\mathsf{C}_I(W), \mathsf{C}_\mu(W), \mathsf{C}_\delta(W)$; for $\mathsf{C}_\gamma(W)$, the trick consists just in seeing the subset $\mathbb{H} \setminus A$ (resp. $\mathbb{H} \setminus B$) as defined by the system of disequations $\bigwedge_{a \in A} v \neq a$ (resp. $\bigwedge_{b \in B} v \neq b$). □

11.3 Constants

Here, the sets of constraints 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 11. *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 satisfiability problem for systems of equations and disequations with constants in $\mathbb{H}$.*

Proof sketch. We adapt the reductions given in the proof of Theorem 5 as follows:

– Lemma 65 is replaced by Lemma 67.
– For every $W \in \mathcal{W}'_t$, $\mathsf{C}(W)$ is recognized by an fta with labeling set $\mathrm{DEQ}(\mathbb{H}, \mathcal{C}_{\mathbb{H}})$, i.e. the set of subsets of $\mathbb{H}$ which are definable by systems of equations and disequations with constants. □

12 Equations and disequations over an amalgamated product

12.1 Equations and disequations

In this section we adapt the transfer result about the operation of HNN-extension (i.e. Theorem 9) as a transfer result about *free product with amalgamation* (see Theorem 12 below). We recalled in Section 2 Theorem 1 for equations and disequations and the operation of free product. Let us use here the same notation $\mathcal{L}(\mathcal{C}_{\mathbb{H}_1}, \mathcal{C}_{\mathbb{H}_2})$ and state a more general theorem.

Theorem 12. *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 $\varphi : A_1 \to A_2$. 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*

– *S_1 is the satisfiability problem for systems of equations and disequations with rational constraints in $\mathbb{H}_1$ and*
– *S_2 is the satisfiability problem for systems of equations and disequations with rational constraints in $\mathbb{H}_2$.*

Proof. Let us use the embedding $\eta : \mathbb{G} \to \widehat{\mathbb{G}}$ defined in Section 2.2 by formula (12), where $\widehat{\mathbb{G}} = \langle \mathbb{H}_1 * \mathbb{H}_2, t;\ t^{-1}at = \varphi(a)(a \in A_1)\rangle$. By Lemma 20 the satisfiability problem for systems of equations and disequations with rational constraints in $\mathbb{G}$ is reduced to the same problem in $\widehat{\mathbb{G}}$. By Theorem 5 this problem reduces to the same problem in the product $\mathbb{H}_1 * \mathbb{H}_2$ and by Theorem 1 this last problem reduces to the same problem in every factor, i.e., to (S_1, S_2). □

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 12 where equations and disequations *with constants* are considered.

12.2 Equations

We strongly believe that one can adapt the main transfer result about equations and the operation of HNN-extension (i.e. Theorem 5) 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 6, dealing with equations with positive rational constraints, and of Theorem 8, dealing with equations with constants, should hold for free products with amalgamation.

13 Equations and disequations over a graph of groups

A (finite) graph in the sense of Serre [Ser77] is a tuple (V, E, ι, τ), where V is a finite set of vertices, E is a finite set of edges, and $\iota : E \to V$ (resp., $\tau : E \to V$) maps each edge to its initial (resp., terminal) vertex. Recall that a *graph of groups* is a tuple $\mathcal{G} = (V, E, \iota, \tau, (G_v)_{v\in V}, (\varphi_e)_{e\in E})$, where (V, E, ι, τ) is a finite graph, G_v is a group for every vertex $v \in V$, and for every edge $e \in E$, φ_e is a partial isomorphism from $G_{\iota(e)}$ into $G_{\tau(e)}$. 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 13. *Let $\mathcal{G} = (V, E, \iota, \tau, (G_v)_{v\in V}, (\varphi_e)_{e\in E})$ be a finite graph of groups where all the partial isomorphisms φ_e have finite domain and let $v_0 \in V$. For a vertex v let* Sat_v *be the satisfiability problem for systems of equations and disequations with rational constraints in the group G_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* Sat_v *$(v \in V)$.*

Proof. We can assume that (V, E, ι, τ) is connected (otherwise adding some edges with trivial partial isomorphisms would preserve the fundamental group and makes the graph connected). Let $T \subseteq E$ be a spanning tree, and let $k = |T| - |E|$ and $\ell = |T|$. The group $\pi_1(\mathcal{G}, v_0)$ can be obtained as a k-fold HNN-extension of an ℓ-fold free product with amalgamation of the vertex groups G_v, where the associated (or amalgamated) subgroups are $\mathrm{dom}(\varphi_e)$ and $\mathrm{im}(\varphi_e)$ for $e \in E$. Hence, using k times Theorem 9 and ℓ times Theorem 12, we obtain the desired Turing reduction. □

Related works In [DG07], Dahmani and Guirardel proved Theorem 3 by geometrical methods. Using this result, they get an algorithm that solves equations in any word hyperbolic

group (even with torsion) [DG10]. As mentioned in the introduction, Myasnikov and Kharlampovich showed that the full first-order theory of a free group of finite rank is decidable. Their solution includes methods for solving equations in so called fully residually free groups [KM05a,KM05b].

Perspectives We think that part of the techniques exposed here can be extended to HNN-extensions where the subgroups A and 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

[BO93] Ronald V. Book and Friedrich Otto. *String–Rewriting Systems*. Springer-Verlag, 1993.

[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.

[DG10] F. Dahmani and V. Guirardel. Foliations for solving equations in groups: free, virtually-free and hyperbolic groups. *arXiv:09101.1830v2*, pages 1–70, 2010.

[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 free partially commutative groups is decidable. *International Journal of Algebra and Computation*, 2006. to appear.

[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 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] M. Lohrey and G. Sénizergues. Rational subsets in HNN-extensions and amalgamated products. *Internat. J. Algebra Comput.*, 18(1):111–163, 2008.

[Mak83] Gennadiĭ 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] Gennadiĭ 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 *Proc. 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.

[Sén96] G. Sénizergues. On the rational subsets of the free group. *Acta Informatica*, 33:281–296, 1996.

[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.