Positive theories of HNN-extensions and amalgamated free products

Markus Lohrey
Universität Stuttgart, FMI, Germany
lohrey@informatik.uni-stuttgart.de

Géraud Sénizergues
Université Bordeaux I, LaBRI, France
ges@labri.u-bordeaux.fr

Abstract

It is shown that the positive first-order theory of an HNN-extension $G = \langle H, t; t^{-1}at = \varphi(a)(a \in A)\rangle$ can be reduced to the existential first-order theory of G provided that A and B are proper subgroups of the base group H with $A \cap B$ finite. For an amalgamated free product $G = H *_A J$, we show that the positive first-order theory of G can be reduced to the existential first-order theory of G in case A is finite.

1 Introduction

This paper is the third paper in a serious of papers on equations over HNN-extensions and amalgamated free products. These two operations are of fundamental importance in combinatorial group theory [15]. Recall that an amalgamated free product

$$G = H *_A J \tag{1}$$

of two groups H and J, where A is a subgroup of H and J and w.l.o.g. $A = H \cap J$, results from the free product $H * J$ by identifying every element of $A \leq H$ with its corresponding element in $A \leq J$. An HNN extension

$$G = \langle H, t; t^{-1}at = \varphi(a)(a \in A)\rangle \tag{2}$$

of a group H, where A and B are isomorphic subgroups of H and $\varphi : A \to B$ is an isomorphism, results from adding to H a new generator t such that the conjugation of the subgroup $A \leq H$ by t equals the isomorphism φ.

In [14] we proved several decidability results for algorithmic problems for rational subsets in HNN-extensions and amalgamated free products. Based on theses results, we continued our investigations with existential theories of equations (together with additional constraints for variables) in HNN-extensions and amalgamated free products [13]. Equations over groups and also monoids 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, Tarksi, and others in the first half of the 20th century. For a given group G, we are mainly concerned with two theories associated with G: (i) the existential theory of G contains all true statements about G of the form $\exists x_1 \in G \cdots \exists x_n \in G : \varphi$, where φ is a boolean combination of equations over G. The left- and right hand sides of these equations are products of elements from the group G as well as variables x_i and their inverses. The positive theory of G consists of all true statements about G, where also universally quantified variables are allowed, but the use of negations is forbidden, i.e., conjunction and disjunction are the only allowed boolean connectives.

Basically, Merzlyakov has shown that the positive theory of a free group can be reduced to the existential theory of another free group [19], see also [11]. Toghether with the later result of Makanin concerning the decidability of the existential theory of a free group [16, 17], this shows that every free group has a decidable positive theory [17]. This result is an important step in the recent proof of Tarski's conjecture by Kharlampovich and Myasnikov, namely that the full first-order theory of a free group is decidable [12]. Roughly speaking, Merzlyakov proved that a positive sentence ψ, which is interpreted in a free group F, is equivalent to the existential sentence θ that results from ψ by replacing its universally quantified variables $x_1, \dots, x_n$ by new constants $k_1, \dots, k_n$. These new constants do not interact with the free group F, i.e., the resulting sentence θ is interpreted in the free product $F * F(k_1, \dots k_n)$ (where $F(k_1, \dots k_n)$ is the free group generated by $k_1, \dots k_n$), which is again a free group.

Merzlyakov's technique was recently extended to larger classes of groups: [6] deals with graph products of free and finite groups and [10] considers groups with a free regular length function. In [5] a general transfer theorem for positive theories was shown for graph products: under some algebraic restrictions, the decidability of the existential theory of a graph product implies the decidability of the positive theory of the graph product. Graph products are a well-known mathematical construction that generalize both free and direct products, see e.g. [9].

In this paper we adapt Merzlyakov's technique to certain HNN-extensions and amalgamated free products. In order to do this for an HNN-extension $G = \langle H, t; t^{-1}at = \varphi(a) (a \in A)\rangle$, we have to assume that A and $B = \varphi(A)$ have finite intersection. In this situation, we are again able to replace the universally quantified variables $x_1, \dots, x_n$ of a positive sentence ψ by new constants $k_1, \dots, k_n$. But unlike for the case of a free group, we cannot avoid some interaction between these new constants and the group G. More precisely, there exists a (necessarily finite) subgroup $X \subseteq A \cap B \leq G$ such that for every $1 \leq i \leq n$ we have to impose the defining relation $k_i^{-1} a k_i = f_i(a)$ $(a \in X)$ for some automorphism $f_i : X \to X$. Thus, the existential sentence θ that results from ψ by replacing the universally quantified variable x_i by the constant k_i is interpreted in a multiple HNN-extension $\mathbb{G}$ of G, where in each single HNN-extension the finite subgroup X is associated with itself. Finally we can apply [13,] in order to reduce the existential theory of the this HNN-extension $\mathbb{G}$ to the existential theory of the initial HNN-extension G. This shows that for an HNN-extension $G = \langle H, t; t^{-1}at = \varphi(a)(a \in A)\rangle$ with $A \cap \varphi(A)$ finite, the positive theory of G is decidable if the existential theory of G is decidable (Theorem 3.1). Similarly, for an amalgamated free products $G = H *_A J$, where A is finite, we show that the positive theory of G is decidable if the existential theory of G is decidable (Theorem 4.1). Finally, from Theorem 3.1, 4.1, and [13,], we can easily deduce that every virtually free group (i.e., a group with a free subgroup of finite index) has a decidable positive theory. This result relies on the fact that every virtually free group can be built up from finite groups using the operations of amalgamated free products and HNN-extensions, both subject to the finiteness restrictions above, see e.g. [4].

2 Preliminaries

For sets A and B we write $f : A \to_p B$ in order to express that f is a partial mapping from A to B. For $C \subseteq A$ we denote by $f\restriction_C$ the restriction of f to C. The identity function on a set A is denoted by id_A.

Let us fix a group G. Formulas of first-order logic over G are built up from atomic formulas of the form $xy = z$, $x^{-1} = y$, and $x = g$ (where x and y are variables ranging over elements of G, and $g \in G$ is a constant) using boolean connectives and quantifications over variables. A boolean formula is a formula without quantifiers. A formula φ is called *positive* if there are no negations in φ, i.e., it is built up from conjunctions, disjunctions and (universal and existential) quantifiers. A formula φ is called *existential* (resp. *existential positive*) if it is of the form $\exists x_1 \cdots \exists x_n : \psi(x_1, \dots, x_n)$, where ψ is a boolean (resp. positive boolean) combination of atomic formulas. For G *countable*, we denote with $\mathrm{Th}_\exists(G)$ (resp. $\mathrm{Th}_+(G)$, $\mathrm{Th}_{\exists+}(G)$) the set of all existential (resp. positive, existential positive) sentences that are true in G, this set is countable again. For a countable set $\mathcal{C} \subseteq 2^G$ of *constraints* we denote with $\mathrm{Th}_\exists(G, \mathcal{C})$ the extension of $\mathrm{Th}_\exists(G)$, where also atomic formulas of the form $x \in L$ for $L \in \mathcal{C}$ are allowed. We restrict here to a countable G and a countable $\mathcal{C}$, in order to ensure that the above theories are countable. Hence, it makes sense to ask for the decidability of these theories. We will use the following result from [13]:

Theorem 2.1. *Let H be a group and let A be a finite subgroup of H. Let $\mathcal{C} = \{B_i \mid i \in I\}$ be a class of constraints in H, where every B_i is a subgroup of H, which contains A. Let $G = \langle H, t; t^{-1}at = \varphi(a)(a \in A)\rangle$ be an HNN-extension of H, where $\varphi : A \to A$ is an automorphism of A. For every $i \in I$ let C_i be the subgroup of G generated by B_i and the stable letter t. Let $\mathcal{D} = \{B_i \mid i \in I\} \cup \{C_i \mid i \in I\}$ If $\mathrm{Th}_{\exists+}(H, \mathcal{C})$ is decidable, then also $\mathrm{Th}_{\exists+}(G, \mathcal{D})$ is decidable.*

For a subgroup X of G, we denote with $\mathrm{In}(X, G)$ the group of all automorphisms f of X such that for some $g \in G$ we have: $f(x) = g^{-1}xg$ for all $x \in X$.

The notation $\mathrm{In}(X, G)$ is intended to refer to the inner automorphism group $\mathrm{In}(X) = \mathrm{In}(X, X)$ of X.

3 HNN-extensions

In this section we consider positive theories of HNN-extensions. Let us fix throughout this section a group H (the base group), two proper subgroups $A < H, B < H$ and an isomorphism $\varphi : A \to B$. The subgroups A and B are not necessarily finite. Let

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

be the corresponding HNN-extension. The aim of this section is to prove the following result:

Theorem 3.1. *Let $G = \langle H, t; t^{-1}at = \varphi(a)(a \in A)\rangle$ be an HNN-extension, where A and B are proper subgroups of H with $A \cap B$ finite. If $\mathrm{Th}_{\exists +}(G)$ is decidable, then also $\mathrm{Th}_{+}(G)$ is decidable.*

Remark 3.2. *Theorem 3.1 can be slightly generalized by only assuming that for some $h \in H$, $h^{-1}Ah \cap B$ is finite, because by applying a Tietze transformation [15], which replaces t by ht, this case can be reduced to the case that $A \cap B$ is finite.*

3.1 Reduced t-sequences

Recall from [14] that a *t-sequence* is an element from the free product $H * \{t, t^{-1}\}^*$. A t-sequence is *reduced* if it does not contain a factor from $\mathrm{Forbid} = \{t^{-1}at \mid a \in A\} \cup \{tbt^{-1} \mid b \in B\}$. Alternatively, we can view a reduced t-sequence as a word from the language $\mathrm{Red}(H, t) = ((H\{t, t^{-1}\})^*H)\backslash\Gamma^* \,\mathrm{Forbid}\, \Gamma^*$, where $\Gamma = H \cup \{t, t^{-1}\}$. Usually, we omit a factor 1 in a reduced t-sequence, e.g., we identify the reduced t-sequence $1t1t1$ with the word tt. For $u, v, w \in \mathrm{Red}(H, t)$ we write $u \cdot v = w$ if and only if $uv = w$ as words over the alphabet Γ. Note that this implies that we cannot have $u \in \Gamma^*(H \setminus \{1\})$ and $v \in (H \setminus \{1\})\Gamma^*$ at the same time. In this case, we also say that the *concatenation* $u \cdot v$ of u and v is defined.

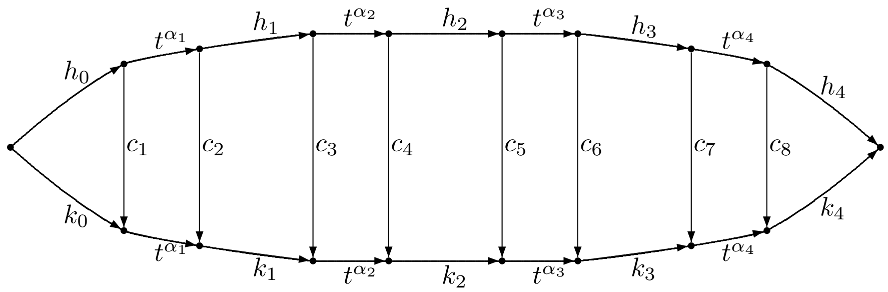
With $\sim$ we denote the smallest congruence on $H * \{t, t^{-1}\}^*$ containing all pairs $(t, a^{-1}t\varphi(a))$ for $a \in A$ and $(t^{-1}, b^{-1}t^{-1}\varphi^{-1}(b))$ for $b \in B$. Then $u, v \in \mathrm{Red}(H, t)$ represent the same element of the HNN-extension G if and only if $u \sim v$ [14]. Equivalently, if

$$u = h_0 t^{\alpha_1} h_1 t^{\alpha_2} \cdots h_{n-1} t^{\alpha_n} h_n \text{ and} \quad (3)$$
$$v = k_0 t^{\beta_1} k_1 t^{\beta_2} \cdots k_{m-1} t^{\beta_m} k_m \quad (4)$$

(with $n, m \geq 0$, $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m \in \{1, -1\}$ and $h_0, \ldots h_n, k_0, \ldots, k_m \in H$) are reduced t-sequences, then $u \sim v$ if and only if $n = m$, $\alpha_i = \beta_i$ for $1 \leq i \leq n$, and there exist $c_1, \ldots, c_{2n} \in A \cup B$ such that:

- if $\alpha_i = 1$ then $c_{2i-1} \in A$ and $c_{2i} = \varphi(c_{2i-1}) \in B$ $(1 \leq i \leq n)$
- if $\alpha_i = -1$ then $c_{2i} \in A$ and $c_{2i-1} = \varphi(c_{2i}) \in B$ $(1 \leq i \leq n)$
- $h_i c_{2i+1} = c_{2i} k_i$ in H for $0 \leq i \leq n$ (here we set $c_0 = c_{2n+1} = 1$)

This situation can be visualized by a diagram of the following form (also called a Van Kampen diagram, see [15] for more details):



Note that if $e_i = 1$ (resp. $e_i = -1$), then we must have $c_{2i-1} \in A$ and $c_{2i} \in B$ (resp. $c_{2i-1} \in B$ and $c_{2i} \in A$).

In Section 3.4 we will reason a lot with diagrams of the above form. The elements c_i are also called the *connecting elements*. Sometimes we will also omit in diagrams some of the connecting elements. The two paths between the leftmost and the rightmost point in the above diagram are also called the upper and lower bow, respectively. An interval on one of these bows is called a segment.

For the above $u \in \mathrm{Red}(H,t)$ in (3) define $\pi_t(u) = t^{\alpha_1} t^{\alpha_2} \cdots t^{\alpha_n}$, $u^{-1} = h_n^{-1} t^{-\alpha_n} h_{n-1}^{-1} \cdots t^{-\alpha_2} h_1^{-1} t^{-\alpha_1} h_0^{-1}$, and $|u| = n$. Note that $|u|$ is not the length of u as a word over $\Gamma = H \cup \{t, t^{-1}\}$ but only the number of occurrences of t and t^{-1} in u. This definition has the advantage that $u \sim v$ implies $|u| = |v|$ for $u, v \in \mathrm{Red}(H,t)$. In fact, $u \sim v$ even implies $\pi_t(u) = \pi_t(v)$.

In the following, we identify the set $\mathrm{Red}(H,t)$ with the relational structure that contains the following predicates and constants:

- the ternary relation $\{(u,v,w) \mid u \cdot v \sim w\}$
- the ternary relation $\{(u,v,w) \mid u,v,w \in H, uv = w \text{ in } H\}$
- the binary relation $\{(u,v) \mid u \sim v^{-1}\}$
- every element of $\mathrm{Red}(H,t)$ as a constant

We will use the following lemma from [13]:

Lemma 3.3. *For a given boolean combination $\phi(x_1, \ldots, x_n)$ of word equations over the HNN-extension G we can effectively construct an existential formula $\exists y_1 \cdots \exists y_m : \chi(x_1, \ldots, x_n, y_1, \ldots, y_m)$ over the structure $\mathrm{Red}(H,t)$ such that for all $s_1, \ldots, s_n \in \mathrm{Red}(H,t)$ we have:*

$$\phi(s_1, \ldots, s_n) \text{ in } G \quad \Leftrightarrow \quad \exists y_1 \cdots \exists y_m : \chi(s_1, \ldots, s_n, y_1, \ldots, y_m) \text{ in } \mathrm{Red}(H,t)$$

(here, when writing $\phi(s_1, \dots, s_n)$ in G, we identify $s_i \in \mathrm{Red}(H, t)$ with the element from G it represents).

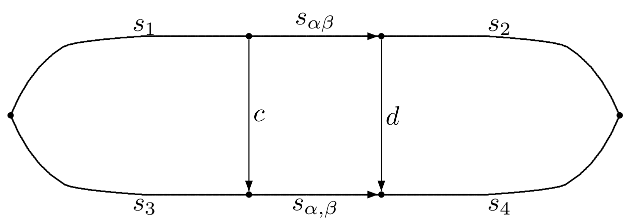
3.2 The finite normal subgroup X and stabilizing sequences

For a (necessarily finite) subgroup $X \leq A \cap B$ and $g \in G$ we define the partial automorphism $\mathrm{act}[g, X] : X \to_p X$ by conjugation: $\mathrm{act}[g, X](y) = z$ if and only if $y, z \in X$ and $g^{-1}yg = z$. For a reduced t-sequence u, $\mathrm{act}[u, X]$ is defined as $\mathrm{act}[g, X]$, where g is the element of G represented by u. The goal of this section is to prove the following lemma:

Lemma 3.4. *There exists a subgroup $X \leq A \cap B$ and for all $\alpha, \beta \in \{1, -1\}$ there exist $s_{\alpha\beta} \in \mathrm{Red}(H, t)$ such that*

- *$s_{\alpha\beta} \in t^\alpha \cdot \mathrm{Red}(H, t) \cdot t^\beta$,*
- *X is a normal subgroup of G, i.e., for all $g \in G$: $\mathrm{act}[g, X]$ is an (totally defined) automorphism of X, and*
- *for all $c, d \in A \cup B$, if $c\, s_{\alpha\beta} = s_{\alpha\beta}\, d$ in G then $c = d \in X$.*

The subgroup X and the reduced t-sequences $s_{\alpha\beta}$ will be used in Section 3.4 in order to construct reduced t-sequences with some desired behavior. The sequence $s_{\alpha\beta}$ has a stabilizing behaviour in the following sense: Note that for all $c, d \in A \cup B$, $c\, s_{\alpha\beta}$ and $s_{\alpha\beta}\, d$ are reduced t-sequences. If we have a diagram of the form



then we must have $c = d \in X$ by the last point from Lemma 3.4.

We will construct the subgroup X as the limit of a decreasing chain $A \cap B \supseteq X_0 \supsetneq X_1 \supsetneq X_2 \cdots$. Since $A \cap B$ is finite, this chain has to terminate with some $X_i = X$.

Recall that $\varphi : A \to B$ is an isomorphism. We start with the subgroup

$$Y = \{x \in A \cap B \mid \forall k \geq 0 : \varphi^k(x) \in A \cap B\} \leq A \cap B.$$

Note that Y is closed under φ. Since φ is injective and Y is finite, $\varphi\restriction_Y$ is a permutation on the finite set Y. In particular, Y is also closed under φ^{-1}. Let us fix a number $n \in \mathbb{N}$ such that $n - 1 > |A \cap B|$ and $(\varphi\restriction_Y)^n = \mathrm{id}_Y$.

Lemma 3.5. *For all $c, d \in A \cup B$, if $c\,t^n = t^n d$ in G then $c = d \in Y$.*

Proof. Assume that $c\,t^n = t^n d$ in G for some $c, d \in A \cup B$. Since $c\,t^n$ and $t^n d$ are reduced t-sequences, we obtain a Van Kampen diagram of the following kind:

$$\begin{tikzcd}
\bullet \arrow[r, "t"] \arrow[d, "c = c_0"'] & \bullet \arrow[r, "t"] \arrow[d, "c_1"'] & \bullet \arrow[r, "t"] \arrow[d, "c_2"'] & \bullet \arrow[r, dotted, no head] \arrow[d, "c_3"'] & \bullet \arrow[r, "t"] \arrow[d, "c_{n-1}"'] & \bullet \arrow[d, "c_n = d"] \\
\bullet \arrow[r, "t"'] & \bullet \arrow[r, "t"'] & \bullet \arrow[r, "t"'] & \bullet \arrow[r, dotted, no head] & \bullet \arrow[r, "t"'] & \bullet
\end{tikzcd}$$

We get $c_0 = c \in A$, $c_n = d \in B$, $c_1, \ldots, c_{n-1} \in A \cap B$, and $\varphi(c_i) = c_{i+1}$ for $0 \leq i < n$. Since $n - 1 > |A \cap B|$, there are $1 \leq i < j < n$ such that $c_i = c_j$. Thus, φ enters a cycle at $c_i \in A \cap B$, i.e., $c_i \in Y$. Since Y is closed under φ and φ^{-1}, we get $c, c_1, \ldots, c_{n-1}, d \in Y$. Moreover, $(\varphi{\restriction_Y})^n = \mathrm{id}_Y$ implies that $c = d$. $\square$

Next we define sequences $s[\alpha, \beta]_i \in \mathrm{Red}(H, t)$ $(\alpha, \beta \in \{1, -1\})$ and a subgroup $X_i \leq Y$ for all $i \geq 0$ inductively. We start with $i = 0$: Choose an element

$$h \in H \setminus (A \cup B), \tag{5}$$

which will be fixed for the rest of Section 3.[1] Let $\mathrm{act} := \mathrm{act}[h, Y] : Y \to_p Y$ and let

$$X_0 = \{x \in Y \mid \forall k \geq 0 : \mathrm{act}^k(x) \text{ is defined}\} \leq Y.$$

Thus, $\mathrm{act}{\restriction_{X_0}}$ is a permutation on the finite subgroup X_0. Now choose a number $m \in \mathbb{N}$ such that $m + 1 > |Y|$ and $(\mathrm{act}{\restriction_{X_0}})^m = \mathrm{id}_{X_0}$, and define ($n > 0$ is the constant from Lemma 3.5):

$$\begin{aligned}
s[1,1]_0 &= (t^n h)^m t^n \\
s[1,-1]_0 &= (t^n h)^m t^{-n} \\
s[-1,1]_0 &= (t^{-n} h)^m t^n \\
s[-1,-1]_0 &= (t^{-n} h)^m t^{-n}
\end{aligned}$$

Note that $s[\alpha, \beta]_0$ is a reduced t-sequence (because $h \notin A \cup B$) and $s[\alpha, \beta]_0 \in t^\alpha \cdot \mathrm{Red}(H, t) \cdot t^\beta$.

Lemma 3.6. *For all $c, d \in A \cup B$, if $c\, s[\alpha, \beta]_0 = s[\alpha, \beta]_0\, d$ in G, then $c = d \in X_0$.*

Proof. We restrict to the case that $\alpha = \beta = 1$, the other cases can be dealt analogously. Assume that we have $c, d \in A \cup B$ with $c(t^n h)^m t^n = (t^n h)^m t^n d$. Due to Lemma 3.5 we obtain a diagram of the following form, where $c_0, c_1, \ldots, c_m \in Y$:

$$\begin{tikzcd}
\bullet \arrow[r, "t^n"] \arrow[d, "c = c_0"'] & \bullet \arrow[r, "h"] \arrow[d, "c_0"'] & \bullet \arrow[r, "t^n"] \arrow[d, "c_1"'] & \bullet \arrow[r, "h"] \arrow[d, "c_1"'] & \bullet \arrow[r, dotted, no head] \arrow[d, "c_2"'] & \bullet \arrow[r, "t^n"] \arrow[d, "c_{m-1}"'] & \bullet \arrow[r, "h"] \arrow[d, "c_{m-1}"'] & \bullet \arrow[r, "t^n"] \arrow[d, "c_m"'] & \bullet \arrow[d, "c_m = d"] \\
\bullet \arrow[r, "t^n"'] & \bullet \arrow[r, "h"'] & \bullet \arrow[r, "t^n"'] & \bullet \arrow[r, "h"'] & \bullet \arrow[r, dotted, no head] & \bullet \arrow[r, "t^n"'] & \bullet \arrow[r, "h"'] & \bullet \arrow[r, "t^n"'] & \bullet
\end{tikzcd}$$

[1] Such an element exists: Recall that we assume that $A \neq H$ and $B \neq H$. Let $x \in H \setminus A$ and $y \in H \setminus B$. If $x \notin B$ (resp. $y \notin A$) then we can choose $h = x$ (resp. $h = y$). Thus, $x \in B$ and $y \in A$. But then $xy \notin A \cup B$.

Hence, $\mathrm{act}(c_i) = c_{i+1}$ for $0 \leq i < m$. Since $m + 1 > |Y|$, there are $i < j$ with $c_i = c_j$. Thus, act enters a cycle at c_i, i.e., $c_i \in X_0$. But since X_0 is closed under act and act^{-1}, we get $c, c_1, \ldots, c_{m-1}, d \in X_0$. Moreover, $(\mathrm{act}\restriction_{X_0})^m = \mathrm{id}_{X_0}$ implies $c = d$. $\square$

Now assume that for some $i \geq 0$, reduced t-sequences $s[\alpha, \beta]_i \in \mathrm{Red}(H, t)$ and a subgroup $X_i \leq A \cap B$ with the following properties are already defined:

- $s[\alpha, \beta]_i \in t^\alpha \cdot \mathrm{Red}(H, t) \cdot t^\beta$
- for all $c, d \in A \cup B$, if $c\, s[\alpha, \beta]_i = s[\alpha, \beta]_i d$ in G then $c = d \in X_i$

If for all $g \in G$, $\mathrm{act}[g, X_i]$ is totally defined, i.e., X_i is a normal subgroup of G, then we stop and set $s_{\alpha\beta} = s[\alpha, \beta]_i$ and $X = X_i$, which proves Lemma 3.4. Otherwise there exists $g \in G$ such that $\mathrm{act} = \mathrm{act}[g, X_i]$ is not totally defined on X_i. We identify g with a reduced t-sequence representing g. Define

$$X_{i+1} = \{x \in X_i \mid \forall k \geq 0 : \mathrm{act}^k(x) \text{ is defined}\} < X_i.$$

Note that there exist $\alpha, \beta \in \{1, -1\}$ such that $t^\alpha \cdot g \cdot t^\beta$ is again a reduced t-sequence. Let us assume that $\alpha = \beta = 1$, the other cases can be dealt analogously.

Clearly, $\mathrm{act}\restriction_{X_{i+1}}$ is a permutation on the subgroup X_{i+1}. Let m be such that $m + 1 > |X_i|$ and $(\mathrm{act}\restriction_{X_{i+1}})^m = \mathrm{id}_{X_{i+1}}$, and define:

$$\begin{aligned}
s[1,1]_{i+1} &= (s[1,1]_i g)^m s[1,1]_i \\
s[1,-1]_{i+1} &= (s[1,1]_i g)^m s[1,-1]_i \\
s[-1,1]_{i+1} &= s[-1,1]_i (g s[1,1]_i)^m \\
s[-1,-1]_{i+1} &= s[-1,1]_i (g s[1,1]_i)^{m-1} g s[1,-1]_i
\end{aligned}$$

By construction we have $s[\alpha, \beta]_{i+1} \in t^\alpha \cdot \mathrm{Red}(H, t) \cdot t^\beta$. The following lemma can be proved analogously to Lemma 3.6:

Lemma 3.7. *For all $c, d \in A \cup B$, if $c\, s[\alpha, \beta]_{i+1} = s[\alpha, \beta]_{i+1}\, d$ in G, then $c = d \in X_{i+1}$.*

This concludes the proof of Lemma 3.4.

3.3 Reducing to the existential positive theory

Our strategy for reducing the positive theory of the HNN-extension G to the existential positive theory of G with rational constraints is similar to [17, 19]: Given a positive sentence θ, which is interpreted over G, we construct an *existential positive sentence* θ' with subgroup constraints of a very restricted form, which is interpreted over a multiple HNN-extension $\mathbb{G}$ of G, where only finite subgroups of $H \leq G$ are associated (in fact, $X \subseteq A \cap B$ from Lemma 3.4 will be associated with itself). Roughly speaking, θ' results from θ by replacing the universally quantified variables by the stable letters of the HNN-extension $\mathbb{G}$.

Let $X \leq A \cap B$ be the subgroup from Lemma 3.4. Recall that with $\mathrm{In}(X, G)$ we denote the group of all automorphisms f of X such that for some $g \in G$ we have: $f(c) = g^{-1} c\, g$ for all $c \in X$. In the following, we use the abbreviation

$$\mathrm{In} = \mathrm{In}(X, G).$$

For new constants $k_1, \ldots, k_m \notin G$ and $f_1, \ldots, f_m \in \mathrm{In}$ we define the HNN-extension

$$G_{k_1,\ldots,k_m}^{f_1,\ldots,f_m} = \langle G, k_1, \ldots, k_j; k_i^{-1} c\, k_i = f_i(c) \ (c \in X, 1 \leq i \leq m)\rangle.$$

The next two lemmas yield the main steps for the reduction from the positive to the existential positive theory. For the further consideration let us fix $m \in \mathbb{N}$, groups $H_1, \ldots, H_m, H'$ such that $H \subseteq H_i \subseteq H'$ for $1 \leq i \leq m$. Let

$$\begin{aligned} G_i &= \langle H_i, t; t^{-1}at = \varphi(a)(a \in A)\rangle \\ G' &= \langle H', t; t^{-1}at = \varphi(a)(a \in A)\rangle \end{aligned}$$

These groups contain $G = \langle H, t; t^{-1}at = \varphi(a)(a \in A)\rangle$. Let $k \notin G'$ be a new constant and let $f \in \mathrm{In}$. In the following symbols with a tilde like $\widetilde{x}$ will denote sequences of arbitrary length over some set that will be always clear form the context. If say $\widetilde{a} = (a_1, \ldots, a_m)$, then $\widetilde{a} \in A$ means $a_1 \in A, \ldots, a_m \in A$.

Lemma 3.8. *Assume that $\phi(x, y_1, \ldots, y_m, \widetilde{z})$ is a positive boolean formula with constants over the group G. If*

$$\exists y_1 \cdots \exists y_m \left\{ \begin{array}{l} \bigwedge\limits_{1\leq i\leq m} y_i \in (G_i)_k^f \wedge \\ \phi(k, y_1, \ldots, y_m, \widetilde{u}) \end{array} \right\} \text{ in } (G')_k^f,$$

then

$$\forall x \in \{g \in G \mid \mathrm{act}[g, X] = f\}\ \exists y_1 \cdots \exists y_m \left\{ \begin{array}{l} \bigwedge\limits_{1\leq i\leq m} y_i \in G_i \wedge \\ \phi(x, y_1, \ldots, y_m, \widetilde{u}) \end{array} \right\} \text{ in } G'.$$

Proof. Assume that there are $g_i \in (G_i)_k^f$ $(1 \leq i \leq m)$ such that $\phi(k, g_1, \ldots, g_m, \widetilde{u})$ is true in $(G')_k^f$. Let $g \in G$ be an arbitrary element with $\mathrm{act}[g, X] = f$. Then we can define a homomorphism $\rho : (G')_k^f \to G'$ by $\rho(k) = g$ and $\rho(g) = g$ for $g \in G'$. This homomorphism is well-defined since $\mathrm{act}[k, X] = \mathrm{act}[g, X]$. Then $\rho(g_i) \in G_i$ for $1 \leq i \leq m$ and, since ϕ is a positive formula, $\phi(g, \rho(g_1), \ldots, \rho(g_m), \widetilde{u})$ is true in G'. This proves the lemma. $\square$

Note that the assertion of Lemma 3.8 does not hold in general, if ϕ involves negations. For example $\forall x : x \neq 1$ is false, but $k \neq 1$ is true. On the other hand, the converse implication of Lemma 3.8 is true for arbitrary formulas:

Lemma 3.9. *Assume that $\phi(x, y_1, \ldots, y_m, \widetilde{z})$ is a (not necessarily positive) boolean formula with constants over the group G. If*

$$\forall x \in \{g \in G \mid \mathrm{act}[g, X] = f\} \; \exists y_1 \cdots \exists y_m \left\{ \begin{array}{l} \bigwedge\limits_{1 \le i \le m} y_i \in G_i \wedge \\ \phi(x, y_1, \ldots, y_m, \widetilde{u}) \end{array} \right\} \text{ in } G',$$

then

$$\exists y_1 \cdots \exists y_m \left\{ \begin{array}{l} \bigwedge\limits_{1 \le i \le m} y_i \in (G_i)_k^f \wedge \\ \phi(k, y_1, \ldots, y_m, \widetilde{u}) \end{array} \right\} \text{ in } (G')_k^f.$$

Let us postpone the quite involved proof of Lemma 3.9. The following theorem yields the reduction from the positive to the existential theory.

Theorem 3.10. *Let $\theta(\widetilde{z}) \equiv \forall x_1 \exists y_1 \cdots \forall x_n \exists y_n \, \phi(x_1, \ldots, x_n, y_1, \ldots, y_n, \widetilde{z})$ where ϕ a positive boolean combination of word equations (with constants) over the group G. For all $\widetilde{u} \in G$ we have $\theta(\widetilde{u})$ in G if and only if*

$$\bigwedge_{f_1 \in \mathrm{In}} \exists y_1 \cdots \bigwedge_{f_n \in \mathrm{In}} \exists y_n \left\{ \begin{array}{l} \bigwedge\limits_{1 \le i \le n} y_i \in G_{k_1, \ldots, k_i}^{f_1, \ldots, f_i} \wedge \\ \phi(k_1, \ldots, k_n, y_1, \ldots, y_n, \widetilde{u}) \text{ in } G_{k_1, \ldots, k_n}^{f_1, \ldots, f_n} \end{array} \right\}. \tag{6}$$

Proof. The proof is similar to the proof of [6, Theorem 17]. We proceed by induction on n. The case $n = 0$ is clear. If $n > 0$, then inductively we can assume that for all $s_1, t_1, \widetilde{u} \in G$ we have

$$\forall x_2 \exists y_2 \cdots \forall x_n \exists y_n \, \phi(s_1, x_2, \ldots, x_n, t_1, y_2, \ldots, y_n, \widetilde{u}) \text{ in } G$$

if and only if

$$\bigwedge_{f_2 \in \mathrm{In}} \exists y_2 \cdots \bigwedge_{f_n \in \mathrm{In}} \exists y_n \left\{ \begin{array}{l} \bigwedge\limits_{2 \le i \le n} y_i \in G_{k_2, \ldots, k_i}^{f_2, \ldots, f_i} \wedge \\ \phi(s_1, k_2, \ldots, k_n, t_1, y_2, \ldots, y_n, \widetilde{u}) \text{ in } G_{k_2, \ldots, k_n}^{f_2, \ldots, f_n} \end{array} \right\}.$$

Thus, for all $\widetilde{u} \in G$ we have

$$\forall x_1 \exists y_1 \cdots \forall x_n \exists y_n \, \phi(x_1, \ldots, x_n, y_1, \ldots, y_n, \widetilde{u}) \text{ in } G$$

if and only if

$$\forall x_1 \in G \; \exists y_1 \bigwedge_{f_2 \in \mathrm{In}} \exists y_2 \cdots \bigwedge_{f_n \in \mathrm{In}} \exists y_n \left\{ \begin{array}{l} \bigwedge\limits_{1 \le i \le n} y_i \in G_{k_2, \ldots, k_i}^{f_2, \ldots, f_i} \wedge \\ \phi(x_1, k_2, \ldots, k_n, y_1, \ldots, y_n, \widetilde{u}) \text{ in } G_{k_2, \ldots, k_n}^{f_2, \ldots, f_n} \end{array} \right\}.$$

Now we replace the universal quantifier $\forall x_1 \in G$ by $\bigwedge_{f_1 \in \mathrm{In}} \forall x_1 \in \{g \in G \mid \mathrm{act}[g, X] = f_1\}$. Hence, by Lemmas 3.8 and 3.9 the above formula is true in

$G^{f_2,\dots,f_n}_{k_2,\dots,k_n}$ if and only if

$$\bigwedge_{f_1\in\mathrm{In}} \exists y_1 \bigwedge_{f_2\in\mathrm{In}} \exists y_2 \cdots \bigwedge_{f_n\in\mathrm{In}} \exists y_n \left\{ \begin{array}{l} \bigwedge\limits_{1\le i\le n} y_i \in G^{f_1,\dots,f_i}_{k_1,\dots,k_i} \wedge \\ \phi(k_1,k_2,\dots,k_n,y_1,\dots,y_n,\widetilde{u}) \text{ in } G^{f_1,\dots,f_n}_{k_1,\dots,k_n} \end{array} \right\}.$$

$\square$

Remark 3.11. *In [5], a result analogous to Theorem 3.10 for the case that G is a free product (in fact, a certain graph product) was shown. In this case, the new generators $k_1,\dots,k_n$ do not interact with the group G, i.e., the HNN-extension $G^{f_1,\dots,f_n}_{k_1,\dots,k_n}$ is replaced by the free product $G * F(k_1,\dots,k_n)$, where $F(k_1,\dots,k_n)$ is the free group generated by $k_1,\dots,k_n$. For the more general case that G is an HNN-extension, we cannot avoid some nontrivial interaction between k_i and G_i: this interaction is expressed by the identities $k_i^{-1}ck_i = f_i(c)$ for $c \in X$ in the HNN-extension $G^{f_1,\dots,f_n}_{k_1,\dots,k_n}$. In order to use Theorem 2.1, it is crucial that the group X is finite.*

Note that the sentence in (6) is not interpreted in a single HNN-extension of G. In order to reduce (6) to an existential statement over a single group $\mathbb{G}$, assume that $\mathrm{In} = \{\rho_1,\dots,\rho_\ell\}$. Let $S = \{1,\dots,\ell\}$. For $\alpha > 0$ let $S^{\le\alpha}$ be the set of all non-empty words over S of length at most α. For $\tau \in S^n$ and $1 \le \alpha \le n$ let $\tau\restriction\alpha \in S^\alpha$ be the prefix of τ of length α, whereas $\tau[\alpha] \in \{1,\dots,\ell\}$ denotes the symbol at position α in τ. Take new constants k_σ for every $\sigma \in S^{\le n}$ and define the multiple HNN-extension $\mathbb{G}$ over G that results by adding to G for every word $\sigma \in S^{\le n}$ the stable letters k_σ together with the defining equation $k_\sigma^{-1}ck_\sigma = \rho_i(c)$ ($c \in X$), when i is the last symbol of the word σ. This is a fixed multiple HNN-extension over G, where only finite subgroups are associated.

Lemma 3.12. *For all $\tilde{u} \in G$, we have*

$$\bigwedge_{f_1\in\mathrm{In}} \exists y_1 \cdots \bigwedge_{f_n\in\mathrm{In}} \exists y_n \left\{ \begin{array}{l} \bigwedge\limits_{1\le i\le n} y_i \in G^{f_1,\dots,f_i}_{k_1,\dots,k_i} \wedge \\ \phi(k_1,\dots,k_n,y_1,\dots,y_n,\widetilde{u}) \textit{ in } G^{f_1,\dots,f_n}_{k_1,\dots,k_n} \end{array} \right\} \tag{7}$$

if and only if

$$(\exists y_\sigma)_{\sigma\in S^{\le n}} \bigwedge_{\tau\in S^n} \left\{ \begin{array}{l} \bigwedge\limits_{\alpha=1}^{n} y_{\tau\restriction\alpha} \in G^{\rho_{\tau[1]},\dots,\rho_{\tau[\alpha]}}_{k_{\tau\restriction 1},\dots,k_{\tau\restriction\alpha}} \wedge \\ \phi(k_{\tau\restriction 1},\dots,k_{\tau\restriction n},y_{\tau\restriction 1},\dots,y_{\tau\restriction n},\tilde{u}) \end{array} \right\} \textit{ in } \mathbb{G}. \tag{8}$$

Proof. By tranforming sentence (7) into prenex normal form, we obtain the equivalent sentence

$$(\exists y_\sigma)_{\sigma\in S^{\le n}} \bigwedge_{\tau\in S^n} \left\{ \begin{array}{l} \bigwedge\limits_{\alpha=1}^{n} y_{\tau\restriction\alpha} \in G^{\rho_{\tau[1]},\dots,\rho_{\tau[\alpha]}}_{k_1,\dots,k_\alpha} \wedge \\ \phi(k_1,\dots,k_n,y_{\tau\restriction 1},\dots,y_{\tau\restriction n},\tilde{u}) \text{ in } G^{\rho_{\tau[1]},\dots,\rho_{\tau[n]}}_{k_1,\dots,k_n} \end{array} \right\}. \tag{9}$$

It remains to show that (8) $\Leftrightarrow$ (9). First assume that (9) holds. For every $\tau \in S^n$ we define an isomorphism

$$h_\tau : G^{\rho_{\tau[1]},\ldots,\rho_{\tau[n]}}_{k_1,\ldots,k_n} \to G^{\rho_{\tau[1]},\ldots,\rho_{\tau[n]}}_{k_{\tau\restriction 1},\ldots,k_{\tau\restriction n}}$$

by $h_\tau(g) = g$ for $g \in G$ and $h_\tau(k_i) = k_{\tau\restriction i}$ for $1 \le i \le n$. Since $G^{\rho_{\tau[1]},\ldots,\rho_{\tau[n]}}_{k_{\tau\restriction 1},\ldots,k_{\tau\restriction n}} \subseteq \mathbb{G}$, we can view h_τ as an embedding of $G^{\rho_{\tau[1]},\ldots,\rho_{\tau[n]}}_{k_1,\ldots,k_n}$ into $\mathbb{G}$. Since (9) is true, there exist y_σ ($\sigma \in S^{\le n}$) such that for every $\tau \in S^n$ we have:

- $y_{\tau\restriction\alpha} \in G^{\rho_{\tau[1]},\ldots,\rho_{\tau[\alpha]}}_{k_1,\ldots,k_\alpha}$ for $1 \le \alpha \le n$
- $\phi(k_1, \ldots, k_n, y_{\tau\restriction 1}, \ldots, y_{\tau\restriction n}, \tilde{u})$ in the group $G^{\rho_{\tau[1]},\ldots,\rho_{\tau[n]}}_{k_1,\ldots,k_n}$

By applying for every $\tau \in S^n$ the embedding h_τ, we obtain y_σ ($\sigma \in S^{\le n}$) such that for every $\tau \in S^n$ we have:

- $y_{\tau\restriction\alpha} \in G^{\rho_{\tau[1]},\ldots,\rho_{\tau[\alpha]}}_{k_{\tau\restriction 1},\ldots,k_{\tau\restriction\alpha}}$ for $1 \le \alpha \le n$
- $\phi(k_{\tau\restriction 1}, \ldots, k_{\tau\restriction n}, y_{\tau\restriction 1}, \ldots, y_{\tau\restriction n}, \tilde{u})$ in the group $\mathbb{G}$

Hence, (8) is true.

Now assume that (8) is true. Then, for every $\tau \in S^n$ we define the isomorphism

$$h_\tau : G^{\rho_{\tau[1]},\ldots,\rho_{\tau[n]}}_{k_{\tau\restriction 1},\ldots,k_{\tau\restriction n}} \to G^{\rho_{\tau[1]},\ldots,\rho_{\tau[n]}}_{k_1,\ldots,k_n}$$

by $h_\tau(g) = g$ for $g \in G$ and $h_\tau(k_{\tau\restriction i}) = k_i$ for $1 \le i \le n$. Since (8) is true there are y_σ ($\sigma \in S^{\le n}$) such that for every $\tau \in S^n$:

- $y_{\tau\restriction\alpha} \in G^{\rho_{\tau[1]},\ldots,\rho_{\tau[\alpha]}}_{k_{\tau\restriction 1},\ldots,k_{\tau\restriction\alpha}}$ for $1 \le \alpha \le n$
- $\phi(k_{\tau\restriction 1}, \ldots, k_{\tau\restriction n}, y_{\tau\restriction 1}, \ldots, y_{\tau\restriction n}, \tilde{u})$ is true in the group $\mathbb{G}$ and hence is also true in $G^{\rho_{\tau[1]},\ldots,\rho_{\tau[n]}}_{k_{\tau\restriction 1},\ldots,k_{\tau\restriction n}} \subseteq \mathbb{G}$

By applying the isomorphisms h_τ we obtain y_σ ($\sigma \in S^{\le n}$) such that for every $\tau \in S^n$ we have:

- $y_{\tau\restriction\alpha} \in G^{\rho_{\tau[1]},\ldots,\rho_{\tau[\alpha]}}_{k_1,\ldots,k_\alpha}$ for $1 \le \alpha \le n$
- $\phi(k_1, \ldots, k_n, y_{\tau\restriction 1}, \ldots, y_{\tau\restriction n}, \tilde{u})$ in the group $G^{\rho_{\tau[1]},\ldots,\rho_{\tau[n]}}_{k_1,\ldots,k_n}$

Thus, (9) is true. $\square$

To complete the proof of Theorem 3.1, notice that an iterated application of Theorem 2.1 enables us to reduce the existential theory of $\mathbb{G}$ with constraints of the form $G^{\rho_{\tau[1]},\ldots,\rho_{\tau[\alpha]}}_{k_{\tau\restriction 1},\ldots,k_{\tau\restriction\alpha}}$ to the existential theory of G.

It remains to prove Lemma 3.9, which will be down by a reduction to reduced t-sequences. For this, we need one more lemma concerning reduced t-sequences. Note that elements from G' (resp. G_i) can be represented by reduced t-sequences from $\mathrm{Red}(H', t)$ (resp. $\mathrm{Red}(H_i, t)$). Fix a tuple

$$\widetilde{w} = (w_1, \ldots, w_N), \tag{10}$$

where $w_i \in \mathrm{Red}(H,t)$ is a reduced t-sequence which represents the fixed group element $u_i \in G$. Recall from Section 3.1 that we view $\mathrm{Red}(F,t)$ (where F is some base group) as a relational structure equipped with the multiplication in the base group F, and the concatenation and inversion of reduced t-sequences.

Lemma 3.13. *Let $\chi(x, y_1, \ldots, y_m, \widetilde{z})$ be a (not necessarily positive) boolean formula over the signature of the structure $\mathrm{Red}(H',t)$ and with constants from $\mathrm{Red}(H,t)$. If*

$$\forall x \in \{u \in \mathrm{Red}(H,t) \mid \mathrm{act}[u,X] = f\}\ \exists y_1 \cdots \exists y_m \left\{ \begin{array}{l} \bigwedge\limits_{1\le i\le m} y_i \in \mathrm{Red}(H_i,t) \\ \wedge\ \chi(x, y_1, \ldots, y_m, \widetilde{w}) \end{array} \right\}$$

in $\mathrm{Red}(H',t)$, then there are $v_1, v_2 \in \mathrm{Red}(H,t)$ with $\mathrm{act}[v_1,X] \circ f \circ \mathrm{act}[v_2,X] = f$ and

$$\exists y_1 \cdots \exists y_m \left\{ \begin{array}{l} \bigwedge\limits_{1\le i\le m} y_i \in \mathrm{Red}((H_i)^f_k,t) \\ \wedge\ \chi(v_1 \cdot k \cdot v_2, y_1, \ldots, y_m, \widetilde{w}) \end{array} \right\} \text{ in } \mathrm{Red}((H')^f_k,t).$$

The proof of Lemma 3.13 is the main technical difficulty and shifted to the next section.

Using Lemma 3.13, we can finish the proof of Lemma 3.9: Assume that

$$\forall x \in \{g \in G \mid \mathrm{act}[g,X] = f\}\ \exists y_1 \cdots \exists y_m \left\{ \begin{array}{l} \bigwedge\limits_{1\le i\le m} y_i \in G_i\ \wedge \\ \phi(x, y_1, \ldots, y_m, \widetilde{u}) \end{array} \right\} \text{ in } G',$$

By Lemma 3.3, we obtain a boolean formula χ over the structure $\mathrm{Red}(H',t)$ such that

$$\forall x \in \{u \in \mathrm{Red}(H,t) \mid \mathrm{act}[u,X] = f\}\ \exists y_1 \cdots \exists y_m\ \exists \widetilde{y} \left\{ \begin{array}{l} \bigwedge\limits_{1\le i\le m} y_i \in \mathrm{Red}(H_i,t) \\ \wedge\ \widetilde{y} \in \mathrm{Red}(H',t)\ \wedge \\ \chi(x, y_1, \ldots, y_m, \widetilde{y}, \widetilde{w}) \end{array} \right\}$$

is true in $\mathrm{Red}(H',t)$. Note that by applying Lemma 3.3, we only introduce a sequence $\widetilde{y}$ of new existentially quantified variables. Thus, by Lemma 3.13 there exist $v_1, v_2 \in \mathrm{Red}(H,t)$ such that $\mathrm{act}[v_1,X] \circ f \circ \mathrm{act}[v_2,X] = f$ and

$$\exists y_1 \cdots \exists y_m \exists \widetilde{y} \left\{ \begin{array}{l} \bigwedge\limits_{1\le i\le m} y_i \in \mathrm{Red}((H_i)^f_k,t) \\ \wedge\ \widetilde{y} \in \mathrm{Red}((H')^f_k,t) \\ \wedge\ \chi(v_1 \cdot k \cdot v_2, y_1, \ldots, y_m, \widetilde{y}, \widetilde{w}) \end{array} \right\} \text{ in } \mathrm{Red}((H')^f_k,t).$$

By applying Lemma 3.3 again (with G replaced by $(G')^f_k$), it follows that

$$\exists y_1 \cdots \exists y_m \left\{ \bigwedge_{1 \le i \le m} y_i \in (G_i)^f_k \;\wedge\; \phi(v_1 k v_2, y_1, \ldots, y_m, \widetilde{u}) \right\} \text{ in } (G')^f_k, \qquad (11)$$

where $v_i \in \mathrm{Red}(H,t)$ is identified with the group element from G it represents. Note that $\mathrm{act}[v_1^{-1} k v_2^{-1}, X] = \mathrm{act}[v_1, X]^{-1} \circ f \circ \mathrm{act}[v_2, X]^{-1} = f = \mathrm{act}[k, X]$. Thus, we can define a group homomorphism $h : (G')^f_k \to (G')^f_k$ by $h(k) = v_1^{-1} k v_2^{-1}$ and $h(x) = x$ for $x \in G'$. First, note that h is injective (the homomorphism defined by $g(k) = v_1 k v_2$ defines an inverse). Hence, since constants from G' are mapped to itself by h, the truth value of all (negated) equations in (11) is preserved by h. Moreover, $h(v_1 k v_2) = v_1 v_1^{-1} k v_2^{-1} v_2 = k$ in $(G')^f_k$. Hence, applying h to the above statement yields

$$\exists y_1 \cdots \exists y_m \left\{ \bigwedge_{1 \le i \le m} y_i \in (G_i)^f_k \;\wedge\; \phi(k, y_1, \ldots, y_m, \widetilde{u}) \right\} \text{ in } (G')^f_k.$$

3.4 Proof of Lemma 3.13

The following data were already fixed:

- the element $h \in H \setminus (A \cup B)$ from (5) in Section 3.2
- the finite normal subgroup $X \le A \cap B$ and the elements $s_{\alpha\beta} \in \mathrm{Red}(H,t)$ ($\alpha, \beta \in \{1, -1\}$) from Lemma 3.4
- $f \in \mathrm{In}$ from Section 3.3
- the sets $\mathrm{Red}(H,t) \subseteq \mathrm{Red}(H_i,t) \subseteq \mathrm{Red}(H',t) \subseteq \mathrm{Red}((H')^f_k, t)$ of reduced t-sequences
- the tuple $\widetilde{w} = (w_1, \ldots, w_N)$ with $w_i \in \mathrm{Red}(H,t)$ from (10) in Section 3.3

Moreover, let us fix a (not necessarily positive) boolean formula $\chi(x, y_1, \ldots, y_m, \widetilde{z})$ over the signature of the structure $\mathrm{Red}(H',t)$. Thus, χ is a boolean combination of propositions of the form $x \cdot y \sim z$, $x \sim y^{-1}$, and $xy = z$ in the base group H', where x, y, and z are either variables or constants from $\mathrm{Red}(H',t)$. Let W be the union of $\{w_1, \ldots, w_N\}$ and the set of all constants appearing in χ, and let d be the number of atomic propositions of the form $x \cdot y \sim z$ that occur in χ. Choose a number $\lambda > 2d$ such that $|X|!$ divides $\lambda - 1$. Finally, choose an element $x_f \in \mathrm{Red}(H,t)$ such that $\mathrm{act}[x_f, X] = f$, which exists since $f \in \mathrm{In}$. By appending suitable sequences $s_{\alpha\beta}$ to the left and right of x_f, we can enforce that x_f is of the form $t \cdot y \cdot t$ for some $y \in \mathrm{Red}(H,t)$.

A *t-system of degree n* ($n \ge 2$) is a tuple $\mathcal{R} = (r_0, \ldots, r_\lambda)$ with

$$r_i \in (th)^{|X|!} \{(th)^{|X|!}, (t^{-1}h)^{|X|!}\}^n t^{|X|!}.$$

The value of n will be made more precise later; but recall that λ is already defined. The idea is to encode sequences over a binary alphabet $\{a, b\}$ using the correspondence $a = (th)^{|X|!}$ and $b = (t^{-1}h)^{|X|!}$. The information density of a sequence r_i is only $\frac{n}{(n+1)2|X|!+|X|!} \geq \frac{1}{5|X|!}$, but since $|X|!$ is a constant, this won't be a problem. The exponent $|X|!$ enforces that the sequences r_i^α ($\alpha \in \{1, -1\}$) have a trivial action by conjugation on the subgroup X. The element h makes sequences reduced: since $h \in H \setminus (A \cup B)$, $t^{-1}ht$ and tht^{-1} are reduced t-sequences. Finally, the initial (resp. final) sequence $(th)^{|X|!}$ (resp. $t^{|X|!}$) ensures that every r_i starts (resp. ends) with t. It follows that for every $1 \leq i \leq \lambda$, $r_{i-1}s_{11}x_f s_{11}r_i$ is a reduced t-sequence with $\mathrm{act}[r_{i-1}s_{11}x_f s_{11}r_i, X] = \mathrm{act}[x_f, X] = f$.

There are $2^{n(\lambda+1)}$ t-systems of degree n. The t-system $\mathcal{R} = (r_0, \ldots, r_\lambda)$ has *no long overlapping*, if for all $0 \leq i, j \leq \lambda$ and $\alpha, \beta \in \{1, -1\}$ we have:[2] if $\pi_t(r_i^\alpha) = xy$ and $\pi_t(r_j^\beta) = yz$, and $|y| \geq \frac{|r_i| - |s_{11}x_f s_{11}|}{2}$ then: $x = z = \varepsilon$, $i = j$, and $\alpha = \beta$.

This condition implies that if we have a Van Kampen diagram of the form shown in Section 3.1, the upper bow contains a segment r_i^α, which overlapps a segment r_j^β in the lower bow, then either these two segments are exactly opposite to each other (and $i = j$ and $\alpha = \beta$), or their overlapping region has length less than $\frac{|r_i| - |s_{11}x_f s_{11}|}{2}$.

The next lemma follows immediately from the above definition:

Lemma 3.14. *Assume that $\mathcal{R}$ has no long overlapping. If*

$$(r_{i-1}s_{11}x_f s_{11}r_i)^\alpha \sim p \cdot r_j^\beta \cdot q$$

for $p, q \in \mathrm{Red}(H, t)$ and $\alpha, \beta \in \{1, -1\}$, then we either have $|p| = 0$ or $|q| = 0$, i.e., r_j^β cannot be properly contained in a segment which is opposite to a segment $(r_{i-1}s_{11}x_f s_{11}r_i)^\alpha$ in a diagram.

Lemma 3.15. *There exists n_0 (depending only on λ) such that for all $n \geq n_0$ there exists a t-system of degree n without long overlapping.*

Proof. There are $2^{n(\lambda+1)}$ t-systems of degree n and every t-system can be described with $n(\lambda + 1)$ bits. We show that if the t-system $\mathcal{R} = (r_0, \ldots, r_\lambda)$ has a long overlapping and n is large enough, then $\mathcal{R}$ can be described with strictly less than $n(\lambda + 1)$ bits. It follows that there is at least one t-system without long overlapping. We can distinguish the following four cases:

Case 1: for some $\alpha \in \{1, -1\}$ and some $0 \leq i, j \leq \lambda$ with $i \neq j$, $\pi_t(r_i^\alpha)$ and $\pi_t(r_j^\alpha)$ have a long overlapping, i.e., $\pi_t(r_i^\alpha) = xy$, $\pi_t(r_j^\alpha) = yz$, and $|y| \geq \frac{|r_i| - |s_{11}x_f s_{11}|}{2}$. Thus, r_j^α can be reconstructed from the pair (i, z) (note that the length of y is fixed by z). Since λ is a fixed constant, $i \in \{0, \ldots, \lambda\}$ can be specified by $O(1)$ many bits. Thus, in the description of $\mathcal{R}$ we can save at least $\frac{|y|}{|X|!} - O(1) \geq \frac{|r_i| - |s_{11}x_f s_{11}|}{2|X|!} - O(1) = \frac{(n+2)|X|! - |s_{11}x_f s_{11}|}{2|X|!} - O(1) = \frac{n}{2} - O(1)$

[2] Recall that the length of a reduced t-sequence s was defined as the number of occurrences of t and t^{-1} in s.

many bits. For a sufficiently large n, this term is strictly greater than 0; note that $|s_{11}x_f s_{11}|$ is a constant.

Case 2: for some $0 \le i \le \lambda$, $\pi_t(r_i)$ has a long overlapping with itself, i.e., $\pi_t(r_i) = xy = yz$, and $|y| \ge \frac{|r_i|-|s_{11}x_f s_{11}|}{2}$. It follows that $\pi_t(r_i) = x^p x'$ for some $p > 0$, where x' is a prefix of x. Thus, r_i can be reconstructed from x. Hence, in the description of $\mathcal{R}$ we can save at least $\frac{|r_i|-|s_{11}x_f s_{11}|}{2|X|!} = \frac{n}{2} - O(1)$ many bits.

Case 3: for some $0 \le i, j \le \lambda$ with $i \ne j$, $\pi_t(r_i)$ and $\pi_t(r_j^{-1})$ have a long overlapping. This case can be treated analogous to Case 1.

Case 4: for some $0 \le i \le \lambda$, $\pi_t(r_i)$ and $\pi_t(r_i^{-1})$ have a long overlapping, i.e., $\pi_t(r_i) = xy$, $\pi_t(r_i^{-1}) = \pi_t(r_i)^{-1} = yz$, and $|y| \ge \frac{|r_i|-|s_{11}x_f s_{11}|}{2}$. From $\pi_t(r_i)^{-1} = yz$ we get $\pi_t(r_i) = z^{-1}y^{-1} = xy$, i.e., $y = y^{-1}$. But this means that the last $\lfloor \frac{|y|}{2} \rfloor$ many symbols in y can be reconstructed from the first $\lceil \frac{|y|}{2} \rceil$ many symbols. Hence, in the description of $\mathcal{R}$ we can save at least $\frac{|r_i|-|s_{11}x_f s_{11}|}{4|X|!} - O(1) = \frac{n}{4} - O(1)$ many bits. $\square$

We will use $\mathcal{R}$ to construct a sequence s, which can be replaced by the sequence $v_1 \cdot k \cdot v_2$ in Lemma 3.13.

Let us fix a t-system $\mathcal{R} = (r_0, \ldots, r_\lambda)$ of degree n without long overlapping, where moreover n is chosen large enough such that

$$\forall w \in W : |r_{i-1}s_{11}x_f s_{11}r_i| > |w|. \tag{12}$$

For $1 \le i \le \lambda$, $u, v \in \mathrm{Red}((H')^f_k, t)$, and $0 \le j \le |u|$ we write $u \xrightarrow{j}_i v$ if there exist $u_1, u_2 \in \mathrm{Red}((H')^f_k, t)$ and $\alpha \in \{1, -1\}$ such that

- $u = u_1 \cdot (r_{i-1}s_{11}x_f s_{11}r_i)^\alpha \cdot u_2$,
- $v = u_1 \cdot (r_{i-1}s_{11}ks_{11}r_i)^\alpha \cdot u_2$, and
- $|u_1| = j$.

We write $u \to_i v$ if there exist $0 \le j \le |u|$ such that $u \xrightarrow{j}_i v$. Thus $\to_i$ can be seen as a string rewriting relation (see e.g. [1]), which is restriced to reduced t-sequences. In the notation $\xrightarrow{j}_i$ we also specify the position, where the rewriting step is carried out. We write $u \overset{j}{\Rightarrow}_i v$ if there exist $u', v' \in \mathrm{Red}((H')^f_k, t)$ such that $u \sim u' \xrightarrow{j}_i v' \sim v$, and we write $u \Rightarrow_i v$ if there exist $0 \le j \le |u|$ such that $u \overset{j}{\Rightarrow}_i v$. Clearly, the relation $\Rightarrow_i$ is terminating, i.e., there does not exist an infinite chain $u_0 \Rightarrow_i u_1 \Rightarrow_i u_2 \Rightarrow_i \cdots$. Let $\mathrm{IRR}_i = \{u \mid \neg\exists v : u \Rightarrow_i v\}$. Note that $W \subseteq \mathrm{IRR}_i$ by (12). Moreover, $s \Rightarrow_i t$ implies also $s^{-1} \Rightarrow_i t^{-1}$.

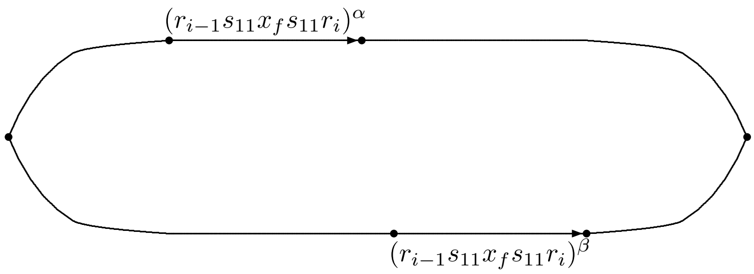
Lemma 3.16. *If $p \;{}_i\!\Leftarrow x \Rightarrow_i q$ then $p \sim q$ or there exists $w \in \mathrm{Red}((H')^f_k, t)$ such that $p \Rightarrow_i w \;{}_i\!\Leftarrow q$.*

Proof. Assume that

$$p \; {}_i\!\overset{j}{\leftarrow} u \sim v \overset{\ell}{\rightarrow}_i q, \tag{13}$$

where w.l.o.g. $j \leq \ell$. We will show that either $p \sim q$ or there exists $w \in \mathrm{Red}((H')^f_k, t)$ such that $p \Rightarrow_i w \; {}_i\!\Leftarrow q$. This proves the lemma.

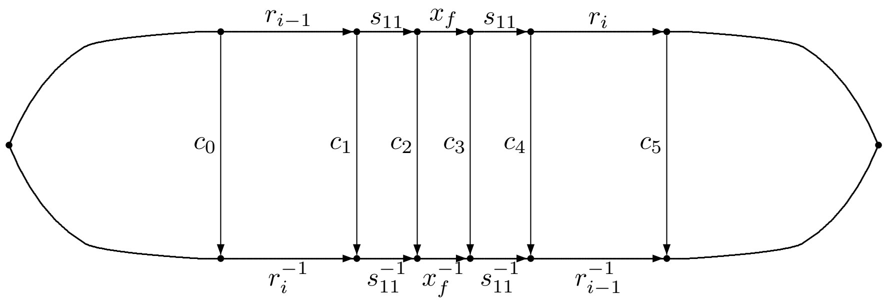
From (13) we obtain a diagram of the following form, where $\alpha, \beta \in \{1, -1\}$, the upper bow is u, and the lower bow is v:



(†)

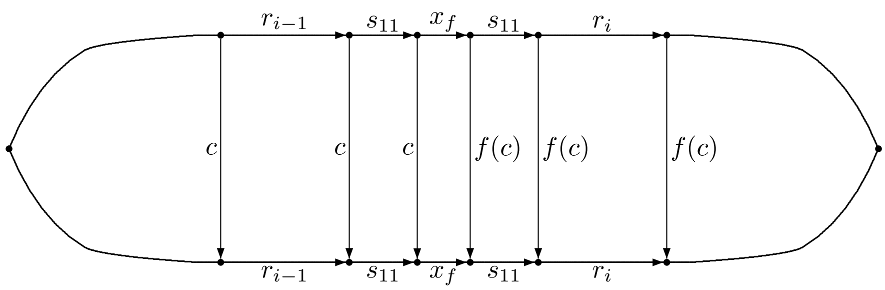
Case 1. $j = \ell$. Then $p \; {}_i\!\overset{j}{\leftarrow} u \sim v \overset{j}{\rightarrow}_i q$. We can distinguish on the values of α and β. This results in four different cases. We only consider the following two cases, the other two cases are symmetric:

Case 1.1 $\alpha = 1$ and $\beta = -1$. We obtain a diagram of the following kind:

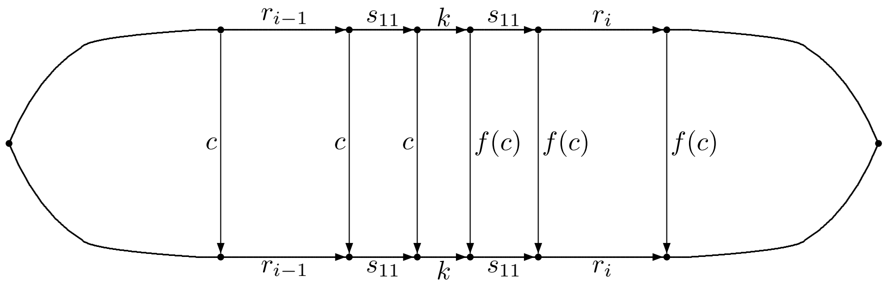


But this is not possible, since $\mathcal{R}$ has no long overlapping and hence r_{i-1} and r_i^{-1} cannot be exactly opposite to each other in a diagram.

Case 1.2. $\alpha = \beta = 1$. Together with Lemma 3.4 and the fact that $\mathrm{act}[r_{i-1}, X] = \mathrm{act}[r_i, X] = \mathrm{id}_X$ and $\mathrm{act}[x_f, X] = f$, we obtain a diagram of the following kind, where $c \in X$, the upper bow represents u and the lower bow represents v:

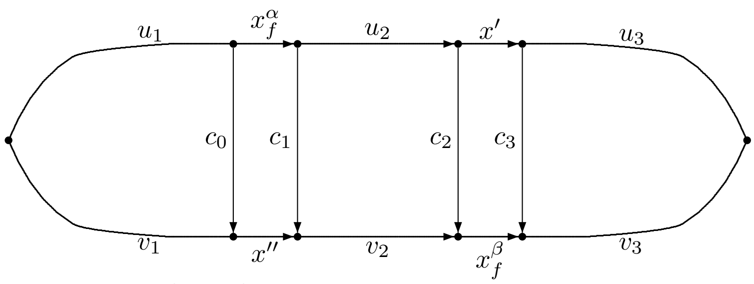


But due to the defining relations for the generator k (namely $k^{-1}ck = f(c)$ for $c \in X$) in $(H')^f_k$, we obtain also the following diagram:



Here, the upper bow is precisely p and the lower bow is q from (13). Thus, $p \sim q$.

Case 2. $j < \ell$. Diagram (†) together with Lemma 3.14 implies that $\ell - j \geq |r_{i-1}s_{11}x_f s_{11}|$. Thus, the x_f^α-segment in the upper bow of diagram (†) and the x_f^β-segment in the lower bow of diagram (†) are separated by a segment of length at least $|s_{11}r_i s_{11}|$, and the diagram (†) looks as follows, where $|u_2| = |v_2| \geq |s_{11}r_i s_{11}|$ (we omit in this diagram the context $(r_{i-1}s_{11}\cdots s_{11}r_i)^\alpha$ around the x_f^α-segment in the upper bow and analogously for the lower bow):



(‡)

Let us assume $\alpha = \beta = 1$ for simplicity. We obtain the derivations in Figure 1, where diagram (c) is diagram (‡) above. Note that the sequence in (e) is identical to the lower bow in diagram (a). It is important to note that in diagram (b), $|u_2| \geq |s_{11}r_i|$. This ensures that the context $u_1 \cdots u_2$ around x_f in the lower bow contains the context $r_{i-1}s_{11}\cdots s_{11}r_i$. This is crucial in order to carry out the reduction $u_1 x_f u_2(c_2kc_3^{-1})u_3 \xrightarrow{j}_i u_1 k u_2(c_2kc_3^{-1})u_3$. The same remark applies to the context $v_1 \cdots v_2$ around x_f in diagram (d). This finishes the proof of the lemma. $\square$

By general results about rewriting systems modulo a congruence (see e.g. [3]), Lemma 3.16 implies:

Lemma 3.17. *The relation $\Rightarrow_i$ is confluent modulo $\sim$, i.e., $u \;{}_i\!\overset{*}{\Leftarrow}\; v \overset{*}{\Rightarrow}_i w$ implies that $u \sim w$ or there exists $p \in \mathrm{Red}((H')^f_k, t)$ such that $u \overset{*}{\Rightarrow}_i p \;{}_i\!\overset{*}{\Leftarrow}\; w$.*

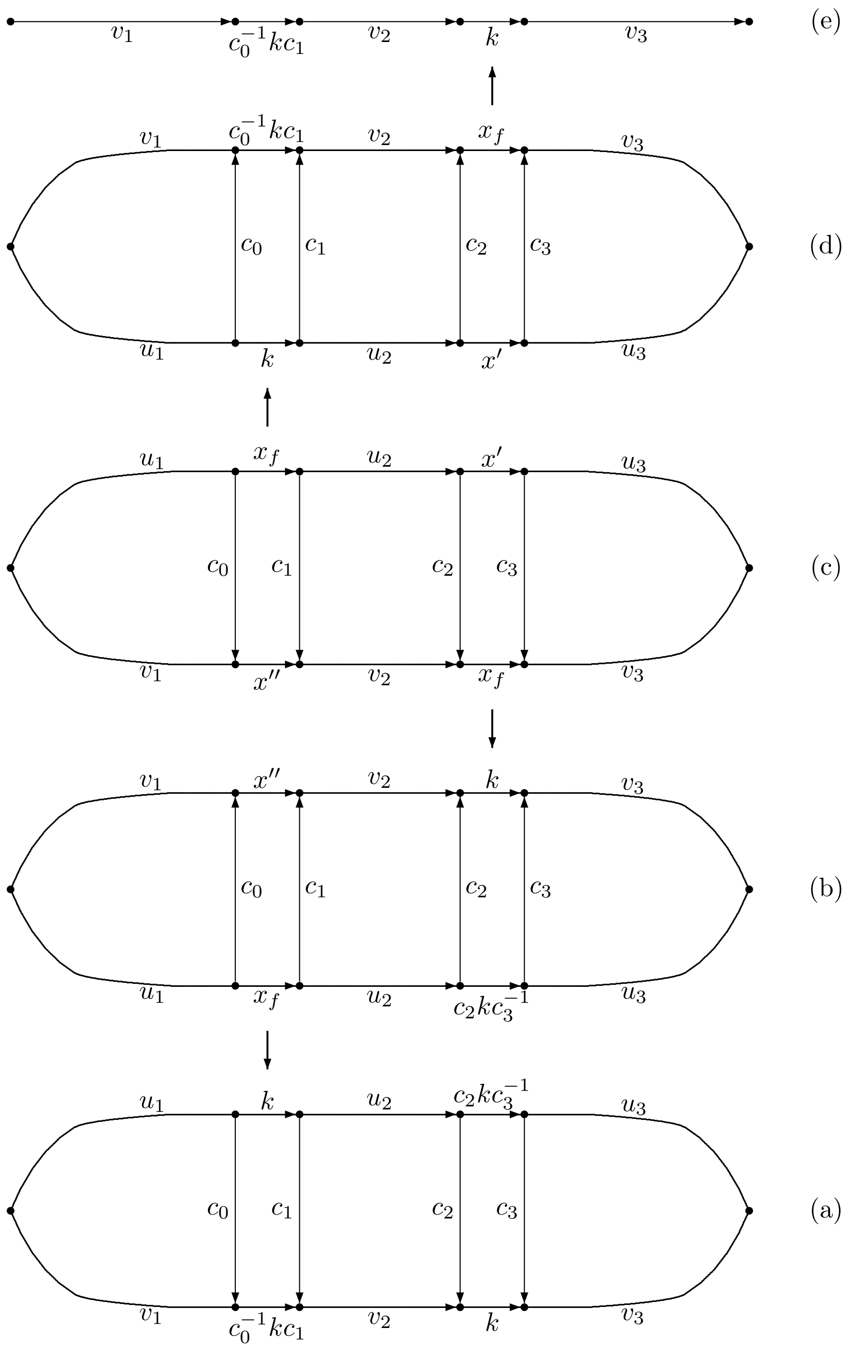


Figure 1:

The previous lemma implies that for every $1 \leq i \leq \lambda$ and every sequence $u \in \mathrm{Red}((H')^f_k, t)$, if $u \overset{*}{\Rightarrow}_i v \in \mathrm{IRR}_i$ and $u \overset{*}{\Rightarrow}_i w \in \mathrm{IRR}_i$, then $v \sim w$. Since the relation $\Rightarrow_i$ is terminating, there exists at least one $v \in \mathrm{IRR}_i$ with $u \overset{*}{\Rightarrow}_i v$. In the following, $\mathrm{NF}_i(u)$ denotes an arbitrary sequence with $u \overset{*}{\Rightarrow}_i \mathrm{NF}_i(u) \in \mathrm{IRR}_i$; we only (w.l.o.g.) require that if u starts (resp. ends) with t^α ($\alpha \in \{1, -1\}$) then also $\mathrm{NF}_i(u)$ starts (resp. ends) with t^α. This ensures that if the concatenation $u \cdot v$ of u and v is defined then also the concatenation $\mathrm{NF}_i(u) \cdot \mathrm{NF}_i(v)$ is defined. Note that the sequence $\mathrm{NF}_i(u)$ is unique up to $\sim$.

Lemma 3.18. *For all $1 \leq i \leq \lambda$ we have:*

- $\mathrm{NF}_i(w) \sim w$ *for all* $w \in W$*,*
- *if* $u \sim v^{-1}$ *for* $u, v \in \mathrm{Red}(H', t)$*, then* $\mathrm{NF}_i(u) \sim \mathrm{NF}_i(v)^{-1}$.

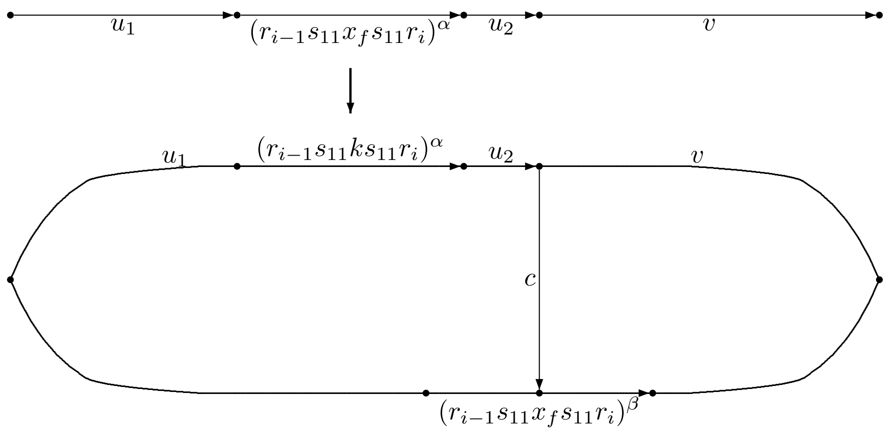
Proof. The first point follows from the fact that $W \subseteq \mathrm{IRR}_i$, see (12). For the second point note that $u \sim v^{-1}$ implies $\mathrm{NF}_i(u) \sim \mathrm{NF}_i(v^{-1})$. Since $x \Rightarrow_i y$ implies $x^{-1} \Rightarrow_i y^{-1}$, we have $\mathrm{NF}_i(v^{-1}) \sim \mathrm{NF}_i(v)^{-1}$. □

Lemma 3.19. *Let $u, v, u', v', w \in \mathrm{Red}((H')^f_k, t)$ such that*

- *the concatenations $u \cdot v$ and $u' \cdot v'$ are defined (as reduced t-sequences),*
- *($u' \to_i u$ and $v' = v$) or ($v' \to_i v$ and $u' = u$) (thus, $u' \cdot v' \to_i u \cdot v$),*
- $u \cdot v \overset{j}{\Rightarrow}_i w$*, and*
- $0 < |u| - j < |r_{i-1}s_{11}x_f s_{11}r_i|$.

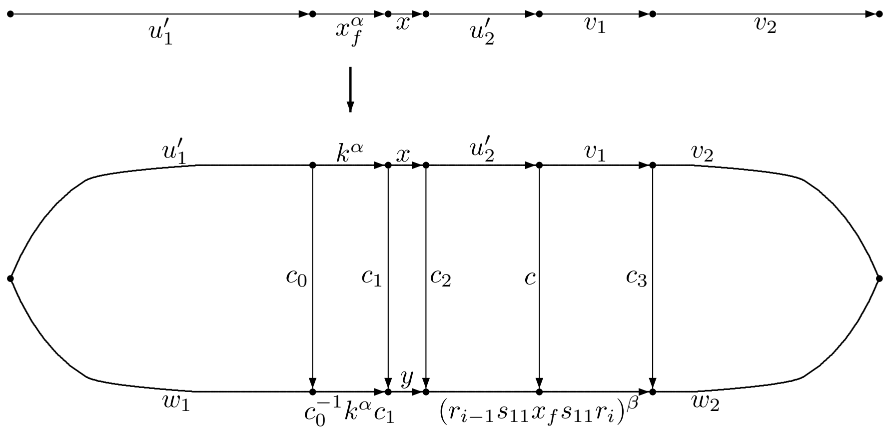
Then there exists $w' \in \mathrm{Red}((H')^f_k, t)$ and $j' \in \mathbb{N}$ such that $u' \cdot v' \overset{j'}{\Rightarrow}_i w'$ and $|u'| - j' = |u| - j$.

Proof. Let us assume that $u' \to_i u$ and $v' = v$, the other case is only simpler. Since $u' \to_i u$, there exists a factorization $u' = u_1(r_{i-1}s_{11}x_f s_{11}r_i)^\alpha u_2$ and $u = u_1(r_{i-1}s_{11}ks_{11}r_i)^\alpha u_2$. Together with $u \cdot v \overset{j}{\Rightarrow}_i w$ and $0 < |u| - j < |r_{i-1}s_{11}x_f s_{11}r_i|$ we obtain a diagram of the following form, where $\beta \in \{1, -1\}$ and $c \in A \cup B$:



Note that $0 < |u| - j < |r_{i-1}s_{11}x_fs_{11}r_i|$ means that the end point of the vertical c-edge lies strictly within the segment $(r_{i-1}s_{11}x_fs_{11}r_i)^\beta$ of the lower bow.

Lemma 3.14 implies that the segment $(r_{i-1}s_{11}ks_{11}r_i)^\alpha$ in the upper bow overlaps the segment $(r_{i-1}s_{11}x_fs_{11}r_i)^\beta$ in the lower bow by at most $|r_{i-1}| = |r_i|$ (these two segments cannot be exactly opposite to each other, since the segment $(r_{i-1}s_{11}ks_{11}r_i)^\alpha$ in the upper bow is completely contained in the left factor u but the segment $(r_{i-1}s_{11}x_fs_{11}r_i)^\beta$ in the lower bow contains the end point of the vertical c-edge). Thus, the above diagram looks in fact as follows, where we omit the context $(r_{i-1}s_{11}\cdots s_{11}r_i)^\alpha$ in the rewriting step within u:

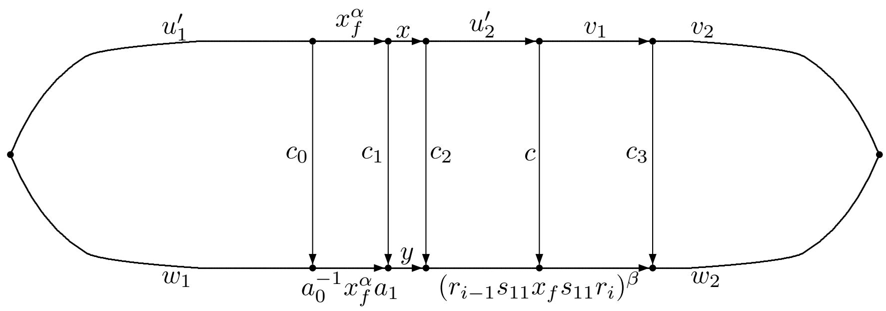


Here $v = v_1v_2$ and

$$u_1' = \begin{cases} u_1r_{i-1}s_{11} & \text{if } \alpha = 1 \\ u_1r_i^{-1}s_{11}^{-1} & \text{if } \alpha = -1 \end{cases}$$

$$x \cdot u_2' = \begin{cases} s_{11}r_iu_2 & \text{if } \alpha = 1 \\ s_{11}^{-1}r_{i-1}^{-1}u_2 & \text{if } \alpha = -1 \end{cases}$$

The existence of the sequences x and y follows from Lemma 3.14. Moreover, $u = u_1' k^\alpha x u_2'$ and $j = |u_1' k^\alpha x|$ and hence $|u| - j = |u_2'|$. By replacing k^α by x_f^α, we get the following diagram:



which shows that there exist w' and j' with $u_1' x_f^\alpha x u_2' v_1 v_2 = u'v = u'v' \overset{j'}{\Rightarrow}_i w'$. Moreover, $u' = u_1' x_f^\alpha x u_2'$ and $j' = u_1' x_f^\alpha x$, and hence $|u'| - j' = |u_2'| = |u| - j$. This proves the lemma. □

By Lemma 3.18, every normal form mapping NF_i preserves sequences from W and the inverse mapping $^{-1}$ modulo $\sim$. On the other hand, concatenation on $\mathrm{Red}(H', t)$ is in general not preserved, but the following statement will suffice:

Lemma 3.20. *Let $v, w \in \mathrm{Red}(H', t)$ such that $v \cdot w$ is defined (as a reduced t-sequence). There are at most two $i \in \{1, \ldots, \lambda\}$ with $\mathrm{NF}_i(v) \cdot \mathrm{NF}_i(w) \not\sim \mathrm{NF}_i(v \cdot w)$.*

Proof. Since $\Rightarrow_i$ is confluent modulo $\sim$ we have $v \cdot w \overset{*}{\Rightarrow}_i \mathrm{NF}_i(v) \cdot \mathrm{NF}_i(w) \overset{*}{\Rightarrow}_i x \sim \mathrm{NF}_i(v \cdot w)$ for some x. Now assume that $\mathrm{NF}_i(v) \cdot \mathrm{NF}_i(w) \not\sim \mathrm{NF}_i(v \cdot w)$. Thus, $v \cdot w \overset{*}{\Rightarrow}_i \mathrm{NF}_i(v) \cdot \mathrm{NF}_i(w) \overset{j}{\Rightarrow}_i z$ for some position j and some sequence z. If $j \geq |\mathrm{NF}_i(v)|$, then we would have $\mathrm{NF}_i(w) \notin \mathrm{IRR}_i$. Similarly, if $j \leq |\mathrm{NF}_i(v)| - |r_{i-1} s_{11} x_f s_{11} r_i|$, then $\mathrm{NF}_i(v) \notin \mathrm{IRR}_i$. Thus, we obtain $0 < |\mathrm{NF}_i(v)| - j < |r_{i-1} s_{11} x_f s_{11} r_i|$. By applying Lemma 3.19 to every rewriting step in the derivations $v \overset{*}{\Rightarrow}_i \mathrm{NF}_i(v)$ and $w \overset{*}{\Rightarrow}_i \mathrm{NF}_i(w)$, it follows that $v \cdot w \overset{j'}{\Rightarrow}_i z'$ for some sequence z' and some position j' such that $0 < |v| - j' < |r_{i-1} s_{11} x_f s_{11} r_i|$.

Now assume that there are three different $i_1, i_2, i_3 \in \{1, \ldots, \lambda\}$ such that $\mathrm{NF}_{i_\ell}(v) \cdot \mathrm{NF}_{i_\ell}(w) \not\sim \mathrm{NF}_{i_\ell}(v \cdot w)$ for $\ell \in \{1, 2, 3\}$. By the above consideration, we obtain $v \cdot w \overset{j_\ell}{\Rightarrow}_{i_\ell} z_\ell$ for sequences z_1, z_2, z_3 and positions j_1, j_2, j_3 such that $0 < |v| - j_\ell < |r_{i-1} s_{11} x_f s_{11} r_i|$. W.l.o.g. assume that $j_1 \leq j_2 \leq j_3$. Then either $j_2 - j_1 < \frac{|r_{i-1} s_{11} x_f s_{11} r_i|}{2}$ or $j_3 - j_2 < \frac{|r_{i-1} s_{11} x_f s_{11} r_i|}{2}$. W.l.o.g. assume that $j_2 - j_1 < \frac{|r_{i-1} s_{11} x_f s_{11} r_i|}{2}$. Lemma 3.14 implies $j_2 = j_1$. But with $i_1 \neq i_2$ this leads to a contradiction. □

Recall that λ was chosen to be larger than $2d$, where d is the number of atomic propositions of the form $x \cdot y \sim z$ that occur in our boolean formula χ.

Lemma 3.21. *Let $x_j, y_j, z_j \in \mathrm{Red}(H', t)$ for $1 \leq j \leq d$. Then there exists $1 \leq i \leq \lambda$ such that for all $1 \leq j \leq d$, $x_j \cdot y_j \sim z_j$ if and only if $\mathrm{NF}_i(x_j) \cdot \mathrm{NF}_i(y_j) \sim \mathrm{NF}_i(z_j)$.*

Proof. The "only if"-direction follows from Lemma 3.20 and the fact that $\lambda > 2d$, where d is the number of equations in the formula χ. For the "if"-direction assume that $\mathrm{NF}_i(x_j) \cdot \mathrm{NF}_i(y_j) \sim \mathrm{NF}_i(z_j)$. Thus, $\mathrm{NF}_i(x_j) \cdot \mathrm{NF}_i(y_j) \in \mathrm{IRR}_i$, which implies $\mathrm{NF}_i(x_j \cdot y_j) \sim \mathrm{NF}_i(x_j) \cdot \mathrm{NF}_i(y_j) \sim \mathrm{NF}_i(z_j)$. Hence, it suffices to show that $\mathrm{NF}_i(u) \sim \mathrm{NF}_i(v)$ for $u, v \in \mathrm{Red}(H', t)$ implies $u \sim v$. For this, define a morphism $\sigma : (H')^f_k \to H'$ by $\sigma(k) = x_f$ and $\sigma(x) = x$ for all $x \in H'$, which is well-defined. This morphism can be extended to a mapping $\sigma : \mathrm{Red}((H')^f_k, t) \to \mathrm{Red}(H', t)$ in the natural way. Note that $p \sim q$ (for $p, q \in \mathrm{Red}((H')^f_k, t)$) implies $\sigma(p) \sim \sigma(q)$.

We claim that $p \Rightarrow_i q$ (for $p, q \in \mathrm{Red}((H')^f_k, t)$) implies $\sigma(p) \sim \sigma(q)$. If $p \Rightarrow_i q$ then there exist p', q' such that $p \sim p' \to_i q' \sim q$. This implies $\sigma(p) \sim \sigma(p') = \sigma(q') \sim \sigma(q)$, i.e., $\sigma(p) \sim \sigma(q)$.

Now assume that $\mathrm{NF}_i(u) \sim \mathrm{NF}_i(v)$ for $u, v \in \mathrm{Red}(H', t)$. Since $u \Rightarrow_i^* \mathrm{NF}_i(u)$ and $v \Rightarrow_i^* \mathrm{NF}_i(v)$, we obtain $u = \sigma(u) \sim \sigma(\mathrm{NF}_i(u)) \sim \sigma(\mathrm{NF}_i(v)) \sim \sigma(v) = v$. □

Now we are able to prove Lemma 3.13: Assume that

$$\forall x \in \{s \in \mathrm{Red}(H, t) \mid \mathrm{act}[s, X] = f\} \; \exists y_1 \cdots \exists y_m \left\{ \begin{array}{l} \bigwedge\limits_{1 \leq i \leq m} y_i \in \mathrm{Red}(H_i, t) \\ \wedge\, \chi(x, y_1, \ldots, y_m, \widetilde{w}) \end{array} \right\}$$

in $\mathrm{Red}(H', t)$. Let

$$s = r_0 s_{11} x_f s_{11} r_1 s_{11} x_f s_{11} r_2 \cdots s_{11} x_f s_{11} r_{\lambda-1} s_{11} x_f s_{11} r_\lambda \in \mathrm{Red}(H, t).$$

Note that $\mathrm{act}[s, X] = \mathrm{act}[x_f, X]^\lambda = \mathrm{act}[x_f, X] = f$ since $\lambda - 1$ is a multiple of $|X|!$. Thus, there exist sequences $t_i \in \mathrm{Red}(H_i, t)$ $(1 \leq i \leq m)$ with $\chi(s, t_1, \ldots, t_m, \widetilde{w})$ in $\mathrm{Red}(H', t)$. By Lemma 3.18 and Lemma 3.21 there exists $1 \leq j \leq \lambda$ such that $\chi(\mathrm{NF}_j(s), \mathrm{NF}_j(t_1), \ldots, \mathrm{NF}_j(t_m), \widetilde{w})$ in the structure $\mathrm{Red}((H')^f_k, t)$. Moreover, we have $\mathrm{NF}_j(t_i) \in \mathrm{Red}((H_i)^f_k, t)$. Since $\mathcal{R}$ has no long overlapping, there exists exactly one occurrence of $r_{j-1} s_{11} x_f s_{11} r_j$ in every sequence which is $\sim$-equivalent to s. Hence, we can write $s = v_1 \cdot x_f \cdot v_2$ and $\mathrm{NF}_j(s) \sim v_1 \cdot k \cdot v_2$ for $v_1, v_2 \in \mathrm{Red}(H, t)$. Thus,

$$\begin{aligned} f = \mathrm{act}[s, X] &= \mathrm{act}[v_1 \cdot x_f \cdot v_2, X] = \\ &\mathrm{act}[v_1, X] \circ \mathrm{act}[x_f, X] \circ \mathrm{act}[v_2, X] = \mathrm{act}[v_1, X] \circ f \circ \mathrm{act}[v_2, X] \end{aligned}$$

and

$$\exists y_1 \cdots \exists y_m \left\{ \begin{array}{l} \bigwedge\limits_{1 \leq i \leq m} y_i \in \mathrm{Red}((H_i)^f_k, t) \\ \wedge\, \chi(v_1 \cdot k \cdot v_2, y_1, \ldots, y_m, \widetilde{w}) \end{array} \right\} \text{ in } \mathrm{Red}((H')^f_k, t).$$

This finishes the proof of Lemma 3.13.

4 Amalgamated free products

In this section we consider positive theories of amalgamated free products. Let us fix throughout Section 4 two groups H and J where $A = H \cap J$ is a proper subgroup of both H and J. Let

$$G = H *_A J. \tag{14}$$

The aim of this section is to prove the following result:

Theorem 4.1. *Let $G = H *_A J$ be an amalgamated free product, where $A = H \cap J$ is a proper subgroup of both H and J and such that A is finite. If $\mathrm{Th}_{\exists+}(G)$ is decidable, then $\mathrm{Th}_+(G)$ is decidable.*

Remark 4.2. *Note that Theorem 3.1 cannot be extended by allowing monoids for H and J, since already the $\forall\exists^3$-theory of the free monoid $\{a,b\}^*$ is undecidable [7, 18].*

Let us first consider a special case of Theorem 4.1, namely the case that the index of A in H and J is both 2: $[H : A] = [J : A] = 2$. In this case, $G = H *_A J$ has $\mathbb{Z}$ as a subgroup of finite index [2, p. 31], hence, the whole first-order theory of G is decidable [8]. Thus, we may assume that either $[H : A] \geq 3$ or $[J : A] \geq 3$ in the following. W.l.o.g. we assume for the rest of Section 4 that $[J : A] \geq 3$.

4.1 Reduced (H, J)-sequences

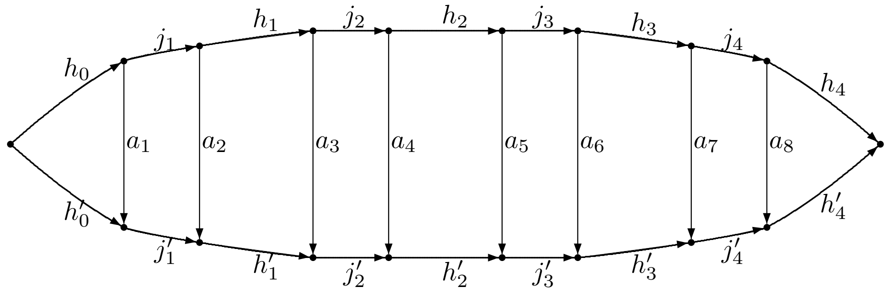
Recall from [14] that an (H, J)-*sequence* is an element from the free product $H * J$. Similarly to HNN-extensions, elements from $H *_A J$ can be represented by certain reduced sequences: An (H, J)-sequence s is *reduced* if either $s \in A$ or s does not contain a factor from A. Alternatively, we can view a reduced t-sequence as a word from the language $\mathrm{Red}(H, J) = A \cup \Gamma^* \setminus \Gamma^*\{xy \mid x, y \in H \text{ or } x, y \in J\}\Gamma^*$, where $\Gamma = (H \cup J) \setminus A$. For $u, v, w \in \mathrm{Red}(H, J)$ we write $u \cdot v = w$ if and only if $uv = w$ as words over the alphabet Γ. In this case, we also say that the *concatenation* $u \cdot v$ of u and v is defined. With $\sim$ we denote the smallest congruence on $H * J$ such that $j(ah) \sim (ja)h$ and $h(aj) \sim (ha)j$ for $a \in A$, $h \in H$, and $j \in J$. Then $u, v \in \mathrm{Red}(H, J)$ represent the same element of the amalgamated free product G if and only if $u \sim v$ [14]. Equivalently, if

$$u = h_0 j_1 h_1 j_2 \cdots h_{n-1} j_n h_n \text{ and} \tag{15}$$
$$v = h'_0 j'_1 h'_1 j'_2 \cdots h'_{m-1} j'_m h'_m \tag{16}$$

(with $n, m \geq 0$, $h_0, \cdots h_n, h'_0, \ldots, h'_m \in H$, and $j_1, \cdots j_n, j'_1, \ldots, j'_m \in J$) are reduced (H, J)-sequences, then $u \sim v$ if and only if $n = m$ and there exist $a_1, \ldots, a_{2n} \in A$ such that:

- $h_i a_{2i+1} = a_{2i} h'_i$ in H for $0 \leq i \leq n$ (here we set $a_0 = a_{2n+1} = 1$)
- $j_i a_{2i} = a_{2i-1} j'_i$ in J for $1 \leq i \leq n$

In other words, there exists a Van Kampen diagram of the following kind:



As for HNN-extensions, the elements a_i are called the *connecting elements* and occasionally we will omit in diagrams some of the connecting elements.

For the above $u \in \mathrm{Red}(H, J)$ in (15) let $u^{-1} = h_n^{-1} j_n^{-1} h_{n-1}^{-1} \cdots j_2^{-1} h_1^{-1} j_1^{-1} h_0^{-1}$. The length $|u|$ of $u \in \mathrm{Red}(H, J)$ is the number of occurences of letters from $(H \cup J) \setminus A$ in the sequence u. As for reduced t-sequences in the case of HNN-extensions, $u \sim v$ implies $|u| = |v|$. We identify the set $\mathrm{Red}(H, J)$ with the relational structure that contains the following predicates and constants:

- the ternary relation $\{(u, v, w) \mid u \cdot v \sim w\}$
- the ternary relation $\{(u, v, w) \mid u, v, w \in H, uv = w \text{ in } H\}$
- the ternary relation $\{(u, v, w) \mid u, v, w \in J, uv = w \text{ in } J\}$
- the binary relation $\{(u, v) \mid u \sim v^{-1}\}$
- every element of $\mathrm{Red}(H, J)$ as a constant

We will use the following lemma from [13]:

Lemma 4.3. *For a given boolean combination $\phi(x_1, \ldots, x_n)$ of word equations over the amalgamated free product G we can effectively construct an existential formula $\exists y_1 \cdots \exists y_m : \chi(x_1, \ldots, x_n, y_1, \ldots, y_m)$ over the structure $\mathrm{Red}(H, J)$ such that for all $s_1, \ldots, s_n \in \mathrm{Red}(H, J)$ we have:*

$$\phi(s_1, \ldots, s_n) \text{ in } G \quad \Leftrightarrow \quad \exists y_1 \cdots \exists y_m : \chi(x_1, \ldots, x_n, y_1, \ldots, y_m) \text{ in } \mathrm{Red}(H, J)$$

(here, when writing $\phi(s_1, \ldots, s_n)$ in G, we identify $s_i \in \mathrm{Red}(H, J)$ with the element from G it represents).

4.2 The finite normal subgroup X and stabilizing sequences

Analogously to Section 3.2 we define stabilizing reduced (H, J)-sequences and a normal finite subgroup X of A in this section.

For a subgroup $X \leq A$ and $g \in G$ we define a partial automorphism $\mathrm{act}[g, X] : X \to_p X$ by conjugation: $\mathrm{act}[g, X](y) = z$ if and only if $y, z \in X$ and $g^{-1} y g = z$. For a reduced (H, J)-sequence u, $\mathrm{act}[u, X]$ is defined as $\mathrm{act}[g, X]$, where g is the element of G represented by u. The goal of this section is to prove the following lemma:

Lemma 4.4. *There exists a finite subgroup $X \leq A$ and there exist sequences $s_{HH}, s_{JJ}, s_{JH}, s_{HJ} \in \mathrm{Red}(H,J)$ such that*

- $s_{\alpha\beta} \in (\alpha \setminus A) \cdot \mathrm{Red}(H,J) \cdot (\beta \setminus A)$,
- *X is a normal subgroup of G, i.e., for all $g \in G$: $\mathrm{act}[g,X]$ is an (totally defined) automorphism of X, and*
- *for all $a, b \in A$, if $a\, s_{\alpha\beta} = s_{\alpha\beta} b$ in G then $a = b \in X$.*

Recall that we assume $[J : A] \geq 3$ and that A is finite. For reasons, which will become clear in Section 4.3, we will assume the following weaker restriction in this Section 4.2:

$$[J : A] \geq 3 \text{ and } \exists h \in H \setminus A : A \cap hAh^{-1} \text{ is finite} \tag{17}$$

Choose an arbitrary $j \in J \setminus A$ and let

$$j' \in J \setminus (A \cup j^{-1}A), \tag{18}$$

which exists since $[J : A] \geq 3$. Next, let $h \in H \setminus A$ such that

$$Y = A \cap hAh^{-1}$$

is finite, which exists by assumption (17). Note that $ah = hb$ for $a, b \in A$ implies $a \in Y$.

We will first construct the sequences s_{JH} and s_{HJ} together with the normal and finite subgroup $X \leq A$. We will construct the subgroup X as the limit of a decreasing chain $Y \supseteq X_0 \supsetneq X_1 \supsetneq X_2 \cdots$. Let $\mathrm{act} = \mathrm{act}[hj, Y]$ and define the subgroup

$$X_0 = \{x \in Y \mid \forall k \geq 0 : \mathrm{act}^k(x) \text{ is defined}\}.$$

The restriction $\mathrm{act}{\restriction_{X_0}}$ is a permutation on the finite subgroup X_0. Hence we can fix a number $n \in \mathbb{N}$ such that $n > |Y|$ and $(\mathrm{act}{\restriction_{X_0}})^n = \mathrm{id}_{X_0}$.

Lemma 4.5. *For all $a, b \in A$, if $a\,(hj)^n = (hj)^n b$ in G then $a = b \in X_0$.*

Proof. Assume that $a\,(hj)^n = (hj)^n b$ in G for some $a, b \in A$, i.e., $(ah)j(hj)^{n-1} = (hj)^{n-1}h(jb)$. Since $(ah)j(hj)^{n-1}$ and $(hj)^{n-1}h(jb)$ are reduced (H,J)-sequences, we obtain a Van Kampen diagram of the following kind:

$$\begin{tikzcd}
\bullet \arrow[r, "hj"] \arrow[d, "a=a_0"'] & \bullet \arrow[r, "hj"] \arrow[d, "a_1"'] & \bullet \arrow[r, "hj"] \arrow[d, "a_2"'] & \bullet \arrow[r, dotted, no head] \arrow[d, "a_3"'] & \bullet \arrow[r, "hj"] \arrow[d, "a_{n-1}"'] & \bullet \arrow[d, "a_n = b"] \\
\bullet \arrow[r, "hj"'] & \bullet \arrow[r, "hj"'] & \bullet \arrow[r, "hj"'] & \bullet \arrow[r, dotted, no head] & \bullet \arrow[r, "hj"'] & \bullet
\end{tikzcd}$$

We get $a_0, \ldots, a_{n-1} \in Y$, $\mathrm{act}(a_i) = a_{i+1}$ for $0 \leq i < n-1$, and $\mathrm{act}[hj, A](a_{n-1}) = a_n$. Since $n > |Y|$ there are $0 \leq i < j \leq n-1$ such that $a_i = a_j$, i.e., act enters a cycle at a_i and $a_i \in X_0$. Since X_0 is closed under act and act^{-1}, we obtain $a, a_1, \ldots, a_{n-1}, b \in X_0$. Moreover, $(\mathrm{act}{\restriction_{X_0}})^n = \mathrm{id}_{X_0}$ implies $a = b$. $\square$

Let $s_0^{HJ} = (hj)^n$ and $s_0^{JH} = (j^{-1}h^{-1})^n$. Next we define $s_i^{JH}, s_i^{HJ} \in \mathrm{Red}(H,J)$ and a subgroup $X_i \leq Y$ for larger i inductively:

Assume that for some $i \geq 0$, reduced (H,J)-sequences $s_i^{JH}, s_i^{HJ} \in \mathrm{Red}(H,J)$ and a finite subgroup $X_i \leq A$ with the following properties are already defined:

- $s_i^{\alpha\beta} \in (\alpha \setminus A) \cdot \mathrm{Red}(H,J) \cdot (\beta \setminus A)$
- for all $a, b \in A$, if $a\, s_i^{\alpha\beta} = s_i^{\alpha\beta} b$ in G then $a = b \in X_i$

If for all $g \in G$, $\mathrm{act}[g, X_i]$ is totally defined, then we stop and set $s_{\alpha\beta} = s_i^{\alpha\beta}$ and $X = X_i$. Otherwise there exists $g \in G$ such that $\mathrm{act}[g, X_i]$ is not totally defined on X_i. We can assume that $g \in (H \cup J) \setminus A$.[3] Hence, we can choose elements $h_0 \in H \setminus A$ and $j_0 \in J \setminus A$ such that either $\mathrm{act}[h_0, X_i]$ is not totally defined on X_i or $\mathrm{act}[j_0, X_i]$ is not totally defined on X_i.

Let $s = s_i^{HJ} h_0 s_i^{JH} j_0 s_i^{HJ} \in \mathrm{Red}(H,J)$ and let $\mathrm{act} = \mathrm{act}[s, X_i]$. If $\mathrm{act}[h_0, X_i]$ is not totally defined on X_i, then $\mathrm{dom}(\mathrm{act}) \subsetneq X_i$ and if $\mathrm{act}[j_0, X_i]$ is not totally defined on X_i, then $\mathrm{ran}(\mathrm{act}) \subsetneq X_i$. Hence, act is not totally defined on X_i. Define

$$X_{i+1} = \{x \in X_i \mid \forall k \geq 0 : \mathrm{act}^k(x) \text{ is defined}\} < X_i.$$

Clearly, $\mathrm{act}\!\restriction_{X_{i+1}}$ is a permutation on X_{i+1}. Let m be such that $m + 1 > |X_i|$ and $(\mathrm{act}\!\restriction_{X_{i+1}})^m = \mathrm{id}_{X_{i+1}}$, and define

$$s_{i+1}^{HJ} = s^m.$$

The sequence s_{i+1}^{JH} is constructed similarly, we only have to take $s_{i+1}^{HJ} = s^m$ for $s = s_i^{JH} j_0 s_i^{HJ} h_0 s_i^{JH} \in \mathrm{Red}(H,J)$. By construction we have $s_{i+1}^{\alpha\beta} \in (\alpha \setminus A) \cdot \mathrm{Red}(H,J) \cdot (\beta \setminus A)$.

Lemma 4.6. *For all $a, b \in A$ and $\alpha\beta \in \{JH, HJ\}$, if $a\, s_{i+1}^{\alpha\beta} = s_{i+1}^{\alpha\beta} b$ in G, then $a = b \in X_{i+1}$.*

Proof. We restrict to the case that $\alpha\beta = HJ$, the other case can be dealt analogously. Assume that we have $a, b \in A$ with

$$a(s_i^{HJ} h_0 s_i^{JH} j_0 s_i^{HJ})^m = (s_i^{HJ} h_0 s_i^{JH} j_0 s_i^{HJ})^m b \text{ in } G.$$

We obtain a diagram of the following form, where $a_0 = a$, $a_{2m} = b$, and $a_0, a_1, \ldots, a_{2m} \in X_i$ due to the assumptions on s_i^{HJ} and s_i^{JH}:

$$\begin{tikzcd}[column sep=small]
\bullet \arrow[r, "s_i^{HJ}"] \arrow[d, "a_0"] & \bullet \arrow[r, "h_0"] \arrow[d, "a_0"] & \bullet \arrow[r, "s_i^{JH}"] \arrow[d, "a_1"] & \bullet \arrow[r, "j_0"] \arrow[d, "a_1"] & \bullet \arrow[r, "s_i^{HJ}"] \arrow[d, "a_2"] & \bullet \arrow[r, "s_i^{HJ}"] \arrow[d, "a_2"] & \bullet \arrow[r, "h_0"] \arrow[d, "a_2"] & \bullet \arrow[r, "s_i^{JH}"] \arrow[d, "a_3"] & \bullet \arrow[r, "j_0"] \arrow[d, "a_3"] & \bullet \arrow[r, "s_i^{HJ}"] \arrow[d, "a_4"] & \bullet \arrow[r, dotted, no head] \arrow[d, "a_4"] & \bullet \arrow[r, "s_i^{HJ}"] \arrow[d, "a_{2m-2}"] & \bullet \arrow[r, "h_0"] \arrow[d] & \bullet \arrow[r, "s_i^{JH}"] \arrow[d, "a_{2m-1}"] & \bullet \arrow[r, "j_0"] \arrow[d] & \bullet \arrow[r, "s_i^{HJ}"] \arrow[d, "a_{2m}"] & \bullet \arrow[d, "a_{2m}"] \\
\bullet \arrow[r, "s_i^{HJ}"'] & \bullet \arrow[r, "h_0"'] & \bullet \arrow[r, "s_i^{JH}"'] & \bullet \arrow[r, "j_0"'] & \bullet \arrow[r, "s_i^{HJ}"'] & \bullet \arrow[r, "s_i^{HJ}"'] & \bullet \arrow[r, "h_0"'] & \bullet \arrow[r, "s_i^{JH}"'] & \bullet \arrow[r, "j_0"'] & \bullet \arrow[r, "s_i^{HJ}"'] & \bullet \arrow[r, dotted, no head] & \bullet \arrow[r, "s_i^{HJ}"'] & \bullet \arrow[r, "h_0"'] & \bullet \arrow[r, "s_i^{JH}"'] & \bullet \arrow[r, "j_0"'] & \bullet \arrow[r, "s_i^{HJ}"'] & \bullet
\end{tikzcd}$$

[3]Since $H \cup J$ generates G, we can assume that $g \in H \cup J$. If $g = a \in A$ but $\mathrm{act}[h, X_i]$ is a permutation on X_i for all $h \in H \setminus A$, then set $h' = ha \in H \setminus A$. We obtain that also $\mathrm{act}[h', X_i]$ is not totally defined on X_i, a contradiction.

Hence, $\mathrm{act}(a_{2i}) = a_{2i+2}$ for $0 \leq i < m$. Since $m + 1 > |X_i|$, there are $i < j$ with $a_{2i} = a_{2j}$. Thus, act enters a cycle at a_{2i}, i.e., $a_{2i} \in X_{i+1}$. But since X_{i+1} is closed under act and act^{-1}, we get $a, a_2, \ldots, a_{2(m-1)}, b \in X_{i+1}$. Moreover, $(\mathrm{act}\restriction_{X_{i+1}})^m = \mathrm{id}_{X_{i+1}}$ implies $a = b$. $\square$

This concludes the construction of the sequences s_{HJ} and s_{JH} as well as the normal finite subgroup $X \leq A$. In order to construct s_{HH} note that $s_{HJ} = s \cdot j$ for some sequence s and that j' was chosen in (18) such that $j' \in J \setminus (A \cup j^{-1}A)$, i.e., $jj' \notin A$. Now define

$$s_{HH} = s_{HJ}\, s\,(jj')\, h\,(j'h)^{|X|!-1} s_{JH} \in (H \setminus A) \cdot \mathrm{Red}(H, J) \cdot (H \setminus A).$$

In the group G, this sequence equals $s_{HJ} s_{HJ}\,(j'h)^{|X|!} s_{JH}$. Now assume that $as_{HH} = s_{HH} b$ in G for some $a, b \in A$. We have to show that $a = b \in X$. From $as_{HH} = s_{HH} b$ and the properties of s_{HJ} and s_{JH} we obtain the following Van Kampen diagram, where $a, b \in X$.

$$\begin{tikzcd}
\bullet \arrow[r, "s_{HJ}"] \arrow[d, "a"'] & \bullet \arrow[r, "s\,(jj')\,h\,(j'h)^{|X|!-1}"] \arrow[d, "a"'] & \bullet \arrow[r, "s_{JH}"] \arrow[d, "b"'] & \bullet \arrow[d, "b"] \\
\bullet \arrow[r, "s_{HJ}"'] & \bullet \arrow[r, "s\,(jj')\,h\,(j'h)^{|X|!-1}"'] & \bullet \arrow[r, "s_{JH}"'] & \bullet
\end{tikzcd}$$

Moreover, we have $b = \mathrm{act}[s_{HH}, X](a) = \mathrm{act}[s_{HJ} s_{HJ}\,(j'h)^{|X|!} s_{JH}, X](a) = a$.

Finally, it remains to construct s_{JJ}. We set

$$s_{JJ} = s_{JH} j'(s_{HH}(jj'))^{|X!|-1} s_{HH} j s_{HJ} \in (J \setminus A) \cdot \mathrm{Red}(H, J) \cdot (J \setminus A),$$

which is a reduced (H, J)-sequence, since $jj' \in J \setminus A$. Note that $\mathrm{act}[s_{JJ}, X] = \mathrm{act}[s_{JH}(j' s_{HH} j)^{|X!|} s_{HJ}, X] = \mathrm{id}_X$. This concludes the proof of Lemma 4.4.

4.3 Reducing to the existential positive theory

The reduction of the positive theory of the amalgamated free product $G = H *_A J$ to the existential positive theory of G is very similar to the case of an HNN-extension in Section 3.3: Given a positive sentence θ, which is interpreted over G, we construct an *existential positive sentence* θ', which is interpreted over a multiple HNN-extension $\mathbb{G}$ of G, where only finite subgroups of $A \leq G$ are associated (in fact, $X \subseteq A$ from Lemma 4.4 will be associated with itself).

Let us fix a formula

$$\theta(\widetilde{z}) \;\equiv\; \forall x_1 \exists y_1 \cdots \forall x_n \exists y_n\, \phi(x_1, \ldots, y_n, y_1, \ldots, y_n, \widetilde{z}),$$

with ϕ a positive boolean combination of word equations (with constants) over the group G. Let $X \leq A$ be the subgroup from Lemma 4.4. Recall that with $\mathrm{In}(X, G)$ we denote the group of all automorphisms f of X such that for some $g \in G$ we have: $f(c) = g^{-1} c g$ for all $c \in X$. In the following, we use the abbreviation $\mathrm{In} = \mathrm{In}(X, G)$.

The following theorem yields the reduction from the positive to the existential positive theory; $k_1, \ldots, k_n \notin G$ are new constants.

Theorem 4.7. *Let $\theta(\widetilde{z}) \equiv \forall x_1 \exists y_1 \cdots \forall x_n \exists y_n\, \phi(x_1, \ldots, x_n, y_1, \ldots, y_n, \widetilde{z})$ be as above. For all $\widetilde{u} \in G$ we have $\theta(\widetilde{u})$ in G if and only if*

$$\bigwedge_{f_1 \in \mathrm{In}} \exists y_1 \cdots \bigwedge_{f_n \in \mathrm{In}} \exists y_n \left\{ \begin{array}{l} \bigwedge_{1 \le i \le n} y_i \in G^{f_1, \ldots, f_i}_{k_1, \ldots, k_i} \wedge \\ \phi(k_1, \ldots, k_n, y_1, \ldots, y_n, \widetilde{u}) \end{array} \right\} \text{ in } G^{f_1, \ldots, f_n}_{k_1, \ldots, k_n}. \tag{19}$$

Theorem 4.7 will be deduced completely analogous to Theorem 3.10. The only new ingredient will be the proof of Lemma 4.8 below, which corresponds to Lemma 3.13.

Fix a number $m \in \mathbb{N}$, groups $H_1, \ldots, H_m, H'$ such that $H \subseteq H_i \subseteq H'$ and $H_i \cap J = H' \cap J = H \cap J = A$ for $1 \le i \le m$. Let $G_i = H_i *_A J$ and $G' = H' *_A J$. Thus, elements from G' (resp. G_i) can be represented by elements from $\mathrm{Red}(H', J)$ (resp. $\mathrm{Red}(H_i, J)$). Let $k \notin G'$ be a new constant, let $f \in \mathrm{In}$, and let $\widetilde{w} = (w_1, \ldots, w_N)$, where $w_i \in \mathrm{Red}(H, J)$ is a reduced (H, J)-sequence. Recall from Section 4.1 that we view $\mathrm{Red}(F, J)$ (where F is some base group) as a relational structure equipped with the multiplication in the base groups F and J and the concatenation and inversion of reduced (F, J)-sequences.

Lemma 4.8. *Let $\chi(x, y_1, \ldots, y_m, \widetilde{z})$ be a (not necessarily positive) boolean formula over the signature of the structure $\mathrm{Red}(H', J)$ and with constants from $\mathrm{Red}(H, J)$. If*

$$\forall x \in \{u \in \mathrm{Red}(H, J) \mid \mathrm{act}[u, X] = f\}\ \exists y_1 \cdots \exists y_m \left\{ \begin{array}{l} \bigwedge_{1 \le i \le m} y_i \in \mathrm{Red}(H_i, J) \\ \wedge\, \chi(x, y_1, \ldots, y_m, \widetilde{w}) \end{array} \right\}$$

in $\mathrm{Red}(H', J)$, then there are $v_1, v_2 \in \mathrm{Red}(H, J)$ with $\mathrm{act}[v_1, X] \circ f \circ \mathrm{act}[v_2, X] = f$ and

$$\exists y_1 \cdots \exists y_m \left\{ \begin{array}{l} \bigwedge_{1 \le i \le m} y_i \in \mathrm{Red}((H_i)^f_k, J) \\ \wedge\, \chi(v_1 \cdot k \cdot v_2, y_1, \ldots, y_m, \widetilde{w}) \end{array} \right\} \text{ in } \mathrm{Red}((H')^f_k, J).$$

Remark 4.9. *The reader may observe some asymmetry in the above consideration: We put the new generator k into the left factor (which is initially H) of the amalgamated free product. But this is an arbitrary choice. If G_1 and G_2 are groups such that $G_1 \cap G_2 = A$ is a subgroup of G_1 and G_2, $X \le A$, and f is an automorphism of X, then $(G_1)^f_k *_A G_2 = G_1 *_A (G_2)^f_k$. In particular, in Theorem 4.7 one gets $G^{f_1, \ldots, f_i}_{k_1, \ldots, k_i} \simeq H^{f_1, \ldots, f_i}_{k_1, \ldots, k_i} *_A J \simeq H *_A J^{f_1, \ldots, f_i}_{k_1, \ldots, k_i}$.*

4.4 Proof of Lemma 4.8

The following data were already fixed:

- the finite normal subgroup $X \le A$ and the elements $s_{\alpha\beta}$ from Lemma 4.4

- $f \in \mathrm{In}$
- the sets $\mathrm{Red}(H,J) \subseteq \mathrm{Red}(H_i,J) \subseteq \mathrm{Red}(H',J) \subseteq \mathrm{Red}((H')^f_k,J)$ of reduced sequences from Section 4.3
- elements $w_1,\ldots,w_N \in \mathrm{Red}(H,J)$ from Section 4.3

Moreover, let us fix a (not necessarily positive) boolean formula $\chi(x,y_1,\ldots,y_m,\widetilde{z})$ over the signature of the structure $\mathrm{Red}(H',J)$. Thus, χ is a boolean combination of propositions of the form $x\cdot y \sim z$, $x \sim y^{-1}$, and $xy = z$ in the base group H' or J, where x, y, and z are either variables or constants from $\mathrm{Red}(H',J)$. Let W be the union of $\{w_1,\ldots,w_N\}$ and the set of all constants appearing in χ and let d be the number of atomic propositions of the form $x\cdot y \sim z$ that occur in χ. Choose a number $\lambda > 2d$ such that $|X|!$ divides $\lambda - 1$. Finally, choose an element $x_f \in \mathrm{Red}(H,J)$ such that $\mathrm{act}[x_f,X] = f$, which exists since $f \in \mathrm{In}$. By appending, if necessary, suitable sequences $s_{\alpha\beta}$ to the left (right) of x_f, we may w.l.o.g. assume that $x_f = (H\setminus A)\cdot \mathrm{Red}(H,J)\cdot(H\setminus A)$.

Fix an element $h \in H\setminus A$ and two elements $j_0, j_1 \in J\setminus A$ with $j_1 \notin j_0A$. Since we assume that $[J:A] \geq 3$, j_0 and j_1 exist.

A *J-system of degree n* ($n \geq 2$) is a tuple $\mathcal{R} = (r_0,\ldots,r_\lambda)$ with

$$r_i \in \{(hj_0)^{|X|!}, (hj_1)^{|X|!}\}^n.$$

There are $2^{n(\lambda+1)}$ J-systems of degree n. Note that $r_{i-1}s_{HJ}x_f s_{JJ} r_i \in \mathrm{Red}(H,J)$. The J-system $\mathcal{R} = (r_0,\ldots,r_\lambda)$ has *no long overlapping*, if for all $0 \leq i,j \leq \lambda$ and all $\alpha,\beta \in \{1,-1\}$ we have:[4] if $r_i^\alpha = u_1\cdot u_2$, $r_j^\beta = v_1 \cdot v_2$, $|u_2| = |v_1| \geq \frac{|r_i| - |s_{HJ}x_f s_{JJ}|}{2}$, and there exist $a,b \in A$ with $av_1 = u_2 b$ in G, then: $u_1 = v_2 = \varepsilon$, $i = j$, and $\alpha = \beta$.

The next lemma follows immediately from the previous definition:

Lemma 4.10. *Assume that $\mathcal{R}$ has no long overlapping. If*

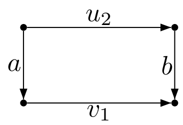
$$(r_{i-1}s_{HJ}x_f s_{JJ} r_i)^\alpha \sim p \cdot r_j^\beta \cdot q$$

for $p,q \in \mathrm{Red}(H,J)$ and $\alpha,\beta \in \{1,-1\}$, then either $p = \varepsilon$ or $q = \varepsilon$, i.e., r_j^β cannot be properly contained in a segment which is opposite to a segment $(r_{i-1}s_{HJ}x_f s_{JJ} r_i)^\alpha$ in a diagram.

Note the difference between the definition of a J-system without long overlappings and a t-system without long overlappings in Section 3.4. For t-systems we formulated the restrictions concerning overlappings in terms of the projections $\pi_t(r_i^\alpha)$ ($\alpha \in \{1,-1\}$). One might think that for J-systems we may use the projections of the sequences r_i^α onto the letters j_i^α ($\alpha \in \{1,-1\}$, $i \in \{0,1\}$). But this would not work. For reduced t-sequences, it was crucial that $u \sim v$ implies $\pi_t(u) = \pi_t(v)$. A corresponding property for reduced (H,J)-sequences does not hold: for instance, for every choice of $j_0 \in J\setminus A$ above, we may have $j_0^{-1} \in Aj_0A$.

[4] Recall that the length of a sequence $s \in \mathrm{Red}(H,J)$ was defined as the the number of occurences of symbols from $(H \cup J)\setminus A$ in the sequence s.

Hence we may have $j_0 \sim j_0^{-1}$. Therefore, in the above definition, we have to exclude long overlappings by directly forbidding certain Van Kampen diagrams in order to obtain Lemma 4.10: Note that excluding an identity $av_1 = u_2 b$ in the group G (with u_2 a "long" suffix of some r_i^α and v_1 a "long" prefix of some r_j^β), means that we exclude the existence of a Van Kampen diagram of the following form:

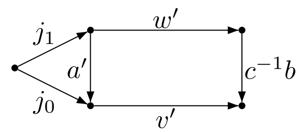


For reduced t-sequences, in order to exclude such a diagram, one only has to require $\pi_t(u_2) \neq \pi_t(v_1)$. Nevertheless, thanks to the finiteness of A, we can prove the existence of J-systems (of sufficiently high degree) without long overlapping:

Lemma 4.11. *There exists n_0 (depending only on λ) such that for all $n \geq n_0$ there exists a J-system of degree n without long overlapping.*

Proof. Analogously to the proof of Lemma 3.15 it suffices to show that if the J-system $\mathcal{R} = (r_0, \ldots, r_\lambda)$ has a long overlapping, then it can be described with strictly less than $n(\lambda + 1)$ bits. Again, we distinguish four cases:

Case 1: for some $\alpha \in \{1, -1\}$ and some $0 \leq i, j \leq \lambda$ with $i \neq j$, r_i^α and r_j^α have a long overlapping. Thus, assume that $r_i^\alpha = u_1 \cdot u_2$, $r_j^\alpha = v_1 \cdot v_2$, $|u_2| = |v_1| \geq \frac{|r_i| - |s_{HJ} x_f s_{JJ}|}{2}$, and $av_1 = u_2 b$ in G for some $a, b \in A$. W.l.o.g. assume that $\alpha = 1$. We first claim that the sequence v_1 can be reconstructed from the sequence u_2, and $a \in A$: We know that $v_1 \in \mathrm{Red}(H, J)$ is a sequence over the letter h, j_0, j_1. Assume that $w \in \mathrm{Red}(H, J)$ is a sequence over the letters h, j_0, j_1 such that $aw = u_2 c$ in G for some $c \in A$. Thus, $v_1 = w(c^{-1}b)$ in G. This implies $|v_1| = |w|$. We have to show that $v_1 = w$ (as reduced (H, J)-sequences). We prove this by induction over $|v_1| = |w|$. If $|v_1| = 0$, then $v_1 = \varepsilon = w$. If $v_1 = h \cdot v'$, then we must have also $w = h \cdot w'$ for some sequence w'. It follows $v' = w'(c^{-1}b)$ in G. Inductively we obtain $v' = w'$ and thus $v_1 = w$. Now assume that (w.l.o.g.) $v_1 = j_0 \cdot v'$. If also $w = j_0 \cdot w'$ for some w', then we can conclude as above. Hence, assume that $w = j_1 \cdot w'$. We obtain a Van Kampen diagram of the following form, where $a' \in A$:



Thus, $j_1 \in j_0 A$, which contradicts our choice for j_0 and j_1.

From the above consideration, it follows that r_j can be reconstructed from the triple (i, a, v_2) (note that the length of v_1 can be calculated from $|v_2|$). Hence, in the description of $\mathcal{R}$ we can save at least $\frac{|r_i| - |s_{HJ} x_f s_{JJ}|}{2} \frac{1}{2|X|!} - O(\lambda + |A|) =$

$\frac{2n|X|!-|s_{HJ}x_f s_{JJ}|}{2} \cdot \frac{1}{2|X|!} - O(1) = \frac{n}{2} - O(1)$ many bits. For a sufficiently large n, this term is strictly greater than 0; note that $|s_{HJ}x_f s_{JJ}|$, λ, and $|A|$ are constants.

Case 2: for some $0 \leq i \leq \lambda$, r_i has a long overlapping with itself. Thus, assume that $r_i = u_1 \cdot u' = v_1 \cdot v_2$, $|u'| = |v_1| \geq \frac{|r_i|-|s_{HJ}x_f s_{JJ}|}{2}$, and $av_1 = u'b$ in G for some $a, b \in A$, see the following diagram:

$$\begin{tikzcd}
\bullet \arrow[r, dotted, "u_1"] & \bullet \arrow[r, "u'"] \arrow[d, "a"'] & \bullet \arrow[d, "b"] & \\
& \bullet \arrow[r, "v_1"'] & \bullet \arrow[r, dotted, "v_2"'] & \bullet
\end{tikzcd}$$

It follows that there exists $p > 1$, a factorization $r_i = u_1 \cdot u_2 \cdots u_p$, and $a_1, \ldots, a_p \in A$ (we have $a_1 = a$ and $a_p = b$) such that

- $|u_1| = |u_2| = \cdots |u_{p-1}| \geq |u_p|$,
- $a_{i-1}u_{i-1} = u_i a_i$ in G for $1 < i \leq p-1$, and
- $a_{p-1}w = u_p a_p$ in G, where w is the prefix of u_{p-1} of length $|u_p|$,

see also the following diagram:

$$\begin{tikzcd}
\bullet \arrow[r, dotted, "u_1"] & \bullet \arrow[r, "u_2"] \arrow[d, "a_1"'] & \bullet \arrow[r, "u_3"] \arrow[d, "a_2"'] & \bullet \arrow[r, dotted] \arrow[d, "a_3"'] & \bullet \arrow[r, "u_{p-1}"] \arrow[d, "a_{p-2}"'] & \bullet \arrow[r, "u_p"] \arrow[d, "a_{p-1}"'] & \bullet \arrow[d, "a_p"] & & \\
& \bullet \arrow[r, "u_1"'] & \bullet \arrow[r, "u_2"'] & \bullet \arrow[r, dotted] & \bullet \arrow[r, "u_{p-2}"'] & \bullet \arrow[r, "w"'] & \bullet \arrow[r, dotted] & \bullet \arrow[r, dotted, "u_p"'] & \bullet
\end{tikzcd}$$

We claim that r_i can be reconstructed from the pair (u_1, a_1): First, u_1 and a_1 determine u_2. The idea is the same as in Case 1. If $x \in \mathrm{Red}(H, J)$ is a sequence over the letters h, j_0, j_1 with $a_1 u_1 = xc$ in G (for some $c \in A$), then $xc = u_2 a_2$, i.e., $u_2 = x(ca_2^{-1})$ in G. We then obtain $u_2 = x$ as in Case 1. Next from u_1, u_2, and a_1 we can determine $a_2 \in A$ by the equation $a_1 u_1 = u_2 a_2$. Having u_2 and a_2 available, we can determine u_3. We continue in this way.

By the previous paragraph, in the description of $\mathcal{R}$ we can save at least $\frac{|r_i|-|s_{HJ}x_f s_{JJ}|}{2} \frac{1}{2|X|!} - O(1) = \frac{n}{2} - O(1)$ many bits.

Case 3: for some $0 \leq i, j \leq \lambda$ with $i \neq j$, r_i and r_j^{-1} have a long overlapping. This case is analogous to Case 1.

Case 4: for some $0 \leq i \leq \lambda$, r_i and r_i^{-1} have a long overlapping. Hence, $r_i = u_1 \cdot u_2$, $r_i^{-1} = v_1 \cdot v_2$, $|u_2| = |v_1| \geq \frac{|r_i|-|s_{HJ}x_f s_{JJ}|}{2}$, and $av_1 = u_2 b$ in G for some $a, b \in A$. Thus, we have a diagram of the following form:

$$\begin{tikzcd}
\bullet \arrow[r, dotted, "u_1"] & \bullet \arrow[r, "u_2"] \arrow[d, "a"'] & \bullet \arrow[d, "b"] & \\
& \bullet \arrow[r, "v_1"'] & \bullet \arrow[r, dotted, "v_2"'] & \bullet
\end{tikzcd}$$

From $r_i^{-1} = v_1 \cdot v_2$ we get $r_i = v_2^{-1} \cdot v_1^{-1} = u_1 \cdot u_2$. With $|u_2| = |v_1| = |v_1^{-1}|$ we get $v_1 = u_2^{-1}$, i.e., $au_2^{-1} = u_2 b$ in G. Assume that $|u_2|$ is even (the case that $|u_2|$ is odd is similar) and write $u_2 = w_1 \cdot w_2$ with $|w_1| = |w_2|$. Thus, the above diagram looks as follows:

$$\begin{tikzcd}
\bullet \arrow[r, dotted, "u_1"] & \bullet \arrow[r, "w_1"] \arrow[d, "a"'] & \bullet \arrow[r, "w_2"] \arrow[d, "c"'] & \bullet \arrow[d, "b"'] & \\
& \bullet \arrow[r, "w_2^{-1}"'] & \bullet \arrow[r, "w_1^{-1}"'] & \bullet \arrow[r, dotted, "v_2"'] & \bullet
\end{tikzcd}$$

But then we can shorten the description of $\mathcal{R}$ to less than $n(\lambda+1)$ bits as follows: Instead of writing down r_i using n bits, we write down the triple (u_1, w_1, a). From w_1 and a we can reconstruct w_2^{-1} in the same way as v_1 was reconstructed from u_2 and a in Case 1. This saves at least $\frac{|u_2|}{2} \cdot \frac{1}{2|X|!} - O(1) \geq \frac{|r_i| - |s_{HJ} x_f s_{JJ}|}{4} \cdot \frac{1}{2|X|!} - O(1) = \frac{n}{4} - O(1)$ many bits. $\square$

The proof of Lemma 4.11 is the only place, where we need the assumption that A is finite.

Remark 4.12. *With some other restrictions on J and A, we can prove the existence of a J-system without long overlapping also in the case that A is not necessarily finite. Recall that a double coset of A in J is a set of the form AjA for some $j \in J$. The group J can be partitioned into double cosets of A. Now assume for a moment that there are at least three double cosets of A in J. Clearly, A is one of them. If follows that we can choose $j_0, j_1 \in J$ such that (i) $j_0, j_1 \notin A$ and (ii) $j_1 \notin Aj_0A$. With these restrictions, it is not difficult to prove again the existence of a J-system without long overlapping. The proof is similar to the proof of Lemma 4.11. One only has to notice that in each of the four cases, we never have to specify an element from the subgroup A in order to reduce the size of the description of the J-system $\mathcal{R}$. Since the finiteness of A was only used in the proof of Lemma 4.11, it follows together with the weaker restrictions (17), which where sufficient in order to prove the main Lemma 4.4 from Section 4.2, that* $\mathrm{Th}_+(G)$ *can be reduced to* $\mathrm{Th}_\exists(G)$ *also in case one of the following restrictions hold for $G = H *_A J$:*

- *$[H : A] = [J : A] = 2$ or*
- *A has at least three double cosets in H (this implies that $[H : A] \geq 3$) and $\exists j \in J \setminus A : A \cap jAj^{-1}$ finite or*
- *A has at least three double cosets in J (this implies that $[J : A] \geq 3$) and $\exists h \in H \setminus A : A \cap hAh^{-1}$ finite.*

Let us fix a J-system $\mathcal{R} = (r_0, \ldots, r_\lambda)$ of degree n without long overlapping, where moreover $|r_{i-1} s_{HJ} x_f s_{JJ} r_i| > |w|$ for all $w \in W$. For $1 \leq i \leq \lambda$, $u, v \in \mathrm{Red}((H')^f_k, J)$, and $0 \leq j \leq |u|$ we write $u \xrightarrow{j}_i v$ if there exist $u_1, u_2 \in \mathrm{Red}((H')^f_k, J)$ and $\alpha \in \{1, -1\}$ such that

- $u = u_1 \cdot (r_{i-1} s_{HJ} x_f s_{JJ} r_i)^\alpha \cdot u_2$,
- $v = u_1 \cdot (r_{i-1} s_{HJ} k s_{JJ} r_i)^\alpha \cdot u_2$, and
- $|u_1| = j$

We write $u \Rightarrow_i v$ if there exist $u', v' \in \mathrm{Red}((H')^f_k, J)$ and $0 \leq j \leq |u| = |u'|$ such that $u \sim u' \xrightarrow{j}_i v' \sim v$. Clearly, the relation $\Rightarrow_i$ is terminating. Let $\mathrm{IRR}_i = \{u \mid \neg\exists v : u \Rightarrow_i v\}$. Note that $W \subseteq \mathrm{IRR}_i$ by the choice of n, Moreover, $s \Rightarrow_i t$ implies also $s^{-1} \Rightarrow_i t^{-1}$.

The next four lemmas can be shown analogously to the corresponding lemmas in Section 3.4.

Lemma 4.13. *The relation $\Rightarrow_i$ is confluent modulo $\sim$, i.e., $u \;{}_i\!\overset{*}{\Leftarrow} v \overset{*}{\Rightarrow}_i w$ implies that $u \sim w$ or there exists $p \in \mathrm{Red}((H')^f_k, J)$ such that $u \overset{*}{\Rightarrow}_i p \;{}_i\!\overset{*}{\Leftarrow} w$.*

The previous lemma implies that for every $1 \leq i \leq \lambda$ and every sequence $u \in \mathrm{Red}((H')^f_k, J)$, if $u \overset{*}{\Rightarrow}_i v \in \mathrm{IRR}_i$ and $u \overset{*}{\Rightarrow}_i w \in \mathrm{IRR}_i$, then $v \sim w$. Let $\mathrm{NF}_i(u)$ denote an arbitrary sequence with $u \overset{*}{\Rightarrow}_i \mathrm{NF}_i(u) \in \mathrm{IRR}_i$; it is unique up to $\sim$. Note that if the concatenation $u \cdot v$ of u and v is defined then also the concatenation $\mathrm{NF}_i(u) \cdot \mathrm{NF}_i(v)$ is defined.

Lemma 4.14. *For all $1 \leq i \leq \lambda$ we have:*

- *$\mathrm{NF}_i(w) \sim w$ for all $w \in W$,*
- *if $u \sim v^{-1}$ for $u, v \in \mathrm{Red}(H', J)$, then $\mathrm{NF}_i(u) \sim \mathrm{NF}_i(v)^{-1}$.*

Lemma 4.15. *Let $v, w \in \mathrm{Red}(H', J)$ such that $v \cdot w$ is defined (as a reduced (H', J)-sequence). There are at most two $i \in \{1, \ldots, \lambda\}$ with $\mathrm{NF}_i(v) \cdot \mathrm{NF}_i(w) \not\sim \mathrm{NF}_i(v \cdot w)$.*

Lemma 4.16. *Let $x_j, y_j, z_j \in \mathrm{Red}(H', J)$ for $1 \leq j \leq d$. Then there exists $1 \leq i \leq \lambda$ such that for all $1 \leq j \leq d$, $x_j \cdot y_j \sim z_j$ if and only if $\mathrm{NF}_i(x_j) \cdot \mathrm{NF}_i(y_j) \sim \mathrm{NF}_i(z_j)$.*

Now, Lemma 4.8 can be shown analogously to Lemma 3.13: Assume that

$$\forall x \in \{s \in \mathrm{Red}(H, J) \mid \mathrm{act}[s, X] = f\} \; \exists y_1 \cdots \exists y_m \left\{ \begin{array}{c} \bigwedge\limits_{1 \leq i \leq m} y_i \in \mathrm{Red}(H_i, J) \\ \wedge\, \chi(x, y_1, \ldots, y_m, \widetilde{w}) \end{array} \right\}$$

in $\mathrm{Red}(H', J)$. Let

$$s = r_0 s_{HJ} x_f s_{JJ} r_1 s_{HJ} x_f s_{JJ} r_2 \cdots s_{HJ} x_f s_{JJ} r_{\lambda-1} s_{HJ} x_f s_{JJ} r_\lambda \in \mathrm{Red}(H, J).$$

Note that $\mathrm{act}[s, X] = \mathrm{act}[x_f, X]^\lambda = \mathrm{act}[x_f, X] = f$ since $\lambda - 1$ is a multiple of $|X|!$. Thus, there exist sequences $t_i \in \mathrm{Red}(H_i, J)$, $1 \leq i \leq m$, with $\chi(s, t_1, \ldots, t_m, \widetilde{w})$ in $\mathrm{Red}(H', J)$. By Lemma 4.14 and Lemma 4.16 there exists $1 \leq j \leq \lambda$ such that $\chi(\mathrm{NF}_j(s), \mathrm{NF}_j(t_1), \ldots, \mathrm{NF}_j(t_m), \widetilde{w})$ in $\mathrm{Red}((H')^f_k, J)$. Since

$\mathcal{R}$ has no long overlapping, there exists exactly one occurrence of $r_{j-1}s_{HJ}x_f s_{JJ}r_j$ in every sequence which is $\sim$-equivalent to s. Hence, we can write $s = v_1 \cdot x_f \cdot v_2$ and $\mathrm{NF}_j(s) \sim v_1 \cdot k \cdot v_2$ for some $v_1, v_2 \in \mathrm{Red}(H, J)$. Thus,

$$f = \mathrm{act}[s, X] = \mathrm{act}[v_1 \cdot x_f \cdot v_2, X] = \\ \mathrm{act}[v_1, X] \circ \mathrm{act}[x_f, X] \circ \mathrm{act}[v_2, X] = \mathrm{act}[v_1, X] \circ f \circ \mathrm{act}[v_2, X]$$

and

$$\exists y_1 \cdots \exists y_m \left\{ \begin{array}{l} \bigwedge\limits_{1 \le i \le m} y_i \in \mathrm{Red}((H_i)_k^f, J) \\ \wedge\, \chi(v_1 \cdot k \cdot v_2, y_1, \ldots, y_m, \widetilde{w}) \end{array} \right\} \text{ in } \mathrm{Red}((H')_k^f, J).$$

This finishes the proof of Lemma 4.8.

5 Applications

The number of ends of a group G is, roughly speaking, the maximal number of connected components in the Cayley-graph of G which can be obtained by removing an arbitrary finite set of nodes, see e.g. [4] for more details. It is well known that the number of ends of G is either 1, 2, or ∞. Moreover, a famous result of Stallings states that a group G has more than one end if and only if it can be written as $G = H *_A J$ or $G = \langle H, t; t^{-1}at = \varphi(a)(a \in A)\rangle$ with A finite [24]. Hence we obtain:

Theorem 5.1. *If the group G has more than one end and $\mathrm{Th}_{\exists+}(G)$ is decidable, then $\mathrm{Th}_+(G)$ is decidable.*

Recall that a group is virtually free if it has a free subgroup of finite index. Every virtually-free group has more than one end. Moreover, in [13], we have shown that every virtually-free group has a decidable existential theory. Thus, Theorem 5.1 implies:

Theorem 5.2. *Let G be a virtually-free group. Then $\mathrm{Th}_+(G)$ is decidable.*

In [20, 23], it is shown that the existential theory of a torsion-free hyperbolic group is decidable. Again, with Theorem 5.1 we get:

Theorem 5.3. *Let G be a torsion-free hyperbolic group. If G has more than one end, then $\mathrm{Th}_+(G)$ is decidable.*

It should be noted that the statements of Theorem 5.2 and Theorem 5.3 are orthogonal: By a result of Stallings [24], a torsion-free virtually-free group is already free.

6 Open problems

We presented quite general conditions under which the positive theory of a group G can be reduced to the existential positive theory of G. To the knowledge of the authors there is currently no example of a group G such that the existential positive theory of G is decidable but the positive theory of G is undecidable. The decidability of the positive theory of a virtually-free group leads of course to the question, whether the full first-order theory of a virtually-free group is decidable. One might try to extend the techniques developed by Kharlampovich and Myasnikov in their solution of Tarski's problem about the theory of a free group [12] to the virtually-free case.

Underlying the definition of a t-system (resp. J-system) without long overlapping is a certain small cancellation condition. Similar conditions were also used in the construction of SQ-universal HNN-extensions [21] and amalgamated free products [22]. Recall that a group G is SQ-universal if every countable group embedds into a quotient of G. One might ask, whether there is some relation between SQ-universality and the positive theory of a group.

References

[1] R. V. Book and F. Otto. *String–Rewriting Systems*. Springer, 1993.

[2] D. E. Cohen. *Groups of Cohomological Dimension One*. Number 245 in Lecture Notes in Mathematics. Springer, 1972.

[3] N. Dershowitz and J.-P. Jouannaud. Rewriting systems. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, pages 243–320. Elsevier Publishers, Amsterdam, 1990.

[4] W. Dicks and M. J. Dunwoody. *Groups Acting on Graphs*. Cambridge University Press, 1989.

[5] V. Diekert and M. Lohrey. Word equations over graph products. In *Proceedings of the 23rd Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2003), Mumbai (India)*, number 2914 in Lecture Notes in Computer Science, pages 156–167. Springer, 2003. long version available from the authors.

[6] V. Diekert and M. Lohrey. Existential and positive theories of equations in graph products. *Theory of Computing Systems*, 37(1):133–156, 2004.

[7] V. G. Durnev. Undecidability of the positive $\forall\exists^3$-theory of a free semigroup. *Sibirsky Matematicheskie Jurnal*, 36(5):1067–1080, 1995. English translation.

[8] Y. Ershov. Elementary group theories. *Soviet Math. Dokl.*, 13:528–532, 1972. English translation.

[9] E. R. Green. *Graph Products of Groups.* PhD thesis, The University of Leeds, 1990.

[10] B. Khan, A. G. Myasnikov, and D. E. Serbin. On positive theories of groups with regular free length function. *International Journal of Algebra and Computation*, 17(1): 1–26, 2007.

[11] O. Kharlampovich and A. Myasnikov. Implicit function theorem over free groups. *Journal of Algebra*, 290(1):1–203, 2005.

[12] O. Kharlampovich and A. Myasnikov. Elementary theory of free non-abelian groups. *Journal of Algebra*, 302(2):451–552, 2006.

[13] M. Lohrey and G. Sénizergues. Equations in HNN-extensions. Manuscript, 2006.

[14] M. Lohrey and G. Sénizergues. Rational subsets of HNN-extensions. to appear in *International Journal of Algebra and Computation*, 2007.

[15] R. C. Lyndon and P. E. Schupp. *Combinatorial Group Theory.* Springer, 1977.

[16] G. S. 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.*

[17] G. S. 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.

[18] S. S. Marchenkov. Unsolvability of the positive $\forall\exists$-theory of a free semi-group. *Sibirsky Matematicheskie Jurnal*, 23(1):196–198, 1982.

[19] Y. I. Merzlyakov. Positive formulas on free groups. *Algebra i Logika Sem.*, 5(4):25–42, 1966. In Russian.

[20] E. Rips and Z. Sela. Canonical representatives and equations in hyperbolic groups. *Inventiones Mathematicae*, 120:489–512, 1995.

[21] G. S. Sacerdote and P. E. Schupp. SQ-universality in HNN groups and one relator groups. *Journal of the London Mathematical Society. Second Series*, 7:733–740, 1974.

[22] P. E. Schupp. Small cancellation theory over free products with amalgamation. *Mathematische Annalen*, 193:255–264, 1971.

[23] Z. Sela. Diophantine geometry over groups VIII: The elementary theory of a hyperbolic group. Available via `http://www.ma.huji.ac.il/zlil/`, 2002.

[24] J. R. Stallings. *Group Theory and Three-Dimensional Manifolds.* Number 4 in Yale Mathematical Monographs. Yale University Press, 1971.