HAL
open science

Homological computations for term rewriting systems

Philippe Malbos, Samuel Mimram

To cite this version:

Philippe Malbos, Samuel Mimram. Homological computations for term rewriting systems. 1st International Conference on Formal Structures for Computation and Deduction (FSCD 2016), Jun 2016, Porto, Portugal. pp.27:1-27:17. hal-01678175

HAL Id: hal-01678175

https://hal.science/hal-01678175v1

Submitted on 9 Jan 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Homological Computations for Term Rewriting Systems

Philippe Malbos[1] and Samuel Mimram[2]

1 **LIX, École Polytechnique**
samuel.mimram@lix.polytechnique.fr
2 **ICJ, Université de Lyon**
malbos@math.univ-lyon1.fr

Abstract

An important problem in universal algebra consists in finding presentations of algebraic theories by generators and relations, which are as small as possible. Exhibiting lower bounds on the number of those generators and relations for a given theory is a difficult task because it a priori requires considering all possible sets of generators for a theory and no general method exists. In this article, we explain how homological computations can provide such lower bounds, in a systematic way, and show how to actually compute those in the case where a presentation of the theory by a convergent rewriting system is known. We also introduce the notion of coherent presentation of a theory in order to consider finer homotopical invariants. In some aspects, this work generalizes, to term rewriting systems, Squier's celebrated homological and homotopical invariants for string rewriting systems.

1 Introduction

An algebraic theory is a mathematical structure specified by operations, with given arities, and relations between those, i.e. a term rewriting system if we consider the relations as being oriented. For instance, the theory of *groups* is given by three operations m of arity two (the multiplication), e of arity zero (the neutral element) and i of arity one (the inverse), subject to the five expected relations:

$$\begin{array}{ccc} m(e,x_1)=x_1 & m(x_1,e)=x_1 & m(m(x_1,x_2),x_3)=m(x_1,m(x_2,x_3)) \\ m(i(x_1),x_1)=e & m(x_1,i(x_1))=e & \end{array}$$

Of course there are many ways of specifying, or *presenting*, an algebraic theory. For instance, the relations in the second column are derivable from the other, and we could therefore as well remove them and still get a presentation for the theory of groups, with only three relations. This observation is in fact the starting point of the work of Knuth and Bendix in rewriting theory [10]: by adding derivable relations, in good cases one can obtain a set of relations which are much better behaved from a computational point of view, such as being confluent and terminating, without changing the presented theory. In the case of the theory of groups, one can actually come up with an even smaller presentation by considering other generators; it can be axiomatized with only two generators a of arity zero (standing for any element, in order to exclude the "empty group") and d of arity two (standing for division) subject to only one relation [7]:

$$d(x_1,d(d(d(d(x_1,x_1),x_2),x_3),d(d(d(x_1,x_1),x_1),x_3))) \quad = \quad x_2 \tag{1}$$

see also [23, 24] for other possible axiomatizations of the theory of groups with one relation.

This quest for small presentations was initiated by Tarski who first gave a similar presentation of abelian groups with one rule [30]: those with only one relation are of particular interest and are sometimes called *one-based* theories in the literature. As illustrated in the example above, this is not an easy task: in the case of groups, one had to think of completely changing the set of generators and relations... Let us briefly recall some achievements

© Philippe Malbos and Samuel Mimram;
licensed under Creative Commons License CC-BY
Conference title on which this volume is based on.
Editors: Billy Editor and Bill Editors; pp. 1–18
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

in the field, a detailed overview of the subject can be found in [17]. The theories of semi-lattices [27] and distributive lattices [20] are not one-based. In contrast the theory of lattices is one-based: first, a unique relation was shown to exist by general methods [20], giving rise to a relation of length 300000 on 34 variables, and was then reduced to one of length 29 on 8 variables [18]. Similarly, for boolean algebras a single axiom was provided [26], but its size was more than 40 million symbols [17], and shorter axioms (around a dozen of symbols) were found afterward [19] by using intensive combinatorial computations.

In this article, we provide a novel method of showing that a theory is not one-based, using homological invariants, when the theory is given by a convergent rewriting system. The results mentioned above (such as semi- and distributive lattices) required lots of inventivity and are specific to the considered cases. By contrast, our methods are completely mechanical: by performing a series of computations, one obtains a lower bound on the number of rules in any presentation of the theory, and if this lower bound is greater than two, we know that we need at least two relations to present it, and therefore that the theory is not one-based. Of course, our method does not always gives interesting results: it might answer zero as a lower bound, from which we cannot conclude anything.

Homological invariants. The homology of a space consists in a sequence of groups which encode the number of "holes" in each dimension, and moreover they constitute invariants of the spaces in the sense that two homotopy equivalent spaces have the same associated groups [15, 6]. Homology can also be computed for algebraic structures which are not obviously spaces, such as monoids, groups, algebras, operads, etc. In the case of monoids, Squier has shown how to compute those invariants in small dimensions [28, 12] when the monoid is presented by a convergent string rewriting system, and this construction has since then been generalized in every dimension [11]. Here also, the interest of this construction lies in the fact that, even though it is constructed from a particular presentation, it does not actually depend on the choice of the presentation, only the presented monoid. In particular, the rank of the second homology group is, by construction, an integer which is smaller than the number of relations of the presentation used to compute it, and thus a lower bound for the number of relations of any presentation since it is an invariant.

In this article, we generalize this approach from monoids presented by convergent string rewriting systems to algebraic theories presented by convergent term rewriting systems, and use the resulting homology computations to provide lower bounds on the number of generators or relations required to present an algebraic theory. This work is based on Jibladze and Pirasvili's definition of a cohomology for algebraic theories [8, 9], as well as Malbos' PhD thesis [16]. The first contribution of this article is to reformulate in concrete terms the fairly abstract categorical definitions used in those works. We also introduce a resolution when the algebraic theory admits a convergent presentation, which allows us to compute the homology in practice, using classical constructions in rewriting theory and linear algebra. Finally, we also explain how those invariants can be refined into ones of more homotopical nature by introducing a notion of coherent presentation for algebraic theories. Due to space constraints we cannot detail all the constructions performed here, and advise the reader willing to grasp the details to first understand the simpler case of monoids [28, 12], of which this construction is largely inspired; details shall be given somewhere else, and the present article focuses mainly on computations and applications.

2 Presentations of Lawvere algebraic theories

2.1 Term rewriting systems

Terms. A *signature* (P_1, σ_0) consists of a set P_1 of *operations* together with a function $\sigma_0 : \mathsf{P}_1 \to \mathbb{N}$ associating to each operation its *arity*. Supposing fixed an infinite countable

set $\mathcal{X} = \{x_1, x_2, \ldots\}$ of variables, one can consider *terms* generated by operations with variables in this set, which are defined as usual. We write $\mathrm{FV}(t)$ for the set of indices of *free variables* occurring in a term, e.g. $\mathrm{FV}(f(x_2, g(x_2, x_5)) = \{2, 5\}$. Parallel *substitution* of x_i by t_i in a term u is denoted $u[t_1/x_1, \ldots, t_n/x_n]$.

The terms generated by the signature form a category, denoted P_1^*, whose objects are natural numbers and morphisms in $\mathsf{P}_1^*(m, n)$ are n-uples $\langle t_1, \ldots, t_n\rangle$ of terms t_i with free variables in $\{x_1, \ldots, x_m\}$. Composition of two morphisms $\langle t_1, \ldots, t_n\rangle : m \to n$ and $\langle u_1, \ldots, u_p\rangle : n \to p$ is induced by substitution as follows:

$$\langle u_1, \ldots, u_p\rangle \circ \langle t_1, \ldots, t_n\rangle \quad = \quad \langle u_1[t_1/x_1, \ldots, t_n/x_n], \ldots, u_p[t_1/x_1, \ldots, t_n/x_n]\rangle$$

and the identity on n is $\langle x_1, \ldots, x_n\rangle : n \to n$. We sometimes overload the notation and denote by $\mathsf{P}_1^* = \coprod_{m,n\in\mathbb{N}} \mathsf{P}_1^*(m, n)$ the class of all morphisms of this category and by $\sigma_0^*, \tau_0^* : \mathsf{P}_1^* \to \mathbb{N}$ the functions respectively associating to a morphism its source and target, also called its *arity* and *coarity*. Note that terms are the morphisms of coarity 1. We write $\iota_1 : \mathsf{P}_1 \to \mathsf{P}_1^*$ for the canonical inclusion, sending an n-ary operation f to the term $f(x_1, \ldots, x_n)$.

Term rewriting systems. We suppose fixed a signature as above. A *term rewriting system* on the signature P_1 consists of a set P_2, whose elements are called *rewriting rules*, together with two functions $\sigma_1, \tau_1 : \mathsf{P}_2 \to \mathsf{P}_1^*$ associating to each rule its source and target which should be (1-uples of) terms. The source and target of a rule should have the same arity, which is called the *arity* of the rule. A rewriting system together with the corresponding signature thus consists of a diagram of sets and functions

$$P \quad = \quad \begin{tikzcd} & \mathsf{P}_1 \arrow[dl, shift right, "\sigma_0"'] \arrow[dl, shift left, "\tau_0"] \arrow[d, "\iota_1"] & \mathsf{P}_2 \arrow[dl, shift right, "\sigma_1"'] \arrow[dl, shift left, "\tau_1"] \\ \mathbb{N} & \mathsf{P}_1^* \arrow[l, shift right, "\sigma_0^*"'] \arrow[l, shift left, "\tau_0^*"] & \end{tikzcd} \qquad \text{such that } \sigma_0^* \circ \sigma_1 = \sigma_0^* \circ \tau_1.$$

We sometimes write $R : t \Rightarrow u$ to denote a rule R with $\sigma_1(R) = t$ and $\tau_1(R) = u$. Note that contrarily to the habit, we consider the signature as being part of the rewriting system.

▶ **Example 1** (Monoids)**.** The rewriting system corresponding to monoids has operations $\mathsf{P}_1 = \{m, e\}$, with $\sigma_0(m) = 2$ and $\sigma_0(e) = 0$, and rewriting rules $\mathsf{P}_2 = \{A, L, R\}$ with $\sigma_1(A) = m(m(x_1, x_2), x_3)$, $\tau_1(A) = m(x_1, m(x_2, x_3))$, $\sigma_1(L) = m(e, x_1)$, $\sigma_1(R) = m(x_1, e)$, $\tau_1(L) = \tau_1(R) = x_1$. Such a rewriting system will often be written more concisely

$$\langle m : 2, e : 0 \mid A : m(m(x_1, x_2), x_3) \Rightarrow m(x_1, m(x_2, x_3)), L : m(e, x_1) \Rightarrow x_1, R : m(x_1, e) \Rightarrow x_1\rangle$$

▶ **Example 2** (Groups)**.** The rewriting system for groups is obtained from the rewriting system for monoids by adding a generator i of arity one and relations $I : m(i(x), x) \Rightarrow e$ and $I' : m(x, i(x)) \Rightarrow e$.

Contexts. An n-ary *context* C is a term with variables in $\{x_1, \ldots, x_n, \square\}$, in which the "variable" $\square$ occurs exactly once and is called the *hole* of C. Given a term t, the substitution $C[t/\square]$ is often denoted $C[t]$. The n-ary contexts form a category $\mathcal{K}_n$ with one object, morphisms being n-ary contexts, with composition given by substitution $D \circ C = D[C]$ and neutral element by the identity context $\square$. In turn, these categories induce a functor $\mathcal{K} : (\mathsf{P}_1^*)^{\mathrm{op}} \to \mathbf{Cat}$, sending an object n to $\mathcal{K}_n$ and a morphism $u = \langle u_1, \ldots, u_n\rangle : m \to n$ to the functor $\mathcal{K}_u : \mathcal{K}_n \to \mathcal{K}_m$ such that the image of an n-ary context C is the m-ary context $\mathcal{K}_u C = C[u_1/x_1, \ldots, u_n/x_n]$. In the following, we simply write Cu instead of $\mathcal{K}_u C$, and the previous categorical discussion boils down to the simple facts that $(Cu)v = C(u \circ v)$, $C\mathrm{id} = C$, $(D \circ C)u = D \circ (Cu)$ and $\square u = \square$. An *occurrence* of a variable x_i in a term t is

a context obtained from t by replacing exactly one instance of the variable x_i by $\square$, those will be formally defined (in a linear context) in Definition 13.

We write $\mathbb{K}$ for the category whose objects are integers and morphisms in $\mathbb{K}(m,n)$ are *bicontexts*, i.e. pairs (C,u) consisting of a context C with variables in $\{x_1,\dots,x_n\}$, and a morphism $u \in \mathsf{P}_1^*(n,m)$. The composition of two morphisms $(C,u) : m \to n$ and $(D,v) : n \to p$ is given by $(D,v) \circ (C,u) = (D \circ Cv, u \circ v)$ and the identity on n is $(\square, \mathrm{id}_n) : n \to n$. Note that composition is reversed in the second component. A bicontext $(C,u) : m \to n$ induces a function $C[-]u : \mathsf{P}_1^*(m,1) \to \mathsf{P}_1^*(n,1)$ which to a term t associates the term $C[t \circ u]$, which we will write $C[t]u$ in the following; for this reason, we will sometimes abusively write $C[-]u$ for a context in order to avoid introducing heavy notations. This function is easily shown to be compatible with composition and substitution:

$$D[C[t]u]v = (D \circ C)[t](u \circ v) \qquad \square[t]\mathrm{id} = t \qquad (C[t]u) \circ v = (Cv)[t](u \circ v)$$

In particular, we have $C[t]\mathrm{id} = C[t]$ which makes the notation unambiguous on this point, and we will always write composition symbol "$\circ$" in order to avoid confusion in wrt the equation on the right above.

In the following, when we need to distinguish between multiple rewriting systems, we will add those in exponent to the constructions, i.e. we write $\mathcal{K}^P$ instead of simply $\mathcal{K}$ for the contexts of P, etc.

Rewriting. Suppose fixed a rewriting system P. We say that a term t *rewrites in one step* into t', what we write $t \longrightarrow t'$, when there exists a rule $R : u \Rightarrow u'$ of arity m and a bicontext $(C,v) : m \to n$ such that $t = C[u]v$ and $t' = C[u']v$. In this situation, we often write $C[R]v : t \longrightarrow t'$ and the term t is said to be *reducible* by the rule R. We write $\overset{*}{\longrightarrow}$ for the reflexive and transitive closure, and $\overset{*}{\longleftrightarrow}$ for the generated equivalence relation. Note that the latter relation is a congruence, in the sense that it is compatible with composition, identities and taking uples.

A rewriting system is *terminating* when there is no infinite sequence $t_0 \longrightarrow t_1 \longrightarrow \dots$ of rewriting steps and *confluent* (resp. *locally confluent*) when for every terms t, u_1, u_2 such that $u_1 \overset{*}{\longleftarrow} t \overset{*}{\longrightarrow} u_2$ (resp. $u_1 \longleftarrow t \longrightarrow u_2$) there exists a term v such that $u_1 \overset{*}{\longrightarrow} v \overset{*}{\longleftarrow} u_2$. A confluent rewriting system is always locally confluent, and Newman's lemma [25] ensures the converse implication when the rewriting system is terminating. A rewriting system is *convergent* when it is both terminating and confluent. In this case, any maximal sequence of rewriting steps starting from a term t will end on the same term $\hat{t}$, called the *normal form* of t, and two terms t and t' are such that $t \overset{*}{\longleftrightarrow} t'$ if and only if $\hat{t} = \hat{t'}$: normal forms provide canonical representatives of equivalence classes under the equivalence relation $\overset{*}{\longleftrightarrow}$.

Critical pairs. Local confluence of a rewriting system can be tested by considering minimal obstructions to confluence. Generalizing the above notion of context, a *context with two holes* E is a term using usual variables as well as $\square$ and $\square'$, in which both $\square$ and $\square'$ occur exactly once; we write $E[t,t']$ instead of $E[t/\square, t'/\square']$. Consider a pair of rewriting steps $C_1[R_1]v_1 : t \longrightarrow u_1$ and $C_2[R_2]v_2 : t \longrightarrow u_2$, with $R_i : t'_i \Rightarrow u'_i$, rewriting the same term t. The pair of rewriting steps is *non-overlapping* when there exists a context E with two holes such that $C_1 = E[\square, t'_2 \circ v_2]$ and $C_2 = E[t'_1 \circ v_1, \square]$. In this situation, the two reductions are always confluent:

$$\begin{tikzcd}
 & t = E[t'_1 \circ v_1, t'_2 \circ v_2] \arrow[dl, "C_1[R_1]v_1"'] \arrow[dr, "C_2[R_2]v_2"] & \\
u_1 = E[u'_1 \circ v_1, t'_2 \circ v_2] \arrow[dr, "*"'] & & E[t'_1 \circ v_1, u'_2 \circ v_2] = u_2 \arrow[dl, "*"] \\
 & \hat{t} = E[u'_1 \circ v_1, u'_2 \circ v_2] &
\end{tikzcd} \tag{2}$$

Given a pair of rewriting steps as above, a context (C, v) induces another pair of rewriting steps rewriting the same terms: $(C \circ C_i)[R](v_i \circ v) : C[t]v \Rightarrow C[u_i]v$. In this case, we say that the former pair is smaller than the latter, and this induces a partial order on pairs of rewriting steps rewriting the same term.

▶ **Definition 3.** A pair of rewriting steps $C_1[R_1]v_1 : t \longrightarrow u_1$ and $C_2[R_2]v_2 : t \longrightarrow u_2$ rewriting the same term t is *critical* when the two steps are distinct, i.e. $(C_1, R_1, v_1) \neq (C_2, R_2, v_2)$, overlapping, and minimal wrt the above partial order. It is *confluent* when there exists a term v such that $u_1 \overset{*}{\longleftarrow} v \overset{*}{\longrightarrow} u_2$.

This reformulates with our formalism the classical notion of critical pair, and the usual associated lemma holds: a rewriting system is locally confluent if and only if all its critical pairs are confluent. In particular, a terminating rewriting system with confluent critical pairs is convergent.

2.2 Lawvere algebraic theories

A rewriting system P induces a category, noted $\overline{\mathsf{P}^*}$ and called the *category presented by the rewriting system*, defined as the quotient of the category of terms P_1^* under the congruence $\overset{*}{\longleftrightarrow}$ generated by the rules: given an uple of terms $t \in P_1^*$, we write $\bar{t}$ (or sometimes even simply t) for its equivalence class. This presented category is easily shown to be a a Lawvere theory [13]:

▶ **Definition 4.** A *Lawvere theory* $\mathcal{T}$ (also sometimes called an *algebraic theory*) is a category with finite products whose objects are integers, products are given on objects by addition, and the terminal object is 0.

In particular, when the rewriting system has no rules, the associated Lawvere theory is P_1^* and called the *Lawvere theory freely generated by the signature*. It can in fact be shown to correspond to a left adjoint to the suitable forgetful functor from Lawvere theories to signatures (for space constraints, we do not detail this construction nor even morphisms of signatures and Lawvere theories because they do not play an important rôle here).

▶ **Lemma 5.** *Any Lawvere theory $\mathcal{T}$ admits a presentation P, called the* standard presentation*, with*

$$\mathsf{P}_1 = \coprod_{n \in \mathbb{N}} \mathcal{T}(n, 1) \qquad \mathsf{P}_2 = \{t \Rightarrow u \mid t, u \in \mathsf{P}_1^* \text{ and } \epsilon(t) = \epsilon(u)\}$$

where we take all morphisms of $\mathcal{T}$ of coarity 1 as operations in P_1, with the expected arity, and write $\epsilon : \mathsf{P}_1^* \to \mathsf{P}_1$ for the morphism which to a term, seen as a formal composite of morphisms in $\mathcal{T}$, associates the result of its compositions. The rules are thus all pairs of formal composites whose result is the same.

A *model* of a Lawvere theory $\mathcal{T}$ is a functor $\mathcal{T} \to \mathbf{Set}$ which preserves finite products. In the case where $\mathcal{T}$ is presented by a rewriting system P, this amounts to the specification of a set X, of a function $[\![f]\!] : X^n \to X$ for each operation f of arity n, in such a way that $[\![t]\!] = [\![u]\!]$ for each rule $R : t \Rightarrow u$.

▶ **Example 6.** A model for the theory of monoids (Example 1) consists of a set X together with functions $[\![m]\!] : X \times X \to X$ and $[\![e]\!] : 1 \to X$ such that for every $x, y, z \in X$, $[\![m]\!]([\![m]\!](x, y), z) = [\![m]\!](x, [\![m]\!](y, z))$, $[\![m]\!]([\![e]\!](), x) = x = [\![m]\!](x, [\![e]\!]())$. The models for this theory are thus precisely monoids in the usual sense. Similarly, the models for the theory of groups (Example 2) are groups.

2.3 Tietze transformations

Two rewriting systems are *Tietze equivalent* when they present isomorphic Lawvere theories, which implies that they have the same models (in fact, the converse is also true). For instance, the theory of groups can be presented by the rewriting system of Example 2. As explained in the introduction, it also admits a presentation with two generators d of arity 2 and a of arity 0, with one rewriting rule corresponding to the equation (1). In the context of presentations of groups, Tietze has shown that the corresponding equivalence is generated by two transformations and their inverse [31]. This property can be adapted to the context of presentation of Lawvere theories as follows.

▶ **Definition 7.** The *Tietze transformations* are the two following operations, transforming a rewriting system P into another one P', as well as their converse (transforming P' into P):

1. *adding a superfluous operation*: given a symbol f not occurring in P_1, a symbol R not occurring in P_2, and a term $t \in \mathsf{P}_1^*$ of arity n, we set
$$\mathsf{P}'_1 = \mathsf{P}_1 \uplus \{f\} \qquad \mathsf{P}'_2 = \mathsf{P}_2 \uplus \{R\}$$
where f is an operation of arity n and $R : t \Rightarrow f(x_1, \dots, x_n)$,
2. *adding a derivable relation*: given a symbol R not occurring in P_2 and two terms t, u such that $t \overset{*}{\longleftrightarrow}_P u$, we set
$$\mathsf{P}'_1 = \mathsf{P}_1 \qquad \mathsf{P}'_2 = \mathsf{P}_2 \uplus \{R\}$$
with $R : t \Rightarrow u$.

▶ **Proposition 8.** *Two rewriting systems* P *and* Q *are* Tietze equivalent *if and only if* Q *can be obtained from* P *by applying a series of Tietze transformations.*

In our quest for minimizing the number of relations (and generators) of a Lawvere theory, the Tietze transformations can be helpful, as illustrated in the following simple example.

▶ **Example 9.** Consider the string rewriting system with generators a, b and c of arity one and two rules:
$$\mathsf{P} = \langle a : 1, b : 1, c : 1 \mid A : a(x_1) \Rightarrow x_1, B : a(b(x_1)) \Rightarrow c(x_1) \rangle$$
We can then apply the following sequence of Tietze transformations:
$$\begin{aligned}
\mathsf{P}' &= \langle a : 1, b : 1, c : 1 \mid A : a(x_1) \Rightarrow x_1, B : a(b(x_1)) \Rightarrow c(x_1), C : b(x_1) \Rightarrow c(x_1) \rangle \\
\mathsf{P}'' &= \langle a : 1, b : 1, c : 1 \mid A : a(x_1) \Rightarrow x_1, C : b(x_1) \Rightarrow c(x_1) \rangle \\
\mathsf{P}''' &= \langle b : 1, c : 1 \mid C : b(x_1) \Rightarrow c(x_1) \rangle \\
\mathsf{P}'''' &= \langle c : 1 \mid \rangle
\end{aligned}$$
We have first added the derivable relation C, then removed the derivable relation B, then removed the definable operation a, then removed the definable operation b. So, in fact, our theory can be presented without any relation and only one operation.

It is clear that, in above example, we had to first add a new relation in order to remove all of them: one cannot simply hope to always reduce the number of relations by Tietze transformations in order to obtain a minimal one (and for similar reasons, one might be forced to add new generators before reducing the presentation, as illustrated for the theory of groups in the introduction). For this reason, it is quite difficult to minimize the number of relations in general, or to decide whether a presentation is minimal wrt to relations or generators.

Note in particular that, in a convergent rewriting system, a critical pair witnesses a derivable relation, and Newman's lemma ensures that any derivable relation can be obtained

via critical pairs: if a presentation has a removable relation, then such a relation can be obtained by inspecting critical pairs.

3 Homology of Lawvere algebraic theories

In this section, we introduce the notion of homology of a Lawvere theory by adapting the general methodology which is now classical for monoids, groups, algebras [15], operads [14], etc. This construction associates to a Lawvere theory a sequence of groups which are invariants of the Lawvere theory: we will see that these can be computed from any presentation with suitable properties, however these groups only depend on the presented theory, and not on the presentation. It thus provides interesting information about all the possible presentations of the theory: its relevance will be illustrated in Section 3.6, where we use it to show that a particular theory admits no presentation with only one rule, *whichever possible signature we use*.

The basic idea of homology is to "count" the number of times a thing is used (positively when it occurs in the target and negatively in the source). For example, a rule $R : g(f(x_1), f(x_1)) \Rightarrow h(x_1)$ "consumes" two instances of f and one of g to "produce" one of h. Therefore, we can think of the associated balance to be $h - 2f - g$. Since this is a relation, it induces the equation $h = 2f + g$ when counting operations, which indicates that the operation h might be superfluous, i.e. we might be able to remove it using a Tietze transformation. A similar process for critical pairs will allow us to provide an "over-approximation" of the superfluous relations, and therefore give lower bounds on necessary relations.

Note that above, we formally consider the "ring" of operations (actually a "ringoid" since operations are typed by their arities) in order to be able to consider sums of operations. Much care is however needed in order to ensure that this way of counting is compatible with duplication and erasure of variables, and independent of the presentation. As customary in homological algebra, we thus begin by introducing the notion of resolution for a Lawvere theory, which is easily shown to be invariant (in a suitable sense) under Tietze equivalences and derive homology from those. Roughly, the resolution amounts to perform a similar linearization process as above, but keeping track of the contexts, i.e. the rule R would give rise to a relation of the form $\underline{h}(x_1) - \underline{g}(f(x_1), f(x_1)) - g(\underline{f}(x_1), f(x_1)) + g(f(x_1), \underline{f}(x_1))$, and to ensure that all (higher-)relations are present.

One could be tempted to use standard notions of homology for a category in order to study Lawvere theories. However, because such a theory contains a terminal object, its homology in this sense will always be trivial. Therefore, one has to adapt the setting of homology in order to take in account the cartesian structure. Following the general methodology of Barr and Beck [3, 2], Jibladze and Pirashvili have been able to define a suitable ringoid of coefficients for cohomology [8, 9], which was later on reworked by Malbos [16]. The section 3.1 to 3.4 are a reformulation, in operational terms, of those (to simplify the presentation, the framework is also less general: we use bimodules instead of cartesian natural systems). We suppose fixed a rewriting system P and write $\mathcal{T} = \overline{\mathsf{P}^*}$ for the theory it presents.

3.1 Modules over ringoids

Ringoids. A monoid is the same as a category with only one object, or thinking backward, a category is a "monoid with multiple objects". Similarly, a ringoid can be thought of as a "ring with multiple objects". We briefly introduce here this algebraic structure and refer the reader to seminal paper [22] for details. The category **Ab** of abelian groups is monoidal when equipped with the usual tensor product $\otimes$ of abelian groups, with $(\mathbb{Z}, +, 0)$ as unit (in the following, we always denote abelian groups additively).

▶ **Definition 10.** A *ringoid* $\mathcal{R}$ is a small category enriched in the monoidal category $\mathbf{Ab}$.

More explicitly, a ringoid consists of a category $\mathcal{C}$ in which each hom-set $\mathcal{C}(A, B)$ is equipped with a structure of abelian group, in such a way that composition is bilinear, i.e. respects addition and zero. For instance, given $f, f' : A \to B$ and $g, g' : B \to C$, we have

$$(g + g') \circ (f + f') = g \circ f + g \circ f' + g' \circ f + g' \circ f' \qquad 0 \circ f = 0 \qquad f \circ 0 = 0 \quad (3)$$

▶ **Lemma 11.** *The category of ringoids with one object is equivalent to the category of rings.*

Any category $\mathcal{C}$ freely generates a ringoid that we denote $\mathbb{Z}\mathcal{C}$. It always exists for general arguments [1] and can be explicitly described as follows. It has the same objects as $\mathcal{C}$ and, given objects A and B, $\mathbb{Z}\mathcal{C}(A, B)$ is the free abelian group over $\mathcal{C}(A, B)$, which is the same as the free $\mathbb{Z}$-module, i.e. formal sums of morphisms in $\mathcal{C}(A, B)$ with coefficients in $\mathbb{Z}$, quotiented by the usual axioms of groups, and composition is induced by the one of $\mathcal{C}$ and satisfies the axioms of ringoids such as (3).

Modules. The usual notion of module over a ring, can also easily be generalized to "multiple objects" as follows.

▶ **Definition 12.** A *(left) module* $\mathcal{M}$ over a ringoid $\mathcal{R}$, or $\mathcal{R}$*-module*, is a functor $\mathcal{M} : \mathcal{R} \to \mathbf{Ab}$ which is enriched in $\mathbf{Ab}$. A morphism $f : \mathcal{M} \to \mathcal{N}$ of $\mathcal{R}$-modules, or $\mathcal{R}$*-linear map*, is an enriched natural transformation: it consists of a group morphism $f_A : \mathcal{M}A \to \mathcal{N}A$ for every object A of $\mathcal{R}$, satisfying naturality conditions. We write $\mathbf{Mod}(\mathcal{R})$ for the category of $\mathcal{R}$-modules.

A right $\mathcal{R}$-module is defined as a left $\mathcal{R}^{\mathrm{op}}$-module, which explains why we will only need to consider left modules in the following. More explicitly, an $\mathcal{R}$-module $\mathcal{M}$ consists of an abelian group $\mathcal{M}A$ for every object A of $\mathcal{R}$, and a morphism $\mathcal{M}f : \mathcal{M}A \to \mathcal{M}B$ of groups for every morphism $f : A \to B$ in such a way that $\mathcal{M}(f + f') = \mathcal{M}f + \mathcal{M}f'$ (we are considering the pointwise addition on the right) and $\mathcal{M}0 = 0$ (on the right, 0 is the constant map). The category $\mathbf{Mod}(\mathcal{R})$ is enriched in $\mathbf{Ab}$ and can be shown to have enough structure to support usual computations in homological algebra: it is abelian and has enough projectives [22].

Free modules. Suppose given a set X_A for every object A of $\mathcal{R}$. The *free module* generated by this family of sets, written $\mathcal{R}\underline{X}$, can be described as the functor which to every object A associates the formal finite sums $\sum_i f_i \underline{x}_i$, with $x_i \in X_{A_i}$ and coefficients $f_i : A_i \to A$, subject to the usual laws of left modules, e.g.

$$g\left(\sum_i f_i \underline{x}_i\right) = \sum_i (g \circ f_i)\underline{x}_i \qquad g \circ 0 = 0 \qquad \left(\sum_i g_i\right)(f\underline{x}) = \sum_i (g_i \circ f)\underline{x} \qquad 0(f\underline{x}) = 0$$

Above, the "underline" notation is here only to make the distinction between the elements of $\mathcal{R}$ and those of X, and as customary we write $g(f\underline{x})$ instead of $((\mathcal{R}\underline{X})g)(f\underline{x})$ for the left action.

Tensor product of modules. The usual definition of the tensor product of modules can be generalized to modules over ringoids as follows. Given a right $\mathcal{R}$-module $\mathcal{M} : \mathcal{R}^{\mathrm{op}} \to \mathbf{Ab}$ and a left $\mathcal{R}$-module $\mathcal{M} : \mathcal{R} \to \mathbf{Ab}$, their tensor product is the ringoid defined by the (enriched) coend $\mathcal{M} \otimes \mathcal{N} = \int^A \mathcal{M}A \otimes \mathcal{N}A$. This means that an element of $(\mathcal{M} \otimes \mathcal{N})(B)$ is a quotient of $\bigoplus_{A \in \mathcal{R}} \mathcal{M}A \otimes \mathcal{N}A$ by the relation identifying elements of the form $(f^{\mathrm{op}}x) \otimes y$ and $x \otimes (fy)$, for any suitably typed morphism f of $\mathcal{R}$.

3.2 The ringoid of bicontexts

The ringoid we will be mainly interested in is a quotient of $\mathbb{Z}\mathbb{K}$, the free ringoid over bicontexts. We begin by first defining a similar quotient on contexts.

▶ **Definition 13.** We define $\kappa_i : \mathbb{Z}\mathsf{P}_1^* \to \mathbb{Z}\mathcal{K}$ as the linear map which sends a term t to the formal sum of occurrences of the variable x_i in t. Formally, it is defined, for $j \neq i$ and $t = \langle t_1, \ldots, t_n \rangle$, by

$$\kappa_i(x_i) = \square \qquad \kappa_i(x_j) = 0 \qquad \kappa_i(u \circ t) = \sum_{j \in \mathrm{FV}(u)} (\kappa_j(u)t)[\kappa_i(t_j)]$$

On the right, the notations for contexts introduced in Section 2.1 are implicitly extended by linearity, e.g. $(C + D)[t] = C[t] + D[t]$, $C[t + u] = C[t] + C[u]$, etc.

▶ **Example 14.** Consider the term $t = f(g(x_1, x_2), x_1)$. We have

$$\kappa_1(t) = f(g(\square, x_2), x_1) + f(g(x_1, x_2), \square) \qquad \kappa_2(t) = f(g(x_1, \square), x_1) \qquad \kappa_3(t) = 0$$

We write $\overline{\mathbb{Z}\mathcal{K}}$ for the quotient of $\mathbb{Z}\mathcal{K}$ by the ideal generated by all elements of the form $\kappa_i(u) - \kappa_i(t)$ for a rule $R : t \Rightarrow u$ of arity n and $1 \leq i \leq n$; we thus have a well-defined quotient morphism $\kappa_i : \mathbb{Z}\overline{\mathsf{P}_1^*} \to \overline{\mathbb{Z}\mathcal{K}}$. The ringoid of bicontexts $\overline{\mathbb{Z}\mathbb{K}}$ is defined as the quotient of the free ringoid $\mathbb{Z}\mathbb{K}$ by quotienting contexts as above and morphisms by the rewriting rules: we identify element $\sum_i n_i(C_i, u)$ to 0 whenever $\sum_i n_i C_i = 0$ in $\overline{\mathbb{Z}\mathcal{K}}$, and $\sum_i n_i(C, u_i)$ to 0 whenever $\sum_i n_i u_i = 0$ in $\mathbb{Z}\mathcal{C}$.

▶ **Example 15.** Consider the rewriting system with operations and arities $a : 0$, $b : 0$, $f : 1$, $g : 2$, and two rules $A : a \Rightarrow b$ and $B : f(x_1) \Rightarrow g(x_1, x_1)$. The quotient on contexts is generated by $g(\square, x_1) + g(x_1, \square) - f(\square)$.

In the rest of the paper, we write $\mathcal{R} = \overline{\mathbb{Z}\mathbb{K}}$ for the ringoid of bicontexts of $\mathcal{T}$, which will be where coefficients will be taken in. In a free module, of the form $\mathcal{R}\underline{X}$, the elements are sums of monomials of the form $(C, u)\underline{x}$ where (C, u) is an equivalence class of bicontexts and $x \in X_n$ for some $n \in \mathbb{N}$. In the following, we will adopt the notation $C\underline{x}u$ instead: this makes it clear that contexts $C \in \overline{\mathbb{Z}\mathcal{K}}_n$ are acting on the left and morphisms in $\mathcal{T}$ are acting on the right (since their composition is reversed in the composition of bicontexts). In fact, the definition of $\overline{\mathcal{R}}$ does not depend on the choice of the presentation P, but only on the presented theory $\mathcal{T}$. Since every Lawvere theory admits a presentation (Lemma 5), the notions developed here will apply to any theory.

▶ **Lemma 16.** *Given two Tietze equivalent rewriting systems* P *and* Q*, the ringoids* $\mathcal{R}^{\mathsf{P}}$ *and* $\mathcal{R}^{\mathsf{Q}}$ *are isomorphic.*

3.3 Resolutions for Lawvere algebraic theories

The *trivial* $\mathcal{R}$*-module* $\mathcal{Z} : \mathcal{R} \to \mathbf{Ab}$ is the quotient of the free $\mathcal{R}$-module $\mathcal{R}\underline{X}$, with $X_n = \{\star_n\}$ for $n \in \mathbb{N}$, quotiented by relations of the form $\sum_i \kappa_i(u)t\underline{\star}t_i = \underline{\star_n}$ for every term $u \circ t$ of arity n (we write $\star$ instead of $\star_1$).

▶ **Example 17.** Given a signature with a binary operation m, since $m \circ \mathrm{id}_2 = \mathrm{id} \circ \langle m(x_1, x_2) \rangle$, we have the following relation in $\mathcal{Z}$: $m(\square, x_2)\underline{\star}\,\langle x_1 \rangle + m(x_1, \square)\underline{\star}\,\langle x_2 \rangle = \underline{\star_2} = \underline{\star}m(x_1, x_2)$.

The general idea of a free resolution is to start with the trivial module $\mathcal{Z}$ and equip it with a sequence of free $\mathcal{R}$-modules $\mathcal{M}_i$ such that $\mathcal{M}_0$ contains the sorts of the theory (there is always only one in our setting), $\mathcal{M}_1$ the operations, $\mathcal{M}_2$ the relations, $\mathcal{M}_3$ the relations between relations, and so on:

▶ **Definition 18.** A *free resolution* $\mathcal{M}_\bullet$ of $\mathcal{Z}$ consists of a sequence

$$\cdots \xrightarrow{\partial_1} \mathcal{M}_1 \xrightarrow{\partial_0} \mathcal{M}_0 \xrightarrow{\varepsilon} \mathcal{Z} \longrightarrow 0$$

of free $\mathcal{R}$-modules $\mathcal{M}_i = \mathcal{R}\underline{X_i}$ and $\mathcal{R}$-linear maps ∂_i and ε such that for any two successive arrows the image of the first is equal to the kernel of the second: $\mathrm{im}\,\partial_{i+1} = \ker \partial_i$, $\mathrm{im}\,\partial_0 = \ker \varepsilon$ and $\mathrm{im}\,\varepsilon = \mathcal{Z}$. The resolution is *partial* when it is finite on the left.

Note that the relation $\operatorname{im}\varepsilon = \mathcal{Z}$ means that ε is surjective and therefore $\mathcal{M}_0$ is free on at least one generator. Suppose that the theory contains an operation, for instance m as in Example 17: the kernel of ε will contain $m(\square, x_2)\underline{1}\langle x_1\rangle + m(x_1, \square)\underline{1}\langle x_2\rangle - \underline{1}m(x_1, x_2)$ as non-trivial element, and therefore $\mathcal{M}_1$ will need to contain a generator for m in order for the relation $\operatorname{im}\partial_0 = \ker\varepsilon$ to be satisfied. More generally, $\mathcal{M}_1$ should be free on a set of operations generating $\mathcal{T}$. For similar reasons, $\mathcal{M}_2$ should be free on a set of elements generating all the relations of $\mathcal{T}$, and $\mathcal{M}_3$ should be free on enough generators so that any two relations between the same (linearized) terms should be equal modulo them.

A major interest of free resolutions is that they can be shown to be essentially unique:

▶ **Proposition 19.** *Any two free resolutions of $\mathcal{Z}$ are homotopy equivalent.*

We do not detail further here the meaning of the above classical equivalence. Its main interest is that it will enable us to show that the definition of homology makes sense in next section (Proposition 21).

3.4 Homology of Lawvere algebraic theories

We are now in position to introduce the notion of homology of a Lawvere theory. The chain complex $(\mathcal{M}_\bullet, \partial_\bullet)$ of a resolution by $\mathcal{R}$-modules is acyclic, that is $\operatorname{im}\partial_{i+1} = \ker\partial_i$ holds. We are going to tensor it by $\mathcal{Z}^{\mathrm{op}}$, which means that we "erase" the coefficients in $\mathcal{R}$ everywhere, e.g. if $\mathcal{M}_i$ is free on the set X_i (i.e. $\mathcal{M}_i = \mathcal{R}\underline{X_i}$) then we have $\mathcal{Z}^{\mathrm{op}} \otimes \mathcal{M}_i = \mathbb{Z}X_i$. The resulting chain complex $(\mathcal{Z}^{\mathrm{op}} \otimes \mathcal{M}_\bullet, \tilde{\partial}_\bullet)$ still satisfies $\operatorname{im}\tilde{\partial}_{i+1} \subseteq \ker\tilde{\partial}_i$, but the converse inclusion is not true anymore in general. It thus makes sense to consider the following homology groups:

▶ **Definition 20.** Suppose given a Lawvere theory $\mathcal{T}$ and a resolution of the associated trivial $\mathcal{R}$-module $\mathcal{Z}$ as in Definition 18. The *homology* $H_\bullet(\mathcal{T})$ of $\mathcal{T}$ (with coefficients in the trivial $\mathcal{R}$-module $\mathcal{Z}$) is the homology of the chain complex

$$\ldots \xrightarrow{\tilde{\partial}_2} \mathcal{Z}^{\mathrm{op}} \otimes \mathcal{M}_2 \xrightarrow{\tilde{\partial}_1} \mathcal{Z}^{\mathrm{op}} \otimes \mathcal{M}_1 \xrightarrow{\tilde{\partial}_0} \mathcal{Z}^{\mathrm{op}} \otimes \mathcal{M}_0$$

where $\tilde{\partial}_i = \mathcal{Z}^{\mathrm{op}} \otimes \partial_i$. More explicitly, the homology consists of a sequence $H_\bullet(\mathcal{T})$ of groups defined by $H_i(\mathcal{T}) = \ker\tilde{\partial}_{i-1}/\operatorname{im}\tilde{\partial}_i$ where, by convention, $\tilde{\partial}_{-1}$ is the constant null map.

Proposition 19 ensures that it is well defined, because two homotopic chain complexes will give rise to the same homology:

▶ **Proposition 21.** *The homology $H_\bullet(\mathcal{T})$ of a Lawvere theory $\mathcal{T}$ does not depend on the choice of the resolution.*

Any theory can be shown to admit a resolution, called the *standard resolution*, by easily adapting usual constructions performed for monoids. More generally any partial resolution can be extended into a full one. We do not detail it here however, because it involves modules of infinite rank, and difficult to work with: in order to actually compute the homology of a theory, one should start with a resolution which is reasonably small. The purpose of next section is to construct such a (partial) resolution in the case where we start from a convergent presentation of the Lawvere theory.

3.5 A partial resolution for convergent Lawvere theories

In this section, we suppose that the Lawvere theory $\mathcal{T}$ we are considering is presented by a convergent reduced rewriting system P, and construct from it a partial free resolution of the trivial $\mathcal{R}$-module $\mathcal{Z}$. Writing $\mathsf{P}_0 = \{1\}$ for the set with one element and P_3 for the set of critical pairs of the rewriting system, the resolution we consider is of the form

$$\mathcal{R}\underline{\mathsf{P}_3} \xrightarrow{\partial_2} \mathcal{R}\underline{\mathsf{P}_2} \xrightarrow{\partial_1} \mathcal{R}\underline{\mathsf{P}_1} \xrightarrow{\partial_0} \mathcal{R}\underline{\mathsf{P}_0} \xrightarrow{\varepsilon} \mathcal{Z} \longrightarrow 0 \tag{4}$$

where the maps are defined as follows, and will be illustrated in next section. The map $\varepsilon : \mathcal{R}\underline{\mathsf{P}_0} \to \mathcal{Z}$ is the $\mathcal{R}$-linear map preserving the unit, i.e. such that $\varepsilon(\underline{1}) = \underline{\star}$. More generally, because of relations defining $\mathcal{Z}$, we have $\varepsilon(C\underline{1}u) = \underline{\star_n}$. The map $\partial_0 : \mathcal{R}\underline{\mathsf{P}_1} \to \mathcal{R}\underline{\mathsf{P}_0}$ is the $\mathcal{R}$-linear map such that for each operation $f \in \mathsf{P}_1$ of arity n, we have

$$\partial_0(\underline{f}) \quad = \quad \left(\sum_{i=1}^{n} \kappa_i(f)\underline{1}\,\langle x_i\rangle\right) - \underline{1}\,\langle f\rangle$$

The map $\partial_1 : \mathcal{R}\underline{\mathsf{P}_2} \to \mathcal{R}\underline{\mathsf{P}_1}$ is the $\mathcal{R}$-linear map such that for each rule $R : t \Rightarrow u$ in P_2 we have

$$\partial_1(R) \quad = \quad \underline{u} - \underline{t}$$

where the notation $\underline{t}$ generalizes the notation $\underline{f}$ for operations, and is defined inductively by

$$\underline{u \circ t} \quad = \quad \underline{u}t + \sum_{i=1}^{n}(\kappa_i(u)t)[\underline{t_i}] \qquad\qquad \underline{\mathrm{id}} = 0$$

for $t = \langle t_1, \ldots, t_n\rangle$. The map $\partial_2 : \mathcal{R}\underline{\mathsf{P}_3} \to \mathcal{R}\underline{\mathsf{P}_2}$ is the $\mathcal{R}$-linear map such that the image of a critical pair $(C_1[R_1]v_1, C_2[R_2]v_2)$, with $C_i[R_1]v_i : t \longrightarrow u_i$, is

$$\partial_2(C_1[R_1]v_1, C_2[R_2]v_2) \quad = \quad C_2\underline{R_2}v_2 - C_1\underline{R_1}v_1 + \underline{S_2} - \underline{S_1} \tag{5}$$

where $S_i : u_i \xrightarrow{*} \hat{t}$ are a choice of rewriting paths from u_i to $\hat{t}$, the normal form of t, see (2), which exist because the rewriting system is supposed to be convergent. Again, writing $\cdot$ for the concatenation of rewriting paths and Id for the empty one, the notation $\underline{T}$ is extended to rewriting paths by

$$\underline{C[R]v} = C\underline{R}v \qquad\qquad \underline{T' \cdot T} = \underline{T'} + \underline{T} \qquad\qquad \underline{\mathrm{Id}} = 0$$

The main result of this article is the following one:

▶ **Theorem 22.** *The sequence* (4) *as defined above is a partial free resolution of the trivial $\mathcal{R}$-module $\mathcal{Z}$.*

This theorem allows us to explicitly compute low-dimensional homology of a theory with a convergent presentation. Moreover, since the homology is independent of the choice of the presentation (Proposition 21), and any partial resolution can be extended into a full one (Section 3.4), it provides us with invariants for any presentation of $\mathcal{T}$. In particular, since $H_1(\mathcal{T})$ is defined as a quotient of $\mathbb{Z}\mathsf{P}_1$, and similarly for $H_2(\mathcal{T})$, we have

▶ **Proposition 23.** *The rank of $H_1(\mathcal{T})$ (resp. $H_2(\mathcal{T})$) is a lower bound of the number of operations (resp. relations) in any presentation of $\mathcal{T}$.*

3.6 An example

Let us illustrate the previous definitions on a simple example. Consider the term rewriting system with a generator m of arity 2 and three generators p_1, p_2, t of arity 1, together with the five following rules

$$\begin{array}{rcl@{\qquad\qquad}rcl} M_1 & : & p_1(m(x_1,x_2)) \Rightarrow x_1 & M_2 & : & p_2(m(x_1,x_2)) \Rightarrow x_2 \\ P_1 & : & p_1(t(x_1)) \Rightarrow p_2(x_1) & P_2 & : & p_2(t(x_1)) \Rightarrow p_1(x_1) \\ T & : & t(t(x_1)) \Rightarrow x_1 & & & \end{array}$$

A model of the resulting theory $\mathcal{T}$ consists of a set X together with operations $m : X \times X \to X$ (with we think of as injectively coding pairs of elements of X in X), $p_1, p_2 : X \to X$ (the two projections of the coding of pairs) and $t : X \to X$ (the function exchanging the two components in the coding of pairs). The rules M_1 and M_2 ensure that the projections recover

the components of a pair, the rules P_1 and P_2 ensure that the transposition exchanges the components, and the rule T enforces the involutivity of the transposition operation. For instance, writing $|n|_p$ for the exponent of a prime p in the prime factorization of an integer n, a model could be given by $X = \mathbb{N}$ and

$$m(n_1, n_2) = 2^{n_1} \times 3^{n_2} \qquad p_1(n) = |n|_2 \qquad p_2(n) = |n|_3 \qquad t(n) = n \times 2^{|n|_3} \times 3^{|n|_2} / (2^{|n|_2} \times 3^{|n|_3})$$

The rewriting system is locally confluent, with three critical pairs being

$$\begin{tikzcd}
p_1(t(t(x_1))) \arrow[r, "\square[P_1]\langle t(x_1)\rangle"] \arrow[d, "p_1(\square)[T]\langle x_1\rangle"'] & p_2(t(x_1)) \arrow[dl, "\square[P_2]\langle x_1\rangle"] \\
p_1(x_1) \arrow[ur, phantom, "\Pi_1"] &
\end{tikzcd}
\qquad
\begin{tikzcd}
p_2(t(t(x_1))) \arrow[r, "\square[P_2]\langle t(x_1)\rangle"] \arrow[d, "p_2(\square)[T]\langle x_1\rangle"'] & p_1(t(x_1)) \arrow[dl, "\square[P_1]\langle x_1\rangle"] \\
p_2(x_1) \arrow[ur, phantom, "\Pi_2"] &
\end{tikzcd}
\qquad
\begin{tikzcd}
t(t(t(x_1))) \arrow[d, bend right, "\square[T]\langle t(x_1)\rangle"'] \arrow[d, bend left, "t(\square)[T]\langle x_1\rangle"] \arrow[d, phantom, "\Theta"] \\
t(x_1)
\end{tikzcd}$$

It is also terminating, because all the rules decrease the size of the terms, and thus convergent. Therefore we can construct a resolution (4), as described in Section 3.5. The boundary maps are defined by

$$\partial_0(\underline{m}) = m(\square, x_2)\underline{1}\,\langle x_1\rangle + m(x_1, \square)\underline{1}\,\langle x_2\rangle - \underline{1}\,\langle m(x_1, x_2)\rangle \qquad \partial_0(\underline{p_i}) = p_i(\square)\underline{1} - \underline{1}\,\langle p_i(x_1)\rangle$$

and $\partial_0(\underline{t})$ is similar to $\partial_0(\underline{p_i})$,

$$\partial_1(\underline{M_1}) = -\underline{p_1}\,\langle m(x_1, x_2)\rangle - p_1(\square)\underline{m} \qquad \partial_1(\underline{P_1}) = \underline{p_2} - \underline{p_1}\,\langle t(x_1)\rangle - p_1(\square)\underline{t}$$
$$\partial_1(\underline{T}) = -\underline{t}\,\langle t(x_1)\rangle - t(\square)\underline{t}$$

and cases $\underline{M_2}$ and $\underline{P_2}$ are similar,

$$\partial_2(\underline{\Pi_1}) = p_1(\square)\underline{T} - \underline{P_1}\,\langle t(x_1)\rangle - \underline{P_2} \qquad \partial_2(\underline{\Theta}) = t(\square)\underline{T} - \underline{T}\,\langle t(x_1)\rangle$$

and case $\underline{\Pi_2}$ is similar. The homology is the one of the chain complex obtained by tensoring with $\mathcal{Z}^{\mathrm{op}}$, which amounts to "erase contexts", i.e. all symbols which are not elements of $\mathbb{Z}$ or underlined:

$$\mathbb{Z}\underline{\{\Pi_1, \Pi_2, \Theta\}} \xrightarrow{\tilde{\partial}_2} \mathbb{Z}\underline{\{M_1, M_2, P_1, P_2, T\}} \xrightarrow{\tilde{\partial}_1} \mathbb{Z}\underline{\{m, p_1, p_2, t\}} \xrightarrow{\tilde{\partial}_0} \mathbb{Z}$$

above, $\mathbb{Z}\underline{X}$ denotes the free abelian group (or equivalently $\mathbb{Z}$-module) on a set X and the linear maps are defined by

$$\tilde{\partial}_0(\underline{m}) = \underline{1} \qquad \tilde{\partial}_0(\underline{p_i}) = 0 \qquad \tilde{\partial}_0(\underline{t}) = 0$$
$$\tilde{\partial}_1(\underline{M_i}) = -\underline{p_i} - \underline{m} \qquad \tilde{\partial}_1(\underline{P_i}) = \underline{p_{1-i}} - \underline{p_i} - \underline{t} \qquad \tilde{\partial}_1(\underline{T}) = -2\underline{t}$$
$$\tilde{\partial}_2(\underline{\Pi_i}) = \underline{T} - \underline{P_1} - \underline{P_2} \qquad \tilde{\partial}_2(\underline{\Theta}) = 0$$

and therefore the homology groups are

$$\begin{aligned}
H_0 &= \mathbb{Z}\underline{\{1\}}/(\underline{1}) = 0 \\
H_1 &= \mathbb{Z}\underline{\{m, p_1, p_2, t\}}/(-\underline{p_i} - \underline{m}, \underline{p_{1-i}} - \underline{p_i} - \underline{t}, -2\underline{t}) = \mathbb{Z} \\
H_2 &= \mathbb{Z}\underline{\{M_1, M_2, P_1, P_2, T\}}/(\underline{T} - \underline{P_1} - \underline{P_2}) = \mathbb{Z}^4
\end{aligned}$$

The homology groups are of the form $\mathbb{Z}^{r_i}$ and their rank is r_i. From $r_1 = 1$, we deduce that any presentation of the theory will have at least one generating operation (a fact which would have been quite obvious to establish directly), and from $r_2 = 4$ that any presentation has at least four relations (it is not one-based!). The fact that the relations M_1 and M_2 are needed is more or less expected because they do not interact with other rules (see below). However, the rule P_1, P_2 and T are forming critical pairs, and a priori those could have been used to remove two of the relations, as explained in Section 2.3. In fact, we would have reached a similar conclusion by considering the variant of the example without m, M_1 and M_2 (we would have had $H_2 = \mathbb{Z}^2$ and thus a theory which is not one-based), but the

models would have been less intuitive.

In passing, we can formalize the fact observed above that when a rule does not occur in any critical pair, it will be involved in no relation in homology and thus will contribute to one in the rank of the homology. Again, the above example shows that homology gives interesting results even outside this "trivial case".

▶ **Proposition 24.** *Consider a theory with a convergent presentation containing n rules which form no critical pair other rules. Any presentation of this theory has at least n rules. In particular, any rewriting system without critical pairs is minimal wrt relations.*

4 Coherent presentations

A resolution of a Lawvere theory is obtained by an "abelianization" process: in $\mathcal{M}_1$ we only recall which operations in which context are used, but not the order they are used in, similarly for the rules in $\mathcal{M}_2$, etc. This suggests extending the notion of presentation, so that the module $\mathcal{M}_3$ is the abelianization of something too, as we briefly mention.

▶ **Definition 25.** An *extended rewriting system* consists of a rewriting system P together with a set P_3 of *homotopy generators* and two functions $\sigma_2, \tau_2 : \mathsf{P}_3 \to \mathsf{P}_2^\top$:

$$P \quad = \quad \begin{tikzcd}
\mathsf{P}_0 \arrow[d, "\iota_0"] & \mathsf{P}_1 \arrow[d, "\iota_1"] \arrow[l, shift right, "\sigma_0"'] \arrow[l, shift left, "\tau_0"] & \mathsf{P}_2 \arrow[d, "\iota_2"] \arrow[l, shift right, "\sigma_1"'] \arrow[l, shift left, "\tau_1"] & \mathsf{P}_3 \arrow[l, shift right, "\sigma_2"'] \arrow[l, shift left, "\tau_2"] \\
\mathsf{P}_0^* & \mathsf{P}_1^* \arrow[l, shift right, "\sigma_0^*"'] \arrow[l, shift left, "\tau_0^*"] & \mathsf{P}_2^\top \arrow[l, shift right, "\sigma_1^\top"'] \arrow[l, shift left, "\tau_1^\top"] &
\end{tikzcd} \qquad \text{such that} \quad \begin{array}{l} \sigma_1^\top \circ \sigma_2 = \sigma_1^\top \circ \tau_2 \\ \tau_1^\top \circ \sigma_2 = \tau_1^\top \circ \tau_2 \end{array}$$

where $\mathsf{P}_0 = \{1\}$, thus $\mathsf{P}_0^* = \mathbb{N}$ as before, and $\mathsf{P}_2^\top$ is the set of 2-cells of the cartesian (2,1)-category freely generated by adding the elements of P_2 as invertible 2-cells to the free cartesian category P_1^*. It is *coherent* when any 2-cells with same source and target are related by the smallest congruence generated by P_3.

Intuitively, in a coherent rewriting system the set P_3 is big enough to relate two possible rewriting paths (or zig-zags) between the same terms. Newman's lemma thus reformulate as follows in this context:

▶ **Lemma 26.** *Given a convergent rewriting system P, its extension obtained by taking the set of confluence diagrams induced by critical pairs as P_3 is coherent.*

Finally, the abelianization process mentioned above can be formulated as follows:

▶ **Proposition 27.** *To any coherent presentation P one can associate a partial free resolution with $\mathcal{R}\mathsf{P}_i$ as modules, for $0 \leq i \leq 3$, as in (4).*

Notice that by Lemma 26, we recover the construction of Section 3.5 as a particular case. Also, it can be noticed that all the constructions we have been performing are compatible with the laws induced by the cartesian structure on cells (the definitions have in fact been chosen so that this is true).

▶ **Example 28.** Consider the following term rewriting system

$$\mathsf{P} \quad = \quad \langle d : 2, t : 0, f : 0 \quad | \quad T : d(t, x_1) \Rightarrow t, \quad T' : d(x_1, t) \Rightarrow t, \quad F : d(f, f) \Rightarrow f \rangle$$

corresponding to the famous *parallel* implementation of the disjunction, sometimes called *por* (d stands for disjunction, t for true and f for false), which was used by Melliès as a central example for standardization [21] (incidentally, this paper notices the similarity with

algebraic topology...). There is one confluent critical pair $\begin{tikzcd} d(t,t) \arrow[r, bend left, "{[T]\langle t\rangle}"] \arrow[r, bend right, "{[T']\langle t\rangle}"'] \arrow[r, phantom, "\Theta"] & t \end{tikzcd}$ and thus the presentation can be extended into a coherent one by setting $\mathsf{P}_3 = \{\Theta\}$ with expected source and target. By Proposition 27, we recover the resolution of Section 3.5, and one can easily compute the associated homology: we have $H_0(\mathcal{T}) = 0$, $H_1(\mathcal{T}) = \mathbb{Z}$ and $H_2(\mathcal{T}) = \mathbb{Z}^3$. Any presentation of this theory thus has at least 3 rules, providing another example of a non-trivial theory which is not one-based.

The above definition constitutes a generalization of polygraphs to Lawvere theories, using which one can show an analogous of Squier's homotopical theorem [29], which implies the homological one. Burroni's original paper on polygraphs shows that those theories can be described by polygraphs by considering explicitly the cartesian structure (duplications and erasures of variables) [4]. By contrast, this structure is implicit in this work, thus giving rise to much smaller and manipulable rewriting systems. It would be interesting to compare the two resulting homologies though. Also, as in the case of polygraphs, the formulation of Definition 25 should make it clear that this definition can be generalized in any dimension. Finally, we should mention that in the case of presentations of monoids, Tietze transformations and completion procedures can be generalized to coherent presentations [5]; we expect that similar constructions can be performed in the setting developed in this paper.

5 Extensions and future work

In conclusion, we would like to mention some other possible generalizations of this work, which we plan to investigate and detail in future work. For instance, the generalization to term rewriting systems with multiple sorts is easy (it roughly consists in allowing P_0 to contain multiple elements and use P_0^* instead of $\mathbb{N}$ for the objects of our ringoids).

One should be able to continue the resolution in higher dimension, as done for monoids [11], by using critical n-uples for P_{n+1}. In particular, the next dimension of the resolution can easily be done and allows to compute $H_3(\mathcal{T})$ for a theory $\mathcal{T}$, whose rank provides a lower bound on the number of critical pairs of any convergent presentation of $\mathcal{T}$. Consider the rewriting system with generators i, h and k of arity one, generators a and f of arity two, and three rules

$$h(a(x_1,x_2)) \Rightarrow a(f(x_1,x_1),x_2) \quad k(a(x_1,x_2)) \Rightarrow a(f(x_1,x_1),x_2) \quad a(f(i(x_1),i(x_1)),x_2) \Rightarrow a(x_1,x_2)$$

One can compute that $H_3(\mathcal{T})$ is not finitely generated, showing that it cannot be presented by a finite convergent rewriting system (since any such would have a finite number of critical pairs), even though this theory $\mathcal{T}$ has a decidable equality. This generalizes to terms rewriting systems Squier's example for monoids [28].

Computations are quite time-consuming: we plan on implementing those to be able to study more full-fledged examples. Also, many natural examples (e.g. lattices) contain commutative operations, for which there is no hope of obtaining a terminating rewriting system, which suggests that we should investigate a generalization of the construction for rewriting modulo.

References

1 J. Adámek and J. Rosicky. *Locally presentable and accessible categories*, volume 189. Cambridge University Press, 1994.

2 M. Barr. Cartan-Eilenberg cohomology and triples. *Journal of Pure and Applied Algebra*, 112(3):219–238, 1996.

3 J. M. Beck. *Triples, algebras and cohomology.* PhD thesis, Columbia Univ, 1967.
4 A. Burroni. Higher-dimensional word problems with applications to equational logic. *Theoretical computer science*, 115(1):43–62, 1993.
5 Y. Guiraud, P. Malbos, and S. Mimram. A homotopical completion procedure with applications to coherence of monoids. In *RTA*, volume 21, pages 223–238. Dagstuhl, 2013.
6 A. Hatcher. *Algebraic Topology.* Cambridge University Press, 2002.
7 G. Higman and B. H. Neumann. Groups as groupoids with one law. *Publicationes Mathematicae Debrecen*, 2(215-227):228, 1952.
8 M. Jibladze and T. Pirashvili. Cohomology of algebraic theories. *Journal of Algebra*, 137(2):253–296, 1991.
9 M. Jibladze and T. Pirashvili. Quillen cohomology and Baues-Wirsching cohomology of algebraic theories. *Cahiers de top. et géom. diff. cat.*, 47(3):163–205, 2006.
10 D. E. Knuth and P. B. Bendix. Simple word problems in universal algebras. In *Automation of Reasoning*, pages 342–376. Springer, 1983.
11 Y. Kobayashi. Complete rewriting systems and homology of monoid algebras. *Journal of Pure and Applied Algebra*, 65(3):263–275, 1990.
12 Y. Lafont and A. Prouté. Church-rooser property and homology of monoids. *Mathematical Structures in Computer Science*, 1(03):297–326, 1991.
13 F. W. Lawvere. Functorial semantics of algebraic theories. *Proceedings of the National Academy of Sciences of the United States of America*, 50(5):869, 1963.
14 J.-L. Loday and B. Vallette. *Algebraic operads*, volume 346 of *Grundlehren der Mathematischen Wissenschaften.* Springer, Heidelberg, 2012.
15 S. Mac Lane. *Homology.* Springer-Verlag, Berlin, 1995.
16 P. Malbos. *Critères de finitude homologique pour la non convergence des systèmes de réécriture de termes.* PhD thesis, Université de Montpellier II, 2004.
17 W. Mccune et al. Single Axioms: With and Without Computers. In *Computer Mathematics: Proceedings of the Fourth Asian Symposium (ASCM 2000)*, page 83. World Scientific, 2000.
18 W. McCune, R. Padmanabhan, and R. Veroff. Yet another single law for lattices. *Algebra Universalis*, 50(2):165–169, 2003.
19 W. McCune, R. Veroff, B. Fitelson, K. Harris, A. Feist, and L. Wos. Short single axioms for Boolean algebra. *Journal of Automated Reasoning*, 29(1):1–16, 2002.
20 R. McKenzie. Equational Bases for Lattice Theories. *Math. Scandinavica*, 27:24–38, 1970.
21 P.-A. Melliès. Axiomatic rewriting theory VI: Residual theory revisited. In *Rewriting techniques and applications*, pages 24–50. Springer, 2002.
22 B. Mitchell. Rings with several objects. *Advances in Mathematics*, 8(1):1–161, 1972.
23 B. H. Neumann. Another single law for groups. *Bulletin of the Australian Mathematical Society*, 23(01):81–102, 1981.
24 B. H. Neumann et al. Yet another single law for groups. *Illinois Journal of Mathematics*, 30(2):295–300, 1986.
25 M. H. A. Newman. On theories with a combinatorial definition of "equivalence". *Annals of mathematics*, pages 223–243, 1942.
26 R. Padmanabhan and R. Quackenbush. Equational theories of algebras with distributive congruences. *Proceedings of the American Mathematical Society*, 41(2):373–377, 1973.
27 D. Potts. Axioms for semi-lattices. *Canad. Math Bulletin*, 8:519, 1965.
28 C. Squier and F. Otto. The word problem for finitely presented monoids and finite canonical rewriting systems. In *Rewriting Techniques and Applications*, pages 74–82. Springer, 1987.
29 C. C. Squier, F. Otto, and Y. Kobayashi. A finiteness condition for rewriting systems. *Theoretical Computer Science*, 131(2):271–294, 1994.
30 A. Tarski. Ein Beitrag zur Axiomatik der Abelschen Gruppen. *Fundamenta Mathematicae*, 1(30):253–256, 1938.
31 H. Tietze. Über die topologischen Invarianten mehrdimensionaler Mannigfaltigkeiten. *Monatsh. Math. Phys.*, 19(1):1–118, 1908.

A Proof of Theorem 22

The proof given here, is similar to the "standard" one given for the construction of Squier's resolution [28]; the reader is advised to read the presentation of this construction given in [12]. We first show that the sequence is a chain complex, i.e. that the composite of two successive boundary maps is zero: $\partial_i \circ \partial_{i+1} = 0$, which implies immediately that $\operatorname{im} \partial_{i+1} \subseteq \ker \partial_i$.

- *Case* $\varepsilon \circ \partial_0$. Suppose given an operation $f \in \mathsf{P}_1$ of arity n. We have

$$\varepsilon \circ \partial_0(f) = \varepsilon\left(\sum_{i=1}^{n} \kappa_i(f)\underline{1}\langle x_i\rangle\right) - \varepsilon\left(\underline{1}\langle f\rangle\right) = \sum_{i=1}^{n} \kappa_i(f)\underline{\star}\langle x_i\rangle - \underline{\star}\langle f\rangle = 0$$

  because, by definition, $\varepsilon(\underline{1}) = \underline{\star}$ and the relations defining $\mathcal{Z}$ (as illustrated in Example 17).

- *Case* $\partial_0 \circ \partial_1$. Suppose given a relation $R \in \mathsf{P}_2$, with $R : t \Rightarrow u$. We have

$$\begin{aligned}\partial_0 \circ \partial_1(R) = \partial_0(\underline{u}) - \partial_0(\underline{t}) &= \sum_{i=1}^{n} \kappa_i(u)\underline{1}\langle x_i\rangle - \underline{1}\langle u\rangle - \sum_{i=1}^{n} \kappa_i(t)\underline{1}\langle x_i\rangle + \underline{1}\langle t\rangle \\ &= \sum_{i=1}^{n} (\kappa_i(u) - \kappa_i(t))\,\underline{1}\langle x_i\rangle - \underline{1}(u-t) = 0\end{aligned}$$

  The second equality follows from the lemma stating that $\partial_0(\underline{t}) = (\sum_{i=1}^{n} \kappa_i(t)\underline{1}\langle x_i\rangle) - \underline{1}\langle t\rangle$ which is easily shown by induction on t. The last equality is due to the relations defining $\mathcal{R}$ (as illustrated in Example 15).

- *Case* $\partial_1 \circ \partial_2$. Suppose given a critical pair $(C_1[R_1]v_1, C_2[R_2]v_2) \in \mathsf{P}_3$ with $R_i : t_i \to u_i$ and $C_1[t_1]v_1 = t = C_2[t_2]v_2$. We have

$$\begin{aligned}\partial_1 \circ \partial_2(C_1[R_1]v_1, C_2[R_2]v_2) &= \partial_1(C_2\underline{R_2}v_2) - \partial_1(C_1\underline{R_1}v_1) + \partial_1(\underline{S_2}) - \partial_1(\underline{S_1}) \\ &= C_1\underline{u_1}v_1 - \underline{t} - C_2\underline{u_2}v_2 + \underline{t} + C_2\underline{u_2}v_2 - \underline{\hat{t}} - C_1\underline{u_1}v_1 + \underline{\hat{t}} \\ &= 0\end{aligned}$$

  where $S_1 : C_1[u_1]v_1 \xrightarrow{*} \hat{t}$ and $S_2 : C_1[u_1]v_1 \xrightarrow{*} \hat{t}$ are paths witnessing the confluence of the critical pair, as in (5), which corresponds algebraically to the fact that the following square is a cycle:

$$\begin{tikzcd} & t \arrow[dl, "C_1[R_1]v_1"'] \arrow[dr, "C_2[R_2]v_2"] & \\ C_1[u_1]v_1 \arrow[dr, "S_1"'] & & C_2[u_2]v_2 \arrow[dl, "S_2"] \\ & \hat{t} & \end{tikzcd}$$

  In the second equality, we have used a lemma stating that for any rewriting path $S : t \xrightarrow{*} u$ we have $\partial_1 S = \underline{u} - \underline{t}$, which is easily shown by induction on S.

In order to show that the sequence is exact, we need to prove the reverse inclusions, i.e. $\ker \partial_i \subseteq \operatorname{im} \partial_{i+1}$. We do this by constructing a *contracting homotopy*, i.e. $\mathbb{Z}$-linear (not $\mathcal{R}$-linear!) maps s_i,

$$\mathcal{R}\underline{\mathsf{P}_3} \underset{s_2}{\overset{\partial_2}{\rightleftarrows}} \mathcal{R}\underline{\mathsf{P}_2} \underset{s_1}{\overset{\partial_1}{\rightleftarrows}} \mathcal{R}\underline{\mathsf{P}_1} \underset{s_0}{\overset{\partial_0}{\rightleftarrows}} \mathcal{R}\underline{\mathsf{P}_0} \xrightarrow{\varepsilon} \mathcal{Z} \longrightarrow 0$$

satisfying $\partial_{i+1} \circ s_{i+1} + s_i \circ \partial_i = \mathrm{id}_{\mathcal{R}\underline{\mathsf{P}_i}}$. It is well-known that the existence of such a family of maps ensure that the chain complex is acyclic at $\mathcal{R}\underline{\mathsf{P}_i}$ [15]. The intuition here is that s_0 "chooses" a representative for each morphism in $\mathcal{T}$, the term in normal form, s_1 a rewriting path from a term to is normal form, s_2 a standardization of each rewriting path, etc.

- *Case* $\mathcal{Z}$. Because of its defining relations, the module $\mathcal{Z}$ is easily shown to be generated by $\star$ and therefore ε is surjective since $\star = \varepsilon(\underline{1})$.

- *Case* $\mathcal{R}\underline{\mathsf{P}_0}$. Because of the relations defining $\mathcal{Z}$, $\ker\varepsilon$ can easily be shown to be generated by $\sum_i \kappa_i(f)\underline{1}\,\langle x_i\rangle - \underline{1}\,\langle f\rangle$, from which we immediately have that $\operatorname{im}\partial_0 = \ker\varepsilon$. We define a $\mathbb{Z}$-linear map $s_0 : \mathcal{R}\underline{\mathsf{P}_0} \to \mathcal{R}\underline{\mathsf{P}_1}$ as follows. Given an element $C\underline{1}t$ in $\mathcal{R}\underline{\mathsf{P}_0}$ in arity n, t is an equivalence class of terms by definition. Since the rewriting system is convergent, there is a unique term $\hat{t}$ in normal form in this class and we define $s_0(C\underline{1}t) = -C\underline{\hat{t}}$. For such an element, we have

$$\partial_0(s_0(C\underline{1}t)) = \partial_0(C\underline{\hat{t}}) = -\sum_{i=1}^{n} C\circ(\kappa_i(t))\underline{1}\,\langle x_i\rangle + C\underline{1}t = C\underline{1}t - \eta\circ\varepsilon(C\underline{1}t)$$

- *Case* $\mathcal{R}\underline{\mathsf{P}_1}$. We define $s_1 : \mathcal{R}\underline{\mathsf{P}_1} \to \mathcal{R}\underline{\mathsf{P}_2}$ as follows. Given a term $t \in \mathsf{P}_1^*$, we write $\hat{\hat{t}} : t \xrightarrow{*} \hat{t}$ for the path rewriting t into its normal form using the *leftmost innermost strategy*; given a term $u\circ t$ with $t = \langle t_1,\dots,t_n\rangle$, it schematically reduces in the following way:

$$\begin{aligned} u\circ\langle t_1,t_2,\dots,t_n\rangle &\xrightarrow{*} u\circ\left\langle \hat{t}_1,t_2,\dots,t_n\right\rangle \xrightarrow{*} u\circ\left\langle \hat{t}_1,\hat{t}_2,\dots,t_n\right\rangle \xrightarrow{*} \dots \\ &\xrightarrow{*} u\circ\left\langle \hat{t}_1,\hat{t}_2,\dots,\hat{t}_n\right\rangle \xrightarrow{*} \hat{u}\circ\left\langle \hat{t}_1,\hat{t}_2,\dots,\hat{t}_n\right\rangle \xrightarrow{*} \widehat{u\circ t} \end{aligned}$$

Given $C\underline{f}u$ in $\mathcal{R}\underline{\mathsf{P}_1}$, we define $s_1(C\underline{f}u) = -C\widehat{\widehat{\underline{f\circ\hat{u}}}}$, where given $u = \langle u_1,\dots,u_n\rangle$, $\hat{u}$ is a notation for $\langle \hat{u}_1,\dots,\hat{u}_n\rangle$. We have

$$\begin{aligned} s_0(\partial_0(C\underline{f}u)) &= s_0\left(\sum_i (C\circ(\kappa_i(f))u)\,\underline{1}\,\langle u_i\rangle\right) - s_0\left(C\underline{1}\,(f\circ u)\right) \\ &= -\sum_i (C\circ(\kappa_i(f))u)\,\underline{\hat{u}_i} + C\widehat{\underline{f\circ u}} \end{aligned}$$

and

$$\begin{aligned} \partial_1(s_1(C\underline{f}u)) &= -\partial_1(C\widehat{\widehat{\underline{f\circ\hat{u}}}}) = -C\widehat{\underline{f\circ u}} + C\underline{f\circ\hat{u}} \\ &= -C\widehat{\underline{f\circ u}} + \sum_i (C\circ(\kappa_i(f))u)\,\underline{\hat{u}_i} + C\underline{f}u \end{aligned}$$

and therefore

$$s_0\circ\partial_0 + \partial_1\circ s_1 = \mathrm{id}_{\mathcal{R}\mathsf{P}_1}$$

- *Case* $\mathcal{R}\underline{\mathsf{P}_2}$. We define $s_2 : \mathcal{R}\underline{\mathsf{P}_2} \to \mathcal{R}\underline{\mathsf{P}_3}$ as follows. Suppose given $C\underline{R}v \in \mathcal{R}\underline{\mathsf{P}_2}$ for some rewriting rule $R : t \Rightarrow u$ in P_2. We then distinguish two cases:

  1. If the term $t\circ\hat{v}$ is not reducible by any other rule than R then we define $s_2(C\underline{R}v) = 0$.

  2. Otherwise, we choose the left innermost rule $R' : t' \Rightarrow u'$ which reduces $t\circ\hat{v}$, i.e. $t\circ\hat{v} = D[t']v'$. The critical pair $([R]\hat{v}, D[R']v')$ is confluent because the rewriting system is supposed to be:

$$\begin{tikzcd} & {[t]\hat{v} = D[t']v'} \arrow[dl, "{[R]\hat{v}}"'] \arrow[dr, "{D[R']v'}"] & \\ {[u]\hat{v}} \arrow[dr, "{\widehat{\widehat{[u]\hat{v}}}}"'] & & D[u']v' \arrow[dl, "{\widehat{\widehat{D[u']v'}}}"] \\ & {\widehat{t\circ v}} & \end{tikzcd}$$

This suggests defining

$$s_2(C\underline{R}v) \quad = \quad -C(\underline{[R]\hat{v}, D[R']v'}) + s_2\left(\widehat{\widehat{[u]\hat{v}}}\right) - s_2\left(\widehat{\widehat{D[u']v'}}\right)$$

We then proceed by noetherian induction to show that

$$s_1 \circ \partial_1 + \partial_2 \circ s_2 \quad = \quad \mathrm{id}_{\mathcal{R}\underline{\mathsf{P}_2}}$$

In the first case, R is the only rule which can reduce $t \circ \hat{v}$ and hence

$$\widehat{\widehat{t \circ \hat{v}}} \quad = \quad [R]\hat{v} \cdot \widehat{\widehat{[u]\hat{v}}}$$

Therefore

$$s_1 \circ \partial_1(C\underline{R}v) = s_1(C\underline{u}v) - s_1(C\underline{t}v) = -C\widehat{\widehat{\underline{u \circ \hat{v}}}} + C\widehat{\widehat{\underline{t \circ \hat{v}}}} = C\underline{R}v$$

On the other hand, we have $\partial_2 \circ s_2(C\underline{R}v) = 0$ and therefore $s_1 \circ \partial_1 + \partial_2 \circ s_2(C\underline{R}v) = (C\underline{R}v)$. In the second case, we have, by induction

$$(s_1 \circ \partial_1 + \partial_2 \circ s_2)(C\widehat{\widehat{\underline{[u]\hat{v}}}}) = C\widehat{\widehat{\underline{[u]\hat{v}}}} \qquad\qquad (s_1 \circ \partial_1 + \partial_2 \circ s_2)(C\widehat{\widehat{\underline{D[u']v'}}}) = C\widehat{\widehat{\underline{D[u']v'}}}$$

from which follows

$$\begin{aligned}
\partial_2 \circ s_2(C\underline{R}v) &= -\partial_2\left(C(\underline{[R]\hat{v}, D[R']v'})\right) + \partial_2 \circ s_2\left(C\widehat{\widehat{\underline{[u]\hat{v}}}}\right) - \partial_2 \circ s_2\left(C\widehat{\widehat{\underline{D[u']v'}}}\right) \\
&= -CD\underline{R'}v' + C\underline{R}\hat{v} - s_1 \circ \partial_1\left(C\widehat{\widehat{\underline{[u]\hat{v}}}}\right) + s_1 \circ \partial_1\left(C\widehat{\widehat{\underline{D[u']v'}}}\right)
\end{aligned}$$

On the other hand, we have

$$s_1 \circ \partial_1(C\underline{R}v) = s_1(C\underline{u}v) - s_1(C\underline{t}v) = -C\widehat{\widehat{\underline{u \circ \hat{v}}}} + C\widehat{\widehat{\underline{t \circ \hat{v}}}}$$

The rule R' is innermost in $t \circ \hat{v}$. Therefore

$$\widehat{\widehat{t \circ \hat{v}}} = D[R']v' \cdot \widehat{\widehat{D[u']v'}}$$

and we have

$$\begin{aligned}
s_1 \circ \partial_1(C\underline{R}v) &= -C\widehat{\widehat{\underline{u \circ \hat{v}}}} + C\widehat{\widehat{\underline{t \circ \hat{v}}}} \\
&= -C\widehat{\widehat{\underline{u \circ \hat{v}}}} + C\underline{D[R']v'} + C\widehat{\widehat{\underline{D[u']v'}}} \\
&= CD\underline{R'}v' + s_1 \circ \partial_1\left(C\widehat{\widehat{\underline{[u]\hat{v}}}}\right) - s_1 \circ \partial_1\left(C\widehat{\widehat{\underline{D[u']v'}}}\right)
\end{aligned}$$

from which follows once again that

$$s_1 \circ \partial_1 + \partial_2 \circ s_2(C\underline{R}v) = (C\underline{R}v)$$

and we conclude. ◀