

CONFLUENCE OF ALGEBRAIC REWRITING SYSTEMS

CYRILLE CHENAVIER - BENJAMIN DUPONT – PHILIPPE MALBOS

Abstract – Convergent rewriting systems on algebraic structures give methods to solve decision problems, to prove coherence results, and to compute homological invariants. These methods are based on higher-dimensional extensions of the critical branching lemma that proves local confluence from confluence of the critical branchings. The analysis of local confluence of rewriting systems on algebraic structures, such as groups or linear algebras, is complicated because of the underlying algebraic axioms. This article introduces the structure of algebraic polygraph modulo that formalizes the interaction between the rules of an algebraic rewriting system and the inherent algebraic axioms, and we show a critical branching lemma for algebraic polygraphs. We deduce a critical branching lemma for rewriting systems on algebraic models whose axioms are specified by convergent modulo rewriting systems. We illustrate our constructions for string, linear, and group rewriting systems.

Keywords – Term rewriting modulo, algebraic polygraphs, string rewriting, linear rewriting, group rewriting.

M.S.C. 2010 – Primary: 68Q42, 18C10. **Secondary:** 16S36, 13P10.

1. INTRODUCTION

Completion procedures. The critical-pair completion (CPC) is an approach developed in the mid sixties that combines completion procedures and the notion of *critical pair*, also called *critical branching* [3, 5, 45]. It originates from theorem proving [44], polynomial ideal theory [4, 25], word problem in algebras [29, 33, 42], and has found many applications to solve algorithmic problems, see [5, 24] for an historical account. In the mid eighties CPC has found original and deep applications in algebra in order to solve coherence problems for monoids [20, 47], and monoidal categories [10, 18], or to compute homological invariants of associative algebras [1], and monoids [30, 46]. The CPC was extended to two-dimensional rewriting systems in [17, 41]. More recently, higher-dimensional extensions of the CPC were applied to the computation of free resolutions and cofibrant replacements of algebraic and categorical structures [15, 16, 19, 35] and operads [37, 38]. The obstructions in each dimension are formulated in terms of critical branchings. While generators and rules are in dimension 1 and 2 respectively, the critical branchings, and the critical triple branchings, that is overlappings of rules on critical branchings, describe 3-dimensional and 4-dimensional cocycles respectively. This generalizes in higher-dimensions, where for $n \geq 4$, the n -dimensional cocycles are described by overlappings of a rule on a critical $(n - 1)$ -branching. These constructions based on CPC are known for monoids, small categories, and algebras. However, the extension to a wide range of algebraic structures is complicated due to the interaction between the rewriting rules and the inherent axioms of the algebraic structure. For this reason, the higher-dimensional extensions of the CPC for a wide range of algebraic structures, including groups, Lie rings, is still an open problem.

1. Introduction

Critical branching lemma. One of the main tools to reach confluence in CPC procedures for algebraic rewriting systems is the *critical branching lemma*, by Knuth-Bendix, [29], and Nivat, [42]. Nivat showed that the local confluence of a string rewriting system (SRS) is decidable, whether it is terminating or not. The proof is based on classification of the local branchings into *orthogonal* branchings, that involve two rules that do not overlap, and *overlapping* branchings. A *critical branching* is a minimal overlapping application of two rules on the same redex. When the orthogonal branchings are confluent, if all critical branchings are confluent, then local confluence holds. Thus, the main argument to achieve critical branching lemma is to prove that orthogonal and overlapping branchings are confluent. For SRS and term rewriting systems (TRS), orthogonal branchings are always confluent, and confluence of critical branchings implies confluence of overlapping branchings. The situation is more complicated for rewriting systems on a linear structure.

The well known approaches of rewriting in the linear context consist in orienting the rules with respect to an ambient monomial order, and critical branching lemma is well known in this context. However, some algebras do not admit any higher-dimensional finite convergent presentation on a fixed set of generators with respect to a monomial order, [16]. Due to algebraic perspectives, an approach of linear rewriting where the orientation of rules does not depend of a monomial order was introduced in [16]. However, in that setting there are two conditions to guarantee a critical branching lemma, namely termination and positivity of reductions. A positive reduction for a linear rewriting system (LRS), as defined in [16], is the application of a reduction rule on a monomial that does not appear in the polynomial context. For instance, consider the LRS on an associative algebra given in [16] defined by the following two rules

$$\alpha : xy \rightarrow xz, \quad \beta : zt \rightarrow 2yt.$$

It has no critical branching, but it has the following non-confluent additive branching:

$$\begin{array}{c}
 \begin{array}{l}
 \alpha t + xzt \\
 xy t + xzt \\
 xy t + x\beta
 \end{array}
 \begin{array}{l}
 \xrightarrow{\quad} 2xzt \\
 = \\
 \xrightarrow{\quad} 3xyt
 \end{array}
 \begin{array}{l}
 \xrightarrow{2x\beta} 4xyt \\
 \xrightarrow{xzt + x\beta} xzt + 2xyt \\
 \xrightarrow{\alpha t + 2xyt} \alpha t + 2xyt \\
 \xrightarrow{3\alpha t} 3xzt
 \end{array}
 \begin{array}{l}
 \xrightarrow{4\alpha t} 4xz t \\
 \xrightarrow{3x\beta} 3xzt \\
 \xrightarrow{6\alpha t} 6xyt
 \end{array}
 \begin{array}{l}
 \xrightarrow{4x\beta} \dots \\
 \xrightarrow{6\alpha t} \dots
 \end{array}
 \end{array}$$

The dotted arrows correspond to non positive reductions. This example illustrates that the lack of termination is an obstruction to confluence of orthogonal branchings in a *left-monomial LRS*, that is whose rules transform a monomial into a polynomial. Indeed, the critical branching lemma for linear 2-dimensional polygraphs states that a terminating left-monomial linear polygraph is locally confluent if and only if all its critical branchings are confluent, [16, Theorem 4.2.1]

Rewriting modulo. Rewriting modulo appears naturally in algebraic rewriting when studied reductions are defined modulo the axioms of an ambient algebraic or categorical structure, *e.g.* rewriting in commutative, groupoidal, linear, pivotal, weak structures. Furthermore, rewriting modulo facilitates the analysis of confluence. In particular, rewriting modulo a set of relations makes the property of confluence easier to prove. Indeed, the family of critical branchings that should be considered in the analysis of confluence is reduced, and the non-orientation of a part of the relations allows more flexibility when reaching confluence.

The most naive approach of rewriting modulo is to consider the rewriting system $\rho R \rho$ consisting in rewriting on congruence classes modulo the axioms P . This approach works for some equational theories, such as associative and commutative theories. However, it appears inefficient in general for the analysis of confluence. Indeed, the reducibility of an equivalence class needs to explore all the class, hence it requires all equivalence classes to be finite. Another approach of rewriting modulo has been considered by Huet in [22], where rewriting sequences involve only oriented rules and no equivalence steps, and the confluence property is formulated modulo equivalence. However, for algebraic rewriting systems such rewriting modulo is too restrictive for computations, see [27]. Peterson and Stickel introduced in [43] an extension of Knuth-Bendix's completion procedure, [29], to reach confluence of a rewriting system modulo an equational theory, for which a finite, complete unification algorithm is known. They applied their procedure to rewriting systems modulo axioms of associativity and commutativity, in order to rewrite in free commutative groups, commutative unitary rings, and distributive lattices. Jouannaud and Kirchner enlarged this approach in [26] with the definition of rewriting properties for any rewriting system modulo S such that $R \subseteq S \subseteq \rho R \rho$. They also proved a critical branching lemma and developed a completion procedure for rewriting systems modulo ρR , whose one-step reductions consist in application of a rule in R using P -matching at the source. Their completion procedure is based on a finite P -unification algorithm. Bachmair and Dershowitz in [2] developed a generalisation of Jouannaud-Kirchner's completion procedure using inference rules. Several other approaches have also been studied for TRS modulo to deal with various equational theories, see [28, 39, 40, 49].

Algebraic and categorical rewriting. In this article, we use the notion of cartesian polygraphs as categorical models of TRSs introduced in [36] to formulate our constructions and prove our results. The polygraphic language provides a unified categorical framework for algebraic rewriting paradigms: abstract, string, term, linear rewriting and their higher-dimensional versions. Polygraphs also provide a natural setting to formulate higher-dimensional rewriting concepts such as coherence, that is two-dimensional word problems [9, 20, 31, 47], and normalisation strategies as rewriting tools to prove homotopical properties in higher algebra theory, [15, 19]. In Section 2, we recall the notion of cartesian 2-dimensional polygraphs introduced in [36] as categorical interpretations of TRS and presentations of Lawvere algebraic theories. A *cartesian 2-polygraph* is defined by an equational signature (P_0, P_1) and a cellular extension P_2 of the free algebraic theory P_1^\times on (P_0, P_1) . A rewriting path corresponds to a 2-cell in the free algebraic 2-theory generated by the 2-polygraph (P_0, P_1, P_2) .

Algebraic polygraphs. In Section 3, we introduce a categorical model for rewriting in algebraic structures which formalizes the interaction between the rules of the rewriting system and the inherent axioms of the algebraic structure. We define the structure of *algebraic polygraph* as a data (P, Q, R) made of a cartesian 2-polygraph P and a set Q of generating ground terms and a cellular extension R on the ground terms. In Section 3.1, we introduce a notion of *positive reduction strategy* on an algebraic polygraph in order to select admissible rewriting steps used to formulate rewriting properties modulo. The idea is to avoid termination and confluence obstructions from the underlying axioms for the quotiented algebraic rewriting system defined as a projection of the positive reductions in Section 3.3.

Algebraic critical branching lemma. Following [14], in Section 3.2 we define the structure of algebraic polygraph modulo as a data $\mathcal{P} = (P, Q, R, S)$ made of an algebraic polygraph (P, Q, R) and a cellular extension S on the ground terms, and that depends on the cellular extension R and the algebraic axioms of P_2 . As a consequence, the rewriting properties of \mathcal{P} depend on the interaction between the rules of the

2. Preliminaries on algebraic theories

rewriting system and the inherent axioms of the algebraic structure. In Section 4, we prove the Newman lemma for quasi-terminating algebraic polygraphs modulo, stated as follows:

Theorem 4.1.5. *Let \mathcal{P} be a quasi-terminating algebraic polygraph modulo, and σ be a positive strategy on \mathcal{P} . If \mathcal{P} is locally σ -confluent modulo, then it is σ -confluent modulo.*

Then we prove a critical branching lemma for quasi-terminating algebraic polygraphs modulo.

Theorem 4.3.2. *Let $\mathcal{P} = (P, Q, R, S)$ be an algebraic polygraph modulo with a positive confluent strategy σ . If ${}_{\mathcal{P}}R_{\mathcal{P}}$ is quasi-terminating, then an algebraic rewriting system on \mathcal{P} is locally confluent if, and only if, its critical branchings are confluent.*

We deduce from this result a critical branching lemma for rewriting systems on algebraic structures, whose axioms are specified by TRS satisfying appropriate convergence properties modulo AC. Finally, we apply the above results to the linear rewriting setting. In particular, we explain why termination is a necessary condition to characterize local confluence in that case.

Convention and notations. An *abstract rewriting system* (ARS) is a data (X, R) made of a set X and a set R equipped with source and target maps $\partial^-, \partial^+ : R \rightarrow X$ called a *cellular extension* of X . An element r of R is denoted by $r_- \rightarrow r_+$, where $r_- := \partial^-(r)$ and $r_+ := \partial^+(r)$. We say that r composes with r' if $\partial^+(r) = \partial^-(r')$. We denote by $\xrightarrow{*}$ the symmetric, transitive closure of \rightarrow with respect to this composition. We say that x *rewrites into* y if $x \xrightarrow{*} y$.

The ARS (X, R) is *terminating* (resp. *quasi-terminating*) if there is no sequence $(x_n)_{n \in \mathbb{N}}$ such that $x_n \rightarrow x_{n+1}$ (resp. if for each sequence $(x_n)_{n \in \mathbb{N}}$ such that $x_n \rightarrow x_{n+1}$, the sequence $(x_n)_{n \in \mathbb{N}}$ contains an infinite number of occurrences of the same element). It is *confluent* if, whenever $x \xrightarrow{*} y$ and $x \xrightarrow{*} z$, there exists t such that $y \xrightarrow{*} t$ and $z \xrightarrow{*} t$. An element x of X is called a *normal form* for (X, R) if there is no y such that $x \rightarrow y$. Given an equivalence relation \equiv on X , we say that (X, R) is *confluent modulo* \equiv if, whenever $x \equiv y$ and $x \xrightarrow{*} x', y \xrightarrow{*} y'$, there exist $z, z' \in X$ such that $x' \xrightarrow{*} z, y' \xrightarrow{*} z'$, and $z \equiv z'$.

2. PRELIMINARIES ON ALGEBRAIC THEORIES

In this section we recall notions on algebraic theories from [32] and the structure of cartesian polygraph introduced in [36] as a categorical model of term rewriting systems.

2.1. Cartesian polygraphs and theories

2.1.1. Signature and terms. A *signature* on a set P_0 of *sorts* is a directed graph

$$P_0^* \begin{array}{c} \xleftarrow{\partial_0^-} \\ \xrightarrow{\partial_0^+} \end{array} P_1$$

on the free monoid P_0^* over P_0 . From a higher-dimensional rewriting approach, the data (P_0, P_1) is called a *1-polygraph*. An element α of P_1 is called an *operation*, and its source $\partial_0^-(\alpha) \in P_0^*$ is called its *arity*

2.1. Cartesian polygraphs and theories

and its target $\partial_0^+(\alpha) \in P_0$ its *coarity*. For sorts s_1, \dots, s_k , we denote $\underline{s} = s_1 \dots s_k$ their product in the free monoid P_0^* . We denote $|\underline{s}| = k$ the *length* of \underline{s} and the sort s_i in \underline{s} will be denoted by \underline{s}_i , so that $\underline{s}_i \in P_0$.

Recall from [32] that a (*multityped Lawvere algebraic*) *theory* on a set P_0 of sorts is a category with finite products \mathbb{T} together with a map $\iota : P_0 \rightarrow \mathbb{T}_0$, where \mathbb{T}_0 denotes the set of 0-cells, and such that every 0-cell in \mathbb{T}_0 is isomorphic to a finite product of 0-cells in $\iota(P_0)$. We denote by P_1^\times the *free theory generated* by a signature (P_0, P_1) . Its products on 0-cells are induced by products of sorts in P_0^* , and its 1-cells are *terms* over P_1 defined by induction as follows:

- i) the canonical projections $x_i^{\underline{s}} : \underline{s} \rightarrow \underline{s}_i$, for $1 \leq i \leq |\underline{s}|$ are terms, called *variables*,
- ii) for all terms $f : \underline{s} \rightarrow r$ and $f' : \underline{s} \rightarrow r'$ in P_1^\times , there exists a unique 1-cell $\langle f, f' \rangle : \underline{s} \rightarrow rr'$, called the *pairing* of terms f, f' , such that $x_1^{rr'} \langle f, f' \rangle = f$ and $x_2^{rr'} \langle f, f' \rangle = f'$,
- iii) for every operation $\varphi : \underline{r} \rightarrow \underline{s}$ in P_1 , \underline{s} in P_0^* and terms $f_i : \underline{s} \rightarrow \underline{r}_i$ in P_1^\times for $1 \leq i \leq |\underline{r}|$, there is a term $\varphi \langle f_1, \dots, f_{|\underline{r}|} \rangle : \underline{s} \rightarrow \underline{s}$.

We define the *size* of a term f as the minimal number, denoted by $|f|$, of operations used in its definition. The composition of terms f and g is denoted by concatenation fg . For all 0-cells $\underline{s}, \underline{s}'$ in P_1^\times , we denote by $\text{id}_{\underline{s}}$ the identity 1-cell on a 0-cell \underline{s} , we denote by $e_{\underline{s}}$ the *eraser* 1-cell defined as the unique 1-cell from \underline{s} to the terminal 0-cell 0. We denote respectively by $x_{\underline{s}}^{\underline{ss}'} : \underline{ss}' \rightarrow \underline{s}$ (resp. $x_{\underline{s}'}^{\underline{ss}'} : \underline{ss}' \rightarrow \underline{s}'$) the canonical projections. Finally, we denote by $\tau_{\underline{s}, \underline{s}'} : \underline{ss}' \rightarrow \underline{s}'\underline{s}$ the *exchange* 1-cell defined by $\tau_{\underline{s}, \underline{s}'} = \langle x_{\underline{s}'}^{\underline{ss}'}, x_{\underline{s}}^{\underline{ss}'} \rangle$.

2.1.2. Two-dimensional cartesian polygraphs. A *cartesian 2-polygraph* P is a data (P_0, P_1, P_2) made of

- i) a signature (P_0, P_1) ,
- ii) a cellular extension of the free theory P_1^\times , that is a set P_2 equipped with two maps

$$P_1^\times \begin{array}{c} \xleftarrow{\partial_1^-} \\ \xrightarrow{\partial_1^+} \end{array} P_2$$

satisfying the following *globular conditions* $\partial_0^\mu \circ \partial_1^- = \partial_0^\mu \circ \partial_1^+$, for $\mu \in \{-, +\}$.

In the sequel, by abuse of notation, we let P_i stand for the underlying of a polygraph P . An element A of P_2 is called a *rule* with *source* $\partial_1^-(A)$ and target $\partial_1^+(A)$, denoted respectively by A_- and A_+ . The globular conditions impose that a rule relates terms of same arity and coarity, and it will be pictured as follows:

$$\begin{array}{c} A_- \\ \curvearrowright \\ \underline{s} \quad \Downarrow A \quad r \\ \curvearrowleft \\ A_+ \end{array} \quad \text{with} \quad \underline{s} = \partial_0^-(A_-) = \partial_0^-(A_+), \quad r = \partial_0^+(A_-) = \partial_0^+(A_+).$$

2. Preliminaries on algebraic theories

2.1.3. Two-dimensional theories. Recall that a *2-category* is a category enriched in categories. Explicitly, a 2-category is a data \mathcal{C} made of a set \mathcal{C}_0 , whose elements are called the *0-cells* of \mathcal{C} , and, for all 0-cells x, y of \mathcal{C} , a category $\mathcal{C}(x, y)$, whose 0-cells and 1-cells are respectively the *1-cells* and *2-cells* from x to y of \mathcal{C} . This data is equipped with a functor

$$\star_0^{x,y,z} : \mathcal{C}(x, y) \times \mathcal{C}(y, z) \rightarrow \mathcal{C}(x, z),$$

for all 0-cells x, y, z of \mathcal{C} , and a specified 0-cell id_x of the category $\mathcal{C}(x, x)$. The composition \star_0 is associative, and the identities are local units for the composition. For $f_1 \in \mathcal{C}(x, y)$ and $f_2 \in \mathcal{C}(y, z)$, we write $f_1 \star_0 f_2$ instead of $f_1 \star_0^{x,y,z} f_2$. For 2-cells f_1, g_1 in $\mathcal{C}(x, y)$ such that $(f_1)_+ = (g_1)_-$, we denote by $f_1 \star_1 g_1$ their composition along a 1-cell from x to y . The compositions \star_0 and \star_1 satisfy the *exchange law*:

$$(f_1 \star_0 f_2) \star_1 (g_1 \star_0 g_2) = (f_1 \star_1 g_1) \star_0 (f_2 \star_1 g_2),$$

for all composable 2-cells f_i, g_i in \mathcal{C} .

Recall that a *2-theory* on a set of sorts P_0 is a 2-category with the additional following cartesian structure:

- i) it has a terminal 0-cell 0 , that is for every 0-cell \underline{s} there exists a unique *eraser* 1-cell $e_{\underline{s}} : \underline{s} \rightarrow 0$, and the identity 2-cell is the unique endo-2-cell on an eraser,
- ii) it has products, that is for all 0-cells $\underline{r}, \underline{r}'$ there is a product 0-cell $\underline{r}\underline{r}'$ and 1-cells $x_{\underline{r}'}^{\underline{r}} : \underline{r}\underline{r}' \rightarrow \underline{r}$ and $x_{\underline{r}}^{\underline{r}'} : \underline{r}\underline{r}' \rightarrow \underline{r}'$ satisfying the following two conditions:
 - for all 1-cells $f_1 : \underline{s} \rightarrow \underline{r}$ and $f_2 : \underline{s} \rightarrow \underline{r}'$, there exists a unique *pairing* 1-cell $\langle f_1, f_2 \rangle : \underline{s} \rightarrow \underline{r}\underline{r}'$, such that $x_{\underline{r}'}^{\underline{r}} \langle f_1, f_2 \rangle = f_1$, and $x_{\underline{r}}^{\underline{r}'} \langle f_1, f_2 \rangle = f_2$,
 - for all 2-cells $\alpha_i : f_i \Rightarrow f'_i$, $i = 1, 2$, there exists a unique 2-cell $\langle \alpha_1, \alpha_2 \rangle : \langle f_1, f_2 \rangle \Rightarrow \langle f'_1, f'_2 \rangle$. For 1-cells f_1, \dots, f_k , we will abbreviate $\langle \text{id}_{f_1}, \dots, \text{id}_{f_k} \rangle$ to $\langle f_1, \dots, f_k \rangle$.

A *(2, 1)-theory* is a 2-theory whose every 2-cell is invertible with respect to the \star_1 -composition, *i.e.*, every 2-cell α has an inverse $\alpha^- : \alpha_+ \Rightarrow \alpha_-$ satisfying the relations $\alpha \star_1 \alpha^- = \text{id}_{\alpha_-}$ and $\alpha^- \star_1 \alpha = \text{id}_{\alpha_+}$.

2.1.4. Free 2-theories. We denote by P_2^\times the free 2-theory generated by a cartesian 2-polygraph P . Its underlying 1-category is the free theory P_1^\times generated by the signature (P_0, P_1) . Its 2-cells are defined inductively as follows:

- i) for all 2-cell $A : f \Rightarrow g$ in P_2 and 1-cell h in P_1^\times , there is a 2-cell $Ah : fh \Rightarrow gh$ in P_2^\times ,
- ii) for all 2-cells a, b in P_2^\times , there is a 2-cell $\langle a, b \rangle : \langle a_-, b_- \rangle \Rightarrow \langle a_+, b_+ \rangle$ in P_2^\times ,
- iii) for every 2-cell a in P_2^\times , there is a 2-cell in P_2^\times of the form $\Gamma[a] : \Gamma[a_-] \Rightarrow \Gamma[a_+]$, where Γ denotes a *context* of the form:

$$\Gamma := f \langle f_1, \dots, \square_j, \dots, f_k \rangle : \underline{s} \rightarrow \underline{r},$$

where $f_i : \underline{s} \rightarrow \underline{r}_i$ and $f : \underline{r} \rightarrow \underline{r}$ are 1-cells of P_1^\times , and \square_j is the j -th element of the pairing.

iv) these 2-cells are submitted to the following exchange relations

$$f\langle f_1, \dots, a, \dots, f_j, \dots, f_k \rangle \star_1 f\langle f_1, \dots, f_i, \dots, b, \dots, f_k \rangle = f\langle f_1, \dots, f_i, \dots, b, \dots, f_k \rangle \star_1 f\langle f_1, a, \dots, f_j, \dots, f_k \rangle$$

where $f_i : \underline{s} \rightarrow \underline{r}_i$ and $f : \underline{r} \rightarrow r$ are 1-cells in P_1^\times , and a, b are 2-cells in P_2^\times . We will denote by $f\langle f_1, \dots, a, \dots, b, \dots, f_k \rangle$ the 2-cell defined above.

v) The \star_1 -composition of 2-cells in P_2 is given by sequential composition.

The source and target maps ∂_1^\pm extend to P_2^\times and we denote a_- and a_+ for $\partial_1^-(a)$ and $\partial_1^+(a)$ respectively.

The *free (2, 1)-theory* generated by P , denoted by P_2^\top , is constructed as the 2-theory generated by cells of P and formal inverses of the 2-cells of P_2^\times , and submitted to the relations $a \star_1 a^- = \text{id}_{a_-}$ and $a^- \star_1 a = \text{id}_{a_+}$, for every 2-cell a . We define the congruence relation on P_1^\times by $f \equiv_P g$ if there is a 2-cell of P_2^\top with source f and target g . The *theory presented* by P is the algebraic theory, denoted by \overline{P} , and defined as the quotient of the free theory P_1^\times by the congruence \equiv_P .

2.1.5. Ground terms. Let P be a cartesian 2-polygraph. A *ground term* in the free theory P_1^\times is a term with source 0. A 2-cell a in the free theory P_2^\times is called *ground* when a_- is a ground term. Finally, a context $f\langle f_1, \dots, \square_j, \dots, f_{|J|} \rangle$ is called *ground* when all the f_i are ground terms.

2.1.6. Rewriting properties of cartesian polygraphs. The contexts can be composed in a natural way, and we will denote by $\Gamma \Gamma'[\square] := \Gamma[\Gamma'[\square]]$ the composition of contexts Γ and Γ' . We define a *multi-context* (of arity 2) as

$$\Delta[\square_i, \square_j] := f\langle f_1, \dots, \square_i, \dots, \square_j, \dots, f_k \rangle,$$

where the $f_k : \underline{s} \rightarrow \underline{r}_k$ and $f : \underline{r} \rightarrow r$ are 1-cells in P_1^\times , and \square_i (resp. \square_j) has to be filled by a 1-cell $g_i : \underline{s} \rightarrow \underline{r}_i$ (resp. $g_j : \underline{s} \rightarrow \underline{r}_j$).

A 2-cell of the form $\Gamma[Ah]$, where Γ is a context, h is a 1-cell in P_1^\times and A is a rule in P_2 is called a *rewriting step* of P . We consider the ARS $(P_1^\times, P_{\text{stp}})$ where P_{stp} is the cellular extension made of rewriting steps of P , whose source and target maps extend the ones of P . We say that P is *terminating* (resp. *quasi-terminating*, *confluent*) if the ARS $(P_1^\times, P_{\text{stp}})$ is so. If P' is a cartesian 2-polygraph with the same signature as P , we say that P is *confluent modulo P'* if the ARS $(P_1^\times, P_{\text{stp}})$ is confluent modulo $\equiv_{P'}$.

For the sake of readability, we will denote terms and rewriting rules of cartesian polygraphs as in term rewriting theory, [48]. The canonical projection $x_i^{\underline{s}} : \underline{s} \rightarrow \underline{s}_i$, for $1 \leq i \leq |\underline{s}|$ is identified to the "variable" x_i . A 1-cell $f : \underline{s} \rightarrow r$, is denoted by $f(x_1, \dots, x_{|\underline{s}|})$, and a rule $A : f \Rightarrow g$ with $f, g : \underline{s} \rightarrow r$ will be denoted by

$$A_{x_1, \dots, x_{|\underline{s}|}} : f(x_1, \dots, x_{|\underline{s}|}) \Rightarrow g(x_1, \dots, x_{|\underline{s}|}).$$

2.2. Algebraic examples

2.2.1. Magmas. Denote by Mag the cartesian 2-polygraph, where $\text{Mag}_0 := \{1\}$, $\text{Mag}_1 := \{\mu : 2 \rightarrow 1\}$, and Mag_2 is empty. Denote by Ass the cartesian 2-polygraph, where $\text{Ass}_1 = \text{Mag}_1$ and with a unique generating 2-cell:

$$A_{x,y,z}^{(\mu)} : \mu(\mu(x, y), z) \Rightarrow \mu(x, \mu(y, z)). \quad (2.2.2)$$

2. Preliminaries on algebraic theories

Denote by \mathbf{AC} the cartesian 2-polygraph, where $\mathbf{AC}_1 = \mathbf{Mag}_1$, and \mathbf{AC}_2 is the disjoint union $\mathbf{Ass}_2 \sqcup \{C^{(\mu)}\}$ with

$$C^{(\mu)} : \mu(x, y) \Rightarrow \mu(y, x), \quad (2.2.3)$$

that corresponds to the rule $C^{(\mu)} : \mu\tau \Rightarrow \mu$, where τ is the exchanging operator defined in (2.1.1). Note that the cartesian polygraph \mathbf{AC} is not terminating, and that the rule $C^{(\mu)}$ can not be oriented in a terminating way. As a consequence, for cartesian 2-polygraphs whose set of rules contains commutativity and associativity for some operation, we will chose to work modulo the polygraph \mathbf{AC} .

The polygraphs \mathbf{Mag} , \mathbf{Ass} , and \mathbf{AC} will be sometimes denoted by $\mathbf{Mag}^{(\mu)}$, $\mathbf{Ass}^{(\mu)}$, and $\mathbf{AC}^{(\mu)}$ to refer to the label of the operation.

2.2.4. Monoids. Denote by \mathbf{Mon} , or $\mathbf{Mon}^{(\mu, e)}$, the cartesian 2-polygraph with $\mathbf{Mon}_0 := \{1\}$, $\mathbf{Mon}_1 := \mathbf{Ass}_1^{(\mu)} \sqcup \{e : 0 \rightarrow 1\}$, and $\mathbf{Mon}_2 := \mathbf{Ass}_2^{(\mu)} \sqcup \{E_l^{(\mu)}, E_r^{(\mu)}\}$, where

$$E_l^{(\mu)} : \mu(e, x) \Rightarrow x, \quad \text{and} \quad E_r^{(\mu)} : \mu(x, e) \Rightarrow x. \quad (2.2.5)$$

The presented theory $\overline{\mathbf{Mon}}$ is the theory of monoids. We also define the cartesian polygraph \mathbf{CMon} , with same 0-cells and 1-cells, and $\mathbf{CMon}_2 := \mathbf{Mon}_2^{(\mu, e)} \sqcup \{C^{(\mu)}\}$, where $C^{(\mu)}$ is the commutativity 2-cell (2.2.3).

2.2.6. Groups. Denote by \mathbf{Grp} , or $\mathbf{Grp}^{(\mu, e, \iota)}$, the cartesian 2-polygraph, where $\mathbf{Grp}_0 := \{1\}$, $\mathbf{Grp}_1 := \mathbf{Mon}_1^{(\mu, e)} \sqcup \{\iota : 1 \rightarrow 1\}$, and $\mathbf{Grp}_2 := \mathbf{Mon}_2^{(\mu, e)} \sqcup \{I_l^{(\mu, \iota)}, I_r^{(\mu, \iota)}\}$, with

$$I_l^{(\mu, \iota)} : \mu(\iota(x), x) \Rightarrow e, \quad \text{and} \quad I_r^{(\mu, \iota)} : \mu(x, \iota(x)) \Rightarrow e. \quad (2.2.7)$$

The presented theory $\overline{\mathbf{Grp}}$ is the theory of groups. Following [23], the set of generating 2-cells

$$\begin{aligned} E_l^{(\mu)}, E_r^{(\mu)}, I_l^{(\mu, \iota)}, I_r^{(\mu, \iota)}, G_1^{(\mu, \iota)} : \iota(e) \Rightarrow e, \quad G_2^{(\mu, \iota)} : \iota(\mu(x, y)) \Rightarrow \mu(\iota(y), \iota(x)), \\ G_3^{(\mu, \iota)} : \iota(\iota(x)) \Rightarrow x, \quad G_4^{(\mu, \iota)} : \mu(x, \mu(\iota(x), y)) \Rightarrow y, \quad G_5^{(\mu, \iota)} : \mu(\iota(x), \mu(x, y)) \Rightarrow y, \end{aligned}$$

defines a polygraph, denoted by $\widetilde{\mathbf{Grp}}$, that is convergent modulo $\mathbf{Ass}^{(\mu)}$, and presents the theory $\overline{\mathbf{Grp}}$.

2.2.8. Abelian groups. Denote by \mathbf{Ab} , or $\mathbf{Ab}^{(\mu, e, \iota)}(1)$, the cartesian 2-polygraph, where $\mathbf{Ab}_0 := \{1\}$, $\mathbf{Ab}_1 = \mathbf{Grp}_1^{(\mu, e, \iota)}$ and $\mathbf{Ab}_2 = \mathbf{Grp}_2^{(\mu, e, \iota)} \sqcup \{C^{(\mu)}\}$, where $C^{(\mu)}$ is the commutativity 2-cell (2.2.3).

2.2.9. Rings. Denote by \mathbf{Ring} the cartesian 2-polygraph, where $\mathbf{Ring}_0 := \{1\}$,

$$\mathbf{Ring}_1 = \mathbf{Ab}_1^{(+, 0, -)} \sqcup \mathbf{Mon}_1^{(\cdot, 1)}, \quad \text{and} \quad \mathbf{Ring}_2 = \mathbf{Ab}_2^{(+, 0, -)} \sqcup \mathbf{Mon}_2^{(\cdot, 1)} \sqcup \{D_l, D_r\},$$

with

$$D_l : x \cdot (y + z) \Rightarrow x \cdot y + x \cdot z, \quad D_r : (y + z) \cdot x \Rightarrow y \cdot x + z \cdot x. \quad (2.2.10)$$

Denote by \mathbf{CRing} , or $\mathbf{CRing}^{(+, 0, -, 1)}(1)$, the cartesian 2-polygraph with $\mathbf{CRing}_i = \mathbf{Ring}_i$, for $i = 0, 1$, and $\mathbf{CRing}_2 = \mathbf{Ring}_2 \sqcup \{C^{(\cdot)}\}$, where $C^{(\cdot)}$ is the commutativity 2-cell (2.2.3) The theory $\overline{\mathbf{CRing}}$ is the theory of commutative rings. Following [43], see also [23], the set of generating 2-cells:

$$E_r^{(+)}, I_r^{(+, -)}, G_1^{(+, -)}, G_2^{(+, -)}, G_3^{(+, -)}, D_r, R_1 : x \cdot 0 \Rightarrow 0, R_2 : x \cdot (-y) \Rightarrow -(x \cdot y), E_r^{(\cdot)}, \quad (2.2.11)$$

defines a cartesian polygraph, that is convergent modulo $\mathbf{AC}^{(+)} \sqcup \mathbf{AC}^{(\cdot)}$, and presents the theory $\overline{\mathbf{CRing}}$.

2.2.12. Modules over a commutative ring. Denote by Mod the cartesian 2-polygraph defined as follows. We set $\text{Mod}_0 = \{m, r\}$, $\text{Mod}_1 = \text{CRing}^{(+,0,-,1)}(r)_1 \sqcup \text{Ab}^{(\oplus,0^\oplus,\iota)}(m)_1 \sqcup \{\eta : rm \rightarrow m\}$, and we will denote $\eta(\lambda, x) = \lambda.x$, for λ and x of type r and m respectively. We set

$$\text{Mod}_2 = \text{CRing}^{(+,0,-,1)}(r)_2 \sqcup \text{Ab}^{(\oplus,0^\oplus,\iota)}(m)_2 \sqcup \{M_1, M_2, M_3, M_4\},$$

with

$$\begin{aligned} M_1 : \lambda.(\mu.x) &\Rightarrow (\lambda \cdot \mu).x, & M_2 : 1.x &\Rightarrow x, \\ M_3 : \lambda.(x \oplus y) &\Rightarrow (\lambda.x) \oplus (\lambda.y), & M_4 : \lambda.x \oplus \mu.x &\Rightarrow (\lambda + \mu).x \end{aligned}$$

Following [23], the 2-cells in (2.2.11) together with the following set of 2-cells

$$\begin{aligned} M_1, M_2, M_3, M_4, N_1 : x \oplus 0^\oplus &\Rightarrow x, & N_2 : x \oplus (\lambda.x) &\Rightarrow (1 + \lambda).x, \\ N_3 : x \oplus x &\Rightarrow (1 + 1).x, & N_4 : x.0^\oplus &\Rightarrow 0^\oplus, & N_5 : 0.x &\Rightarrow 0^\oplus, & N_6 : \iota(x) &\Rightarrow (-1).x, \end{aligned} \quad (2.2.13)$$

gives a convergent presentation of the theory of modules over a commutative ring modulo the cartesian polygraph $\text{AC}^{(+)} \sqcup \text{AC}^{(\cdot)}$. This presentation can be summed up in the following set of rules:

$x + 0 \Rightarrow x$	(ring ₁)	$x + (-x) \Rightarrow 0$	(ring ₂)
$-0 \Rightarrow 0$	(ring ₃)	$-(-x) \Rightarrow x$	(ring ₄)
$-(x + y) \Rightarrow (-x) + (-y)$	(ring ₅)	$x \cdot (y + z) \Rightarrow x \cdot y + x \cdot z$	(ring ₆)
$x \cdot 0 \Rightarrow 0$	(ring ₇)	$x \cdot (-y) \Rightarrow -(x \cdot y)$	(ring ₈)
$1 \cdot x \Rightarrow x$	(ring ₉)	$a \oplus 0^\oplus \Rightarrow a$	(mod ₁)
$x.(y.a) \Rightarrow (x \cdot y).a$	(mod ₂)	$1.a \Rightarrow a$	(mod ₃)
$x.a \oplus y.a \Rightarrow (x + y).a$	(mod ₄)	$x.(a \oplus b) \Rightarrow (x.a) \oplus (y.b)$	(mod ₅)
$a \oplus (r.a) \Rightarrow (1 + r).a$	(mod ₆)	$a \oplus a \Rightarrow (1 + 1).a$	(mod ₇)
$x.0^\oplus \Rightarrow 0^\oplus$	(mod ₈)	$0.a \Rightarrow 0^\oplus$	(mod ₉)
$I(a) \Rightarrow (-1).a$	(mod ₁₀)		

Let us denote by Mod'_2 the set containing the 2-cells (2.2.11) and (2.2.13). We denote by Mod^c the cartesian 2-polygraph $(\text{Mod}_0, \text{Mod}_1, \text{Mod}'_2 \sqcup \text{AC}^{(+)} \sqcup \text{AC}^{(\cdot)})$. It also presents the theory $\overline{\text{Mod}}$ of modules over a commutative ring.

3. ALGEBRAIC POLYGRAPHS MODULO

In this section we introduce the notion of algebraic polygraphs, defined by cellular extensions on ground terms over a signature endowed with constants, and the notion of algebraic polygraphs modulo. We refer the reader to [14] for a categorical formulation of the constructions given in this section.

3. Algebraic polygraphs modulo

3.1. Algebraic polygraphs

3.1.1. Algebraic polygraphs. An *algebraic polygraph* is a data (P, Q, R) made of

- i) a cartesian 2-polygraph P ,
- ii) a cellular extension Q of P_0 whose elements have source 0 , and called *constants*,
- iii) a cellular extension R of the sub-theory of the free theory $(P_0, P_1 \sqcup Q)^\times$ made of all ground terms, denoted by $P_1\langle Q \rangle$.

We have a decomposition

$$P_1\langle Q \rangle = \bigsqcup_{s \in P_0} P_1\langle Q \rangle_s,$$

where $P_1\langle Q \rangle_s$ contains the ground terms of coarity s , hence the cellular extension R is also indexed by the sorts of P_0 , so that it defines a family $(P_1\langle Q \rangle_s, R_s)_{s \in P_0}$ of ARSs.

3.1.2. Rewriting properties of algebraic polygraphs. Let $\mathcal{P} = (P, Q, R)$ be an algebraic polygraph. A *R-rewriting step* is a ground 2-cell in the free 2-theory R^\times generated by $(P_0, P_1 \sqcup Q, R)$ of the form

$$\Gamma[A] : \Gamma[f] \Rightarrow \Gamma[g],$$

where $A : f \Rightarrow g$ is a rule in R , and Γ is a ground context. We denote by R_{stp} the cellular extension made of R -rewriting steps of \mathcal{P} , whose source and target maps extend the ones of R . We say that \mathcal{P} is *terminating* (resp. *quasi-terminating*, *confluent*) if the ARS $(P_1\langle Q \rangle, R_{\text{stp}})$ is so. A *R-rewriting path* is a finite or infinite sequence $\alpha = \alpha_1 * \alpha_2 \dots * \alpha_k * \alpha_{k+1} \dots$ of R -rewriting steps α_i . The *length* of a finite R -rewriting path α , denoted by $\ell(\alpha)$, is the number of R -rewriting steps that it contains.

The cellular extension P_2 of P_1^\times extends to a cellular extension of the free 1-theory $(P_1 \sqcup Q)^\times$. We denote by $P_2\langle Q \rangle$ the set of *ground 2-cells on Q* of the free 2-theory generated by the 2-polygraph $(P_0, P_1 \sqcup Q, P_2)$. The data $(P, Q, P_2\langle Q \rangle)$ defines an algebraic polygraph. Two 1-cells f, g in $P_1\langle Q \rangle$ are *algebraically equivalent* with respect to P , and we denote $f \equiv_{P_2\langle Q \rangle} g$, if there exists a 2-cell in $P_2\langle Q \rangle^\top$ with source f and target g .

Let $P' = (P_0, P_1, P'_2)$ be a cartesian 2-polygraph with the same signature as P . We say that \mathcal{P} is *confluent modulo* the algebraic polygraph $(P', Q, P'_2\langle Q \rangle)$ if the ARS $(P_1\langle Q \rangle, R_{\text{stp}})$ is confluent modulo $\equiv_{P'_2\langle Q \rangle}$. The algebraic polygraph $(P, Q, P_2\langle Q \rangle)$ shares the rewriting properties of the polygraph P . In particular, if P is terminating (resp. quasi-terminating, confluent), then so is $(P, Q, P_2\langle Q \rangle)$. Moreover, if P is confluent modulo P' , then $(P, Q, P_2\langle Q \rangle)$ is confluent modulo $(P', Q, P'_2\langle Q \rangle)$.

3.1.3. Positive reduction strategies. Denote by $\overline{P\langle Q \rangle}$ the quotient of the theory $P_1\langle Q \rangle$ by the congruence relation $\equiv_{P_2\langle Q \rangle}$. In (3.3), we will consider rewriting with respect to a quotient algebraic system on $\overline{P\langle Q \rangle}$ whose rules are the projections of the rules of R . Rewriting properties of this latter depend on P . In many situations, if we consider projections of all the R -rewriting steps we lose termination in the quotient rewriting system. This is the case when the algebraic theory is equipped with inverse operators, such as theories $\overline{\text{Mod}}$ and $\overline{\text{Grp}}$. To prevent this, we need to select admissible R -rewriting steps compatible with P using the following notion of strategy.

Let $\pi : P_1\langle Q \rangle \rightarrow \overline{P\langle Q \rangle}$ be the canonical projection. We define a *positive strategy* σ as a map that associates to every $\bar{f} \in \overline{P\langle Q \rangle}$ a non-empty subset $\sigma(\bar{f})$ of $\pi^{-1}(\bar{f})$. A R-rewriting step α is called σ -*positive* if α_- belongs to $\sigma(\pi(\alpha_-))$, and a R-rewriting path is called σ -*positive* if every of its rewriting steps is positive.

In most cases, a positive strategy is defined uniformly with respect to P as follows. Suppose that P has a decomposition $P_2 = P'_2 \sqcup P''_2$, where P'_2 is terminating and confluent modulo P''_2 . For every 1-cell \bar{f} in $\overline{P\langle Q \rangle}$, we set

$$\sigma(\bar{f}) = \bigsqcup_{f \in \pi^{-1}(\bar{f})} \text{NF}(f, P'_2),$$

where $\text{NF}(f, P'_2)$ is the set of normal forms of $f \in P_1\langle Q \rangle$ with respect to P'_2 . By confluence of P'_2 modulo P''_2 , we deduce from [22, Lemma 2.6] that any two elements of $\sigma(\bar{f})$ are congruent modulo P''_2 .

3.1.4. Remarks. In many algebraic rewriting contexts, we have $\text{Ass}^{(\mu)} \subseteq P''_2$. For instance, in the case of algebraic polygraphs over $\text{Mon}^{(\mu)}$, the usual strategy is obtained with P'_2 empty and $P''_2 = \text{Ass}^{(\mu)}$. Hence, every 1-cell in $P_1\langle Q \rangle$ is a normal form for the empty polygraph modulo $\text{Ass}^{(\mu)}$, and thus the positive strategy consists in taking all the congruence class. In the case of algebraic polygraphs over Mod , we set $P''_2 = \text{AC}^{(+)} \sqcup \text{AC}^{(\cdot)}$, and P'_2 is the convergent presentation of Mod'_2 modulo AC given in (2.2.12).

3.1.5. Example. Consider the cartesian polygraph $P = \text{Mon}$, a set Q of constants, and a cellular extension R of $P_1\langle Q \rangle$ as follows:

$$Q = \{s, t : 0 \rightarrow 1\}, \quad R = \{A : \mu(\mu(s, t), s) \Rightarrow \mu(t, \mu(s, t))\}. \quad (3.1.6)$$

This data defines an algebraic polygraph (P, Q, R) . For example, if we consider the context $\Gamma = \mu(\mu(s, \square), t)$, the rule A induces the following rewriting step

$$\Gamma[A] : \mu(\mu(s, \mu(\mu(s, t), s)), t) \Rightarrow \mu(\mu(s, \mu(t, \mu(s, t))), t).$$

The set $P_2\langle Q \rangle$ is defined by the associativity relations on ground terms on the constants s and t . For instance, $P_2\langle Q \rangle$ contains the following ground 2-cell:

$$\mu(\mu(s, t), s) \Rightarrow \mu(s, \mu(t, s)).$$

For this algebraic polygraph over Mon , we consider the positive strategy as in (3.1.4) with $P'_2 = \emptyset$ and $P''_2 = \text{Ass}$, so that for every $\bar{f} \in \overline{P\langle Q \rangle}$ we have $\sigma(\bar{f}) = \pi^{-1}(\bar{f})$. In other words, $\sigma(\bar{f})$ is the set of all representatives of \bar{f} modulo associativity. For example, if $\bar{f} = sts$, then $\sigma(\bar{f}) = \{\mu(s, \mu(t, s)), \mu(\mu(s, t), s)\}$.

3.1.7. Example. As aforementioned, for algebraic theories with inverse operators we need positive strategies σ such that $\sigma(\bar{f}) \neq \pi^{-1}(\bar{f})$. Consider the cartesian polygraph $P = \text{Grp}$, and Q, R as defined in (3.1.6). There is a R-rewriting step of the form

$$\mu(\mu(\mu(s, t), s), s^-) \Rightarrow \mu(\mu(t, \mu(s, t)), s^-).$$

The left hand side being algebraically equivalent to $\mu(s, t)$, this rewriting step yields a reduction $st \Rightarrow tsts^-$ in the quotient algebraic system on $\overline{P\langle Q \rangle}$ defined in (3.3), so that the latter cannot be terminating. For this reason, we have to consider a positive strategy for which this R-rewriting step is not

3. Algebraic polygraphs modulo

positive. In (5.3.4), we define a positive strategy for algebraic polygraphs over Grp , that is not defined with respect to normal forms of \mathbf{P} as done in (3.1.4).

Consider the cartesian polygraph $\mathbf{P} = \text{Mod}^c$, and cellular extensions \mathbf{Q}, \mathbf{R} as follows:

$$\mathbf{Q} = \{x, y : 0 \rightarrow m\}, \quad \mathbf{R} = \{A : x \Rightarrow y\}.$$

There is a \mathbf{R} -rewriting step $\alpha : x + (-x) \Rightarrow x + (-y)$ that projects onto a reduction $0 \Rightarrow x - y$ in the quotient algebraic system on $\overline{\mathbf{P}\langle\mathbf{Q}\rangle}$. In this case, we choose the positive strategy σ defined in (3.1.4), where the positive rewriting steps are those whose source is a normal form with respect to Mod'_2 modulo AC . Since $x + (-x)$ is not a normal form with respect to the set of 2-cells of Mod'_2 , the rewriting step α is not σ -positive.

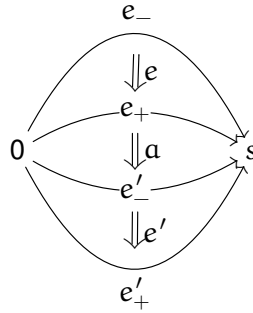
Finally, let us note that whenever we work with a cartesian 2-polygraph \mathbf{P} that admits an inverse operator ι and a neutral operator e , then for every algebraic polygraph $(\mathbf{P}, \mathbf{Q}, \mathbf{R})$ and every rule A in \mathbf{R} , there is a \mathbf{R} -rewriting step

$$e \Rightarrow \mu(A_-, \iota(A_+)).$$

In order to make the quotient algebraic rewriting system on $\overline{\mathbf{P}\langle\mathbf{Q}\rangle}$ terminating, we need to consider a strategy σ such that the above 2-cell is not positive. Hence, we cannot have $\sigma(\bar{f}) = \pi^{-1}(\bar{f})$.

3.2. Algebraic polygraphs modulo

3.2.1. Algebraic polygraph modulo. Let $(\mathbf{P}, \mathbf{Q}, \mathbf{R})$ be an algebraic polygraph. We denote by ${}_{\mathbf{P}}\mathbf{R}_{\mathbf{P}}$ the cellular extension of the theory $\mathbf{P}_1\langle\mathbf{Q}\rangle$ made of triple (e, α, e') , where e, e' are 2-cells in $\mathbf{P}_2\langle\mathbf{Q}\rangle^{\top}$, and α is a \mathbf{R} -rewriting step such that $e_+ = \alpha_-$ and $\alpha_+ = e'_-$. Such a triple, also denoted by $e \star_1 \alpha \star_1 e'$, is called a ${}_{\mathbf{P}}\mathbf{R}_{\mathbf{P}}$ -rule, and pictured by



Given a positive strategy σ on \mathcal{P} , a rule (e, α, e') is σ -positive if α is a σ -positive \mathbf{R} -rewriting step. An algebraic polygraph modulo is a data $\mathcal{P} = (\mathbf{P}, \mathbf{Q}, \mathbf{R}, \mathbf{S})$ made of

- i) an algebraic polygraph $(\mathbf{P}, \mathbf{Q}, \mathbf{R})$,
- ii) a cellular extension \mathbf{S} of $\mathbf{P}_1\langle\mathbf{Q}\rangle$ such that $\mathbf{R} \subseteq \mathbf{S} \subseteq {}_{\mathbf{P}}\mathbf{R}_{\mathbf{P}}$.

We say that \mathcal{P} is *terminating* (resp. *quasi-terminating*) if the algebraic polygraph $(\mathbf{P}, \mathbf{Q}, \mathbf{S})$ is terminating (resp. quasi-terminating).

3.2.2. Example. Let us consider the algebraic polygraph (P, Q, R) defined in (3.1.6), then the following composition gives a rewriting step in ${}_{\mathcal{P}}R_{\mathcal{P}}$:

$$(s \cdot (s \cdot (t \cdot s))) \cdot t \equiv_{P_2\langle Q \rangle} (s \cdot ((s \cdot t) \cdot s)) \cdot t \xrightarrow{\Gamma[A]} (s \cdot (t \cdot (s \cdot t))) \cdot t \equiv_{P_2\langle Q \rangle} ((s \cdot t) \cdot (s \cdot t)) \cdot t.$$

3.2.3. Quasi-normal forms. Let $\mathcal{P} = (P, Q, R, S)$ be an algebraic polygraph modulo. A 1-cell f of $P_1\langle Q \rangle$ is *quasi-irreducible* if for every S -rewriting step $f \Rightarrow g$ there exists a S -rewriting path from g to f . A *quasi-normal form (with respect to \mathcal{P})* of a 1-cell f in $P_1\langle Q \rangle$ is a quasi-irreducible 1-cell \tilde{f} of $P_1\langle Q \rangle$ such that there exists a S -rewriting path from f to \tilde{f} . If \mathcal{P} is quasi-terminating, every 1-cell f of $P_1\langle Q \rangle$ admits at least a quasi-normal form, that is neither S -irreducible nor unique in general. A *quasi-normal form strategy* is a map

$$s : P_1\langle Q \rangle \rightarrow P_1\langle Q \rangle$$

sending a 1-cell f on a chosen quasi-normal \tilde{f} .

3.3. Algebraic rewriting systems

3.3.1. Algebraic rewriting systems. Let $\mathcal{P} = (P, Q, R, S)$ be an algebraic polygraph modulo. A cellular extension S of $P_1\langle Q \rangle$ extends to a cellular extension of the theory $\overline{P\langle Q \rangle}$, with source $\overline{\partial}_1^- := \pi \circ \partial_1^-$, and target $\overline{\partial}_1^+ := \pi \circ \partial_1^+$. An *algebraic rewriting system* on \mathcal{P} is a cellular extension \overline{S} of $\overline{P\langle Q \rangle}$ defined in such a way that the following diagram commutes

$$\begin{array}{ccc} & S & \\ & \swarrow \overline{\partial}_1^+ & \downarrow \pi' \\ \overline{P\langle Q \rangle} & \xrightarrow{\overline{\partial}_1^-} & \overline{S} \end{array}$$

where the map π' assigns to a S -rule $e \star_1 a \star_1 e'$ an element \overline{a} in \overline{S} with source \overline{a}_- and target \overline{a}_+ . Since $R \subseteq S \subseteq {}_{\mathcal{P}}R_{\mathcal{P}}$, note that the quotient cellular extensions \overline{R} and \overline{S} coincide.

Given a positive strategy σ on \mathcal{P} , let define $\overline{S}^\sigma := \{\overline{a} \in \overline{S} \mid a \text{ is a } \sigma\text{-positive } S\text{-rule}\}$. A *\overline{S} -rewriting step* (resp. *\overline{S}^σ -rewriting step*) is the quotient of a S -rewriting step (resp. σ -positive S -rewriting step) by the canonical projection π , that is a 2-cell of the form $\overline{\Gamma}[a] : \overline{\Gamma}[a_-] \Rightarrow \overline{\Gamma}[a_+]$, where Γ is a ground context of $P_1\langle Q \rangle$ and $\Gamma[a]$ is a S -rewriting step (resp. σ -positive S -rewriting step). A *\overline{S} -rewriting path* (resp. *\overline{S}^σ -rewriting path*) is a sequence of \overline{S} -rewriting steps (resp. \overline{S}^σ -rewriting steps).

3.3.2. Examples. A *string rewriting system* (SRS) is an algebraic rewriting system on an algebraic polygraph modulo (Mon, Q, R, S) . The set Q is the alphabet of the SRS, and the quotient of the cellular extension R with respect to the congruence $\equiv_{\text{Mon}_2\langle Q \rangle}$ is the set of rules of the SRS. For instance, as a quotient of the algebraic polygraph defined in (3.1.6), we obtain the SRS

$$\langle s, t \mid sts \Rightarrow tst \rangle,$$

that presents the monoid B_3^+ of braids on 3 strands.

A *linear rewriting system* (LRS) is an algebraic rewriting system on an algebraic polygraph modulo (P, Q, R, S) such that $\text{Mod}^c \subseteq P$.

4. Confluence of algebraic polygraphs modulo

4. CONFLUENCE OF ALGEBRAIC POLYGRAPHS MODULO

In this section we study confluence properties of algebraic polygraphs modulo with respect to positive strategies. Here $\mathcal{P} = (P, Q, R, S)$ denotes an algebraic polygraph modulo, and σ a positive strategy on \mathcal{P} .

4.1. Confluence modulo with respect to a positive strategy

4.1.1. Branchings in algebraic polygraphs modulo. A σ -branching of \mathcal{P} is a triple (α, e, β) , where α, β are σ -positive 2-cells of S^\times and e is a 2-cell of $P_2\langle Q \rangle^\top$ as in the following diagram

$$\begin{array}{ccc} f & \xrightarrow{\alpha} & f' \\ e \downarrow & & \\ g & \xrightarrow{\beta} & g' \end{array}$$

In the rest of this article, for a better readability of the diagrams, the 2-cells will be represented by simple arrows. The *source* of a σ -branching (α, e, β) is the pair of 1-cells (f, g) , where $f = \alpha_- = e_-$, and $g = \beta_- = e_+$. When β (resp. α) is an identity 2-cell, the σ -branching is written (α, e) (resp. (e, β)). When e is an identity 2-cell, the σ -branching is written (α, β) . A σ -branching (α, e, β) is *local* if $\ell(\alpha) = \ell(\beta) + \ell(e) = 1$, that is it is either of the form (α, e) or (α, β) .

A σ -branching (α, e, β) is σ -confluent modulo if there exist σ -positive S -rewriting paths α', β' , and a 2-cell e' in $P_2\langle Q \rangle^\top$ as in the following diagram:

$$\begin{array}{ccccc} f & \xrightarrow{\alpha} & f' & \xrightarrow{\alpha'} & h \\ e \downarrow & & & & \downarrow e' \\ g & \xrightarrow{\beta} & g' & \xrightarrow{\beta'} & h' \end{array}$$

The triple (α', e', β') is called a σ -confluence modulo of the branching (α, e, β) . We say that \mathcal{P} is σ -confluent modulo (resp. *locally* σ -confluent modulo) if every σ -branching modulo (resp. local σ -branching modulo) is σ -confluent modulo.

4.1.2. Remark. As noted in [2], the algebraic polygraph R is the polygraph for which it is the most difficult to reach σ -confluence modulo. Indeed, if R is confluent modulo P , then every algebraic polygraph modulo (P, Q, R, S) is confluent modulo P . For this reason, in many situations we relax by proving σ -confluence of ${}_{\rho}R$ or ${}_{\rho}R_{\rho}$ modulo P . In [2], it is also noticed that when ${}_{\rho}R_{\rho}$ is terminating, R_{ρ} is confluent modulo P if and only if ${}_{\rho}R_{\rho}$ is confluent modulo P , and in that case R_{ρ} defines the same set of normal forms than ${}_{\rho}R_{\rho}$. As a consequence, we will either prove σ -confluence of R_{ρ} and ${}_{\rho}R_{\rho}$, leading to the same quotient algebraic rewriting system. Note finally that when ${}_{\rho}R \subseteq S \subseteq {}_{\rho}R_{\rho}$, every local σ -branching modulo of the form (α, e) is trivially σ -confluent modulo via the σ -confluence modulo $(\text{id}_{\alpha_-}, e^- \star_1 \alpha, \text{id}_{\alpha_+})$.

4.1.3. Rewrite order on an algebraic polygraph modulo. Denote by $\preceq_{\mathcal{P}}$ the relation on the 1-cells of $P_1\langle Q \rangle$ defined, for all 1-cells f, g in $P_1\langle Q \rangle$, by $g \preceq_{\mathcal{P}} f$ if $f = g$ or f S -rewrites into g . The *rewrite order* of \mathcal{P} , denoted by $\prec_{\mathcal{P}}$, is the strict order on $P_1\langle Q \rangle$ defined by $g \prec_{\mathcal{P}} f$ if $g \preceq_{\mathcal{P}} f$ but not $f \preceq_{\mathcal{P}} g$. Note that when \mathcal{P} is quasi-terminating, the relation $\preceq_{\mathcal{P}}$ does not define an order when there exists two 1-cells which rewrite into each other, but the relation $\prec_{\mathcal{P}}$ is a well-founded strict order.

4.1. Confluence modulo with respect to a positive strategy

4.1.4. Double induction principle. Let us recall from Huet [22] the double induction principle, that we apply to quasi-terminating algebraic polygraphs modulo. From \mathcal{P} , we construct an auxiliary algebraic polygraph $\mathcal{P}^{\text{db}} := (\mathbf{P} \times \mathbf{P}, \mathbf{Q}, S^{\text{db}})$, where $\mathbf{P} \times \mathbf{P}$ is the cartesian product of the polygraph \mathbf{P} by itself, and the cellular extension S^{db} on $(\mathbf{P} \times \mathbf{P})_1 \langle \mathbf{Q} \rangle := \mathbf{P}_1 \langle \mathbf{Q} \rangle \times \mathbf{P}_1 \langle \mathbf{Q} \rangle$ contains a 2-cell $(f, g) \Rightarrow (f', g')$, for all 1-cells f, f', g, g' in $\mathbf{P}_1 \langle \mathbf{Q} \rangle$ in any of the following situations:

- i) there exists a 2-cell $f \Rightarrow f'$ in S^\times and $g = g'$;
- ii) there exists a 2-cell $g \Rightarrow g'$ in S^\times and $f = f'$;
- iii) there exist 2-cells $f \Rightarrow f'$ and $f \Rightarrow g'$ in S^\times ;
- iv) there exist 2-cells $g \Rightarrow f'$ and $g \Rightarrow g'$ in S^\times ;
- v) there exist 2-cells e_1, e_2, e_3 in $\mathbf{P}_2 \langle \mathbf{Q} \rangle^\top$, such that $\ell(e_1) > \ell(e_3)$, and as in the following diagram

$$f \xrightarrow{e_1} g \xrightarrow{e_2} f' \xrightarrow{e_3} g'.$$

As a consequence of the definition, if there exist 2-cells $f \Rightarrow f'$ and $g \Rightarrow g'$ in S^\times , then there is a 2-cell $(f, g) \Rightarrow (f', g')$ in \mathcal{P}^{db} given by the composition $(f, g) \Rightarrow (f', g) \Rightarrow (f', g')$. Following [22, Prop. 2.2], if \mathcal{P} is terminating, then so is \mathcal{P}^{db} . This result extends as follows: if \mathcal{P} is quasi-terminating, then so is \mathcal{P}^{db} . Indeed, termination cycles that come from quasi-termination of \mathcal{P} also appear in \mathcal{P}^{db} , and these are the only infinite rewriting paths that can arise. In the sequel, we will prove rewriting results using double induction on a quasi-terminating algebraic polygraph modulo \mathcal{P} , consisting in using well-founded induction on the rewrite order $\prec_{\mathcal{P}^{\text{db}}}$ defined in (4.1.3).

4.1.5. Theorem. *Let \mathcal{P} be a quasi-terminating algebraic polygraph modulo, and σ be a positive strategy on \mathcal{P} . If \mathcal{P} is locally σ -confluent modulo, then it is σ -confluent modulo.*

Proof. Let \mathcal{P} be locally σ -confluent modulo. We prove the result by well-founded induction with respect to the order $\prec_{\mathcal{P}^{\text{db}}}$. Let (a, e, b) be a σ -branching modulo of \mathcal{P} with source (f, g) . Suppose that for every σ -branching modulo (a', e', b') with source (f', g') such that there is a 2-cell $(f, g) \Rightarrow (f', g')$ in $(S^{\text{db}})^\times$, the σ -branching modulo (a', e', b') is confluent modulo. We proceed in two steps.

Step 1: First, we prove that every σ -branching modulo (a, e) with source (f, g) , where a is a σ -positive S -rewriting step and e is a 2-cell in $\mathbf{P}_2 \langle \mathbf{Q} \rangle^\top$, is σ -confluent modulo. We proceed by induction on $\ell(e) \geq 1$. If $\ell(e) = 1$, (a, e) is local, hence it is σ -confluent modulo by assumption. Now, assume that for $k \geq 1$, every σ -branching modulo (a'', e'') , such that a'' is a σ -positive S -rewriting step and $\ell(e'') = k$ is σ -confluent modulo, and consider a σ -branching modulo (a, e) such that $\ell(e) = k + 1$. We write $e = e_1 \star e_2$ with e_1 of length 1. By local σ -confluence of the σ -branching modulo (a, e_1) , there exists a σ -confluence modulo (a', e'_1, a_1) of this σ -branching. We write $a_1 = a_1^1 \star a_1^2$ with a_1^1 of length 1 and $\ell(a_1^2) \geq 0$. By induction hypothesis on the σ -branching modulo (a_1^1, e_2) , there exists a σ -confluence

4. Confluence of algebraic polygraphs modulo

modulo (α'_1, e'_2, b) as in the following diagram:

$$\begin{array}{ccccc}
 f & \xrightarrow{\alpha} & f' & \xrightarrow{\alpha'} & f'' \\
 e_1 \downarrow & \text{Local } \sigma\text{-conf mod} & & & \downarrow e'_1 \\
 f_1 & \xrightarrow{\alpha_1^1} & f'_1 & \xrightarrow{\alpha_1^2} & f''_1 \\
 \parallel \downarrow & = & \downarrow \parallel & & \\
 f_1 & \xrightarrow{\alpha_1^1} & f'_1 & \xrightarrow{\alpha'_1} & f'_2 \\
 e_2 \downarrow & \text{Induction on } \ell(e) & & & \downarrow e'_2 \\
 g & \xrightarrow{b} & g' & &
 \end{array}$$

Now, since $\ell(e_1) = 1$ and $\ell(e_2) \geq 1$, we have the following rewriting path in \mathcal{P}^{db} :

$$(f, g) \Rightarrow (f_1, g) \Rightarrow (f_1, f_1) \Rightarrow (f_1, f'_1) \Rightarrow (f'_1, f'_1).$$

We apply the double induction on the σ -branching (α_1^2, α'_1) with source (f'_1, f'_1) to prove the existence of a σ -confluence modulo $(\alpha_2, e_3, \alpha'_2)$. By a similar argument, we use double induction on the σ -branchings modulo (e'_1, α_2) and (α'_2, e'_2) with respective sources (f'', f''_1) and (f'_2, g') . Therefore, there exist 2-cells $\alpha'', \alpha_3, \alpha'_3, b'$ in S^\times and 2-cells e''_1, e''_2 in $\mathcal{P}_2\langle Q \rangle^\top$ as in the following diagram:

$$\begin{array}{ccccccc}
 f & \xrightarrow{\alpha} & f' & \xrightarrow{\alpha'} & f'' & \xrightarrow{\alpha''} & f''' \\
 e_1 \downarrow & \text{Local } \sigma\text{-conf. mod} & & & \downarrow e'_1 & \text{Double Induction} & \downarrow e''_1 \\
 f_1 & \xrightarrow{\alpha_1^1} & f'_1 & \xrightarrow{\alpha_1^2} & f''_1 & \xrightarrow{\alpha_2} & h_1 \xrightarrow{\alpha_3} h'_1 \\
 \parallel \downarrow & = & \downarrow \parallel & \text{Double Induction} & \downarrow e_3 & & \\
 f_1 & \xrightarrow{\alpha_1^1} & f'_1 & \xrightarrow{\alpha'_1} & f'_2 & \xrightarrow{\alpha'_2} & h_2 \xrightarrow{\alpha'_3} h'_2 \\
 e_2 \downarrow & \text{Induction on } \ell(e) & & & \downarrow e'_2 & \text{Double Induction} & \downarrow e''_2 \\
 g & \xrightarrow{b} & g' & & & \xrightarrow{b'} & g''
 \end{array}$$

Finally, we use once again double induction on the σ -branching modulo $(\alpha_3, e_3, \alpha'_3)$ of source (h_1, h_2) , satisfying $(h_1, h_2) \prec_{\mathcal{P}^{\text{db}}} (f, g)$, and repeat this process. Since the order $\prec_{\mathcal{P}^{\text{db}}}$ is well-founded, it terminates in finitely many steps until we reach quasi-normal forms \tilde{f} and \tilde{g} of f and g respectively. This yields the σ -confluence of the σ -branching (α, e) .

Step 2: Now, we prove that every σ -branching modulo (α, e, b) with source (f, g) is σ -confluent modulo. Suppose that every σ -branching (α', e', b') modulo with source (f', g') such that there is a 2-cell $(f', g') \Rightarrow (f'', g'')$ in $(S^{\text{db}})^\times$ is σ -confluent modulo. We use the proof scheme of [22, Lemma 2.7]. Let us denote by $n := \ell(\alpha)$ and $m := \ell(b)$. If both m and n are 0, there is no branching modulo, so that we assume without loss of generality that $n > 0$. We write $\alpha = \alpha_1 \star_1 \alpha_2$ with α_1 of length 1.

4.1. Confluence modulo with respect to a positive strategy

If $m = 0$, by Step 1 on the σ -branching modulo (α_1, e) , there exists a σ -confluence modulo (α'_1, e', b') of this σ -branching. Then, we use double induction on the σ -branching modulo (α_2, α'_1) with source (f_1, f_1) , since there is a rewriting path in $(S^{\text{db}})^\times$ of the form

$$(f, g) \Rightarrow (f, f) \Rightarrow (f, f_1) \Rightarrow (f, f_1).$$

There exist σ -positive 2-cells α'_2, α''_1 in S^\times and a 2-cell e'' in $P_2\langle Q \rangle^\top$ as follows:

$$\begin{array}{ccccccc}
 f & \xrightarrow{\alpha_1} & f_1 & \xrightarrow{\alpha_2} & f_2 & \xrightarrow{\alpha'_2} & f'_2 \\
 \parallel \downarrow & = & \parallel \downarrow & & \text{Double Induction} & & \downarrow e'' \\
 f & \xrightarrow{\alpha_1} & f_1 & \xrightarrow{\alpha'_1} & f_2 & \xrightarrow{\alpha''_1} & f'_2 \\
 e \downarrow & & \text{Step 1} & & \downarrow e' & & \\
 g & \xrightarrow{\quad} & \quad & & g' & &
 \end{array}$$

We conclude the proof of this case with a similar argument as in Step 1, using repeated double inductions terminating after a finite number of steps by well-foundedness of the order \prec_{pab} .

Now, assume that $m > 0$ and write $b = b_1 \star_1 b_2$ with b_1 of length 1. By Step 1 on the σ -branching modulo (α_1, e) , there exists a σ -confluence modulo (α'_1, e_1, c_1) of this σ -branching. We distinguish two cases whether c_1 is trivial or not.

If c_1 is trivial, the σ -confluence of (α, e, b) is obtained from the following diagram

$$\begin{array}{cccccccccccc}
 f & \xrightarrow{\alpha_1} & f_1 & \xrightarrow{\alpha_2} & f_2 & \xrightarrow{\quad} & f'_2 \\
 \parallel \downarrow & = & \parallel \downarrow & & \text{Double Induction} & & \downarrow \\
 f & \xrightarrow{\alpha_1} & f_1 & \xrightarrow{\alpha'_1} & f'_1 & \xrightarrow{\alpha_3} & f_3 & \xrightarrow{\alpha_4} & f_4 & \xrightarrow{\alpha_5} & f_5 \\
 e \downarrow & & \text{Step 1} & & \downarrow e' & & \text{Step 1} & & \downarrow e_1 & & \text{Double Induction} & & \downarrow \\
 g & \xrightarrow{\text{id}_g} & g & \xrightarrow{b_1} & g'_1 & \xrightarrow{b'_1} & g''_1 & \xrightarrow{b''_1} & h_1 & \xrightarrow{b_3} & h_3 \\
 \parallel \downarrow & = & \parallel \downarrow & = & \parallel \downarrow & & \text{Double Induction} & & \downarrow \\
 g & \xrightarrow{\text{id}_g} & g & \xrightarrow{b_1} & g'_1 & \xrightarrow{b_2} & g_2 & \xrightarrow{b'_2} & h_2 & & & & \downarrow
 \end{array}$$

where the σ -branchings modulo (α_1, e) and (b_1, e') are σ -confluent modulo by Step 1, and double induction applies on the σ -branchings $(\alpha_2, \alpha'_1 \star_1 \alpha_3)$, (b'_1, b_2) and (α_4, e_1, b''_1) of respective sources (f_1, f_1) , (g'_1, g'_1) and (f_3, g'_1) which are all strictly smaller than (f, g) for \prec_{pab} . We then reach a σ -confluence modulo of the σ -branching modulo (α, e, b) similarly using repeated double inductions.

If c_1 is not trivial, write $c_1 = c_1^1 \star_1 c_1^2$ with c_1^1 of length 1. The σ -confluence of the σ -branching modulo (α, e, b) is obtained from the following diagram:

4. Confluence of algebraic polygraphs modulo

$$\begin{array}{ccccccccccc}
 f & \xrightarrow{a_1} & f_1 & \xrightarrow{a_2} & f_2 & \xrightarrow{a'_2} & f'_2 & & & & \\
 \parallel & = & \downarrow & \text{Double Induction} & & & \downarrow & & & & \\
 f & \xrightarrow{a_1} & f_1 & \xrightarrow{a'_1} & f'_1 & \xrightarrow{a_3} & f_3 & \xrightarrow{a_4} & f_4 & & \\
 e & & \text{Step 1} & & \text{Double Induction} & & & & & & \\
 g & \xrightarrow{c_1^1} & g_1 & \xrightarrow{c_1^2} & h_1 & \xrightarrow{c_2} & h_2 & \xrightarrow{c_2'} & h_2' & & \\
 \parallel & = & \downarrow & \text{Double Induction} & & & \downarrow & & & & \\
 g & \xrightarrow{c_1^1} & g_1 & \xrightarrow{c_1'} & h_1' & \xrightarrow{c_3} & h_3 & \xrightarrow{c_3'} & h_3' & & \\
 \parallel & & \text{Local } \sigma\text{-conf mod} & & \text{Double Induction} & & & & & & \\
 g & \xrightarrow{b_1} & g' & \xrightarrow{b_1'} & g_1' & \xrightarrow{b_2'} & g_2' & \xrightarrow{b_3'} & g_3' & & \\
 \parallel & = & \downarrow & \text{Double Induction} & & & \downarrow & & & & \\
 g & \xrightarrow{b_1} & g' & \xrightarrow{b_2} & g_2 & \xrightarrow{b_3} & g_3 & & & &
 \end{array}$$

where the σ -branching modulo (a_1, e) is confluent modulo by Step 1, the σ -branching modulo (c_1^1, b_1) is σ -confluent by local σ -confluence modulo, and we check that double induction applies on the σ -branchings (a_2, a'_1) , (c_1^2, c_1') , (b_1', b_2) , (a_3, c_2) and (c_3, b_2') of respective sources (f_1, f_1) , (g_1, g_1) , (g', g') and (f'_1, h_1) and (h_1', g_1') which are all strictly smaller than (f, g) for $\prec_{\mathcal{P}db}$. Similarly, we can repeat inductions to reach a σ -confluence modulo of (a, e, b) . \square

4.2. Critical σ -branchings modulo

4.2.1. Classification of local σ -branchings. The local σ -branchings modulo of \mathcal{P} can be classified in the following families:

i) *trivial* σ -branchings of the form

$$\begin{array}{ccc}
 \Gamma[a_-] & \xrightarrow{\Gamma[a]} & \Gamma[a_+] \\
 \parallel \downarrow & & \\
 \Gamma[a_-] & \xrightarrow{\Gamma[a]} & \Gamma[a_+]
 \end{array}$$

for all ground context Γ and σ -positive S-rewriting step a .

ii) *orthogonal* σ -branchings modulo of the form

$$\begin{array}{ccc}
 \Delta[a_-, b_-] & \xrightarrow{\Delta[a, b_-]} & \Delta[a_+, b_-] \\
 \parallel \downarrow & & \\
 \Delta[a_-, b_-] & \xrightarrow{\Delta[a_-, b]} & \Delta[a_-, b_+]
 \end{array}$$

$$\begin{array}{ccc} \Delta[a_-, e_-] \xrightarrow{\Delta[a, e_-]} \Delta[a_+, e_-] & & \Delta'[e'_-, b_-] \xrightarrow{\Delta'[e'_-, b]} \Delta'[e'_-, b_+] \\ \Delta[a_-, e] \downarrow & & \Delta'[e', b_-] \downarrow \\ \Delta[a_-, e_+] & & \Delta'[e'_+, b_-] \end{array}$$

for all ground multi-contexts Δ, Δ' , σ -positive S -rewriting steps a, b, c , and 2-cells e, e' in $\mathcal{P}_2\langle Q \rangle^\top$ of length 1.

iii) *overlapping* σ -branchings are the remaining local σ -branchings. These branchings can be classified into two families: *inclusion* σ -branchings of the form

$$\begin{array}{ccc} \Gamma[a_-] & \xrightarrow{\Gamma[a]} & \Gamma[a_+] \\ \parallel \downarrow & & \\ \Gamma[\Gamma'[b_-]] & \xrightarrow{\Gamma[\Gamma'[b]]} & \Gamma[\Gamma'[b_+]] \end{array}$$

for all ground contexts Γ, Γ' , and σ -positive S -rewriting steps a, b , and *regular overlapping* σ -branchings of the form

$$\begin{array}{ccc} \Gamma[a_-] & \xrightarrow{\Gamma[a]} & \Gamma[a_+] \\ \parallel \downarrow & & \\ \Lambda[b_-] & \xrightarrow{\Lambda[b]} & \Lambda[b_+] \end{array}$$

for all ground contexts Γ, Λ , and σ -positive S -rewriting steps a, b such that $(\Gamma[a], \Lambda[b])$ is not trivial, not orthogonal and not an inclusion branching. These branchings also admit their modulo counterpart, as in case ii), obtained by replacing the bottom S -rewriting step b by a vertical 2-cell e in $\mathcal{P}_2\langle Q \rangle^\top$ of length 1.

4.2.2. Critical σ -branchings. We define an order relation on σ -branchings modulo of \mathcal{P} by setting $(a, e, b) \sqsubseteq (a', e', b')$ if there exists a ground context Γ of $\mathcal{P}_1\langle Q \rangle$ such that $a' = \Gamma[a]$, $e' = \Gamma[e]$ and $b' = \Gamma[b]$. A *critical σ -branching modulo* is an overlapping σ -branching modulo that is minimal for the order relation \sqsubseteq .

4.2.3. Positive confluence. We say that \mathcal{P} is *positively σ -confluent* if, for every S -rewriting step a , there exists $\widetilde{a_-} \in \sigma(a_-)$ and two σ -positive S -rewriting paths a', b' of length at most 1 as in the following diagram

$$\begin{array}{ccccc} \widetilde{a_-} & \xrightarrow{a'} & & & f' \\ e \downarrow & & & & \downarrow \parallel \\ a_- & \xrightarrow{a} & f & \xrightarrow{b'} & f' \end{array}$$

where e is a 2-cell in $\mathcal{P}_2\langle Q \rangle^\top$. In that case, we say that σ is a *positive confluent strategy* for \mathcal{P} .

4.2.4. Proposition. *Let \mathcal{P} be a quasi-terminating algebraic polygraph modulo, and σ be a positive strategy on \mathcal{P} . If \mathcal{P} is positively σ -confluent, then it is locally σ -confluent modulo if, and only if, both of the following conditions are satisfied:*

4. Confluence of algebraic polygraphs modulo

a₀) every critical σ -branching modulo (a, b) , where a, b are S -rewriting steps, is σ -confluent modulo,

b₀) every critical σ -branching modulo (a, e) , where a is an S -rewriting step and e is a 2-cell in $\mathcal{P}_2\langle Q \rangle^\top$ of length 1, is σ -confluent modulo.

Proof. One of the two implications is trivial. Suppose that condition **a₀**) holds, and prove that every local branching of the form (a, b) , where a, b are σ -positive S -rewriting steps, is σ -confluence modulo. The proof that condition **b₀**) implies that every local branching of the form (a, e) , where a is a σ -positive S -rewriting step and e is a 2-cell of $\mathcal{P}_2\langle Q \rangle^\top$ of length 1, is σ -confluent modulo is similar.

The proof is based on the analysis of all the possible cases of local σ -branchings modulo given in (4.2.1). Local trivial σ -branchings are always σ -confluent modulo. We consider a local orthogonal σ -branching modulo of the form

$$\begin{array}{ccc} \Delta[a_-, b_-] & \xrightarrow{\Delta[a, b_-]} & \Delta[a_+, b_-] \\ \parallel \downarrow & & \\ \Delta[a_-, b_-] & \xrightarrow{\Delta[a_-, b]} & \Delta[a_-, b_+] \end{array}$$

where $\Delta[a, b_-]$ and $\Delta[a_-, b]$ are σ -positive S -rewriting paths. There exist 2-cells of S^\times as the dotted cells in the following diagram:

$$\begin{array}{ccccc} \Delta[a_-, b_-] & \xrightarrow{\Delta[a, b_-]} & \Delta[a_+, b_-] & \xrightarrow{\Delta[a_+, b]} & \Delta[a_+, b_+] \\ \parallel \downarrow & & & & \downarrow \parallel \\ \Delta[a_-, b_-] & \xrightarrow{\Delta[a_-, b]} & \Delta[a_-, b_+] & \xrightarrow{\Delta[a, b_+]} & \Delta[a_+, b_+] \end{array}$$

However, they are generally not σ -positive. Assume that they are both not σ -positive. By positive σ -confluence assumption, there exist a representative 1-cell $\widetilde{\Delta[a_+, b_-]}$ (resp. $\widetilde{\Delta[a_-, b_+]}$) of $\Delta[a_+, b_-]$ (resp. $\Delta[a_-, b_+]$) in $\mathcal{P}_1\langle Q \rangle$, σ -positive S -rewriting paths c_1, c_2, d_1, d_2 , and 2-cells e_1, e_2 in $\mathcal{P}_2\langle Q \rangle^\top$ as in the following diagram:

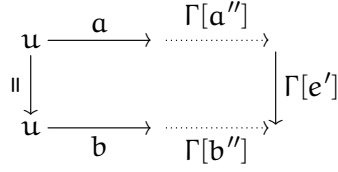
$$\begin{array}{ccccccc} & & \widetilde{\Delta[a_+, b_-]} & \xrightarrow{c_1} & & f & \\ & & \uparrow e_1 & & & \parallel \downarrow & \\ \Delta[a_-, b_-] & \xrightarrow{\Delta[a, b_-]} & \Delta[a_+, b_-] & \xrightarrow{\Delta[a_+, b]} & \Delta[a_+, b_+] & \xrightarrow{d_1} & f \\ \parallel \downarrow & & & & \parallel \downarrow & & \\ \Delta[a_-, b_-] & \xrightarrow{\Delta[a_-, b]} & \Delta[a_-, b_+] & \xrightarrow{\Delta[a, b_+]} & \Delta[a_+, b_+] & \xrightarrow{d_2} & g \\ & & \downarrow e_2 & & & & \parallel \downarrow \\ & & \widetilde{\Delta[a_-, b_+]} & \xrightarrow{c_2} & & g & \end{array}$$

There is a rewriting path $(\Delta[a_-, b_-], \Delta[a_-, b_-]) \Rightarrow (\Delta[a_+, a_+], \Delta[a_+, a_+])$ in $(S^{\text{db}})^\times$ so that we apply double induction on the σ -branching modulo (d_1, d_2) . As a consequence, there exists a σ -confluence

4.3. Algebraic critical branching lemma

modulo (d'_1, e', d'_2) of (d_1, d_2) . Then, we construct a σ -confluence modulo of $(\Delta[a, b_-], \Delta[a_-, b])$ by successive applications of induction as in the proof of Theorem 4.1.5. This process terminates since $\prec_{\mathcal{P}, \text{db}}$ is well-founded.

Let us now consider an overlapping σ -branching modulo of the form (a, b) , where a, b are σ -positive S-rewriting steps. By definition, there exists a ground context Γ of $\mathcal{P}_1\langle Q \rangle$ and a critical σ -branching modulo (a', b') such that $(a, b) = (\Gamma[a'], \Gamma[b'])$. Following condition \mathbf{a}_0 , the critical σ -branching (a', b') is σ -confluent modulo, and there exists a σ -confluence modulo (a'', e', b'') of this σ -branching. However, the S-rewriting paths $\Gamma[a'']$ and $\Gamma[b'']$ that would give a confluence modulo of (a, b) are not necessarily σ -positive:



Using positive σ -confluence of S , we are able to construct a σ -confluence modulo of the σ -branching modulo (a, b) as in the previous case. \square

4.2.5. Full positive strategy. When all rewriting steps are positive, that is when $\sigma(\bar{f}) = \pi^{-1}(\bar{f})$ for every 1-cell \bar{f} in $\overline{\mathcal{P}\langle Q \rangle}$, we say that σ is a *full positive strategy*. In that case, the quasi-termination assumption in Proposition 4.2.4 is not needed to ensure local σ -confluence modulo from confluence of σ -critical branchings modulo. Indeed, the confluences represented by dotted arrows in the diagrams above are σ -positive. Moreover, the positive σ -confluence is always satisfied, by considering $a' = a$ and $b' = \text{id}_{a_+}$.

4.3. Algebraic critical branching lemma

We now prove an algebraic critical branching lemma by quotienting the S-rewriting paths of Proposition 4.2.4.

4.3.1. Critical branchings of algebraic polygraphs. Let \mathcal{A} be an algebraic rewriting system on \mathcal{P} . The *critical branchings* of \mathcal{A} are the projections of the critical σ -branchings modulo of \mathcal{P} of the form \mathbf{a}_0 , that is pairs (\bar{a}, \bar{b}) of \bar{S}^σ -rewriting steps such that there is a σ -branching modulo in \mathcal{P} with source $(\widetilde{\bar{a}}, \widetilde{\bar{b}})$. As a consequence of Proposition 4.2.4, we deduce the following result.

4.3.2. Theorem. *Let $\mathcal{P} = (\mathcal{P}, Q, R, S)$ be an algebraic polygraph modulo with a positive confluent strategy σ . If ${}_{\mathcal{P}}R_{\mathcal{P}}$ is quasi-terminating, then an algebraic rewriting system on \mathcal{P} is locally confluent if, and only if, its critical branchings are confluent.*

As an immediate consequence, we deduce the following critical branching lemma for algebraic polygraphs modulo.

4.3.3. Corollary. *Let \mathcal{P} be an algebraic polygraph modulo with a full positive strategy. Every algebraic rewriting system on \mathcal{P} is locally confluent if, and only if, all its critical branchings are confluent.*

5. Examples of algebraic rewriting systems

5. EXAMPLES OF ALGEBRAIC REWRITING SYSTEMS

In this section, we apply the algebraic critical branching lemma to SRS, LRS, and group rewriting systems.

5.1. String rewriting systems

5.1.1. Critical branching lemma for string rewriting systems. In (3.3.2) we show how to define a SRS as an algebraic rewriting system over the cartesian polygraph Mon given in (2.2.4). In that case, Theorem 4.3.2 is the following critical branching lemma for SRS as proved by Nivat, [42].

5.1.2. Theorem. *Let \mathcal{P} be an algebraic polygraph modulo on the cartesian polygraph Mon . Then an algebraic rewriting system on \mathcal{P} is locally confluent if and only if its critical branchings are confluent.*

In that case, the choice of positive strategy σ making all the 2-cells in S^\times be σ -positive implies that the positive σ -confluence is obvious. Moreover the quasi-terminating hypothesis is not required as explained in (4.2.5).

5.2. Linear rewriting systems

In this subsection, $\mathcal{P} = (\mathcal{P}, Q, R, S)$ denotes an algebraic polygraph modulo, whose cartesian polygraph \mathcal{P} has an underlying linear structure, that is, \mathcal{P} contains the cartesian polygraph Mod^c . We consider a decomposition of \mathcal{P} as in (3.1.3), with $\mathcal{P}_2'' = \text{AC}^{(+)} \sqcup \text{AC}^{(\cdot)}$ and $\mathcal{P}_2' = \text{Mod}^c$, and the positive strategy σ on \mathcal{P} of normal forms modulo $\text{AC}^{(+)} \sqcup \text{AC}^{(\cdot)}$ defined in (3.1.3).

5.2.1. Critical branching lemma for linear rewriting systems. The algebraic polygraph ${}_{\mathcal{P}}\text{R}_{\mathcal{P}}$ is never terminating. Indeed, because of the linear context, for every R-rule $\alpha : f \Rightarrow g$, we have a ${}_{\mathcal{P}}\text{R}_{\mathcal{P}}$ -rewriting step given by

$$g \equiv_{\mathcal{P}} -f + (g + f) \xrightarrow{-\alpha + (g + f)} -g + (g + f) \equiv_{\mathcal{P}} f \quad (5.2.2)$$

However, if the rewriting system \bar{S}^σ is terminating, then ${}_{\mathcal{P}}\text{R}_{\mathcal{P}}$ is quasi-terminating, then as a consequence of Theorem 4.3.2 we have

5.2.3. Theorem. *Let \mathcal{P} be a terminating algebraic polygraph modulo, whose cartesian polygraph has an underlying linear structure, and with a positive confluent strategy σ . Then an algebraic rewriting system on \mathcal{P} is locally confluent if, and only if, its critical branchings are confluent.*

Consider an algebraic rewriting system \bar{S} on \mathcal{P} . The positivity confluence of S with respect to σ implies the factorisation property of [16, Lemma 3.1.3], stating that every rewriting step $\bar{\alpha}$ of \bar{S} can be decomposed in the free $(2, 1)$ -theory on \bar{S} as $\bar{\alpha} = \bar{b} \star \bar{c}^{-1}$, where \bar{b} and \bar{c} are either positive rewriting steps of \bar{S}^σ or identities, as in the following diagram:

$$\begin{array}{ccc}
 & \bar{b} \rightarrow & h \leftarrow \bar{c} \\
 & \curvearrowright & \curvearrowleft \\
 f & \xrightarrow{\bar{\alpha}} & g
 \end{array} \quad (5.2.4)$$

Note that if $\bar{\alpha}$ is a rewriting step of \bar{S}^σ , this factorisation is trivial. When $\bar{\alpha}$ is in \bar{S} but not in \bar{S}^σ , that is $\bar{\alpha}$ is a quotient of a non- σ -positive S -rewriting path, it states that $\bar{\alpha}$ can be factorised using positive reductions. This proves the following critical branching criterion for linear algebraic rewriting systems.

5.2.5. Theorem. *Let \mathcal{P} be a terminating algebraic polygraph modulo, whose cartesian polygraph has an underlying linear structure, and satisfying the factorisation property (5.2.4). Then an algebraic rewriting system on \mathcal{P} is locally confluent if, and only if, its critical branchings are confluent.*

5.2.6. Left-monomial rewriting systems. The rules of an algebraic rewriting system on \mathcal{P} transform linear combinations of terms into linear combinations of terms. The system is called *left-monomial* when the source of every rule is an element of $P_1\langle Q \rangle$ that does not contain neither the operation $\oplus : mm \rightarrow m$ nor $\eta : rm \rightarrow m$ defined in (2.2.12). Equivalently, the source of any rule of the algebraic rewriting system is a *monomial*.

For terminating left-monomial LRS, the local confluence is equivalent to the confluence of critical branchings, [16, Thm. 4.3.2]. The proof of this criterion requires the factorisation property (5.2.4) that always holds in this context. We expect that in the left-monomial linear setting the positive confluence is equivalent to this property. But this remains an open problem, whose answer would explain the criterion for local confluence of LRS as a rewriting modulo result.

5.3. Rewriting with inverses

We conclude these algebraic examples by presenting a notion of group rewriting system defined as an algebraic rewriting system.

5.3.1. Rewriting in groups. In group theory rewriting gives algorithmic methods for decision problems, such as the word/conjugacy/geodesic problems, [6, 7, 11, 12, 33, 34]. In most cases, the method consists in constructing a convergent presentation of the considered group. Note also that homological finiteness conditions for finite convergence of groups were introduced, [8]. Finally, algorithms to compute relations among relations (syzygies) for groups given by generators and relations were developed in [21]. However, in all these works the presentations of the groups are interpreted by SRS, or by Gröbner bases, that present groups, or group rings, as monoids, or monoid rings, with axioms of inverses given explicitly in the set of rules. Namely, for a group G presented by a set of generators X and a set of relations \mathcal{R} , it is associated the following SRS:

$$\langle Q \mid \eta_x : xx^- \rightarrow 1, \eta_x^- : x^-x \rightarrow 1, \rho_r : r \rightarrow 1, \text{ for } r \in \mathcal{R} \rangle.$$

When solving decision problems, or computing homological invariants for groups, the rules η_x and η_x^- make the problem more complicated uselessly. Indeed, these rules should not be considered as those defining the group. In this way, the notion of rewriting in groups is not algebraically well considered yet.

5.3.2. Group rewriting systems. Consider an algebraic polygraph modulo $\mathcal{P} = (P, Q, R, {}_P R_P)$, where $P = \widetilde{\text{Grp}}$. The generating 1-cells of P induce on $\overline{P\langle Q \rangle}$ a structure of group isomorphic to the free group $F(Q)$ on Q . Denote by $P_1\langle Q \rangle_{\text{red}}$ the set of reduced 1-cells of $P_1\langle Q \rangle$ with respect to $P_2\langle Q \rangle$. A cellular extension T of $P_1\langle Q \rangle$ is called *reduced* if, for every A in T , the ground terms A_- and A_+ belong to $P_1\langle Q \rangle_{\text{red}}$.

5. Examples of algebraic rewriting systems

5.3.3. Lemma. *There exists a unique reduced cellular extension R_{red} of the theory $P_1\langle Q \rangle$ such that the algebraic rewriting systems R and R_{red} on $\overline{P\langle Q \rangle}$ coincide.*

Proof. The 2-cells of R_{red} are obtained by reducing the sources and targets of 2-cells of R with respect to $P_2\langle Q \rangle$. \square

From now on, we assume that the cellular extension R is reduced.

5.3.4. Positive strategies for reductions in groups. The free group $\overline{P\langle Q \rangle}$ can be constructed as a quotient monoid. Indeed, consider the free monoid $(Q \sqcup Q^-)^*$ over the set $Q \sqcup Q^-$ of constants and their formal inverses, with $Q^- = \{x^- \mid x \in Q\}$. Then, the group $\overline{P\langle Q \rangle}$ is isomorphic, as a monoid, to the monoid generated by $Q \sqcup Q^-$ and submitted to the relations

$$xx^- \rightarrow 1, \quad \text{and} \quad x^-x \rightarrow 1, \quad \text{for every } x \in Q. \quad (5.3.5)$$

The relations (5.3.5) are convergent, and thus the elements of the group $\overline{P\langle Q \rangle}$ are identified with normal forms of elements of $(Q \sqcup Q^-)^*$ with respect to these relations

Let us fix a total order \prec over $Q \sqcup Q^-$ such that for all $x, y \in Q$, $x \prec y$ implies $x^- \prec y^-$. Denote by \prec_{deglex} the deglex order on the free monoid $(Q \sqcup Q^-)^*$ induced by the order \prec , that is for any $f, g \in (Q \sqcup Q^-)^*$, $f \prec_{\text{deglex}} g$ if f is shorter than g or they have the same length and f is smaller than g for the lexicographic order induced by \prec .

Every 1-cell in $P_1\langle Q \rangle$ can be written $f(\iota^{n_1}(x_1), \dots, \iota^{n_k}(x_k))$, where $n_1, \dots, n_k \in \mathbb{N}$, f is an element of P_1^\times , x_1, \dots, x_k are constants of Q , ι is the inverse operation defined in (2.2.6), and ι^0 denotes the identity 1-cell of the theory P_1^\times . Moreover, if each n_i is chosen to be maximal, then f is uniquely determined, and does not contain the operation ι in its leafs. We define a map

$$[[\]] : P_1\langle Q \rangle \rightarrow (Q \sqcup Q^-)^*,$$

that associates to every 1-cell $f(\iota^{n_1}(x_1), \dots, \iota^{n_k}(x_k))$ in $P_1\langle Q \rangle$, where the n_i 's are maximal as above, the word $x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k}$, where $\varepsilon_i = +$ if n_i is even, and $\varepsilon_i = -$ if n_i is odd.

Let us denote by $\text{red}(f)$ the normal form in $(Q \sqcup Q^-)^*$ of $[[f]]$ with respect to relations (5.3.5). Let \models be the order on $P_1\langle Q \rangle$ defined by $f \models g$ if $\text{red}(f) \prec_{\text{deglex}} \text{red}(g)$.

We define a positive strategy for \mathcal{P} , by setting, for every $\bar{h} \in \overline{P\langle Q \rangle}$, the set $\sigma(\bar{h})$ to be the subset of $\pi^{-1}(\bar{h})$ whose elements are of the form $\mu(\mu(f, r_1^\varepsilon), g)$ and $\mu(f, \mu(r_1^\varepsilon, g))$, where $f, g \in P_1\langle Q \rangle_{\text{red}}$, $r_1 \rightarrow r_2 \in R$, $\varepsilon \in \{-, +\}$, and such that

$$\mu(\mu(f, r_2^\varepsilon), g) \models \mu(\mu(f, r_1^\varepsilon), g),$$

where, for $i = 1, 2$, we let $r_i^\varepsilon := r_i$ if $\varepsilon = +$, and $r_i^\varepsilon := \iota(r_i)$ otherwise.

5.3.6. Proposition. *For the positive strategy σ defined above, the algebraic polygraph modulo $\mathcal{P} = (P, Q, R, \rho R_P)$ is positively σ -confluent.*

Proof. Let us introduce an auxiliary strategy σ' for \mathcal{P} by setting

$$\sigma'(\bar{h}) = \left\{ \Gamma[r_1] \in \pi^{-1}(\bar{h}) \mid \Gamma \text{ is a context of } P_1\langle Q \rangle, r_1 \rightarrow r_2 \in R, \text{ s.t. } \Gamma[r_2] \models \Gamma[r_1] \right\}, \quad (5.3.7)$$

for every $\bar{h} \in \overline{P\langle Q \rangle}$. Prove that \mathcal{P} is positively σ' -confluent. For all rule $r_1 \rightarrow r_2$ in R and ground context Γ of $P_1\langle Q \rangle$ such that $\Gamma[r_2] \models \Gamma[r_1]$, the ρR_P -rewriting step $\Gamma[r_1] \rightarrow \Gamma[r_2]$ is σ' -positive. Otherwise $\Gamma[r_1] \not\models \Gamma[r_2]$, then the ρR_P -rewriting step $\Gamma'[r_1] \rightarrow \Gamma'[r_2]$ is σ' -positive, where $\Gamma'[\square] = \Gamma[\mu(\mu(r_2, \iota(\square)), r_1)]$. Indeed, we have $\text{red}(\Gamma'(r_2)) = \text{red}(\Gamma[r_1]) \prec_{\text{deglex}} \text{red}(\Gamma[r_2]) = \text{red}(\Gamma'(r_1))$. Moreover, $\Gamma[\mu(\mu(r_2, r_1^-), r_1)]$ and $\Gamma[\mu(\mu(r_2, r_2^-), r_1)]$ are equivalent with respect to $\equiv_{P_2\langle Q \rangle}$ to $\Gamma[r_2]$ and $\Gamma[r_1]$, respectively. Now, we show that every σ' -positive ρR_P -rewriting step induces a σ -positive one.

Let us consider a σ' -positive ρR_P -rewriting step $\Gamma[r] : \Gamma[r_1] \rightarrow \Gamma[r_2]$, let n be the largest integer such that $\Gamma[r_1] = \Gamma_1[\iota^n(r_1)]$ and Γ_1 is a (possibly empty) context. Denote by $\varepsilon := +$ if n is even and $-$ if n is odd, then $\iota^n(r_1)$ is equivalent to r_1^ε modulo $\equiv_{P_2\langle Q \rangle}$.

If Γ_1 is empty, then the ρR_P -rewriting step is of the form $r_1^\varepsilon \rightarrow r_2^\varepsilon$. Since $\Gamma[r_2] \models \Gamma[r_1]$, then $r_2^\varepsilon \models r_1^\varepsilon$ and thus it is σ -positive.

Otherwise, $\Gamma_1[r_1^\varepsilon]$ may be written either as $\mu(\mu(f', r_1^\varepsilon), g')$ or $\mu(f', \mu(r_1^\varepsilon, g'))$, where f', g' are 1-cells in $P_1\langle Q \rangle$. Denote by $f := \hat{f}'$ and $g := \hat{g}'$ be the normal forms of f' and g' with respect to $P_2\langle Q \rangle$. Then $\Gamma_1[r_1^\varepsilon]$ is equivalent modulo $\equiv_{P_2\langle Q \rangle}$ to $\mu(\mu(f, r_1^\varepsilon), g)$ or $\mu(f, \mu(r_1^\varepsilon, g))$. Moreover, since $\text{red}(fr_2^\varepsilon g) = \text{red}(\Gamma[r_2]) \prec_{\text{deglex}} \text{red}(\Gamma[r_1]) = \text{red}(fr_1^\varepsilon g)$, the ρR_P -rewriting step $fr_1^\varepsilon g \rightarrow fr_2^\varepsilon g$ is σ -positive, where $fr_1^\varepsilon g$ denotes either $\mu(\mu(f, r_1^\varepsilon), g)$ or $\mu(f, \mu(r_1^\varepsilon, g))$. \square

5.3.8. Example. Let us consider the algebraic polygraph modulo $(P, Q, R, \rho R_P)$, where $P = \widetilde{\text{Grp}}$, $Q = \{s, t\}$ and $R = \{\mu(\mu(s, t), s) \Rightarrow \mu(t, \mu(s, t))\}$. We consider the deglex order induced by the ordering $s > t > s^- > t^-$. The positive ρR_P -rewriting steps are of the form

$$f\mu(\mu(s, t), s)g \Rightarrow f\mu(t, \mu(s, t))g \quad \text{or} \quad f\mu(\mu(s^-, t^-), s^-)g \Rightarrow f\mu(t^-, \mu(s^-, t^-))g,$$

where f, g are reduced elements of $P_1\langle Q \rangle_{\text{red}}$, and the orientation is compatible with the order \models as defined in (5.3.4). For instance, there is a positive ρR_P -rewriting step

$$\mu(\mu(\mu(s, t), s), t) \Rightarrow \mu(\mu(t, \mu(s, t)), t)$$

yielding a reduction $stst \Rightarrow tstt$ in the free group $F(Q)$.

Now suppose that $f = tst$, $g = st$ and $\varepsilon = -1$. There is a σ -positive ρR_P -reduction as follows:

$$tst\mu(\mu(s^-, t^-), s^-)st \equiv_P tst\mu(\mu(s^-, t^-), s^-)stss^- \Rightarrow tst\mu(t^-, \mu(s^-, t^-))stss^- \equiv_P \mu(s, t)$$

that gives a rewriting step $tsts^- \Rightarrow st$ in the quotient. There is a critical branching of ρR_P as follows:

$$\begin{array}{ccc} \mu(\mu(\mu(s, t), s), \mu(t, s)) & \longrightarrow & \mu(\mu(t, \mu(s, t)), \mu(t, s)) \\ \downarrow & & \\ \mu(\mu(s, t), \mu(\mu(s, t), s)) & \longrightarrow & \mu(\mu(s, t), \mu(t, \mu(s, t))) \end{array}$$

that is not confluent modulo. It induces the following non confluent algebraic critical branching in the free group $F(Q)$

$$\begin{array}{ccc} & \searrow & \text{tstts} \\ \text{ststs} & & \\ & \searrow & \text{sttst} \end{array}$$

6. CONCLUSION AND PERSPECTIVES

In this article, we introduced the notion of algebraic rewriting systems as rewriting systems over algebraic theories. We studied algebraic contexts such as string, linear, and group rewriting. We formulated sufficient conditions to prove the critical branching lemma for algebraic rewriting systems. Our results lead us to formulate several perspectives:

- In Section 5.1, we recovered the critical branching lemma for SRS with respect to a convergent presentation of the theory Mon and a positive strategy making all the reductions positive. This corresponds to the classical setting of SRS. One may wonder what happens if we consider another presentation of the theory Mon and another positive strategy. These choices define a paradigm of string rewriting. This raises the question of defining a notion of equivalence between paradigms of string rewriting.
- For left-monomial LRS and Gröbner bases the critical branching lemma only requires termination. Theorem 5.2.5 proves that the factorisation property is also required. This property is always satisfied when we rewrite in left-monomial linear structures such as commutative or associative algebras. We expect that for left-monomial LRS, the factorisation property is equivalent to the positive confluence, and is always satisfied.
- In Section 5.3, we defined a positive strategy to rewrite in a free group. We prove a critical branching lemma with respect to this strategy. However, we do not yet know an algorithm that computes the exhaustive list of critical branchings with respect to this strategy. The same algorithmic problem occurs for the computation of the critical branchings for LRS that are not left-monomial.
- Another issue is to extend the algebraic critical branching lemma to higher-structures such as linear operads. Rewriting was defined on linear operads in terms of shuffle Gröbner bases by Dotsenko and Khoroshkin in [13] and shuffle linear polygraphs by Malbos and Ren in [37]. Algebraic polygraphs introduced in this article describe rewriting in one-dimensional algebraic structures, such as monoids, groups, modules, and algebras. We expect that our constructions can be extended to the setting of linear operads by considering algebraic polygraphs defined over a structure of cartesian 2-polygraphs on shuffle trees.
- Finally, another outlook is to extend the algebraic critical branching lemma to conditional rewriting systems in order to formalise the critical branching lemma for LRS defined over a field. The conditional rules are used to specify the rules depending on the invertibility of scalars in the field.

REFERENCES

- [1] David J. Anick. On the homology of associative algebras. *Trans. Amer. Math. Soc.*, 296(2):641–659, 1986.
- [2] Leo Bachmair and Nachum Dershowitz. Completion for rewriting modulo a congruence. *Theoretical Computer Science*, 67(2):173 – 201, 1989.
- [3] George M. Bergman. The diamond lemma for ring theory. *Adv. in Math.*, 29(2):178–218, 1978.

REFERENCES

- [4] Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal (An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal)*. PhD thesis, Mathematical Institute, University of Innsbruck, Austria, 1965. English translation in *J. of Symbolic Computation, Special Issue on Logic, Mathematics, and Computer Science: Interactions*. Vol. 41, Number 3-4, Pages 475–511, 2006.
- [5] Bruno Buchberger. History and basic features of the critical-pair/completion procedure. *J. Symbolic Comput.*, 3(1-2):3–38, 1987. *Rewriting techniques and applications (Dijon, 1985)*.
- [6] Fabienne Chouraqui. Rewriting systems and embedding of monoids in groups. *Groups Complex. Cryptol.*, 1(1):131–140, 2009.
- [7] Fabienne Chouraqui. The Knuth-Bendix algorithm and the conjugacy problem in monoids. *Semigroup Forum*, 82(1):181–196, 2011.
- [8] Robert Cremanns and Friedrich Otto. For groups the property of having finite derivation type is equivalent to the homological finiteness condition FP_3 . *J. Symbolic Comput.*, 22(2):155–177, 1996.
- [9] Pierre-Louis Curien, Alen Duric, and Yves Guiraud. Coherent presentations of a class of monoids admitting a garside family, 2021. arXiv 2107.00498.
- [10] Pierre-Louis Curien and Samuel Mimram. Coherent presentations of monoidal categories. *Log. Methods Comput. Sci.*, 13(3):Paper No. 31, 38, 2017.
- [11] Volker Diekert, Andrew Duncan, and Alexei G. Myasnikov. Cyclic rewriting and conjugacy problems. *Groups Complex. Cryptol.*, 4(2):321–355, 2012.
- [12] Volker Diekert, Andrew J. Duncan, and Alexei G. Myasnikov. Geodesic rewriting systems and pregroups. In *Combinatorial and geometric group theory*, Trends Math., pages 55–91. Birkhäuser/Springer Basel AG, Basel, 2010.
- [13] Vladimir Dotsenko and Anton Khoroshkin. Gröbner bases for operads. *Duke Math. J.*, 153(2):363–396, 2010.
- [14] Benjamin Dupont and Philippe Malbos. Coherent confluence modulo relations and double groupoids. preprint arXiv:1810.08184, Hal-01898868, 2018.
- [15] Stéphane Gaussent, Yves Guiraud, and Philippe Malbos. Coherent presentations of Artin monoids. *Compos. Math.*, 151(5):957–998, 2015.
- [16] Yves Guiraud, Eric Hoffbeck, and Philippe Malbos. Convergent presentations and polygraphic resolutions of associative algebras. *Math. Z.*, 293(1-2):113–179, 2019.
- [17] Yves Guiraud and Philippe Malbos. Higher-dimensional categories with finite derivation type. *Theory Appl. Categ.*, 22:No. 18, 420–478, 2009.
- [18] Yves Guiraud and Philippe Malbos. Coherence in monoidal track categories. *Math. Structures Comput. Sci.*, 22(6):931–969, 2012.
- [19] Yves Guiraud and Philippe Malbos. Higher-dimensional normalisation strategies for acyclicity. *Adv. Math.*, 231(3-4):2294–2351, 2012.
- [20] Yves Guiraud and Philippe Malbos. Polygraphs of finite derivation type. *Math. Structures Comput. Sci.*, 28(2):155–201, 2018.

REFERENCES

- [21] Anne Heyworth and Christopher D. Wensley. Logged rewriting and identities among relators. In *Groups St. Andrews 2001 in Oxford. Vol. I*, volume 304 of *London Math. Soc. Lecture Note Ser.*, pages 256–276. Cambridge Univ. Press, Cambridge, 2003.
- [22] Gérard Huet. Confluent reductions: abstract properties and applications to term rewriting systems. *J. Assoc. Comput. Mach.*, 27(4):797–821, 1980.
- [23] Jean-Marie Hullot. A catalogue of canonical term rewriting systems. 1980. SRI International, Technical Report CSL 113.
- [24] Kenji Iohara and Philippe Malbos. Maurice Janet’s algorithms on systems of linear partial differential equations. *Archive for History of Exact Sciences*, Springer, to appear, 2020.
- [25] Maurice Janet. Sur les systèmes d’équations aux dérivées partielles. *Journal de mathématiques pures et appliquées*, 8(3):65–151, 1920.
- [26] Jean-Pierre Jouannaud and Helene Kirchner. Completion of a set of rules modulo a set of equations. In *Proceedings of the 11th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages*, POPL ’84, pages 83–92, New York, NY, USA, 1984. ACM.
- [27] Jean-Pierre Jouannaud and Jianqi Li. Church-Rosser properties of normal rewriting. In *Computer science logic 2012*, volume 16 of *LIPICs. Leibniz Int. Proc. Inform.*, pages 350–365. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2012.
- [28] Jean-Pierre Jouannaud and Miguel Muñoz. Termination of a set of rules modulo a set of equations. In *7th international conference on automated deduction (Napa, Calif., 1984)*, volume 170 of *Lecture Notes in Comput. Sci.*, pages 175–193. Springer, Berlin, 1984.
- [29] Donald Knuth and Peter Bendix. Simple word problems in universal algebras. In *Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967)*, pages 263–297. Pergamon, Oxford, 1970.
- [30] Yuji Kobayashi. Complete rewriting systems and homology of monoid algebras. *J. Pure Appl. Algebra*, 65(3):263–275, 1990.
- [31] Yves Lafont. A new finiteness condition for monoids presented by complete rewriting systems (after Craig C. Squier). *J. Pure Appl. Algebra*, 98(3):229–244, 1995.
- [32] F. William Lawvere. Functorial semantics of algebraic theories. *Proc. Nat. Acad. Sci. U.S.A.*, 50:869–872, 1963.
- [33] Philippe Le Chenadec. Canonical forms in finitely presented algebras. In R. E. Shostak, editor, *7th International Conference on Automated Deduction*, pages 142–165, New York, NY, 1984. Springer New York.
- [34] Philippe Le Chenadec. A catalogue of complete group presentations. *J. Symbolic Comput.*, 2(4):363–381, 1986.
- [35] Philippe Malbos and Samuel Mimram. Homological computations for term rewriting systems. In *1st International Conference on Formal Structures for Computation and Deduction*, volume 52 of *LIPICs. Leibniz Int. Proc. Inform.*, pages Art. No. 27, 17. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2016.
- [36] Philippe Malbos and Samuel Mimram. Cartesian polygraphic resolutions. en préparation, 2021.
- [37] Philippe Malbos and Isaac Ren. Shuffle polygraphic resolutions for operads. submitted preprint, arXiv:2012.15718, 2020.

REFERENCES

- [38] Philippe Malbos and Isaac Ren. Completion in operads via essential syzygies. In *Proceedings of the 46th International Symposium on Symbolic and Algebraic Computation, ISSAC '21*, New York, NY, USA, 2021. Association for Computing Machinery.
- [39] Claude Marché. *Réécriture modulo une théorie présentée par un système convergent et décidabilité des problèmes du mot dans certaines classes de théories équationnelles*. PhD thesis, 1993. 1993PA112312.
- [40] Claude Marché. Normalized rewriting: an alternative to rewriting modulo a set of equations. *J. Symbolic Comput.*, 21(3):253–288, 1996.
- [41] Samuel Mimram. Computing critical pairs in 2-dimensional rewriting systems. In *RTA 2010: Proceedings of the 21st International Conference on Rewriting Techniques and Applications*, volume 6 of *LIPICs. Leibniz Int. Proc. Inform.*, pages 227–241. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2010.
- [42] Maurice Nivat. Congruences parfaites et quasi-parfaites. In *Séminaire P. Dubreil, 25e année (1971/72), Algèbre, Fasc. 1, Exp. No. 7*, page 9. Secrétariat Mathématique, Paris, 1973.
- [43] Gerald E. Peterson and Mark E. Stickel. Complete sets of reductions for some equational theories. *J. Assoc. Comput. Mach.*, 28(2):233–264, 1981.
- [44] J. A. Robinson. A machine-oriented logic based on the resolution principle. *J. Assoc. Comput. Mach.*, 12:23–41, 1965.
- [45] Anatoliï Illarionovich Shirshov. Some algorithmic problems for Lie algebras. *Sib. Mat. Zh.*, 3:292–296, 1962.
- [46] Craig C. Squier. Word problems and a homological finiteness condition for monoids. *J. Pure Appl. Algebra*, 49(1-2):201–217, 1987.
- [47] Craig C. Squier, Friedrich Otto, and Yuji Kobayashi. A finiteness condition for rewriting systems. *Theoret. Comput. Sci.*, 131(2):271–294, 1994.
- [48] Terese. *Term rewriting systems*, volume 55 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 2003.
- [49] Patrick Viry. Rewriting modulo a rewrite system. Technical report, 1995.

REFERENCES

CYRILLE CHENAVIER¹
cyrille.chenavier@jku.at

Johannes Kepler University
Altenberger Straße 69
A-4040 Linz, Austria

BENJAMIN DUPONT
bdupont@math.univ-lyon1.fr

Univ Lyon, Université Claude Bernard Lyon 1
CNRS UMR 5208, Institut Camille Jordan
43 blvd. du 11 novembre 1918
F-69622 Villeurbanne cedex, France

PHILIPPE MALBOS
malbos@math.univ-lyon1.fr

Univ Lyon, Université Claude Bernard Lyon 1
CNRS UMR 5208, Institut Camille Jordan
43 blvd. du 11 novembre 1918
F-69622 Villeurbanne cedex, France

¹ The author was supported by the Austrian Science Fund (FWF): P 32301.