Algebra and Geometry of Rewriting*

Yves Lafont†
Institut de Mathématiques de Luminy (UMR 6206 du CNRS)
Université de la Méditerranée (Aix-Marseille 2)

October 9, 2006

Abstract

We present various results of the last twenty years converging towards a *homotopical theory of computation*. This new theory is based on two crucial notions : *polygraphs* (introduced by Albert Burroni) and *polygraphic resolutions* (introduced by François Métayer). There are two motivations for such a theory:

- providing invariants of computational systems to study those systems and prove properties about them;
- finding new methods to make computations in algebraic structures coming from geometry or topology.

This means that this theory should be relevant for mathematicians as well as for theoretical computer scientists, since both may find useful tools or concepts for their own domain coming from the other one.

*This work has been partly supported by project GEOCAL (*Géométrie du Calcul*, ACI *Nouvelles Interfaces des Mathématiques*) and by project INVAL (*Invariants algébriques des systèmes informatiques*, ANR).

†Address: IML - 163 avenue de Luminy, Case 907 - 13288 Marseille CEDEX 9 - France - `http://iml.univ-mrs.fr/~lafont/`

Here are the main notions and results presented in this paper:

1. A presentation of a monoid M is *convergent* if it is *noetherian* and *confluent*. Such a presentation can be used to solve the *word problem for* M [KN85a]. The notion of *critical peak* is crucial here.
2. If a monoid M has a finite convergent presentation, then M satisfies the *homological condition* FP_3 [Sq87]. In particular, the homology group $\mathrm{H}_3(M)$ is of finite type.
3. If a monoid M has a finite convergent presentation, then M has *finite derivation type* [SOK94]. The notion of *2-congruence on derivations* is crucial here.
4. Finite derivation type implies the condition FP_3 [CO94, La95], but the converse does not hold [SOK94]. Hence, we shall present point 3 before point 2.
5. If a monoid M has a finite convergent presentation, then M satisfies the *homological condition* FP_∞ [Ko90]. In particular, all $\mathrm{H}_n(M)$ are of finite type.
6. The notion of 2-congruence corresponds to a special case of 3-*polygraph*. Polygraphs, which are also called *computads*, were introduced for studying higher dimensional word problems [Po91, Bu93].
7. *Polygraphic resolutions* provide a natural framework for generalizing point 3 to higher dimension [Me03]. The homology of such a polygraphic resolution coincides with the homology of the monoid [LM].
8. We conjecture that any finite convergent presentation allows to build a polygraphic resolution of finite type. This would provide an alternative (geometric) proof for point 5.

The following points should also fit in this framework, but they are not presented in this paper:

9. The notion of *Gaussian group* is related to the notion of convergent presentation. A typical example is the *group of braids* $\mathbb{B}_n$. Kobayashi's method [Ko90] has been adapted to build resolutions in this case [DL03]. We would like to build polygraphic resolutions in that case.
10. *Higher dimensional rewriting* is used for encoding term rewriting [Bu93] or for computation in monoidal categories [La03, Gu06]. We would like to build polygraphic resolutions in that case. This would also give an appropriate framework for a general theory of coherence.

Sections 1 and 2 present classical definitions and results used in the rest of the paper. Sections 3 and 4 present the existing theory (in reverse historical order). Section 5 presents the new approach inspired by the previous ones.

The author wishes to thank the anonymous referee for his careful reading and his helpful suggestions.

1 Presentations by generators and relations

1.1 Generators

A *monoid* is a set M together with an associative *product* $x, y \mapsto xy$ and a *unit* 1. If $X \subset M$, we write X^* for the *submonoid of* M *generated by* X, that is the set of finite products $x_1x_2\cdots x_n$ with $x_1, x_2, \ldots, x_n \in X$, including the empty product 1. It is the smallest submonoid of M containing X.

- If $X^* = M$, we say that X *generates* M, or that X is a *set of generators* for M.
- If X is finite and generates M, we say that M is a *finitely generated monoid*.
- If X generates M and no strict subset of X does, we say that X is a *minimal set of generators* for M.

Note that $M^* = M$. In particular, any finite monoid is finitely generated.

Proposition 1 *If M is a finitely generated monoid and X is a set of generators for M, then there is a finite subset of X which generates M. In particular, any minimal set of generators for M is finite.*

Indeed, for any $y = x_1x_2\cdots x_n \in M$ with $x_1, x_2, \ldots, x_n \in X$, we get a finite set $X(y) = \{x_1, x_2, \ldots, x_n\} \subset X$. If $Y = \{y_1, y_2, \ldots, y_p\}$ generates M, so does the finite set $X(Y) = X(y_1) \cup X(y_2) \cup \cdots \cup X(y_p) \subset X$. □

A *group* is a monoid G such that each $x \in G$ has an *inverse* $x^{-1} \in G$. If $X \subset G$, we write $\langle X \rangle$ for the *subgroup of* G *generated by* X, that is $(X \cup X^{-1})^*$. If $\langle X \rangle = G$, we say that X *generates the group* G. We can also define the notion of *finitely generated group* and the notion of *minimal set of generators for a group*.

Note that a group is finitely generated if and only if it is finitely generated as a monoid.

1.2 Presentations of monoids

If Σ is an *alphabet*, that is a set of *symbols*, we write Σ^* for the *free monoid generated by* Σ, that is the set of *words* $\alpha_1\alpha_2\cdots\alpha_n$ with $\alpha_1, \alpha_2, \ldots, \alpha_n \in \Sigma$, including the *empty word* 1. The notation Σ^* is consistent with the previous one, since Σ^* is also the submonoid of Σ^* generated by Σ.

If M is a monoid, then any map $f : \Sigma \to M$ extends to a unique morphism $\dot{f} : \Sigma^* \to M$. For instance, if M is the additive monoid $\mathbb{N}$, and f is defined by $f(\alpha) = 1$ for each $\alpha \in \Sigma$, then $\dot{f}(x)$ is the *length* $|x|$ of the word x.

A *presentation* (*by generators and relations*) is a pair (Σ, R) where Σ is an alphabet and R is a subset of $\Sigma^* \times \Sigma^*$, that is a binary relation on Σ^*. The *congruence generated by* R is defined as follows:

- $uxv \leftrightarrow_R uyv$ whenever $u, v \in \Sigma^*$, and $x\ R\ y$ or $y\ R\ x$;
- $x \leftrightarrow_R^* y$ whenever $x = x_0 \leftrightarrow_R x_1 \leftrightarrow_R \cdots \leftrightarrow_R x_n = y$.

We get a *quotient monoid* $\Sigma^*/{\leftrightarrow_R^*}$ and a *canonical surjection* $\pi_R : \Sigma^* \to \Sigma^*/{\leftrightarrow_R^*}$. Moreover, if $f : \Sigma \to M$ is a map such that $\dot{f}(x) = \dot{f}(y)$ whenever $x\ R\ y$, we get a unique morphism $\tilde{f} : \Sigma^*/{\leftrightarrow_R^*} \to M$ such that $\tilde{f} \circ \pi_R = \dot{f}$.

- If the map $\tilde{f}$ is bijective, we write $M \cong \Sigma^*/{\leftrightarrow_R^*}$ and we say that (Σ, R) is a *presentation of the monoid* M. This means that the set $f(\Sigma)$ generates M, and that $\dot{f}(x) = \dot{f}(y)$ if and only if $x \leftrightarrow_R^* y$.
- If $\tilde{f}$ is bijective and if both $\Sigma = \{\alpha_1, \ldots, \alpha_p\}$ and $R = \{(x_1, y_1), \ldots, (x_q, y_q)\}$ are finite, then we write $M \cong \langle \alpha_1, \ldots, \alpha_p \,|\, x_1 = y_1, \ldots, x_q = y_q \rangle^+$ and we say that M is a *finitely presented monoid*.
- If $\tilde{f}$ is bijective, $f(\Sigma)$ is a minimal set of generators and no strict subset of R generates the congruence $\leftrightarrow_R^*$, then we say that (Σ, R) is a *minimal presentation* of M.

Note that any monoid M has a *standard presentation* (Σ, R), where Σ consists of one symbol a_x for each $x \in M$, and R is defined by $a_1\ R\ 1$ and $a_x a_y\ R\ a_{xy}$ for all $x, y \in M$. In particular, any finite monoid is finitely presented.

Lemma 1 *For any morphism $f : \Sigma^*/{\leftrightarrow_R^*} \to \Omega^*/{\leftrightarrow_S^*}$, there is a morphism $\varphi : \Sigma^* \to \Omega^*$ such that $\pi_S \circ \varphi = f \circ \pi_R$.*

$$\begin{array}{ccc} \Sigma^* & \xrightarrow{\varphi} & \Omega^* \\ \pi_R \downarrow & & \downarrow \pi_S \\ \Sigma^*/{\leftrightarrow_R^*} & \xrightarrow[f]{} & \Omega^*/{\leftrightarrow_S^*} \end{array}$$

Indeed, it suffices to define $\varphi(\alpha)$ for each $\alpha \in \Sigma$, using the fact that π_S is surjective. □

Proposition 2 *If M is a finitely presented monoid and $M \cong \Sigma^*/{\leftrightarrow_R^*}$ where Σ is finite, then there is a finite subset of R which generates $\leftrightarrow_R^*$. In particular, any minimal presentation of M is finite.*

Indeed, if (Ω, S) is a finite presentation of M, there is an isomorphism $f : \Sigma^*/{\leftrightarrow_R^*} \xrightarrow{\sim} \Omega/{\leftrightarrow_S^*}$. Applying lemma 1 to f and f^{-1}, we get two morphisms $\varphi : \Sigma^* \to \Omega^*$ and $\overline{\varphi} : \Omega^* \to \Sigma^*$ such that the following properties hold:

$$\varphi(x) \leftrightarrow_S^* \varphi(y) \text{ whenever } x\ R\ y, \qquad \overline{\varphi}(x) \leftrightarrow_R^* \overline{\varphi}(y) \text{ whenever } x\ S\ y, \qquad x \leftrightarrow_R^* \overline{\varphi}(\varphi(x)) \text{ for any } x \in \Sigma^*.$$

Hence, $\leftrightarrow_R^*$ is generated by the finite relation R' defined by $\overline{\varphi}(x)\ R'\ \overline{\varphi}(y)$ whenever $x\ S\ y$, and $\alpha\ R'\ \overline{\varphi}(\varphi(\alpha))$ for each $\alpha \in \Sigma$. By the same argument as for proposition 1, we get a finite subset of R which generates $\leftrightarrow_R^*$. □

1.3 Presentations of groups

If Σ is an alphabet, we write $\langle \Sigma \rangle$ for the *free group* $(\Sigma \cup \overline{\Sigma})^*/{\leftrightarrow_R^*}$ where $\overline{\Sigma} = \{\overline{\alpha} \,|\, \alpha \in \Sigma\}$ is a disjoint copy of Σ and R is defined by $\alpha\overline{\alpha}\ R\ 1$ and $\overline{\alpha}\alpha\ R\ 1$ for each $\alpha \in \Sigma$.

We identify each $\alpha \in \Sigma$ with its congruence class $\pi_R(\alpha) \in \langle \Sigma \rangle$, so that $\pi_R(\overline{\alpha}) = \alpha^{-1}$ and $\langle \Sigma \rangle = (\Sigma \cup \Sigma^{-1})^*$, that is the subgroup of $\langle \Sigma \rangle$ generated by Σ. Hence, the notation $\langle \Sigma \rangle$ is consistent with the previous one.

A *presentation of group* is a pair (Σ, X), where $X \subset (\Sigma \cup \overline{\Sigma})^*$. It is a *presentation of the group* G if $G \cong \langle \Sigma \rangle / H$, where H is the normal subgroup of $\langle \Sigma \rangle$ generated by $\pi_R(X)$. This means that $G \cong (\Sigma \cup \overline{\Sigma})^*/{\leftrightarrow_{R_X}^*}$ where R_X is defined by $\alpha\overline{\alpha}\ R_X\ 1$ and $\overline{\alpha}\alpha\ R_X\ 1$ for each $\alpha \in \Sigma$, and $x\ R_X\ 1$ for each $x \in X$.

In particular, if both $\Sigma = \{\alpha_1, \ldots, \alpha_p\}$ and $X = \{x_1, \ldots, x_q\}$ are finite, we write $G \cong \langle \alpha_1, \ldots, \alpha_p \,|\, x_1, \ldots, x_q \rangle$, which means $G \cong \langle \alpha_1, \overline{\alpha}_1, \ldots, \alpha_p, \overline{\alpha}_p \,|\, \alpha_1\overline{\alpha}_1 = 1, \overline{\alpha}_1\alpha_1 = 1, \ldots, \alpha_p\overline{\alpha}_p = 1, \overline{\alpha}_p\alpha_p = 1, x_1 = 1, \ldots, x_q = 1 \rangle^+$. Note that a group G is finitely presented if and only if it is finitely presented as a monoid.

1.4 Examples

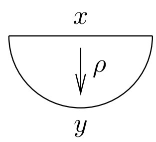
Here are some basic examples of finite presentations of groups and monoids:

- $\mathbb{Z} \cong \mathbb{B}_2 \cong \langle a \rangle \cong \langle a, \overline{a} \,|\, a\overline{a} = 1, \overline{a}a = 1 \rangle^+$ (free group generated by one element, or 2-braids);
- $\mathbb{Z} * \mathbb{Z} \cong \langle a, b \rangle \cong \langle a, \overline{a}, b, \overline{b} \,|\, a\overline{a} = 1, \overline{a}a = 1, b\overline{b} = 1, \overline{b}b = 1 \rangle^+$ (free group generated by two elements);
- $\mathbb{N}^2 \cong \langle a, b \,|\, ab = ba \rangle^+$ (free commutative monoid generated by two elements);
- $\mathbb{Z}^2 \cong \langle a, b \,|\, aba^{-1}b^{-1} \rangle \cong \langle a, \overline{a}, b, \overline{b} \,|\, a\overline{a} = 1, \overline{a}a = 1, b\overline{b} = 1, \overline{b}b = 1, ab = ba \rangle^+$ (free commutative group);
- $\mathbb{Z}_2 \cong \mathbb{S}_2 \cong \langle a \,|\, a^2 \rangle \cong \langle a \,|\, a^2 = 1 \rangle^+$ (integers modulo 2, or permutations of 2 elements);
- $\mathbb{S}_3 \cong \langle a, b \,|\, a^2, b^2, abab^{-1}a^{-1}b^{-1} \rangle \cong \langle a, b \,|\, a^2 = 1, b^2 = 1, aba = bab \rangle^+$ (permutations of 3 elements);
- $\mathbb{B}_3 \cong \langle a, b \,|\, abab^{-1}a^{-1}b^{-1} \rangle \cong \langle a, \overline{a}, b, \overline{b} \,|\, a\overline{a} = 1, \overline{a}a = 1, b\overline{b} = 1, \overline{b}b = 1, aba = bab \rangle^+$ (3-braids);
- $\mathbb{B}_3^+ \cong \langle a, b \,|\, aba = bab \rangle^+$ (positive 3-braids).

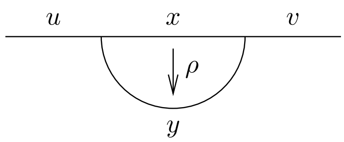
2 Word rewriting

2.1 Rewrite rules and reductions

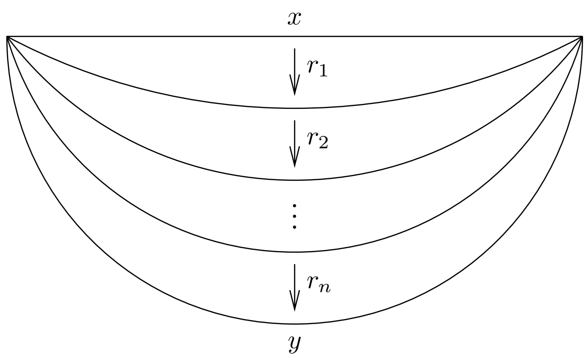
If (Σ, R) is a presentation, each $\rho = (x, y) \in R$ can be seen as a *rewrite rule* $x \overset{\rho}{\to} y$, with *source* x and *target* y:



An *elementary reduction* is a formal product $uxv \overset{u\rho v}{\to} uyv$ where u, v are words and $x \overset{\rho}{\to} y$ is a rule:



A *reduction* $x \overset{r}{\to} y$ is a finite sequence $x = x_0 \overset{r_1}{\to} x_1 \overset{r_2}{\to} x_2 \cdots x_{n-1} \overset{r_n}{\to} x_n = y$ of elementary reductions:



Each rule is considered as an elementary reduction, and any elementary reduction is seen as a reduction of length 1.

If $x \overset{r}{\to} y$ and $y \overset{s}{\to} z$ are reductions, we write $r * s$ for the *composed reduction* $x \overset{r}{\to} y \overset{s}{\to} z$. Furthermore, there is an *empty reduction* $x \overset{x}{\to} x$ for any word $x \in \Sigma^*$. So we get a *category of reductions* $(\Sigma, R)^*$.

Note also that for any word u and for any reduction $x \overset{r}{\to} y$, we can define two reductions $ux \overset{ur}{\to} uy$ and $xu \overset{ru}{\to} yu$.

2.2 Termination and confluence

The *reduction relation generated by* R is the smallest order relation containing R which is compatible with product:

- $uxv \to_R uyv$ whenever $u, v \in \Sigma^*$ and $x \; R \; y$;
- $x \to_R^* y$ whenever $x = x_0 \to_R x_1 \to_R \cdots \to_R x_n = y$.

In other words, $x \to_R^* y$ whenever there is a reduction $x \xrightarrow{r} y$, and $x \to_R y$ whenever there is an elementary one.

We say that a word x is *reducible* if there is some word y such that $x \to_R y$. Otherwise, we say that x is *reduced*.

We say that a property is R*-hereditary* if, whenever it holds for each y such that $x \to_R y$, then it also holds for x. In particular, such a property holds for all reduced words.

Proposition 3 *For any presentation* (Σ, R)*, the following properties are equivalent:*

- *There is no infinite reduction* $x_0 \to_R x_1 \to_R \cdots \to_R x_n \to_R x_{n+1} \to_R \cdots$ *(termination).*
- *Any* R*-hereditary property holds for all words (noetherian induction principle).*

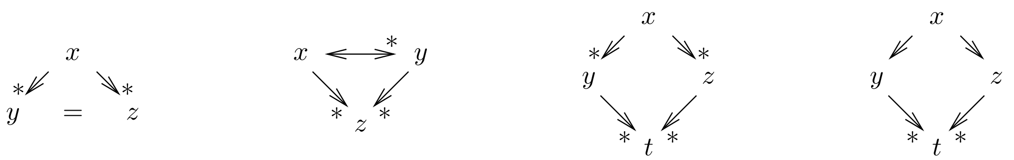
Indeed, if x does not satisfy some R-hereditary property, then we can build an infinite reduction starting from x. Conversely, termination can be proved by noetherian induction. □

In that case, we say that the presentation is *noetherian*. This implies that the source of a rule can never be empty. Moreover, for any word x, there is a reduced x' such that $x \to_R^* x'$. This is proved by noetherian induction on x.

In order to prove that a presentation (Σ, R) is noetherian, it suffices to exhibit a *termination ordering* for it, that is a strict well-founded ordering $\prec$ which contains R and which is compatible with product. For instance, $\prec$ may be defined by $x \prec y$ whenever $|x| < |y|$, or $|x| = |y|$ and x is strictly smaller than y for some lexicographical ordering.

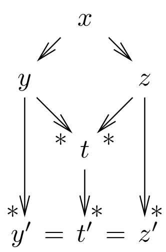
Proposition 4 *If the presentation* (Σ, R) *is noetherian, then the following properties are equivalent:*

- *If* $x \to_R^* y$ *and* $x \to_R^* z$ *where* y *and* z *are reduced, then* $y = z$ *(uniqueness of the reduced form).*
- *If* $x \leftrightarrow_R^* y$*, there is* z *such that* $x \to_R^* z$ *and* $y \to_R^* z$ *(Church-Rosser property).*
- *If* $x \to_R^* y$ *and* $x \to_R^* z$*, there is* t *such that* $y \to_R^* t$ *and* $z \to_R^* t$ *(confluence).*
- *If* $x \to_R y$ *and* $x \to_R z$*, there is* t *such that* $y \to_R^* t$ *and* $z \to_R^* t$ *(local confluence).*



Indeed, it is easy to see that each property implies the next one. Furthermore, assuming local confluence, we prove uniqueness of the reduced form by noetherian induction on x:

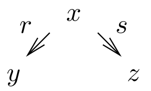
- If x is reduced, then x is the unique reduced form of x.
- Otherwise, assume that $x \to_R y'$ and $x \to_R z'$ where y' and z' are reduced. Since x is reducible, we get y, z such that $x \to_R y \to_R^* y'$ and $x \to_R z \to_R^* z'$. By local confluence, there is t such that $y \to_R^* t$ and $z \to_R^* t$. By termination, there is a reduced t' such that $t \to_R^* t'$, and by induction hypothesis, we get $y' = t' = z'$. □

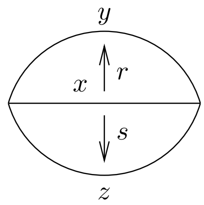


If a notherian presentation satisfies one of the above properties, we say that it is *convergent*.

2.3 Critical peaks

A *peak of source* x is a pair $p = (r, s)$ of elementary reductions whose common source is x:

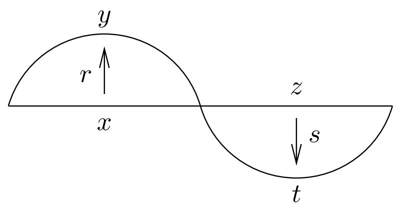




Such a peak is *confluent* if there is t such that $y \to_R^* t$ and $z \to_R^* t$. Note the following points:

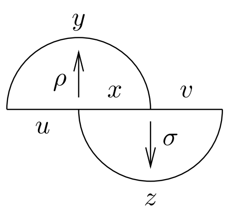
- If $p = (r, s)$ is a confluent peak, so is $q = (s, r)$. Hence we can identify q with p.
- If u is a word and $p = (r, s)$ is a confluent peak, so are the peaks $up = (ur, us)$ and $pu = (ru, su)$.
- If $x \xrightarrow{r} y$ is an elementary reduction, then $p = (r, r)$ is a confluent peak.
- If $x \xrightarrow{r} y$ and $z \xrightarrow{s} t$ are elementary reductions, then $p = (rz, xs)$ is a confluent peak.

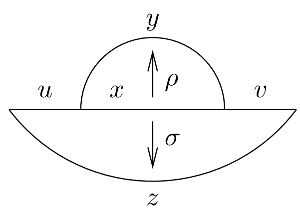
In the latter case, we say that the elementary reductions rz and xs are *disjoint*.



A peak is *critical* if it is not of the form up or pu with $u \neq 1$, and if its reductions are neither equal nor disjoint. Hence it is necessarily of one of the following two forms:

- an *overlap* $(\rho v, u\sigma)$ where $ux \xrightarrow{\rho} y$ and $xv \xrightarrow{\sigma} z$ are rules and $u, x, v \neq 1$;
- an *inclusion* $(u\rho v, \sigma)$ where $x \xrightarrow{\rho} y$ and $uxv \xrightarrow{\sigma} z$ are rules and $ux, xv \neq 1$.





Proposition 5 *If all critical peaks of a presentation are confluent, then all peaks are confluent.*

This follows directly from the above remarks. □

Corollary 1 *If a presentation is notherian and all its critical peaks are confluent, then it is convergent.*

2.4 Decision problems

If (Σ, R) is a convergent presentation, we write $\widehat{x}$ for the *reduced form* of x, that is the unique x' such that $x \to_R^* x'$. By Church-Rosser, we have $x \leftrightarrow_R^* y$ if and only if $\widehat{x} = \widehat{y}$.

Proposition 6 *If (Σ, R) is a finite convergent presentation, then $\leftrightarrow_R^*$ is a decidable relation.*

It suffices indeed to compare reduced forms, which are obviously computable in that case. □

If $\leftrightarrow_R^*$ is a decidable relation, one says that M *has a decidable word problem*. In fact, this property does not depend on the choice of the presentation. It may also happen in the case of an infinite presentation. See for instance [LP91].

Proposition 7 *Convergence is a decidable property for any finite noetherian presentation.*

Indeed, there are finitely many critical peaks in that case, and they are obviously computable. □

2.5 Reduced presentations

We say that a convergent presentation (Σ, R) is *reduced* if each symbol $\alpha \in \Sigma$ is reduced, and for each rule $x \xrightarrow{\rho} y$, the source x is only reducible by ρ, whereas the target y is reduced. So we can identify the rule ρ with its source x. Moreover, each critical peak p is an overlap and is determined by its source x. So we can also identify p with x.

For instance, the standard presentation of a monoid is convergent but not reduced, because a_1 is not reduced.

Proposition 8 [KN85a] *For any convergent presentation, there is a reduced one with no more symbols and rules.*

In particular, any monoid M has a *reduced standard presentation* (Σ, R), where Σ consists of one symbol a_x for each $x \neq 1$ in M, and R is defined by $a_x a_y \; R \; 1$ whenever $xy = 1$ and $a_x a_y \; R \; a_{xy}$ whenever $xy \neq 1$.

Corollary 2 *If M has a finite convergent presentation, then it has a finite reduced convergent presentation.*

Note that a weaker notion of *minimal convergent presentation* is used in [LP91].

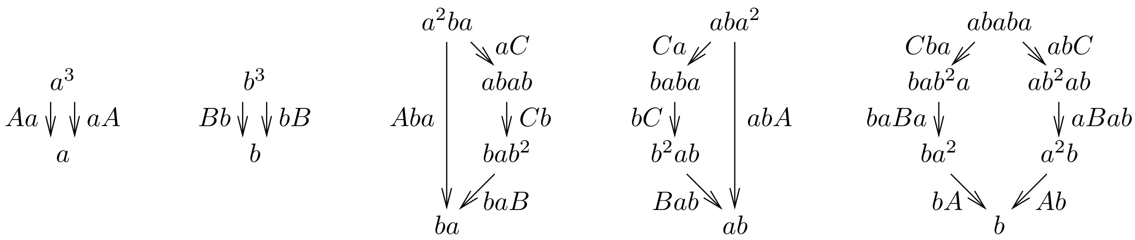
2.6 Examples

Here are some examples of finite reduced convergent presentations:

- $\mathbb{N}^2 \cong \langle a, b \,|\, ab \to ba \rangle^+$, with no critical peak;
- $\mathbb{Z}_2 \cong \langle a \,|\, a^2 \to 1 \rangle^+$, with 1 critical peak: a^3;
- $\mathbb{Z} \cong \langle a, \overline{a} \,|\, a\overline{a} \to 1, \overline{a}a \to 1 \rangle^+$, with 2 critical peaks: $a\overline{a}a$, $\overline{a}a\overline{a}$;
- $\mathbb{Z} * \mathbb{Z} \cong \langle a, \overline{a}, b, \overline{b} \,|\, a\overline{a} \to 1, \overline{a}a \to 1, b\overline{b} \to 1, \overline{b}b \to 1 \rangle^+$, with 4 critical peaks: $a\overline{a}a$, $\overline{a}a\overline{a}$, $b\overline{b}b$, $\overline{b}b\overline{b}$;
- $\mathbb{S}_3 \cong \langle a, b \,|\, a^2 \to 1, b^2 \to 1, aba \to bab \rangle^+$, with 5 critical peaks: a^3, b^3, a^2ba, aba^2, $ababa$.

Note that we write $x \to y$ instead of $x = y$, since we consider each relation as a rewrite rule.

In particular, if we write $a^2 \xrightarrow{A} 1$, $b^2 \xrightarrow{B} 1$, $aba \xrightarrow{C} bab$ for the rules in the latter presentation, the confluence of the critical peaks is given by the following diagrams:



The following presentations are noetherian, but not convergent:

- $\mathbb{Z}^2 \cong \langle a, \overline{a}, b, \overline{b} \,|\, a\overline{a} \to 1, \overline{a}a \to 1, b\overline{b} \to 1, \overline{b}b \to 1, ab \to ba \rangle^+$, since $\overline{a}ab$ and $ab\overline{b}$ are non confluent peaks;
- $\mathbb{B}_3^+ \cong \langle a, b \,|\, aba \to bab \rangle^+$, since $ababa$ is a non confluent peak.

Nevertheless, both monoids have finite (reduced) convergent presentations:

- $\mathbb{Z}^2 \cong \langle a, \overline{a}, b, \overline{b} \,|\, a\overline{a} \to 1, \overline{a}a \to 1, b\overline{b} \to 1, \overline{b}b \to 1, ab \to ba, \overline{a}b \to b\overline{a}, a\overline{b} \to \overline{b}a, \overline{a}\overline{b} \to \overline{b}\overline{a} \rangle^+$;
- $\mathbb{B}_3^+ \cong \langle a, b, c \,|\, ab \to c, ca \to bc, bcb \to cc, ccb \to acc \rangle^+$.

The first presentation is obtained by introducing *derivable relations* in order to make all critical peaks confluent. This algorithm is called the *Knuth-Bendix completion*. See [KN85a]. In fact, the Knuth-Bendix completion does not always terminates, but when it does, it produces a finite convergent presentation which solves the word problem.

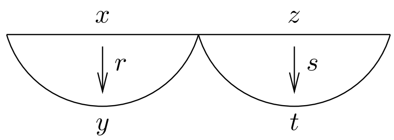
The second one is obtained by introducing a *superfluous generator* c together with the rule $ab \to c$, and by applying the Knuth-Bendix completion. In fact, $\mathbb{B}_3^+$ has no convergent presentation with 2 generators. See [KN85b].

3 Finite derivation type

3.1 2-congruences on reductions

Consider a presentation of monoid (Σ, R). We write $r \parallel s$ if $x \overset{r,s}{\to} y$ are parallel reductions. A *2-congruence on reductions* is an equivalence relation $\sim$ defined on parallel reductions and satisfying the following properties:

- $urv \sim usv$ for any words u, v and for any reductions $x \overset{r,s}{\to} y$ such that $r \sim s$ (*compatibility with product*);
- $r * s \sim r' * s'$ for any reductions $x \overset{r,r'}{\to} y \overset{s,s'}{\to} z$ such that $r \sim r'$ and $s \sim s'$ (*compatibility with composition*);
- $rz * ys \sim xs * rt$ for any reductions $x \overset{r}{\to} y$ and $z \overset{s}{\to} t$ (*exchange*).



For instance, $\parallel$ is the *maximal* or *full 2-congruence*.

If P is any set of pairs of parallel reductions, we define the *2-congruence* $\sim_P$ *generated by* P, that is the smallest 2-congruence containing P. If P is finite, we say that the 2-congruence $\sim_P$ is *finitely generated*.

The exchange property expresses the fact that a 2-congruence does not see the relative order of disjoint reductions. Because of this requirement, $=$ is not a 2-congruence, but it would be the case if we were considering the *strict monoidal category of reductions* $\langle \Sigma, R \rangle^+ = (\Sigma, R)^* / \equiv$, where $\equiv$ is the *minimal 2-congruence* $\sim_\emptyset$.

3.2 2-congruences on derivations

If $x \overset{\rho}{\to} y$ is a rule, we write $y \overset{\rho^{\mathrm{op}}}{\to} x$ for the *reverse rule*. A reduction for the *symmetrized presentation* $(\Sigma, R \cup R^{\mathrm{op}})$, where $R^{\mathrm{op}} = \{\rho^{\mathrm{op}} \mid \rho \in R\}$, is called a *derivation*. The notation ρ^{op} is extended to all derivations as follows:

- $(\rho^{\mathrm{op}})^{\mathrm{op}} = \rho$ for each rule $x \overset{\rho}{\to} y$ in R;
- $(u\rho v)^{\mathrm{op}} = u\rho^{\mathrm{op}} v$ for any words u, v and for each $x \overset{\rho}{\to} y$ in $R \cup R^{\mathrm{op}}$;
- $(r_1 * r_2 * \cdots * r_n)^{\mathrm{op}} = r_n^{\mathrm{op}} * \cdots * r_2^{\mathrm{op}} * r_1^{\mathrm{op}}$ for any derivation $x_0 \overset{r_1}{\to} x_1 \overset{r_2}{\to} x_2 \cdots x_{n-1} \overset{r_n}{\to} x_n$.

A *2-congruence on derivations* is a 2-congruence $\approx$ for $(\Sigma, R \cup R^{\mathrm{op}})$ satisfying the following extra property:

- $r * r^{\mathrm{op}} \approx x$ and $r^{\mathrm{op}} * r \approx y$ for any derivation $x \overset{r}{\to} y$ (*invertibility*).

In fact, it suffices to check this property for each rule $x \overset{\rho}{\to} y$.

For instance, $\parallel$ is the *maximal* or *full 2-congruence on derivations*.

If P is any set of pairs of parallel derivations, we can define the *2-congruence on derivations* $\approx_P$ *generated by* P, that is $\sim_Q$, where Q is defined by $\rho * \rho^{\mathrm{op}}\ Q\ x$ and $\rho^{\mathrm{op}} * \rho\ Q\ y$ for each rule $x \overset{\rho}{\to} y$, and $r\ Q\ s$ whenever $r\ P\ s$.

Again, $=$ is not a 2 congruence on derivations, but it would be the case if we were considering the *strict monoidal groupoid of derivations* $\langle \Sigma, R \rangle = (\Sigma, R \cup R^{\mathrm{op}})^* / \equiv$, where $\equiv$ is the *minimal 2-congruence on derivations* $\approx_\emptyset$.

If P is finite, we say that the 2-congruence $\approx_P$ on derivations is *finitely generated*. This implies that $\approx_P$ is also finitely generated as a 2-congruence for $(\Sigma, R \cup R^{\mathrm{op}})$, at least when R is finite. We say that a monoid M has *finite derivation type* if M has a finite presentation such that the full 2-congruence on derivations $\parallel$ is finitely generated.

Theorem 1 [SOK94] *Assume M has finite derivation type and $M \cong \Sigma^* / \leftrightarrow_R^*$ where (Σ, R) is a finite presentation. If P generates the full 2-congruence $\parallel$ on derivations for (Σ, R), there is a finite subset of P which generates $\parallel$.*

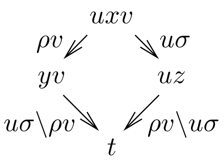
The proof is essentially the same as the one for proposition 2. □

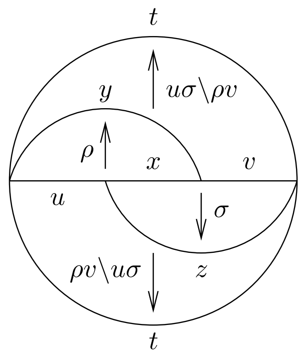
In fact, the statement given in [SOK94] is slightly weaker: It only says that $\parallel$ is finitely generated.

3.3 Case of a convergent presentation

If the presentation (Σ, R) is convergent, we can choose a *closure* for each critical peak $p = (r, s)$, that is a pair of parallel reductions $p^\diamond = (r * s \backslash r, s * r \backslash s)$. We write $R^\diamond$ for the set of all those closures.

In the case of an overlap, we get the following pictures:





In fact, the disk should be seen as a sphere, obtained by identifying the upper boundary t with the lower one.

Lemma 2 *For any peak $p = (r, s)$, there is a closure $p^\diamond = (r * s \backslash r, s * r \backslash s)$ such that $r * s \backslash r \sim_{R^\diamond} s * r \backslash s$.*

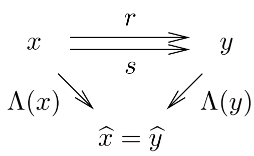
The closure is obtained as in the proof of proposition 5. Then, we use exchange and compatibility with product. □

Lemma 3 *$r \sim_{R^\diamond} s$ for any parallel reductions $x \overset{r,s}{\to} \widehat{x}$.*

This is proved by noetherian induction as for proposition 4, using lemma 2 and compatibility with composition. □

Theorem 2 [SOK94] *If (Σ, R) is a convergent presentation, then $r \approx_{R^\diamond} s$ for any parallel derivations $x \overset{r,s}{\to} y$.*

Indeed, we can choose a reduction $x \overset{\Lambda(x)}{\to} \widehat{x}$ for each word x. By lemma 3, we get $r * \Lambda(y) \sim_{R^\diamond} \Lambda(x)$, so that $r * \Lambda(y) \approx_{R^\diamond} \Lambda(x)$ and $r \approx_{R^\diamond} r * \Lambda(y) * \Lambda(y)^{\mathrm{op}} \approx_{R^\diamond} \Lambda(x) * \Lambda(y)^{\mathrm{op}}$, and similarly for s. Hence, $r \approx_{R^\diamond} s$. □



Corollary 3 *If M has a finite convergent presentation, then M has finite derivation type.*

4 Derivations and homology

4.1 Homology of monoids

If M is a monoid, we write $\mathbb{Z}M$ for the *ring of* M, which is the free abelian group generated by the set M, together with a product extending the one of M. A (*left*) $\mathbb{Z}M$*-module* is an abelian group together with a linear action of M.

A *complex of* $\mathbb{Z}M$*-modules* is an infinite sequence $C_0 \overset{\delta_0}{\leftarrow} C_1 \overset{\delta_1}{\leftarrow} C_2 \cdots C_n \overset{\delta_n}{\leftarrow} C_{n+1} \cdots$ of $\mathbb{Z}M$-linear maps such that $\delta_n \circ \delta_{n+1} = 0$, that is $\operatorname{im} \delta_{n+1} \subset \ker \delta_n$, for each n. Such a complex is *exact* if $\operatorname{im} \delta_{n+1} = \ker \delta_n$ for each n.

If S is a set, the *free action* of M on the set $M \cdot S = M \times S$ is defined by $x \cdot (y, \xi) = (xy, \xi)$. We write ξ for $(1, \xi)$ and $x \cdot \xi$ for (x, ξ). Finally, we write $\mathbb{Z}M \cdot S$ for the *free* $\mathbb{Z}M$*-module generated by* S, which is the free abelian group generated by the set $M \cdot S$, together with a linear action of M extending the one of M on $M \cdot S$.

A *resolution of* $\mathbb{Z}$ *by free* $\mathbb{Z}M$*-modules* is an exact complex $0 \leftarrow \mathbb{Z} \overset{\varepsilon}{\leftarrow} C_0 \overset{\delta_0}{\leftarrow} C_1 \overset{\delta_1}{\leftarrow} C_2 \cdots C_n \overset{\delta_n}{\leftarrow} C_{n+1} \cdots$ where $\mathbb{Z}$ stands for the $\mathbb{Z}M$-module defined by the *trivial action* of M on the abelian group $\mathbb{Z}$, and C_n is a free $\mathbb{Z}M$-module $\mathbb{Z}M \cdot S_n$ for each n. The head $0 \leftarrow \mathbb{Z}$ ensures that ε is surjective (by exactness).

Any *partial resolution* $0 \leftarrow \mathbb{Z} \overset{\varepsilon}{\leftarrow} C_0 \overset{\delta_0}{\leftarrow} C_1 \overset{\delta_1}{\leftarrow} C_2 \cdots C_n \overset{\delta_n}{\leftarrow} C_{n+1}$ extends to a full one. In particular, such a full resolution exists. Moreover, it is *unique up to homotopical equivalence*. See [Ma63, Sp66, Br82] for more details.

By *trivializing the action of* M, we get a complex $\mathbb{Z} \cdot S_0 \overset{\partial_0}{\leftarrow} \mathbb{Z} \cdot S_1 \overset{\partial_1}{\leftarrow} \mathbb{Z} \cdot S_2 \cdots \mathbb{Z} \cdot S_n \overset{\partial_n}{\leftarrow} \mathbb{Z} \cdot S_{n+1} \cdots$ of free abelian groups, which is not exact in general. Hence, we get a *homology group* $\mathrm{H}_n(M) = \ker \partial_{n-1} / \operatorname{im} \partial_n$ for each $n \geq 1$. This abelian group does not depend on the choice of the resolution: it is an *invariant* of the monoid.

4.2 A partial resolution

We choose a presentation (Σ, R) of the monoid M, and if $x \in \Sigma^*$, we write $\widetilde{x}$ for the corresponding element in M. We define $[x]_1 \in \mathbb{Z}M \cdot \Sigma$ for any word x as follows:

- $[1]_1 = 0$, and $[\alpha x]_1 = \alpha + \widetilde{\alpha} \cdot [x]_1$ for each symbol α and for any word x.

Similarly, we define $[r]_2 \in \mathbb{Z}M \cdot R$ for any derivation $x \xrightarrow{r} y$ as follows:

- $[\rho]_2 = \rho$ and $[\rho^{\mathrm{op}}]_2 = -\rho$ for each rule $x \xrightarrow{\rho} y$ in R;
- $[u\rho v]_2 = \widetilde{u} \cdot [\rho]_2$ for any words u, v and for each $x \xrightarrow{\rho} y$ in $R \cup R^{\mathrm{op}}$;
- $[r_1 * r_2 * \cdots * r_n]_2 = [r_1]_2 + [r_2]_2 + \cdots + [r_n]_2$ for any derivation $x_0 \xrightarrow{r_1} x_1 \xrightarrow{r_2} x_2 \cdots x_{n-1} \xrightarrow{r_n} x_n$.

Lemma 4 *The following properties hold:*

- $[xy]_1 = [x]_1 + \widetilde{x} \cdot [y]_1$ *for any words* x, y*;*
- $[urv]_2 = \widetilde{u} \cdot [r]_2$ *for any words* u, v *and for any derivation* $x \xrightarrow{r} y$*;*
- $[r * s]_2 = [r]_2 + [s]_2$ *for any derivations* $x \xrightarrow{r} y \xrightarrow{s} z$*.*

Finally, we fix a set P of pairs of parallel derivations and we build the following partial complex of $\mathbb{Z}M$-modules:

$$0 \leftarrow \mathbb{Z} \xleftarrow{\varepsilon} \mathbb{Z}M \xleftarrow{\delta_0} \mathbb{Z}M \cdot \Sigma \xleftarrow{\delta_1} \mathbb{Z}M \cdot R \xleftarrow{\delta_2} \mathbb{Z}M \cdot P.$$

The *augmentation* ε is defined by $\varepsilon(1) = 1$, and the $\mathbb{Z}M$-linear *boundaries* are defined as follows:

- $\delta_0(\alpha) = \widetilde{\alpha} - 1$ for each symbol $\alpha \in \Sigma$;
- $\delta_1(\rho) = [y]_1 - [x]_1$ for each rule $x \xrightarrow{\rho} y$ in R;
- $\delta_2(r, s) = [s]_2 - [r]_2$ for each pair of parallel derivations $(r, s) \in P$.

Lemma 5 *The following properties hold:*

- $\delta_0[x]_1 = \widetilde{x} - 1$ *for any word* x*;*
- $\delta_1[r]_2 = [y]_1 - [x]_1$ *for any derivation* $x \xrightarrow{r} y$*.*

Clearly, we have $\varepsilon \circ \delta_0 = 0$. By this lemma, we get the other conditions for a complex: $\delta_0 \circ \delta_1 = 0$ and $\delta_1 \circ \delta_2 = 0$.

Lemma 6 $[s]_2 - [r]_2 \in \operatorname{im} \delta_2$ *whenever* $r \approx_P s$*.*

To show this lemma, it suffices to check that the relation $\approx$, defined by $r \approx s$ whenever $r \parallel s$ and $[s]_2 - [r]_2 \in \operatorname{im} \delta_2$, is a 2-congruence on derivations. □

Theorem 3 [CO94, La95] *If* $M \cong \Sigma^*/\leftrightarrow^*_R$ *and* P *generates the full 2-congruence on derivations for* (Σ, R)*, then the complex* $0 \leftarrow \mathbb{Z} \xleftarrow{\varepsilon} \mathbb{Z}M \xleftarrow{\delta_0} \mathbb{Z}M \cdot \Sigma \xleftarrow{\delta_1} \mathbb{Z}M \cdot R \xleftarrow{\delta_2} \mathbb{Z}M \cdot P$ *is a partial resolution of* $\mathbb{Z}$ *by free* $\mathbb{Z}M$*-modules.*

If M has finite derivation type, we get a partial resolution of $\mathbb{Z}$ by free $\mathbb{Z}M$-modules where Σ, R and P are finite. In that case, we say that M satisfies the *homological condition* FP_3.

Corollary 4 *If* M *has finite derivation type, then the homology group* $\mathrm{H}_3(M)$ *is of finite type.*

Indeed, $\ker \partial_2$ is a subgroup of $\mathbb{Z} \cdot P$ where P is finite. Hence $\mathrm{H}_3(M) = \ker \partial_2 / \operatorname{im} \partial_3$ is of finite type. □

The converse does not hold. A counterexample is given in [SOK94], using theorem1. See also [CO96].

Corollary 5 *If* M *has a finite convergent presentation, then the homology group* $\mathrm{H}_3(M)$ *is of finite type.*

This follows from theorem 1 and corollary 4. □

A direct proof of this statement was given in [Sq87]. See also [LP91].

Corollary 6 *If* M *has a convergent presentation without critical peak, then* $\mathrm{H}_n(M) = 0$ *for all* $n \geq 3$*.*

Indeed, if $P = \emptyset$ then $\mathbb{Z}M \cdot P = 0$, so that $0 \leftarrow \mathbb{Z} \xleftarrow{\varepsilon} \mathbb{Z}M \xleftarrow{\delta_0} \mathbb{Z}M \cdot \Sigma \xleftarrow{\delta_1} \mathbb{Z}M \cdot R \leftarrow 0$ is a full resolution. □

4.3 A contracting homotopy

To prove theorem 3, we build a *contracting homotopy*, which consists of four morphisms of abelian groups:

$$\mathbb{Z} \xrightarrow{\eta} \mathbb{Z}M \xrightarrow{\gamma_0} \mathbb{Z}M \cdot \Sigma \xrightarrow{\gamma_1} \mathbb{Z}M \cdot R \xrightarrow{\gamma_2} \mathbb{Z}M \cdot P.$$

Those morphisms, which need not to be $\mathbb{Z}M$-linear, must satisfy the following four conditions:

- $\varepsilon \circ \eta = \mathrm{id}_{\mathbb{Z}}$;
- $\delta_0 \circ \gamma_0 + \eta \circ \varepsilon = \mathrm{id}_{\mathbb{Z}M}$;
- $\delta_1 \circ \gamma_1 + \gamma_0 \circ \delta_0 = \mathrm{id}_{\mathbb{Z}M \cdot \Sigma}$;
- $\delta_2 \circ \gamma_2 + \gamma_1 \circ \delta_1 = \mathrm{id}_{\mathbb{Z}M \cdot R}$.

In that case indeed, ε is surjective by the first condition. Similarly, $\ker \varepsilon = \mathrm{im}\, \delta_0$ follows from the second condition, $\ker \delta_0 = \mathrm{im}\, \delta_1$ from the third one, and $\ker \delta_1 = \mathrm{im}\, \delta_2$ from the last one.

We choose a *canonical form* in each congruence class for $\leftrightarrow^*_R$, and we write $\widehat{x}$ for the canonical form of a word x. Note that $\widehat{x}$ does not need to be reduced, but the following properties hold for any words x, y:

$$\widehat{\widehat{x}} = \widehat{x}, \qquad \widehat{\widehat{x}y} = \widehat{xy} = \widehat{x\widehat{y}}, \qquad \widetilde{x} = \widetilde{y} \text{ if and only if } \widehat{x} = \widehat{y}.$$

We choose a *canonical derivation* $x \xrightarrow{\Lambda(x)} \widehat{x}$ for each word x. Note that $\Lambda(x)$ does not need to be a reduction.

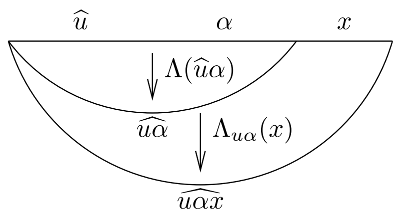
The first morphism is defined by $\eta(1) = 1$, and the next two morphisms are defined as follows:

- $\gamma_0(\widetilde{u}) = [\widehat{u}]_1$ for any $\widetilde{u} \in M$;
- $\gamma_1(\widetilde{u} \cdot \alpha) = -[\Lambda(\widehat{u}\alpha)]_2$ for any $\widetilde{u} \in M$ and $\alpha \in \Sigma$.

The first condition $\varepsilon \circ \eta = \mathrm{id}_{\mathbb{Z}}$ is obviously satisfied, and the next two conditions follow from lemma 5.

Finally, we define the *left derivation* $\widehat{u}x \xrightarrow{\Lambda_u(x)} \widehat{ux}$ by induction on x:

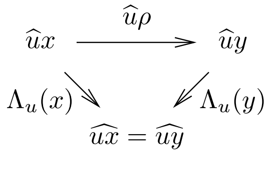
- $\Lambda_u(1)$ is the empty derivation $\widehat{u}$ for any word u;
- $\Lambda_u(\alpha x) = \Lambda(\widehat{u}\alpha)x * \Lambda_{u\alpha}(x)$ for any words u, x and for each symbol α.



Note that in general, $\Lambda_u(x)$ is not the derivation $\Lambda(\widehat{u}x)$. Note also that $\Lambda_u(x)$ depends only on $\widetilde{u}$ and x.

Lemma 7 $\gamma_1(\widetilde{u} \cdot [x]_1) = -[\Lambda_u(x)]_2$ *for any* $\widetilde{u} \in M$ *and for any word* x.

Using this lemma, we get $\gamma_1(\delta_1(\widetilde{u} \cdot \rho)) = [\Lambda_u(x)]_2 - [\Lambda_u(y)]_2$ for any $\widetilde{u} \in M$ and for each rule $x \xrightarrow{\rho} y$, so that $\widetilde{u} \cdot \rho - \gamma_1(\delta_1(\widetilde{u} \cdot \rho)) = [\widehat{u}\rho]_2 + [\Lambda_u(y)]_2 - [\Lambda_u(x)]_2 = [\widehat{u}\rho * \Lambda_u(y)]_2 - [\Lambda_u(x)]_2$, where $\widehat{u}\rho * \Lambda_u(y) \parallel \Lambda_u(x)$.

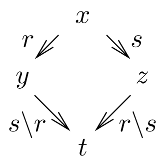


If $\parallel$ coincides with $\approx_P$, we can define $\gamma_2(\widetilde{u} \cdot \rho)$ using lemma 6, in such a way that the last condition is satisfied. Hence, we have proved theorem 3.

4.4 Case of a convergent presentation

If (Σ, R) is a reduced convergent presentation, we can define the resolution using reductions instead of derivations. First, we use the set P of critical peaks as a set of generators for $\ker \delta_1$, and we define δ_2 as follows:

- $\delta_2(p) = [s]_2 + [r\backslash s]_2 - [r]_2 - [s\backslash r]_2$ for each critical peak $p = (r, s)$.



Moreover, for the contracting homotopy, we can choose the reduced form $\widehat{x}$ and the *leftmost reduction* $x \overset{\Lambda(x)}{\to} \widehat{x}$ which consists in reducing the leftmost reducible prefix of x first. In that case, we get $\Lambda_u(x) = \Lambda(\widehat{u}x)$. See [LP91].

Consider for instance the presentation $\mathbb{S}_3 \cong \langle a, b \,|\, a^2 \overset{A}{\to} 1, b^2 \overset{B}{\to} 1, aba \overset{C}{\to} bab \rangle^+$. In that case, we get:

$$\Sigma = \{a, b\}, \qquad R = \{A, B, C\}, \qquad P = \{(Aa, aA), (Bb, bB), (Aba, aC), (Ca, abA), (Cba, abC)\}.$$

The partial resolution $0 \leftarrow \mathbb{Z} \overset{\varepsilon}{\leftarrow} \mathbb{Z}M \overset{\delta_0}{\leftarrow} \mathbb{Z}M \cdot \Sigma \overset{\delta_1}{\leftarrow} \mathbb{Z}M \cdot R \overset{\delta_2}{\leftarrow} \mathbb{Z}M \cdot P$ is defined by the following equations:

$$\begin{cases} \delta_0(a) &=& \widetilde{a} - 1, \\ \delta_0(b) &=& \widetilde{b} - 1, \end{cases} \qquad \begin{cases} \delta_1(A) &=& -a - \widetilde{a} \cdot a, \\ \delta_1(B) &=& -b - \widetilde{b} \cdot b, \\ \delta_1(C) &=& b + \widetilde{b} \cdot a + \widetilde{ba} \cdot b - a - \widetilde{a} \cdot b - \widetilde{ab} \cdot a, \end{cases}$$

$$\begin{cases} \delta_2(Aa, aA) &=& \widetilde{a} \cdot A - A, \\ \delta_2(Bb, bB) &=& \widetilde{b} \cdot B - B, \\ \delta_2(Aba, aC) &=& \widetilde{a} \cdot C + C + \widetilde{ba} \cdot B - A, \\ \delta_2(Ca, abA) &=& \widetilde{ab} \cdot A - C - \widetilde{b} \cdot C - B, \\ \delta_2(Cba, abC) &=& \widetilde{ab} \cdot C + \widetilde{a} \cdot B + A - C - \widetilde{ba} \cdot B - \widetilde{b} \cdot A. \end{cases}$$

The partial complex $\mathbb{Z} \overset{\partial_0}{\leftarrow} \mathbb{Z} \cdot \Sigma \overset{\partial_1}{\leftarrow} \mathbb{Z} \cdot R \overset{\partial_2}{\leftarrow} \mathbb{Z} \cdot P$ is obtained by replacing each $\widetilde{u}$ by 1 in the above equations:

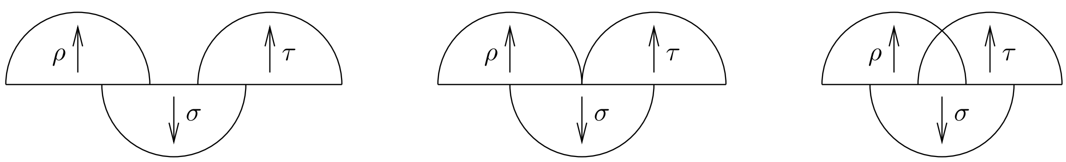
$$\begin{cases} \partial_0(a) &=& 0, \\ \partial_0(b) &=& 0, \end{cases} \qquad \begin{cases} \partial_1(A) &=& -2a, \\ \partial_1(B) &=& -2b, \\ \partial_1(C) &=& b - a, \end{cases} \qquad \begin{cases} \partial_2(Aa, aA) &=& 0, \\ \partial_2(Bb, bB) &=& 0, \\ \partial_2(Aba, aC) &=& 2C + B - A, \\ \partial_2(Ca, abA) &=& A - B - 2C, \\ \partial_2(Cba, abC) &=& 0. \end{cases}$$

Hence, we get the following invariants:

- $\mathrm{H}_1(\mathbb{S}_3) \cong \mathbb{Z}/2\mathbb{Z}$ since $\partial_0 = 0$ and $\operatorname{im} \partial_1$ is the free abelian group generated by $b - a$ and $b + a$;
- $\mathrm{H}_2(\mathbb{S}_3) \cong 0$ since $\ker \partial_1$, as well as $\operatorname{im} \partial_2$, is the free abelian group generated by $2C + B - A$.

We cannot compute $\mathrm{H}_3(\mathbb{S}_3)$ at this stage, since ∂_3 is missing, but we know that it can be generated by 4 elements, since $\ker \partial_2$ is the free abelian group generated by (Aa, aA), (Bb, bB), (Cba, abC) and $(Aba, aC) - (Ca, abA)$.

In fact, another notion is needed in order to extend the partial resolution. A *critical 3-peak* is an overlap of 3 rules:



Theorem 4 [Sq87] *If $M \cong \Sigma^*/\!\leftrightarrow_R^*$ where (Σ, R) is a reduced convergent presentation without critical 3-peak, then the complex $0 \leftarrow \mathbb{Z} \overset{\varepsilon}{\leftarrow} \mathbb{Z}M \overset{\delta_0}{\leftarrow} \mathbb{Z}M \cdot \Sigma \overset{\delta_1}{\leftarrow} \mathbb{Z}M \cdot R \overset{\delta_2}{\leftarrow} \mathbb{Z}M \cdot P \leftarrow 0$ is a resolution of $\mathbb{Z}$ by free $\mathbb{Z}M$-modules.*

Corollary 7 *If M has a reduced convergent presentation without critical 3-peak, then $\mathrm{H}_n(M) = 0$ for all $n \geq 4$.*

Theorem 4 is used in [Sq87] to compute $\mathrm{H}_3(M)$ for some finitely presented monoid M which has a decidable word problem, but no finite convergent presentation. In that case, an infinite presentation is used. See also [LP91, KK97]. However, this theorem is useless for most examples, since in general, there are critical 3-peaks.

4.5 A full resolution

Using a reduced convergent presentation (Σ, R), it is possible to build a full resolution.

A word x is *critical* if x is reducible, but every proper prefix of x is reduced. An n*-chain* is a word $x = u_1 u_2 \cdots u_n$ where u_1 is a symbol α, all words $u_2, u_3, \ldots, u_n$ are reduced, and all words $u_1u_2, u_2u_3, \ldots, u_{n-1}u_n$ are critical. In particular, $u_1, u_2, \ldots, u_n \neq 1$. In that case, it is easy to see that the decomposition $x = u_1 u_2 \cdots u_n$ is unique.

We write $\Sigma^{(n)}$ for the set of all n-chains. Note that $\Sigma^{(1)}$ can be identified with the alphabet Σ, and $\Sigma^{(2)}$ with R. Moreover, $\Sigma^{(3)}$ is a subset of the set of all critical peaks, and $\Sigma^{(4)}$ is a subset of the set of all critical 3-peaks.

Theorem 5 [Ko90] *If $M \cong \Sigma^*/\leftrightarrow^*_R$ where (Σ, R) is a reduced convergent presentation, then there is a resolution of the form* $0 \leftarrow \mathbb{Z} \overset{\varepsilon}{\leftarrow} \mathbb{Z}M \overset{\delta_0}{\leftarrow} \mathbb{Z}M \cdot \Sigma^{(1)} \overset{\delta_1}{\leftarrow} \mathbb{Z}M \cdot \Sigma^{(2)} \cdots \mathbb{Z}M \cdot \Sigma^{(n)} \overset{\delta_n}{\leftarrow} \mathbb{Z}M \cdot \Sigma^{(n+1)} \cdots$

In particular, if (Σ, R) is finite, so is the set $\Sigma^{(n)}$ for each n. Hence, M satisfies the *homological condition* FP_∞.

Corollary 8 *If M has a finite convergent presentation, then the homology group $\mathrm{H}_n(M)$ is of finite type for all n.*

The proof of theorem 5 given in [Ko90] is purely algebraic, and does not use any notion of reduction or derivation. We are looking for a geometric (or homotopical) proof of this result. This will be the point of section 5.

4.6 Bar resolution

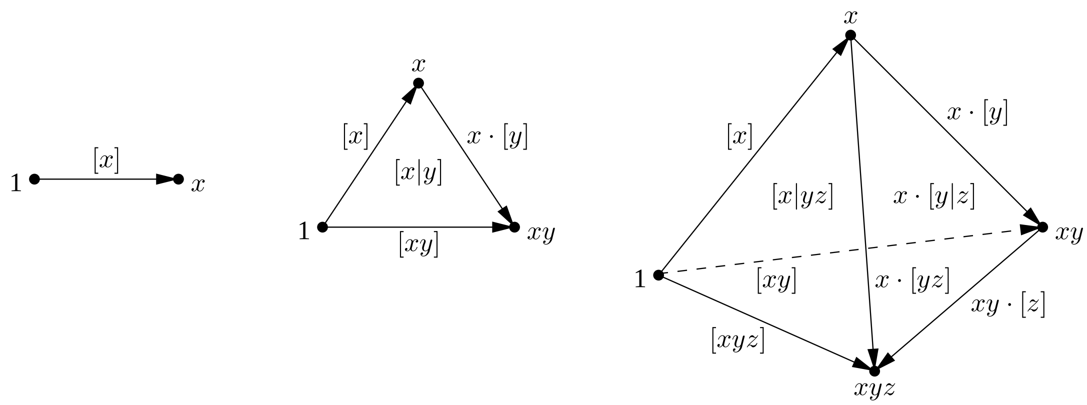
If we apply theorem 5 to the reduced standard presentation of a monoid M, we get the *normalized bar resolution*. In that case, an n-chain is a sequence $x_1, x_2, \ldots, x_n$ in M with $x_1, x_2, \ldots, x_n \neq 1$. We write $[x_1|\cdots|x_n]$ for the corresponding generator in $\mathbb{Z}M \cdot \Sigma^{(n)}$. Then, the normalized bar resolution is given by the following formula:

$$\delta_{n-1}[x_1|\cdots|x_n] = x_1 \cdot [x_2|\cdots|x_n] + \sum_{i=1}^{n-1} (-1)^i [x_1|\cdots|x_{i-1}|x_ix_{i+1}|x_{i+2}|\cdots|x_n] + (-1)^n [x_1|\cdots|x_{n-1}].$$

Here, we use the convention that $[x_1|\cdots|x_n] = 0$ whenever $x_i = 1$ for some i. In particular, we get:

- $\delta_0[x] = x - 1$;
- $\delta_1[x|y] = x \cdot [y] - [xy] + [x]$;
- $\delta_2[x|y|z] = x \cdot [y|z] - [xy|z] + [x|yz] - [x|y]$;
- $\delta_3[x|y|z|t] = x \cdot [y|z|t] - [xy|z|t] + [x|yz|t] - [x|y|zt] + [x|y|z]$.

The geometric interpretation of the normalized bar resolution is a *simplicial set* whose vertices are elements of M:



In this picture, the tetrahedron corresponds to $[x|y|z]$, and the two hidden faces correspond to $[x|y]$ and $[xy|z]$. Those two faces are counted negatively in the boundary $\delta_2[x|y|z]$.

Similarly, the complex $\mathbb{Z} \overset{\partial_0}{\leftarrow} \mathbb{Z} \cdot \Sigma^{(1)} \overset{\partial_1}{\leftarrow} \mathbb{Z} \cdot \Sigma^{(2)} \cdots \mathbb{Z} \cdot \Sigma^{(n)} \overset{\partial_n}{\leftarrow} \mathbb{Z} \cdot \Sigma^{(n+1)} \cdots$ is defined by the following formula:

$$\partial_{n-1}[x_1|\cdots|x_n] = [x_2|\cdots|x_n] + \sum_{i=1}^{n-1} (-1)^i [x_1|\cdots|x_{i-1}|x_ix_{i+1}|x_{i+2}|\cdots|x_n] + (-1)^n [x_1|\cdots|x_{n-1}].$$

This complex corresponds to a simplicial set with only one vertex.

5 Polygraphic approach

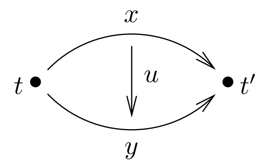
5.1 n-categories

An n-*category* is given by a chain of sets $X_0 \subset X_1 \subset \cdots \subset X_n$ together with:

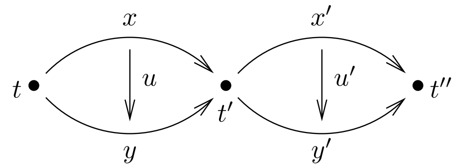
- two maps $X_i \overset{\sigma_i}{\leftarrow} X_n$ (i-*dimensional source*) and $X_i \overset{\tau_i}{\leftarrow} X_n$ (i-*dimensional target*) defined for each $i < n$;
- a product $x *_i y$ defined for each $i < n$ whenever $x, y \in X_n$ and $\tau_i(x) = \sigma_i(y)$.

We write $x \xrightarrow{u}_i y$ whenever $\sigma_i(u) = x$ and $\tau_i(u) = y$. We write $x \parallel_i y$ whenever $\sigma_i(x) = \sigma_i(y)$ and $\tau_i(x) = \tau_i(y)$. The following properties must hold:

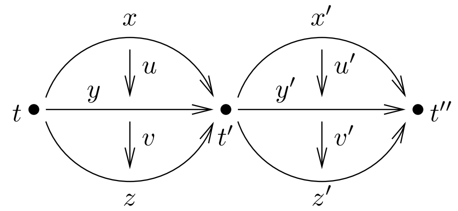
- $x \xrightarrow{x}_i x$ whenever $i < n$ and $x \in X_i$;
- $t \xrightarrow{x}_i t'$ and $t \xrightarrow{y}_i t'$ (so that $x \parallel_i y$) whenever $i < j$, $t \xrightarrow{u}_i t'$ and $x \xrightarrow{u}_j y$;



- $x \xrightarrow{u *_i v}_i z$ and $u *_i v \in X_j$ whenever $i < j$, $x \xrightarrow{u}_i y \xrightarrow{v}_i z$ and $u, v \in X_j$;
- $x *_i x' \xrightarrow{u *_i u'}_j y *_i y'$ whenever $i < j$, $t \xrightarrow{u}_i t' \xrightarrow{u'}_i t''$, $x \xrightarrow{u}_j y$ and $x' \xrightarrow{u'}_j y'$;



- $x *_i u = u = u *_i y$ whenever $x \xrightarrow{u}_i y$;
- $(u *_i v) *_i w = u *_i (v *_i w)$ whenever $x \xrightarrow{u}_i y \xrightarrow{v}_i z \xrightarrow{w}_i t$;
- $(u *_j v) *_i (u' *_j v') = (u *_i u') *_j (v *_i v')$ whenever $i < j$, $t \xrightarrow{u}_i t' \xrightarrow{u'}_i t''$, $x \xrightarrow{u}_j y \xrightarrow{v}_j z$ and $x' \xrightarrow{u'}_j y' \xrightarrow{v'}_j z'$.



The last property corresponds to a higher dimensional version of the exchange property.

An n-*monoid* is an n-category such that X_0 is the singleton 1. In that case, the product $x *_0 y$ can be written xy. For instance, a 1-monoid is a monoid, and a 2-monoid is a strict monoidal category. Note also that a monoid M can be seen as an n-monoid $1 \subset M \subset M \subset \cdots \subset M$, and even as an ∞-*monoid* $1 \subset M \subset M \subset \cdots \subset M \subset \cdots$

5.2 n-polygraphs

A 1-*polygraph* is a *graph*, which is given by two sets Σ_0 and Σ_1 together with two maps $\Sigma_0 \overset{\sigma_1}{\leftarrow} \Sigma_1$ and $\Sigma_0 \overset{\tau_1}{\leftarrow} \Sigma_1$. Such a graph generates a *free category* (or *category of paths*) $\Sigma_0 \subset \Sigma_1^*$. The set Σ_0 is also written Σ_0^*.

Similarly, an n+1-*polygraph* is given inductively by an n-polygraph $\Sigma_0^* \subset \Sigma_1^* \subset \cdots \subset \Sigma_{n-1}^* \subset \Sigma_n$ and a set Σ_{n+1} together with two maps $\Sigma_n^* \overset{\sigma_n}{\leftarrow} \Sigma_{n+1}$ and $\Sigma_n^* \overset{\tau_n}{\leftarrow} \Sigma_{n+1}$ such that $\sigma_n(\alpha) \parallel_{n-1} \tau_n(\alpha)$ whenever $\alpha \in \Sigma_{n+1}$. Such an n+1-polygraph generates a *free* n+1-*category* $\Sigma_0^* \subset \Sigma_1^* \subset \cdots \subset \Sigma_n^* \subset \Sigma_{n+1}^*$. See [Bu93].

An n-polygraph such that $\Sigma_0 = \Sigma_0^* = 1$ is called a *monoidal* n-*polygraph*. For instance, a monoidal 1-polygraph is given by an alphabet Σ. Similarly, a monoidal 2-polygraph is given by a presentation (Σ, R), and a monoidal 3-polygraph is given by a set P of pairs of parallel reductions for such a presentation.

5.3 Polygraphic resolutions

A *(monoidal) polygraphic resolution* of a monoid M is a monoidal ∞-polygraph $1 \subset \Sigma_1^* \subset \Sigma_2^* \subset \cdots \subset \Sigma_n^* \subset \cdots$ together with a surjective morphism $f_1 : \Sigma_1^* \to M$ satisfying the following extra properties:

- for any $x, y \in \Sigma_1^*$, we have $f_1(x) = f_1(y)$ if and only if there is some $x \xrightarrow{u}_1 y$ in Σ_2^*;
- for each $n > 1$ and for any $x, y \in \Sigma_n^*$, we have $x \parallel_{n-1} y$ if and only if there is some $x \xrightarrow{u}_n y$ in Σ_{n+1}^*.

In particular, if R is the relation on words defined by $x \ R \ y$ whenever there is some $x \xrightarrow{\rho}_1 y$ in Σ_2, and if P the relation on reductions defined by $r \ P \ s$ whenever there is some $r \xrightarrow{\omega}_2 s$ in Σ_3, we have the following properties:

- $M \cong \Sigma_1^*/\leftrightarrow_R^*$ and $\leftrightarrow_R^*$ coincides with $\to_R^*$;
- P is a set of pairs of parallel reductions which generates the full 2-congruence on reductions.

In fact, a polygraphic resolution can also be seen as a morphism of ∞-category $f : \Sigma^* \to M$. The extra properties expresses that f is a *trivial fibration*, which is a noncommutative version of the exactness condition for a complex.

Theorem 6 [Me03] *Any monoid has a polygraphic resolution, which is unique up to homotopical equivalence.*

See [Me03] or [LM] for more details on the notions of *homotopy* and of *homotopical equivalence*.

Given such a polygraphic resolution of M, we define the following complex of abelian groups (*abelianization*):

$$\mathbb{Z} \xleftarrow{\partial_0} \mathbb{Z}\cdot\Sigma_1 \xleftarrow{\partial_1} \mathbb{Z}\cdot\Sigma_2 \xleftarrow{\partial_2} \mathbb{Z}\cdot\Sigma_3 \cdots \mathbb{Z}\cdot\Sigma_n \xleftarrow{\partial_n} \mathbb{Z}\cdot\Sigma_{n+1} \cdots$$

Here, $\partial_0 = 0$ and $\partial_n(\alpha) = [y]_n - [x]_n$ for each $x \xrightarrow{\alpha}_n y$ in Σ_{n+1}, where $[u]_n \in \mathbb{Z}\cdot\Sigma_n$ is defined for each $n > 0$ and for any $u \in \Sigma_n^*$ in such a way that the following properties hold:

- $[\alpha]_n = \alpha$ for each symbol $\alpha \in \Sigma_n$;
- $[u]_n = 0$ for any $u \in \Sigma_i^*$ with $i < n$. In particular $[1]_n = 0$;
- $[u *_i v]_n = [u]_n + [v]_n$ for any $x \xrightarrow{u}_i y \xrightarrow{v}_i z$ in Σ_n^* with $i < n$.

Theorem 7 [LM] *If* $1 \subset \Sigma_1^* \subset \Sigma_2^* \subset \cdots \subset \Sigma_n^* \subset \cdots$ *is a polygraphic resolution of the monoid* M*, then the homology of its abelianization coincides with the homology of* M*.*

This is proved by constructing an ∞-polygraph on which the monoid M acts freely.

Corollary 9 *If* M *has a partial polygraphic resolution* $1 \subset \Sigma_1^* \subset \Sigma_2^* \subset \cdots \subset \Sigma_n^*$ *such that* Σ_n *is finite, then the homology group* $\mathrm{H}_n(M)$ *is of finite type.*

5.4 Case of a convergent presentation

The results of the previous sections suggest the following generalization:

Conjecture 1 *If a monoid* M *has a reduced convergent presentation* (Σ, R)*, then* M *has a polygraphic resolution* $1 \subset \Sigma_1^* \subset \Sigma_2^* \subset \cdots \subset \Sigma_n^* \subset \cdots$ *where each* Σ_n *is defined in terms of generalized critical peaks. In particular:*

$$\Sigma_1 = \Sigma, \qquad \Sigma_2 = R \cup R^{\mathrm{op}}, \qquad \Sigma_3 = Q \cup Q^{\mathrm{op}} \text{ where } Q \text{ is the relation defined in 3.2.}$$

Moreover, if the presentation (Σ, R) *is finite, so is* Σ_n *for each* n*.*

This would give an alternative proof for corollary 8, but it seems to be more difficult than theorem 5.

Indeed, this construction would apply to the reduced standard presentation, and this would give a polygraphic version of the normalized bar resolution. In that case, Σ_n would contain (among others) the n-chains $[x_1|\cdots|x_n]$. Here are some conjectural formulas for such a resolution, in the nondegenerate case where $xy, yz, zt \neq 1$:

- $[x][y] \xrightarrow{[x|y]}_1 [xy]$, so that $\partial_1[x|y] = [xy] - [x] - [y]$;
- $[x|y][z] *_1 [xy|z] \xrightarrow{[x|y|z]}_2 [x][y|z] *_1 [x|yz]$, so that $\partial_2[x|y|z] = [y|z] + [x|yz] - [x|y] - [xy|z]$;
- $([x|y|z][t] *_1 [xyz|t]) *_2 ([x][y|z][t] *_1 [x|yz|t]) *_2 ([x][y|z|t] *_1 [x|yzt]) \xrightarrow{[x|y|z|t]}_3 ([x|y][z][t] *_1 [xy|z|t]) *_2 ([x][y][z|t] *_1 [x|y|zt])$, so that $\partial_3[x|y|z|t] = [xy|z|t] + [x|y|zt] - [x|y|z] - [x|yz|t] - [y|z|t]$.

Note that the formulas for ∂_n are the same as for the normalized bar reduction, except for a global change of sign. Note also that the formulas defining σ_3 and τ_3 are significantly more complicated than the formula defining δ_3, and it gets worst in higher dimension, due to the difficulty of describing simplicial sets as polygraphs. See [St87, Bu00].

References

[Br82] K.S. Brown. *Cohomology of groups*. Springer-Verlag, 1982.

[Bu93] A. Burroni. Higher dimensional word problems with applications to equational logic. *Theoretical Computer Science* 115, 43–62, 1993.

[Bu00] A. Burroni. *A new calculation of the Orientals of Street*. Conference given in Oxford in April 2000. Available on `http://www.math.jussieu.fr/~burroni/`

[CO94] R. Cremanns, F. Otto. Finite derivation type implies the homological finiteness condition FP_3. *Journal of Symbolic Computation* 18, 91–12, 1994.

[CO96] R. Cremanns, F. Otto. For groups the property of finite derivation type is equivalent to the homological finiteness condition FP_3. *Journal of Symbolic Computation* 22, 155–177, 1996.

[DL03] P. Dehornoy, Y. Lafont. Homology of gaussian groups. *Annales de l'Institut Fourier* 53 (2), 489–540, 2003.

[Gu06] Y. Guiraud. Termination orders for 3-dimensional rewriting. *Journal of Pure and Applied Algebra* 207 (2), 341–37, 2006.

[KK97] M. Katsura, Y. Kobayashi. Constructing Finitely Presented Monoids Which Have No Finite Complete Presentation. *Semigroup Forum* 54, 292–302, 1997.

[KN85a] D. Kapur, P. Narendran. The Knuth-Bendix completion procedure and Thue systems. *SIAM journal on computing* 14 (4), 1052–1072, 1985.

[KN85b] D. Kapur, P. Narendran. A finite Thue system with decidable word problem and without equivalent finite canonical system. *Theoretical Computer Science* 35, 337–344, 1985.

[Ko90] Y. Kobayashi. Complete rewriting systems and homology of monoid algebras. *Journal of Pure and Applied Algebra* 65 (3), 263–275, 1990.

[La95] Y. Lafont. A new finiteness condition for monoids presented by complete rewriting systems (after Craig Squier). *Journal of Pure and Applied Algebra* 98 (3), 229–244, 1995.

[La03] Y. Lafont. Towards an Algebraic Theory of Boolean Circuits. *Journal of Pure and Applied Algebra*, 184 (2-3), 257–310, 2003.

[LM] Y. Lafont, F. Métayer. Polygraphic resolutions and homology of monoids. Submitted.

[LP91] Y. Lafont, A. Prouté. Church-Rosser property and homology of monoids. *Mathematical Structures in Computer Science* 1 (3), 297–326, 1991.

[Ma63] S. Mac Lane. *Homology*. Springer-Verlag, 1963.

[Me03] F. Métayer. Resolutions by polygraphs. *Theory and Applications of Categories* 1 (7), 148–184, 2003.

[Po91] J. Power. An n-categorical pasting theorem. Proceedings of *Category Theory, Como 1990*, Springer Lecture Notes in Mathematics 1488, 326–358, 1991.

[SOK94] C. Squier, F. Otto, Y. Kobayashi. A finiteness condition for rewriting systems. *Theoretical Computer Science* 131, 271–294, 1994.

[Sp66] C. C. Spanier. *Algebraic Topology*. McGraw-Hill, 1966.

[Sq87] C. Squier. Word problems and a homological finiteness condition for monoids. *Journal of Pure and Applied Algebra* 49, 201–217, 1987.

[St87] R. Street. The algebra of oriented simplexes. *Journal of Pure and Applied Algebra* 49, 283–335, 1987.