

Algèbre et géométrie de la réécriture

Yves Lafont

Ecole Jeunes Chercheurs en Informatique Mathématique

CIRM 2008

1

Leçon 1. Réécriture de mots

- Présentations de monoïdes*
- Présentation standard*
- Réductions et dérivations*
- Terminaison et confluence*
- Complétion de Knuth-Bendix*
- Problèmes de décision*

2

Présentations de monoïdes

générateurs	relations	monoïde
a	$a^2 = 1$	\mathbb{Z}_2 (<i>entiers modulo 2</i>)
a	$a^2 = a$	\mathbb{N}_2 (<i>idempotent libre</i>)
a, a'	$aa' = 1, a'a = 1$	$\mathbf{F}_1 = \mathbb{Z}$ (<i>groupe libre</i>)
a, b	$ab = ba$	$\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$
a, a', b, b'	$aa' = 1, a'a = 1,$ $bb' = 1, b'b = 1$	$\mathbf{F}_2 = \mathbb{Z} * \mathbb{Z}$ (<i>groupe libre</i>)
a, b	$a^2 = 1, b^2 = 1,$ $aba = bab$	\mathbf{S}_3 (<i>groupe symétrique</i>)
a, b	$aba = bab$	\mathbf{B}_3^+ (<i>tresses positives</i>)

Exercice : Donner une présentation pour \mathbb{Z}^2 et pour \mathbf{B}_3 .

3

Présentation standard

Remarque : Tout monoïde (fini) a une présentation (finie).

Soit M un monoïde quelconque.

présentation	générateurs	relations
<i>standard</i>	$a_x (x \in M)$	$a_x a_y = a_{xy},$ $a_1 = 1$
<i>standard réduite</i>	$a_x (x \in M, x \neq 1)$	$a_x a_y = a_{xy} (xy \neq 1),$ $a_x a_y = 1 (xy = 1)$

Exercice : Expliciter la présentation standard et la présentation standard réduite de \mathbb{Z}_2 .

4

Réductions et dérivations

notion	notation	définition
<i>alphabet</i>	Σ	ensemble de symboles
<i>mot</i>	x	suite de symboles $x \in \Sigma^*$
<i>règle</i>	$\rho : x \rightarrow y$	couple $\rho = (x,y) \in \Sigma^* \times \Sigma^*$
<i>réduction élémentaire</i>	$upv : uxv \rightarrow_R uyv$	avec $\rho : x \rightarrow y$ dans $R \subset \Sigma^* \times \Sigma^*$
<i>réduction</i>	$x \rightarrow^*_R y$	chaîne $x \rightarrow_R \dots \rightarrow_R y$
<i>dérivation élémentaire</i>	$x \leftrightarrow_R y$	$x \rightarrow_R y$ ou $y \rightarrow_R x$
<i>dérivation</i>	$x \leftrightarrow^*_R y$	chaîne $x \leftrightarrow_R \dots \leftrightarrow_R y$

Définition : Une *présentation* de M est la donnée d'un alphabet Σ et de $R \subset \Sigma^* \times \Sigma^*$ tels que $M \simeq \Sigma^*/\leftrightarrow^*_R$.

5

Terminaison

Définition : Un *ordre de terminaison* sur Σ^* est un bon ordre compatible avec le produit.

Théorème : Pour une présentation (Σ, R) , les conditions suivantes sont équivalentes :

Il n'existe pas de réduction infinie :
 $x_0 \rightarrow_R x_1 \rightarrow_R \dots \rightarrow_R x_n \rightarrow_R x_{n+1} \rightarrow_R \dots$

Il existe un ordre de terminaison sur Σ^* tel que
 $x > y$ pour chaque règle $\rho : x \rightarrow y$ dans R .

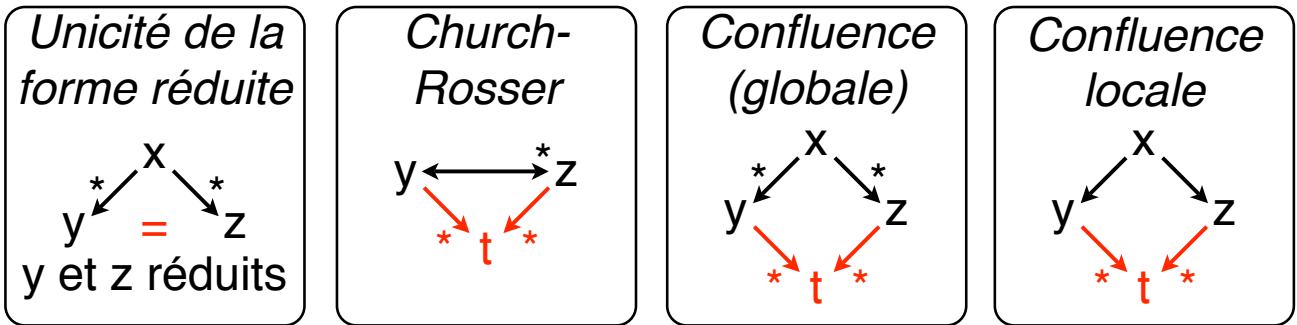
(Σ, R) satisfait le principe de *récurrence noetherienne* :
 $(\forall x (\forall y x \rightarrow_R y \Rightarrow P(y)) \Rightarrow P(x)) \Rightarrow \forall x P(x)$

On dit alors que la présentation (Σ, R) est *noetherienne*.

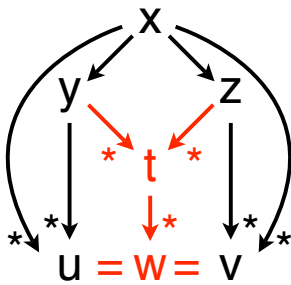
6

Confluence

Théorème : Pour une présentation noetherienne, les quatre conditions suivantes sont équivalentes :



Démonstration : $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4$ (évident)
 $4 \Rightarrow 1$ (par récurrence noetherienne)

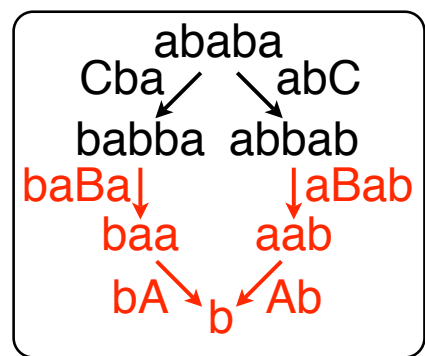
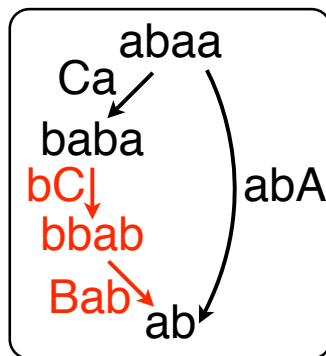
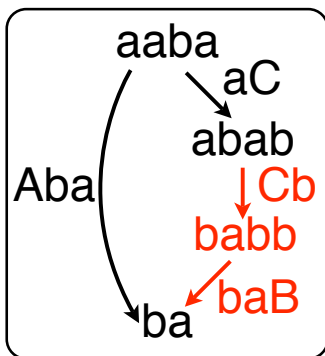
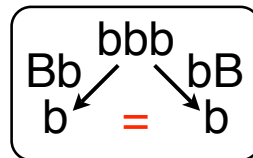
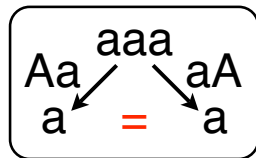


Exercice : Les règles suivantes vérifient la confluence locale, mais pas la confluence :
 $a \rightarrow b, b \rightarrow a, a \rightarrow a', b \rightarrow b'$.

Confluence des pics critiques

Théorème : Pour vérifier la confluence locale, il suffit de tester la confluence des *pics critiques*.

Exemple : $aa \xrightarrow{A} 1, bb \xrightarrow{B} 1, aba \xrightarrow{C} bab$



Exercice : La présentation standard est confluente.

Présentations convergentes

présentation	propriétés
<i>convergente</i>	terminaison + confluence
<i>réduite</i>	générateurs réduits + membres gauches minimaux + membres droits réduits
<i>orthogonale</i>	pas de pics critiques

Remarque : Toute présentation convergente (finie) est équivalente à une présentation convergente réduite (finie).

Exercice : Toute présentation orthogonale est confluente.

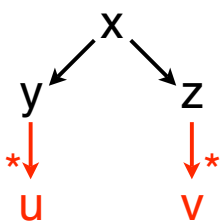
Exercice : Les groupes (non triviaux) n'ont pas de présentation convergente orthogonale.

9

Complétion de Knuth-Bendix

Remarque : Il existe un ordre de terminaison total sur Σ^* .

Algorithme : Réduire les 2 côtés de chaque pic critique :



- si $u = v$, le pic est confluent
- si $u > v$, ajouter la règle $u \rightarrow v$
- si $u < v$, ajouter la règle $v \rightarrow u$
- éliminer les règles superflues

Exercice : Appliquer cet algorithme aux règles suivantes :
 $aa' \rightarrow 1$, $a'a \rightarrow 1$, $bb' \rightarrow 1$, $b'b \rightarrow 1$, $ba \rightarrow ab$

Exercice : Appliquer cet algorithme à la règle $bab \rightarrow aba$.
 Idem en ajoutant le *générateur* c avec la règle $ab \rightarrow c$.

10

Problèmes de décision

Soit (Σ, R) un présentation finie.

problème	données	question
équivalence	$x, y \in \Sigma^*$	$x \leftrightarrow_R^* y ?$
unité (par dérivation)	$x \in \Sigma^*$	$x \leftrightarrow_R^* 1 ?$
unité (par réduction)	$x \in \Sigma^*$	$x \rightarrow_R^* 1 ?$

Remarque : Dans un groupe, $x = y \Leftrightarrow xy^{-1} = 1$.

Remarque : Dans le cas d'une présentation convergente, ces problèmes sont décidables.

Exercice : Il existe une présentation orthogonale telle que ces problèmes soient indécidables. [Coder le *problème de l'arrêt*.]

Théorème (Novikov-Boone) : Il existe un groupe tel que le problème de l'unité (par dérivation) soit indécidable.

11

Leçon 2. Homologie des monoïdes

- Théorie des groupes abéliens*
- Complexes de chaînes*
- Homologie des complexes*
- Homologie des monoïdes*
- Résolutions libres*
- Homologie des réductions*

12

Théorie des groupes abéliens

1. Un sous-groupe de \mathbb{Z} est de la forme :

$$0 \text{ ou } k\mathbb{Z} (\simeq \mathbb{Z}) \text{ avec } k > 0.$$

2. Un groupe abélien à 1 générateur est de la forme :

$$\mathbb{Z} \text{ ou } \mathbb{Z}_k = \mathbb{Z}/k\mathbb{Z} \text{ avec } k > 0.$$

3. Un sous-groupe de $\mathbb{Z}^n = \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$ est isomorphe à :

$$\mathbb{Z}^p \text{ avec } p \leq n.$$

4. Un groupe abélien à n générateurs est de la forme :

$$\mathbb{Z}^p \oplus \mathbb{Z}_{k_1} \oplus \dots \oplus \mathbb{Z}_{k_q} \text{ avec } p + q \leq n.$$

→ classification des groupes abéliens (de type fini)

Exercice : Comparer $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ avec \mathbb{Z}_4 , et $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ avec \mathbb{Z}_6 .

13

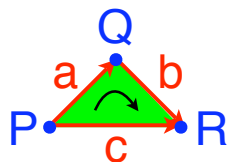
Complexes de chaînes

Définition : Un *complexe de chaînes* est une suite infinie

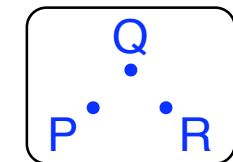
$$C : C_0 \xleftarrow{\partial_0} C_1 \xleftarrow{\partial_1} C_2 \leftarrow \dots \leftarrow C_n \xleftarrow{\partial_n} C_{n+1} \xleftarrow{\partial_{n+1}} C_{n+2} \leftarrow \dots$$

de groupes abéliens, telle que $\partial_n \partial_{n+1} = 0$ pour tout n .

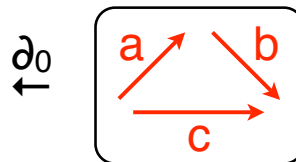
Exemple : Le *triangle (plein)* Δ_2



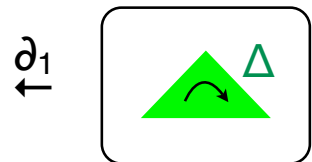
$$\partial_0 a = Q - P$$



$$\partial_0 b = R - Q$$



$$\partial_0 c = R - P$$



$$\partial_1 \Delta = a + b - c$$

$$\Delta_2 : \mathbb{Z}^3 \xleftarrow{\partial_0} \mathbb{Z}^3 \xleftarrow{\partial_1} \mathbb{Z} \leftarrow 0 \leftarrow 0 \leftarrow \dots$$

$$\partial_0 \partial_1 = 0$$

Exercice : Décrire les complexes de chaînes associés au *triangle vide* $\partial\Delta_2$, au *carré* \square_2 , et au *tétraèdre* Δ_3 .

14

Morphismes et homotopies

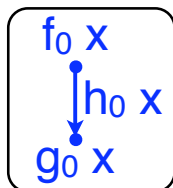
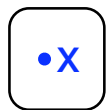
Définition : *morphisme de complexes* $f : C \rightarrow D$

$$\begin{array}{ccccccc}
 C_0 & \xleftarrow{\partial_0} & C_1 & \xleftarrow{\partial_1} & C_2 & \xleftarrow{\dots} & \dots & \xleftarrow{\partial_n} & C_{n+1} & \xleftarrow{\partial_{n+1}} & C_{n+2} & \xleftarrow{\dots} \\
 \downarrow f_0 & & \downarrow f_1 & & \downarrow f_2 & & & \downarrow f_n & \downarrow f_{n+1} & & \downarrow f_{n+2} & & & f_n \partial_n = \partial_n f_{n+1} \\
 D_0 & \xleftarrow{\partial_0} & D_1 & \xleftarrow{\partial_1} & D_2 & \xleftarrow{\dots} & \dots & \xleftarrow{\partial_n} & D_{n+1} & \xleftarrow{\partial_{n+1}} & D_{n+2} & \xleftarrow{\dots}
 \end{array}$$

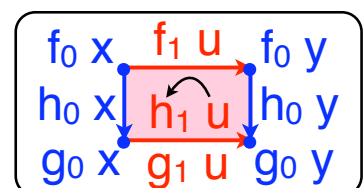
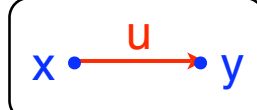
Définition : *homotopie* entre deux morphismes $f, g : C \rightarrow D$

$$\begin{array}{ccccccc}
 C_0 & \xleftarrow{\partial_0} & C_1 & \xleftarrow{\partial_1} & C_2 & \xleftarrow{\dots} & \dots & \xleftarrow{\partial_n} & C_{n+1} & \xleftarrow{\partial_{n+1}} & C_{n+2} & \xleftarrow{\dots} \\
 \Downarrow & \searrow h_0 & \Downarrow & \searrow h_1 & \Downarrow & & & \Downarrow & \searrow h_n & \Downarrow & \searrow h_{n+1} & \Downarrow \\
 D_0 & \xleftarrow{\partial_0} & D_1 & \xleftarrow{\partial_1} & D_2 & \xleftarrow{\dots} & \dots & \xleftarrow{\partial_n} & D_{n+1} & \xleftarrow{\partial_{n+1}} & D_{n+2} & \xleftarrow{\dots}
 \end{array}$$

$$\partial_0 h_0 = g_0 - f_0$$



$$h_0 \partial_0 + \partial_1 h_1 = g_1 - f_1$$



plus généralement : $h_n \partial_n + \partial_{n+1} h_{n+1} = g_{n+1} - f_{n+1}$

15

Homologie des complexes

Soit $C : C_0 \xleftarrow{\partial_0} C_1 \xleftarrow{\partial_1} C_2 \xleftarrow{\dots} C_n \xleftarrow{\partial_n} C_{n+1} \xleftarrow{\partial_{n+1}} C_{n+2} \xleftarrow{\dots}$

Remarque : $\partial_n \partial_{n+1} = 0 \Leftrightarrow \text{im } \partial_{n+1} \subset \text{ker } \partial_n$



→ tout bord est un cycle

Définition : C est *exact* si $\text{im } \partial_{n+1} = \text{ker } \partial_n$ pour tout n .

→ tout cycle est un bord

Exemples : Le complexe Δ_2 est exact, mais pas $\partial \Delta_2$.

Définition : Les *groupes d'homologie* de C sont $H_0(C) = C_0 / \text{im } \partial_0$ et $H_{n+1}(C) = \text{ker } \partial_n / \text{im } \partial_{n+1}$.

16

Homologie des complexes

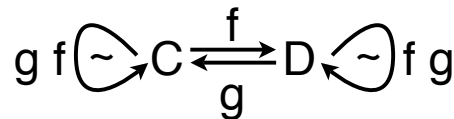
L'homologie des complexes est *fonctorielle* :

- $f : C \rightarrow D$ donne $H_n(f) : H_n(C) \rightarrow H_n(D)$;
- $H_n(g \circ f) = H_n(g) \circ H_n(f)$ et $H_n(\text{id}) = \text{id}$.

Exercice : Si $f, g : C \rightarrow D$ sont homotopes, alors $H_n(f) = H_n(g)$.

Définition : C et D sont *homotopiquement équivalents* s'il existe des morphismes $f : C \rightarrow D$ et $g : D \rightarrow C$ tels que :

- $g \circ f$ et id_C sont homotopes;
- $f \circ g$ et id_D sont homotopes.



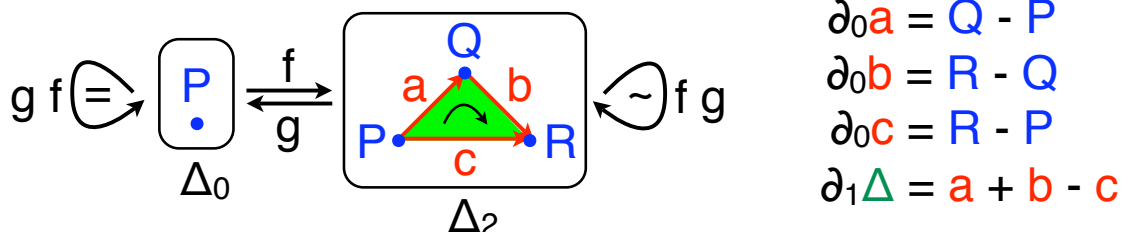
Remarque : Dans ce cas, C et D ont la même homologie.

Exercice : $\Delta_2, \square_2, \Delta_3$ sont homotopiquement équivalents au point $\Delta_0 : \mathbb{Z} \leftarrow 0 \leftarrow 0 \leftarrow \dots$, mais pas à $\partial\Delta_2$.

17

Corrigé de l'exercice

Le triangle Δ_2 est homotopiquement équivalent au point Δ_0 :



$$\begin{aligned} \partial_0 a &= Q - P \\ \partial_0 b &= R - Q \\ \partial_0 c &= R - P \\ \partial_1 \Delta &= a + b - c \end{aligned}$$

$$f_0 P = P \quad g_0 P = g_0 Q = g_0 R = P \quad g_1 a = g_1 b = g_1 c = 0 \quad g_2 \Delta = 0$$

$$\begin{array}{ccc} \mathbb{Z}^3 & \xleftarrow{\partial_0} & \mathbb{Z}^3 & \xleftarrow{\partial_1} & \mathbb{Z} & \leftarrow 0 \\ \Downarrow & \searrow h_0 & \Downarrow & \searrow h_1 & \Downarrow & \\ \mathbb{Z}^3 & \xleftarrow{\partial_0} & \mathbb{Z}^3 & \xleftarrow{\partial_1} & \mathbb{Z} & \leftarrow 0 \end{array} \quad \begin{aligned} \partial_0 h_0 &= \text{id}_0 - f_0 g_0 \\ h_0 \partial_0 + \partial_1 h_1 &= \text{id}_1 - f_1 g_1 = \text{id}_1 \\ h_1 \partial_1 + \partial_2 h_2 &= \text{id}_2 - f_2 g_2 = \text{id}_2 \end{aligned}$$

$$h_0 P = 0 \quad h_0 Q = a \quad h_0 R = c \quad h_1 a = h_1 c = 0 \quad h_1 b = \Delta \quad h_2 \Delta = 0$$

Le triangle vide n'est pas homotopiquement équivalent à Δ_0 :

$$H_1(\partial\Delta_2) = \mathbb{Z} \quad H_1(\Delta_0) = 0$$

18

Homologie des monoïdes

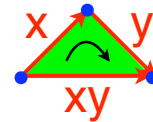
Définition : *Complexe canonique* C associé à un monoïde M :

- C_n est le groupe abélien libre engendré par l'ensemble M^n ;
- les générateurs de C_n sont notés $[x_1 \mid \cdots \mid x_n]$;
- les $\partial_n : C_{n+1} \rightarrow C_n$ sont donnés par les formules suivantes :

$$\partial_0[x] = [] - [] (= 0)$$



$$\partial_1[x \mid y] = [y] - [xy] + [x]$$



$$\partial_2[x \mid y \mid z] = [y \mid z] - [xy \mid z] + [x \mid yz] - [x \mid y]$$

$$\partial_3[x \mid y \mid z \mid t] = [y \mid z \mid t] - [xy \mid z \mid t] + [x \mid yz \mid t] - [x \mid y \mid zt] + [x \mid y \mid z]$$

⋮

Exercice : Ecrire la formule générale pour $\partial_n[x_1 \mid \cdots \mid x_{n+1}]$.

Définition : L'*homologie* de M est celle du complexe C .

19

Homologie des monoïdes

Définition : *Complexe canonique réduit* \hat{C} associé à M :

- \hat{C}_n est le groupe abélien libre engendré par $(M \setminus \{1\})^n$;
- les ∂_n sont définis par les mêmes formules, en posant :

$$[x_1 \mid \cdots \mid x_{i-1} \mid 1 \mid x_{i+1} \mid \cdots \mid x_n] = 0.$$

Exercice : Calculer les complexes C et \hat{C} pour \mathbb{Z}_2 et montrer qu'ils définissent la même homologie.

En fait, C et \hat{C} ont toujours la même homologie.

Exercice : Construire une homotopie entre $\text{id} : C \rightarrow C$ et le morphisme $p : C \rightarrow C$ défini par $p[x_1 \mid \cdots \mid x_n] = [x_1 \mid \cdots \mid x_n]$ si $x_1, \dots, x_n \neq 1$, 0 sinon.

Peut-on calculer l'homologie de M avec d'autres complexes ?

20

ZM-modules

Définition : $\mathbb{Z}M$ est l'*anneau de M*, c'est-à-dire le groupe abélien libre engendré par l'ensemble M , muni du produit

$$(\sum_{x \in M} p_x x)(\sum_{y \in M} q_y y) = \sum_{x, y \in M} p_x q_y xy.$$

Remarque : Un $\mathbb{Z}M$ -module U est donné par une *action additive* de M sur un groupe abélien U :

$$xy \cdot u = x \cdot (y \cdot u), \quad 1 \cdot u = u, \quad x \cdot (u + v) = x \cdot u + x \cdot v.$$

Un *morphisme de $\mathbb{Z}M$ -module* $f : U \rightarrow V$ est alors un morphisme de groupes compatible avec cette action :

$$f(x \cdot u) = x \cdot f u.$$

Définition : Le *$\mathbb{Z}M$ -module libre* $\mathbb{Z}M \cdot S$ engendré par l'ensemble S est le groupe abélien libre engendré par l'ensemble $M \cdot S = \{x \cdot s ; x \in M, s \in S\}$, muni de l'action

$$x \cdot (\sum_{y \in M, s \in S} p_y y \cdot s) = \sum_{y \in M, s \in S} p_y xy \cdot s.$$

21

Résolutions libres

Définition : Une *résolution libre* est un complexe exact

$$\mathbb{Z} \xleftarrow{\varepsilon} C_0 \xleftarrow{\delta_0} C_1 \xleftarrow{\delta_1} C_2 \xleftarrow{\dots} C_n \xleftarrow{\delta_n} C_{n+1} \xleftarrow{\delta_{n+1}} C_{n+2} \xleftarrow{\dots}$$

qui définit un *complexe augmenté* de $\mathbb{Z}M$ -modules libres.

En *trivialisant l'action* de M , on obtient un complexe C^\sim .

Théorème : L'homologie du complexe C^\sim ne dépend pas du choix de la résolution libre : C'est l'homologie de M .

Exemple : Le complexe canonique s'obtient en trivialisant la *bar-résolution*, qui est définie de la façon suivante :

$$\delta_0[x] = x \cdot [] - []$$

$$\delta_1[x | y] = x \cdot [y] - [xy] + [x]$$

$$\delta_2[x | y | z] = x \cdot [y | z] - [xy | z] + [x | yz] - [x | y]$$

⋮

22

Homologie des réductions

Toute présentation convergente (Σ, R) définit un complexe :

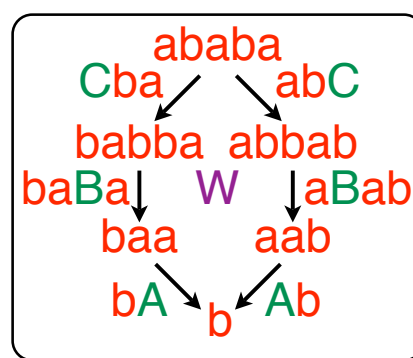
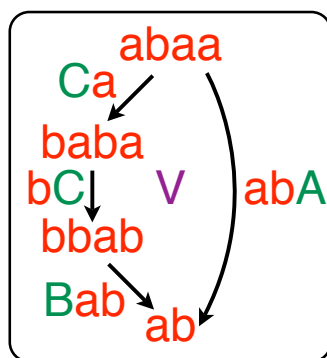
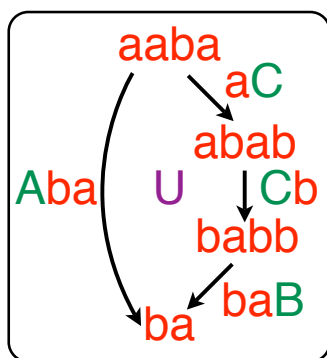
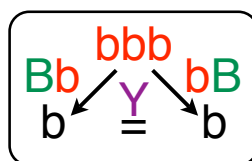
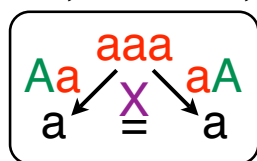
$$\mathbb{Z} \xleftarrow{\partial_0} \mathbb{Z} \cdot \Sigma \xleftarrow{\partial_1} \mathbb{Z} \cdot R \xleftarrow{\partial_2} \mathbb{Z} \cdot P \xleftarrow{\dots} \text{ avec } \partial_0 = 0$$

Exemple : $aa \xrightarrow{A} 1, bb \xrightarrow{B} 1, aba \xrightarrow{C} bab$

$$\partial_1 A = -2a$$

$$\partial_1 B = -2b$$

$$\partial_1 C = b - a$$



$$\partial_2 X = \partial_2 Y = 0 \quad \partial_2 U = 2C + B - A \quad \partial_2 V = A - B - 2C \quad \partial_2 W = 0$$

23

Homologie des réductions

Théorème (Anick, Squier, Kobayashi) : L'homologie de ce complexe est l'homologie du monoïde $M = \Sigma^*/\leftrightarrow^*_R$.

Corollaire : Si M a une présentation convergente finie, alors le groupe abélien $H_3(M)$ est *de type fini*.

Application : Il existe un monoïde M tel que :

- M a une présentation finie (Σ, R) ;
- le problème des mots pour M est décidable ;
- M n'a aucune présentation convergente finie.

Il suffit de montrer que le groupe $H_3(M)$ n'est pas de type fini.

24