

Réécriture et problème du mot

Yves Lafont
Institut de Mathématiques de Luminy
Aix-Marseille 2

mercredi 17 février 2010

1

Problème du mot

Dans un monoïde (non commutatif) :

- sachant que $ab = 1$,
peut-on en déduire que $ba = 1$? **NON**
- sachant que $ab = 1 = bc$,
peut-on en déduire que $ba = 1$? **OUI**
 $ba = babc = bc = 1$

Plus généralement :

- sachant que $u_1 = v_1, \dots, u_n = v_n$,
peut-on en déduire que $u = v$?

mercredi 17 février 2010

2

Systeme de réécriture

Définition :

- ensemble Σ de *symboles* (ou *alphabet*)
- ensemble $R \subset \Sigma^* \times \Sigma^*$ de *règles de réécriture*, où Σ^* est le *monoïde libre* (ou ensemble des *mots*)

On écrit :

- $urv \rightarrow usv$ si $(r,s) \in R$ et $u,v \in \Sigma^*$
- $u_1 \rightarrow^* u_n$ si $u_1 \rightarrow u_2 \rightarrow \dots \rightarrow u_n$

mercredi 17 février 2010

3

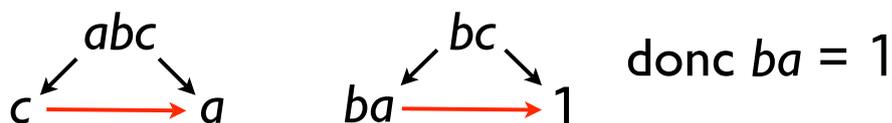
Réécriture convergente

Définition : Un système est *convergent* si :

- il n'existe pas de réécriture infinie :
 $u_1 \rightarrow u_2 \rightarrow \dots \rightarrow u_n \rightarrow \dots$ (*terminaison*)
- si $u \rightarrow v$ et $u \rightarrow v'$, alors il existe w tel que
 $v \rightarrow^* w$ et $v' \rightarrow^* w$ (*confluence*)

Exemples :

- $ab \rightarrow 1$: système convergent
- $ab \rightarrow 1, bc \rightarrow 1$: système non confluent



mercredi 17 février 2010

4

Présentations de groupes

Exemples :

présentation du groupe	éléments du groupe	nom du groupe
$\langle a \rangle$	$a^n, n \in \mathbf{Z}$	$\mathbf{F}_1 = \mathbf{Z}$
$\langle a \mid aa \rangle$	$1, a$	$\mathbf{Z}/2\mathbf{Z}$
$\langle a, b \rangle$???	\mathbf{F}_2
$\langle a, b \mid aba^{-1}b^{-1} \rangle$	$a^p b^q, p, q \in \mathbf{Z}$	$\mathbf{Z}^2 = \mathbf{Z} \times \mathbf{Z}$

Théorème (Novikov-Boone vers 1950) :
Il existe une présentation finie de groupe pour laquelle le problème du mot est *indécidable*.

Groupe libre $\mathbf{F}_1 = \mathbf{Z}$

Présentation convergente :

- 2 symboles (ou *générateurs*) : a, a'
- 2 règles de réécriture : $aa' \rightarrow 1, a'a \rightarrow 1$
- 2 *conflits* (ou *paires critiques*) :

$$\begin{array}{ccc}
 & aa'a & \\
 & \swarrow \quad \searrow & \\
 a & = & a \\
 & & \\
 & a'aa' & \\
 & \swarrow \quad \searrow & \\
 a' & = & a'
 \end{array}$$

formes normales : $1, a, aa, aaa, \dots, a', a'a', a'a'a', \dots$

$$\dots \overset{-3}{\bullet} \overset{-2}{\bullet} \overset{-1}{\bullet} \overset{0}{\bullet} \overset{1}{\bullet} \overset{2}{\bullet} \overset{3}{\bullet} \dots$$

$\leftarrow a' \quad \leftarrow a' \quad \leftarrow a' \quad a \quad a \quad a \rightarrow$

Groupe cyclique $\mathbb{Z}/2\mathbb{Z}$

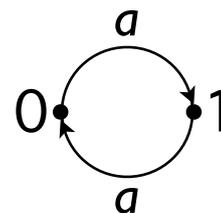
Présentation convergente :

- 1 générateur : a

- 1 règle : $aa \rightarrow 1$

- 1 conflit :
$$\begin{array}{ccc} & aaa & \\ & \swarrow \quad \searrow & \\ a & = & a \end{array}$$

formes normales : $1, a$



Groupe libre F_2

Présentation convergente :

- 4 générateurs : a, a', b, b'

- 4 règles :

$$aa' \rightarrow 1, a'a \rightarrow 1,$$

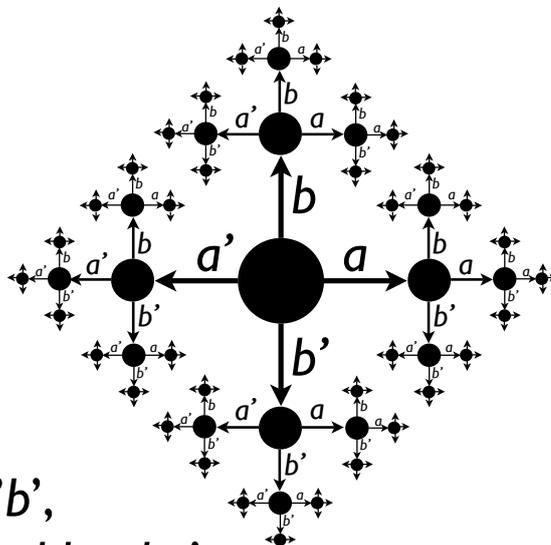
$$bb' \rightarrow 1, b'b \rightarrow 1$$

- 4 conflits ...

formes normales : $1, a, b, a', b',$

$aa, ab, ab', ba, bb, ba', a'b, a'a', a'b',$

$b'a, b'a', b'b', aaa, aab, aab', aba, abb, aba', \dots$



Groupe commutatif libre \mathbf{Z}^2

Présentation convergente :

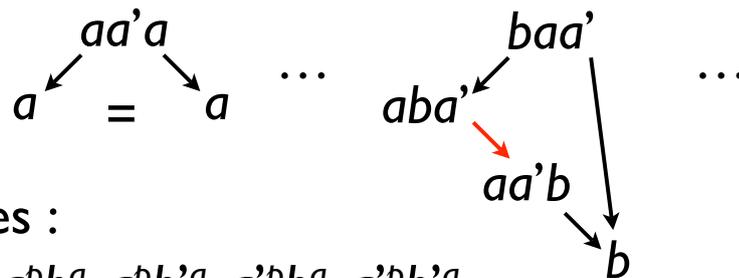
- 4 générateurs : a, a', b, b'

- 8 règles :

$$aa' \rightarrow 1, a'a \rightarrow 1, bb' \rightarrow 1, b'b \rightarrow 1,$$

$$ba \rightarrow ab, ba' \rightarrow a'b, b'a \rightarrow ab', b'a' \rightarrow a'b'$$

- 12 conflits :



formes normales :

$$1, a^p, a'^p, b^q, b'^q, a^p b^q, a^p b'^q, a'^p b^q, a'^p b'^q$$

Preuve par réécriture

Proposition : La famille infinie $(b^n a b^{-n})_{n \in \mathbf{Z}}$ est libre dans le groupe libre $\mathbf{F}_2 = \langle a, b \rangle$.

- on part des générateurs a, a', b, b' et des relations :
 $aa' = 1, a'a = 1, bb' = 1, b'b = 1$

- on ajoute une infinité de générateurs *superflus* :
 $a_n = b^n a b^{-n}, a'_n = b^n a' b^{-n}, a_{-n} = b^{-n} a b^n, a'_{-n} = b^{-n} a' b^n$
et on écrit a_0 pour a, a'_0 pour a'

- on ajoute une infinité d'équations dérivables :

$$a_n a'_n = 1, a'_n a_n = 1,$$

$$b a_n = a_{n+1} b, b a'_n = a'_{n+1} b, b' a_n = a_{n+1} b', b' a'_n = a'_{n+1} b'$$

Preuve par réécriture

- on supprime une infinité d'équations dérivables :
 $a_n = b^n a b'^n, a'_n = b^n a' b'^n, a_{-n} = b'^n a b^n, a'_{-n} = b'^n a' b^n$
- on obtient une présentation convergente :
 $a_n a'_n \rightarrow 1, a'_n a_n \rightarrow 1,$
 $bb' \rightarrow 1, b'b \rightarrow 1,$
 $ba_n \rightarrow a_{n+1} b, ba'_n \rightarrow a'_{n+1} b,$
 $b'a_n \rightarrow a_{n+1} b', b'a'_n \rightarrow a'_{n+1} b'$
- on en déduit un morphisme $\varphi : \mathbf{F}_\omega \rightarrow \mathbf{F}_2$
- ce morphisme est injectif
(préservation des formes normales)

C.Q.F.D.

mercredi 17 février 2010

11

Machines à 2 registres

- 2 registres $x, y \in \mathbf{N}$
- suite d'instructions numérotées de 1 à n
(incrémenter, décrémenter avec test)

Exemple :

- (1) si $x = 0$ alors stop, sinon décrémenter x et aller à 2
- (2) incrémenter y et aller à 3
- (3) incrémenter y et aller à 1

Configuration : $(i, x, y) \in \{1, \dots, n\} \times \mathbf{N} \times \mathbf{N}$

Règles : $(1, 0, y) \rightarrow (0, 0, y), (1, x+1, y) \rightarrow (2, x, y), (2, x, y) \rightarrow (3, x, y+1), (3, x, y) \rightarrow (1, x, y+1)$

mercredi 17 février 2010

12

Problème de l'arrêt

Etant donné (i,x,y) , a-t-on $(i,x,y) \rightarrow^* (0,0,0)$?

Théorème : Il existe une machine à 2 registres pour laquelle le *problème de l'arrêt* est indécidable.

Preuve : On code l'arrêt d'une *machine de Turing*.

Corollaire : Il existe une présentation finie de monoïde pour laquelle le problème du mot est indécidable.

idée : $(i,x,y) \mapsto ab^x c_i d^y e$

$(1,0,y) \rightarrow (0,0,y), (1,x+1,y) \rightarrow (2,x,y), (2,x,y) \rightarrow (3,x,y+1), (3,x,y) \rightarrow (1,x,y+1)$

$ac_1 \rightarrow ac_0, bc_1 \rightarrow c_2, c_2 \rightarrow c_3 d, c_3 \rightarrow c_1 d$

Interférences fatales

Exemple :

(1) si $x = 0$ alors stop, sinon décrémenter x et aller à 2

(2) incrémenter x et aller à 3

(3) si $y = 0$ alors stop, sinon décrémenter y et aller à 3

$ac_1 \rightarrow ac_0, bc_1 \rightarrow c_2, c_2 \rightarrow bc_3, c_3 e \rightarrow c_0 e, c_3 d \rightarrow c_3$

Si on rajoute les inverses, on obtient :

$c_1 = b^{-1} bc_1 = b^{-1} c_2 = b^{-1} bc_3 = c_3$

d'où $ac_1 de = ac_3 de = ac_3 e = ac_0 e$

Et pourtant, on n'a pas $(1,0,1) \rightarrow^* (0,0,0)$!

Il faut trouver un autre codage ...

Machines affines

- positions $z \in \mathbf{Z}$
- règles affines : $p+qz \rightarrow p'+q'z$ ($p,q,p',q' \in \mathbf{Z}, q,q' \neq 0$)

Exemple (*problème de Syracuse*) :

$$2z \rightarrow z, \quad 2z+1 \rightarrow 6z+4$$

Accessibilité de $m \in \mathbf{Z}$: étant donné $z \in \mathbf{Z}$, a-t-on $z \rightarrow^* m$?

Théorème : Il existe une machine affine finie et $m \in \mathbf{Z}$ tels que le problème de l'accessibilité de m est indécidable.

On code l'arrêt d'une machine à registres.

On a fait le plus facile ! Merci pour votre attention.

Références

- Yves Lafont,
Réécriture et problème du mot,
Gazette des mathématiciens 120
(SMF, avril 2009)
- article et diaporama accessibles sur
mon site web : *Google Yves Lafont*