



# Semi-groupoïdes de langages

Géraud Sénizergues

Université de Bordeaux, LaBRI,

11 Mai 2011

Projet FREC, 9-11 Mai 2011

## 1 Semi-groupoïdes

- Definition
- Exemples

## 2 Le semi-groupoïde $DB\langle\langle X \rangle\rangle$

- Definition
  - Les flèches de  $p$  vers  $q$
  - Concaténation ; Action à droite de  $X^*$
  - Les flèches de 1 vers 1
- Problèmes-Motivations-Références
- Trois exemples
- Idéaux à gauche
  - Parties génératrices
  - Parties libres
  - Bases
- Systèmes d'équations
  - Unificateur Principal
  - Caractère Noetherien
  - Lemme du cisaillement
  - Lemme des sous-mots

# Définition

## Définition

Un semi-groïde est un couple  $(S, (A_{s,t})_{s \in S, t \in S})$ , muni d'une opération binaire  $\cdot$  tels que :

$$1- \text{dom}(\cdot) \subseteq \bigcup_{s,t,u \in S} A_{s,t} \times A_{t,u}$$

$$2- \forall s, t, u \in S, a \in A_{s,t}, b \in A_{t,u}, a \cdot b \in A_{s,u}$$

$$3- \forall s, t, u, v \in S, a \in A_{s,t}, b \in A_{t,u}, c \in A_{u,v},$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

$$4- \forall s \in S, \exists e_s \in A_{s,s}, \forall t \in S, \forall a \in A_{t,s}, \forall b \in A_{s,t}$$

$$a \cdot e_s = a, \quad e_s \cdot b = b.$$

# Chemins-Matrices

## Exemple

Soit  $G = (S, A)$  un multi-graphe orienté. Notons  $A_{s,t}$  l'ensemble des chemins allant de  $s$  à  $t$  dans  $G$ .

$(S, (A_{s,t})_{s \in S, t \in S})$  muni du produit de chemins est un semi-groïde.

## Exemple

Soit  $(\mathbb{K}, \cdot, 0, 1)$  un semi-anneau unitaire. Alors

$(\mathbb{N} - \{0\}, (M_{p,q}(K))_{p,q \in \mathbb{N} - \{0\}})$  est un semi-groïde.

# Les matrices de langages prefixes

## Definition

Pour tous entiers  $p, q \in \mathbb{N} - \{0\}$ , notons  $D\mathbb{B}_{p,q}(\langle X \rangle)$  l'ensemble des matrices  $M$  à  $p$  lignes et  $q$  colonnes, à coefficients dans  $\mathbb{B}(\langle X \rangle)$ , dont chaque ligne  $m_{i,1}, \dots, m_{i,q}$ , vérifie la condition de **préfixité** suivante :

- 1- si  $1 \leq j < k \leq q$  alors  $m_{i,j} \cap m_{i,k} = \emptyset$
- 2-  $\cup_{j=1}^q m_{i,j}$  est un code préfixe.

## Proposition

$(\mathbb{N} - \{0\}, (D\mathbb{B}_{p,q}(\langle X \rangle))_{p,q \in \mathbb{N} - \{0\}})$  est un semi-groupeïde.

# Concaténation ;

Pour  $S \in DB_{p,q}\langle\langle X \rangle\rangle$ ,  $S' \in DB_{p',q}\langle\langle X \rangle\rangle$ , le produit de concaténation (verticale) de  $S$  par  $S'$  est

$$S \otimes S' \in DB_{p+p',q}\langle\langle X \rangle\rangle$$

défini par :

$$(S \otimes S')_{i,*} = S_{i,*} \text{ si } 1 \leq i \leq p,$$

$$(S \otimes S')_{i,*} = S'_{i-p,*} \text{ si } p+1 \leq i \leq p+p'.$$

# Action résiduelle

Pour  $S \in D\mathbb{B}_{1,1}\langle\langle X \rangle\rangle$ ,  $u \in X^*$ ,

$$S \bullet u = \{v \in X^* \mid u \cdot v \in S\}$$

Pour  $S \in D\mathbb{B}_{p,q}\langle\langle X \rangle\rangle$ ,  $u \in X^*$ ,

$$S \bullet u = (S_{i,j} \bullet u)_{(i,j) \in [1..p] \times [1..q]}$$

# Langages préfixes

## Théorème

*Le monoïde des langages préfixes est **libre**.*



# Problèmes

Etudier les **systemes d'égalités** de la forme :

$$\sum_{i=1}^n \alpha_i \cdot S_i = \sum_{i=1}^n \beta_i \cdot S_i$$

pour  $\vec{\alpha}, \vec{\beta} \in DB_{1,n}\langle\langle X \rangle\rangle$  et  $\vec{S} \in DB_{n,1}\langle\langle X \rangle\rangle$ .

Quand peut-on déduire une égalité d'autres égalités ?

Pour  $\vec{\alpha}, \vec{\beta}$  fixe, décrire les " solutions en  $\vec{S}$ "

Pour  $\vec{S}$  fixe, décrire l'ensemble des  $\sum_{i=1}^n \alpha_i \cdot S_i$ "

Pour  $\vec{S}$  fixe, décrire l'ensemble des solutions en  $\vec{\alpha}, \vec{\beta}$ "

# Motivations

Tester des égalités de langages.

# Références

[Arnold-Dauchet 79 théorie des Magmoïdes]

[Romanovskii 80, Meitus 89 , Sénizergues 97, Stirling 02 Problème de l' équivalence des automates à pile déterministes].

# Automates finis

la matrice  $M \in DB_{Q,Q}\langle\langle X \rangle\rangle$  :

$$\begin{pmatrix} \dots & \vdots \\ \dots & \{x \in X \mid q_i \odot x = q_j\} \\ \dots & \vdots \end{pmatrix}$$

# Automates à pile

pour tout symbole de pile  $z$  la matrice  $[z] \in DB_{Q,Q}\langle\langle X \rangle\rangle$  :

$$\begin{pmatrix} \dots & \vdots \\ \dots & \{u \in X^* \mid q_i z \xrightarrow{u} q_j\} \\ \dots & \vdots \end{pmatrix}$$

## Termes

Soit  $\begin{pmatrix} t_1 \\ \vdots \\ t_i \\ \vdots \\ t_p \end{pmatrix}$  un  $p$ -uplet d'arbres binaires sur  $q$  variables  $v_1, \dots, v_q$ .

La matrice suivante est dans  $DB_{p,q}\langle\langle X \rangle\rangle$ , où  $X = \{0, 1\}$  :

$$\begin{pmatrix} \dots & \vdots \\ \dots & \{u \in X^* \mid t_i(u) = v_j\} \\ \dots & \vdots \end{pmatrix}$$

# Idéaux à gauche

## Definition

Un idéal à gauche de  $DB\langle\langle X \rangle\rangle$  est une partie  $I$  d'un ensemble  $DB_{1,q}\langle\langle X \rangle\rangle$  (pour un entier  $q \in \mathbb{N} - \{0\}$ ) telle que :  
pour tous  $p \in \mathbb{N} - \{0\}$ ,  $S_1, S_2, \dots, S_p \in I$  et tout vecteur-ligne  $(\alpha_1, \dots, \alpha_p) \in DB_{1,p}\langle\langle X \rangle\rangle$ , on a

$$\sum_{i=1}^p \alpha_i \cdot S_i \in I.$$

# Parties génératrices

## Definition

Soit  $I \subseteq DB_{1,q}\langle\langle X \rangle\rangle$  un idéal à gauche. On appelle partie **génératrice** de  $I$  toute partie  $\mathcal{G} \subseteq DB_{1,q}\langle\langle X \rangle\rangle$  telle que

$$\langle \mathcal{G} \rangle = I.$$



# Indépendance linéaire

## Lemme (Lemme de Meitus, 1989)

Soient  $S_1, \dots, S_j, \dots, S_m \in DB\langle\langle X \rangle\rangle$  et  $\vec{\alpha}, \vec{\beta} \in DB_{1,m}\langle\langle X \rangle\rangle$  tels que

$$(0) \sum_{j=1}^m \alpha_j \cdot S_j = \sum_{j=1}^m \beta_j \cdot S_j$$

Alors l'un des cas (1), (2) est réalisé :

$$(1) \vec{\alpha} = \vec{\beta}$$

(2)  $\exists j_0 \in [1, m], \exists \vec{\gamma} \in DB_{1,m}\langle\langle X \rangle\rangle, \gamma_{j_0} = 0$ , tel que

$$S_{j_0} = \sum_{1 \leq j \leq m} \gamma_j \cdot S_j.$$

On dit que les séries  $S_1, \dots, S_j, \dots, S_m \in DB\langle\langle X \rangle\rangle$  sont **linéairement indépendantes** ssi, il existe des vecteurs  $\vec{\alpha} \neq \vec{\beta}$  réalisant l'égalité (0).

# Bases

## Definition

On appelle **base** de l'idéal à gauche  $I$ , toute famille  $\mathcal{B} = (S_j)_{j \in J}$  qui engendre  $I$  et qui est libre.

## Proposition

*Tout idéal à gauche finiment engendré a une base. De plus cette base est **unique**.*

### Preuve: :

- une base est une famille génératrice minimale
- tout idéal à gauche **finiment** engendré admet une famille génératrice minimale.
- l'unicité résulte du fait que, dans un monoïde libre,  $x \cdot y = 1 \Rightarrow x = y = 1$ .  $\diamond$

## Exemple

Soit

$$\vec{S} = \begin{pmatrix} (ca^*b + d)a^*c \\ a^*ba^*c \\ a^*c \end{pmatrix}$$

Ce vecteur est solution de :

$$ab \cdot S_1 + 0 \cdot S_2 + aab \cdot S_3 = 0 \cdot S_1 + abc \cdot S_2 + (aab + abd) \cdot S_3.$$

En appliquant  $\bullet ab$  aux deux membres on obtient :

$$S_1 = cS_2 + dS_3$$

$$\langle S_1, S_2, S_3 \rangle = \langle S_2, S_3 \rangle$$

Mais  $S_2 = a^*bS_3$ . Une **base** de  $\langle S_1, S_2, S_3 \rangle$  est  $\{S_3\}$ .

On appelle **équation linéaire droite** dans  $DB\langle\langle X \rangle\rangle$  un couple

$$\vec{\alpha}, \vec{\beta} \in DB_{1,q}\langle\langle X \rangle\rangle.$$

Une **solution** de cette équation est un élément  $S \in DB_{q,r}\langle\langle X \rangle\rangle$  tel que :

$$\vec{\alpha} \cdot S = \vec{\beta} \cdot S.$$

Extension à toute conjonction d' équations.

Let  $\vec{\alpha}, \vec{\beta} \in D\mathbb{B}_{1,q}\langle\langle X \rangle\rangle$ . On appelle **unificateur** de la paire  $(\vec{\alpha}, \vec{\beta})$  toute matrice  $U \in D\mathbb{B}_{q,r}\langle\langle X \rangle\rangle$  ( $r \geq 1$ ) telle que :

$$\vec{\alpha} \cdot U = \vec{\beta} \cdot U.$$

$U$  est un **Unificateur principal** ssi, tout unificateur est de la forme  $U \cdot T$  avec  $T \in D\mathbb{B}_{r,s}$  (où  $s \geq 1$ ).

## Théorème

*Tout système fini d'équations linéaires droites admet un **unificateur principal**.*

## Exemple

Une équation :

$$ab \cdot U_1 + 0 \cdot U_2 + aab \cdot U_3, 0 \cdot U_1 + abc \cdot U_2 + (aab + abd) \cdot U_3.$$

Calcul d'un UP :

On applique  $\bullet ab$  aux deux membres :

$$U_1, c \cdot U_2 + d \cdot U_3.$$

on remplace  $U_1$  par le membre droit :

$$abc \cdot U_2 + (aab + abd) \cdot U_3, abc \cdot U_2 + (abd + aab) \cdot U_3,$$

donc :

$$UP((ab, 0, aab), (0, abc, (aab + abd))) = \begin{pmatrix} c & d \\ \varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix}$$

# Caractere Noetherien

## Théorème

- *Tout système d'équations linéaires droites est équivalent à un sous-système **fini**.*
- *Tout système d'équations linéaires droites admet un **unificateur principal**.*

# Problèmes

Problème :

Comment détecter, dans une suite d'équations

$$E_0, E_1, \dots, E_n, \dots$$

la première équation qui est conséquence de celles qui précèdent ?

Notion de conséquence :

$$\forall \vec{S}, \left( \bigwedge_{i=0}^n \vec{\alpha}_i \vec{S} = \vec{\beta}_i \vec{S} \right) \Rightarrow \vec{\alpha}_{n+1} \vec{S} = \vec{\beta}_{n+1} \vec{S}$$

Notion de conséquence **forte** :

$$\forall \vec{S}, \forall \ell \in \mathbb{N}, \left( \bigwedge_{i=0}^n \vec{\alpha}_i \vec{S} =_{\ell} \vec{\beta}_i \vec{S} \right) \Rightarrow \vec{\alpha}_{n+1} \vec{S} =_{\ell} \vec{\beta}_{n+1} \vec{S}$$



# Cisaillement

[Lemme du cisaillement, Romanovskii, 1980] Soient  $K, \lambda \in \mathbb{N}$ .

Alors il existe un entier  $f(K, \lambda)$  tel que,

**pour tout**  $n \geq f(K, \lambda)$ ,  $\alpha, \beta \in D\mathbb{B}_{1,\lambda}\langle\langle X \rangle\rangle$ ,  $A_1, A_2, \dots, A_n \in D\mathbb{B}_{\lambda,\lambda}\langle\langle X \rangle\rangle$ ,  $B_1, B_2, \dots, B_n \in D\mathbb{B}_{\lambda,\lambda}\langle\langle X \rangle\rangle$ ,  $S \in D\mathbb{B}_{\lambda,1}\langle\langle X \rangle\rangle$  telles que les  $A_i$  et les  $B_i$  sont sans  $\varepsilon$  et les coefficients de  $\alpha, \beta$  ont une norme  $\leq K$  **si** les équations suivantes sont vérifiées

$$\alpha A_1 A_2 \cdots A_n \cdot S = \beta \cdot S$$

$$\alpha A_2 \cdots A_n \cdot S = \beta B_1 \cdot S$$

$$\vdots = \vdots$$

$$\alpha A_n \cdot S = \beta B_{n-1} \cdots B_2 B_1 \cdot S$$

$$\alpha \cdot S = \beta B_n B_{n-1} \cdots B_2 B_1 \cdot S$$

# Cisaillement

alors

$$\exists i \in [1, n], \alpha A_i \cdots A_n \cdot S = \beta B_{i-1} \cdots B_1 \cdot S = \mathbf{0}.$$

La fonction  $f(K, \lambda)$  est doublement exponentielle.

# Les sous-mots

## Lemme (Lemme des sous-mots, GS, ICALP'03)

Soient  $\lambda \in \mathbb{N}, \ell \in \mathbb{N}, \alpha, \beta \in DB_{1,\lambda}\langle\langle X \rangle\rangle, A_1, A_2, \dots, A_\lambda \in DB_{\lambda,\lambda}\langle\langle X \rangle\rangle, S \in DB_{\lambda,1}\langle\langle X \rangle\rangle$ . Les égalités :

$$\alpha \cdot A_{i_1} A_{i_2} \cdots A_{i_p} \cdot S =_\ell \beta \cdot A_{i_1} A_{i_2} \cdots A_{i_p} \cdot S$$

pour  $0 \leq p \leq \lambda - 1, 1 \leq i_1 < i_2 < \dots < i_p \leq \lambda$

entraînent que :

$$\alpha \cdot A_1 A_2 \cdots A_\lambda \cdot S =_\ell \beta \cdot A_1 A_2 \cdots A_\lambda \cdot S.$$

# Applications du lemme des sous-mots

## Application 1 :

Soient  $A, B$  deux automates finis déterministes sur  $X$ .

$L(A) = L(B)$  ssi, pour tout  $u \in X^*$  tel que

$$|u| \leq \text{Card}(Q_A) + \text{Card}(Q_B)$$

$u \in L(A) \Leftrightarrow u \in L(B)$ . (Résulte aussi de [Eilenberg, 1973]).

## Application 2 :

Le problème de l'équivalence des apd est **Primitif Récurif**

[C.Stirling, ICALP' 02]

## Problème ouvert :

Trouver d'autres lemmes de cette forme.