Monoïdes

Stéphane Le Roux leroux@lsv.fr

ENS Paris-Saclay

2021-2022

Loi de composition interne

Loi de composition interne

Soit E un ensemble. Une application de $E \times E$ vers E est parfois appelée loi de composition interne. L'image de $(x, y) \in E \times E$ par une telle loi est souvent notée $x + y$, $x \cdot y$, ou tout simplement xy.

Élément neutre

- $e \in E$ est un élément neutre à gauche si $ex = x$ pour tout $x \in E$.
- $e' \in E$ est un élément neutre à droite si $xe' = x$ pour tout $x \in E$.
- Un élément neutre à gauche et à droite est appelé élément neutre.

Proposition

Un élément neutre à gauche et un élément neutre à droite sont égaux.

Associativité

Une loi $E \times E \to E$ est dite associative si $(xy)z = x(yz)$ pour tout $x, y, z \in E$.

Monoïdes

Monoïdes

Un monoïde est un ensemble, communément noté M, muni d'une loi associative et d'un élément neutre.

Exemples de monoïdes ou pas

	monoïde ?
$(\mathbb{N}, +, 0)$	
$(\mathbb{N}, \cdot, 1)$	
$(\mathbb{N} \setminus \{0\}, \cdot, 1)$	
$(\mathbb{N}, \max, ?)$	
$(\mathbb{N}, \min, ?)$	
$(\mathcal{M}_n(\mathbb{N}), \cdot, ?)$	
$(\mathcal{P}(E), \cup, ?)$	
$(E^E, \circ, ?)$	
$(\mathcal{P}(E \times E), \circ, ?)$ où $R \circ S := RS := \{(x, z) \in E \times E \mid \exists y \in E,\ xRySz\}$	
$(\Sigma^*, \cdot, \epsilon)$	

Question

A quelle condition un treillis est-il un monoïde ?

Monoïdes

Monoïdes

Un monoïde est un ensemble, communément noté M, muni d'une loi associative et d'un élément neutre.

- $(\mathbb{N}, +, 0)$, $(\mathbb{N}, \cdot, 1)$ et $(\mathbb{N} \setminus \{0\}, \cdot, 1)$ sont des monoïdes.
- $(\mathbb{N}, \max, 0)$ est un monoïde, mais $(\mathbb{N}, \min)$ n'a pas d'élément neutre.
- $(\mathcal{M}_n(\mathbb{N}), \cdot, I_n)$ est un monoïde.
- $(\mathcal{P}(E), \cup, \emptyset)$ est un monoïde.
- $(E^E, \circ, id_E)$ est un monoïde.
- $(\mathcal{P}(E \times E), \circ, id_E)$ où $R \circ S := RS := \{(x, z) \in E \times E \mid \exists y \in E, xRySz\}$ est un monoïde.
- Soit Σ un alphabet. Alors Σ^* muni de la concaténation est un monoïde avec pour élément neutre le mot vide ϵ.
- Un treillis avec plus petit élément est un monoïde. (Si on prend la borne supérieure de deux éléments comme loi de composition interne.)

Conséquence de l'associativité

Définition

Soient $x_1, \ldots, x_n \in M$. On définit $\prod_{i=1}^{n} x_i = ((x_1 x_2) \ldots x_{n-1}) x_n$ par récurrence.

- $\prod_{i=1}^{0} x_i := e$.
- $\prod_{i=1}^{k+1} x_i = (\prod_{i=1}^{k} x_i) x_{k+1}$ pour tout $k < n$.

Proposition

Soient $x_1, \ldots, x_n \in M$ et $k \leq n$. Alors

$$\left(\prod_{i=1}^{k} x_i\right)\left(\prod_{i=k+1}^{n} x_i\right) = \prod_{i=1}^{n} x_i$$

Commutatitivité

Définition

- Une loi sur E est commutative si $xy = yx$ pour tout $x, y \in E$.
- Un monoïde muni d'une loi commutative est dit commutatif ou abélien.

Exemples de monoïdes commutatifs ou pas

	monoïde	abélien ?
$(\mathbb{N}, +, 0)$	Oui	
$(\mathbb{N}, \cdot, 1)$	Oui	
$(\mathbb{N} \setminus \{0\}, \cdot, 1)$	Oui	
$(\mathbb{N}, \max, 0)$	Oui	
$(\mathbb{N}, \min, ?)$	Non	
$(\mathcal{M}_n(\mathbb{N}), \cdot, I_n)$	Oui	
$(\mathcal{P}(E), \cup, \emptyset)$	Oui	
$(E^E, \circ, id_E)$	Oui	
$(\mathcal{P}(E \times E), \circ, id_E)$ où $R \circ S := RS := \{(x, z) \in E \times E \mid \exists y \in E, xRySz\}$	Oui	
$(\Sigma^*, \cdot, \epsilon)$	Oui	

Question

A quelle condition un treillis est-il un monoïde commutatif ?

Exemples de monoïdes commutatifs ou pas

	monoïde	abélien ?
$(\mathbb{N}, +, 0)$	Oui	Oui
$(\mathbb{N}, \cdot, 1)$	Oui	Oui
$(\mathbb{N} \setminus \{0\}, \cdot, 1)$	Oui	Oui
$(\mathbb{N}, \max, 0)$	Oui	Oui
$(\mathbb{N}, \min, ?)$	Non	Oui
$(\mathcal{M}_n(\mathbb{N}), \cdot, I_n)$	Oui	Non (si $n > 1$)
$(\mathcal{P}(E), \cup, \emptyset)$	Oui	Oui
$(E^E, \circ, id_E)$	Oui	Non
$(\mathcal{P}(E \times E), \circ, id_E)$ où $R \circ S := RS := \{(x, z) \in E \times E \mid \exists y \in E,\ xRySz\}$	Oui	Non
$(\Sigma^*, \cdot, \epsilon)$	Oui	Non (si $\|\Sigma\| > 1$)

Proposition

Un treillis avec plus petit élément est un monoïde abélien. (Si on prend la borne supérieure de deux éléments comme loi de composition interne.)

Produit direct de monoïdes

Définition

Soient deux monoïdes $(M_1, \cdot_1, e_1)$ et $(M_2, \cdot_2, e_2)$. Leur produit direct est $(M_1 \times M_2, \cdot, (e_1, e_2))$, où $\cdot : (M_1 \times M_2)^2 \to M_1 \times M_2$ telle que $(x_1, x_2) \cdot (y_1, y_2) := (x_1 \cdot_1 y_1, x_2 \cdot_2 y_2)$.

Proposition

Le produit direct de deux monoïdes est un monoïde.

Sous-monoïde

Définition

Soit $(M, \cdot, e)$ un monoïde. Une partie $N \subseteq M$ est un sous-monoïde de M si $e \in N$ et $xy \in N$ pour tout $x, y \in N$.

Proposition

Un sous-monoïde est un monoïde.

- $(\mathbb{N} \setminus \{0\}, \cdot, 1)$ est un sous-monoïde de $(\mathbb{N}, \cdot, 1)$.
- $(E^E, \circ, id_E)$ est un sous-monoïde de $(\mathcal{P}(E \times E), \circ, id_E)$.

Un monoïde inclus dans un monoïde M (avec la même loi) n'est pas nécessairement un sous-monoïde de M.

- $(\{E\}, \cup, E)$ est inclus dans $(\mathcal{P}(E), \cup, \emptyset)$.
- $(\mathbb{Z}/6\mathbb{Z}, \cdot, 1)$ est un monoïde. $\{0, 2, 4\} \subseteq \mathbb{Z}/6\mathbb{Z}$ et $(\{0, 2, 4\}, \cdot, 4)$ est un monoïde d'élément neutre $4 \neq 1$.

Sous-monoïde engendré

Définition

Soit X une partie d'une monoïde M. On note $\langle X \rangle$ l'intersection des sous-monoïdes de M contenant X. Si $\langle X \rangle = M$ on dit que X engendre M ou est une partie génératrice de M.

Proposition

- Une intersection non-vide de sous-monoïdes est un sous-monoïde. (I.e. les sous-monoïdes constituent un système de clôture.)
- $\langle \cdot \rangle$ est l'opérateur de clôture associé. Donc $X \subseteq \langle X \rangle$ et $X \subseteq Y \Rightarrow \langle X \rangle \subseteq \langle Y \rangle$ et $\langle \langle X \rangle \rangle = \langle X \rangle$.
- $\langle X \rangle$ est le plus petit sous-monoïde de M contenant X.

Soit M un monoïde d'élément neutre e. Alors, dans ce monoïde, $\langle \emptyset \rangle = \{e\}$. (On devrait écrire $\langle \emptyset \rangle_M$.)

Sous-monoïde engendré (II)

Proposition

Soit X une partie d'une monoïde M. Les trois ensembles suivants sont égaux.

1. $\langle X \rangle$
2. $Y := \{x_1 \dots x_n \mid n \in \mathbb{N} \wedge x_1, \dots, x_n \in X\}$
   $= \cup_{n\in\mathbb{N}} \{\prod_{i=1}^{n} x_i \mid \forall i \in [\![1, n]\!],\ x_i \in X\}$
3. Le plus petit point fixe P de

$$f_X : \begin{array}{rl} \mathcal{P}(M) & \to \mathcal{P}(M) \\ A & \mapsto X \cup \{e\} \cup A^2 \end{array}$$

   où $A^2 := \{ab \mid a, b \in A\}$.

Morphisme de monoïdes

Définition

- Soient deux monoïdes $(M_1, \cdot_1, e_1)$ et $(M_2, \cdot_2, e_2)$. Une application $f : M_1 \to M_2$ est un morphisme de monoïdes si $f(e_1) = e_2$ et $f(x \cdot_1 y) = f(x) \cdot_2 f(y)$ pour tout $x, y \in M_1$.
- $f^{-1}(e_2)$ est appelé le noyau du morphisme.

Proposition

- La composée de deux morphismes de monoïdes est un morphisme.
- La réciproque d'un morphisme de monoïdes bijectif est un morphisme de monoïde. (On parle alors d'isomorphisme.)
- L'image d'un sous-monoïde est un sous-monoïde.
- L'image réciproque d'un sous-monoïde est un sous-monoïde.
- Le noyau d'un morphisme de monoïde est un sous-monoïde.
- Si f est injectif, alors $f^{-1}(e_2) = e_1$, mais la réciproque n'est pas vraie. E.g. $f : (\Sigma^*, \cdot, \epsilon) \to (\mathbb{N}, +, 0)$ tel que $f(a_1 \dots a_n) = n$.

Morphisme de monoïdes et sous-monoïde engendré

Proposition

Soit $f : M \to N$ un morphisme. Pour tout $X \subseteq M$ on a $f[\langle X \rangle] = \langle f[X] \rangle$.

Preuve

$f[\langle X \rangle] = \{f(x_1 \dots x_n) | x_1, \dots, x_n \in X\}$
$= \{f(x_1) \dots f(x_n) | x_1, \dots, x_n \in X\} = \langle f[X] \rangle$

Proposition

Soient $f, g : M \to N$ deux morphismes de monoïdes et $X \subseteq M$ tel que $\langle X \rangle = M$. Si $f\,|_X = g\,|_X$ alors $f = g$.

Preuve

Soit $y \in M$. Il existe $x_1, \dots, x_n \in X$ tels que $y = x_1 \dots x_n$. Donc $f(y) = f(x_1 \dots x_n) = f(x_1) \dots f(x_n) = g(x_1) \dots g(x_n) = g(x_1 \dots x_n) = g(y)$.

Congruence

Définition

Soit M un monoïde. Une congruence sur M est une relation d'équivalence $\sim$ sur M telle que si $x \sim y$, alors $uxv \sim uyv$ pour tout $u, v \in M$.

Proposition

- Soit $\sim$ une relation d'équivalence sur un monoïde M. Alors, $\sim$ est une congruence ssi $x \sim x' \wedge y \sim y' \Rightarrow xy \sim x'y'$.
- Ainsi on peut définir une loi de composition interne sur $M/\sim$ par $[x] \star [y] := [xy]$.
- $(M/\sim, \star, [e])$ est appelé un monoïde quotient.

Proposition

- Soit M un monoïde. Toute intersection de congruences sur M est une congruence.
- Pour tout $R \subseteq M \times M$, il existe donc une plus petit congruence contenant R.

La surjection canonique d'une relation d'équivalence

Définition

- Soit $\sim$ une relation d'équivalence sur un ensemble E. L'application

$$\begin{aligned} \pi : & E \to E/\sim \\ & x \mapsto [x] \end{aligned}$$

  est appelée la surjection canonique (de $\sim$).
- Une application $f : E \to F$ est dite compatible avec $\sim$ si $x \sim y \Rightarrow f(x) = f(y)$.

Proposition

Si une application $f : E \to F$ est compatible avec une relation d'équivalence $\sim$, alors il existe une unique application $\tilde{f} : (E/\sim) \to F$ telle que $f = \tilde{f} \circ \pi$. On dit que f se factorise par π à travers $\tilde{f}$.

$\tilde{f}$ est injective ssi $x \sim y \Leftrightarrow f(x) = f(y)$.

Factorisation d'un morphisme

Proposition

Soit $f : M \to N$ un morphisme de monoïdes compatible avec une congruence $\sim$ sur M, i.e. $x \sim y \Rightarrow f(x) = f(y)$. L'unique application $\tilde{f} : (M/\sim) \to N$ telle que $f = \tilde{f} \circ \pi$ est aussi un morphisme de monoïdes.

Preuve

D'une part $\tilde{f}([e_M]) = f(e_M) = e_N$; d'autre part, pour tout $[x], [y] \in E/\sim$ on a $\tilde{f}([x][y]) = \tilde{f}([xy]) = f(xy) = f(x)f(y) = \tilde{f}([x])\tilde{f}([y])$.

Exemple (cf exemple précédent)

Si $x \sim y \Leftrightarrow f(x) = f(y)$, alors $\sim$ est bien une congruence.

Preuve

Soit $x \sim y$ et $u, v \in M$. Alors
$f(uxv) = f(u)f(x)f(v) = f(u)f(y)f(v) = f(uyv)$, donc $uxv \sim uyv$.

Codes

Définition

Une partie C d'un monoïde est appelée code si

$$\forall x_1, \ldots, x_n, y_1, \ldots, y_p \in C, \prod_{i=1}^{n} x_i = \prod_{j=1}^{p} y_j \Rightarrow (n = p \wedge \forall i \leq n, x_i = y_i)$$

- $C := \{1, 01, 001\}$ est un code dans $\{0, 1\}^*$.
- $C := \{0, 1\}$ est un code dans $\{0, 1\}^*$.

Proposition

1. L'ensemble vide est un code.
2. L'élément neutre n'appartient à aucun code.
3. Un monoïde fini ne contient aucun code (autre que le code vide).
4. Un monoïde abélien n'a que des codes singletons (ou vide).
5. Un sous-ensemble d'un code est un code.

Codes et morphismes

Proposition

Si C est un code dans $(M, \cdot, e_M)$ et $f_C : C \to (N, \cdot, e_N)$, il existe un unique morphisme $f : \langle C \rangle \to N$ qui coïndice avec f_C sur C.

Preuve

On a l'unicité par un résultat précédent.
Existence: pour tout $x \in \langle C \rangle$ soit $x = c_1 \ldots c_n$ l'unique décomposition de x sur le code C. On pose $f(x) := f_C(c_1) \ldots f_C(c_n)$. On a bien $f(e_M) = e_N$ (produit vide). Pour tout $x, y \in \langle C \rangle$, soient $c_1, \ldots, c_n, d_1, \ldots, d_p \in C$ tels que $x = c_1 \ldots c_n$ et $y = d_1, \ldots d_p$. Alors $xy = c_1 \ldots c_n d_1 \ldots d_p$, donc $f(xy) = f_C(c_1) \ldots f_C(c_n) f_C(d_1) \ldots f_C(d_p) = f(x)f(y)$.

Soient $C := \{1, 01\}$ et $f_C(1) := 0$ et $f_C(01) := 1$. Il n'existe pas de morphisme $f : \{0,1\}^* \to \{0,1\}^*$ extension de f_C.
En effet, $1 = f_C(01) = f(0)f(1) = f(0)0$ est absurde.

Codes et morphismes (II)

Proposition

Si un morphisme $f : M \to N$ est injectif, alors $C \subseteq M$ est un code ssi $f[C]$ est un code.

Preuve : Par injectivité, pour tout $x_1, \ldots, x_n, y_1, \ldots, y_p \in C$ on a $x_1 \ldots x_n = y_1 \ldots y_p$ ssi $f(x_1) \ldots f(x_n) = f(y_1) \ldots f(y_p)$.

- Si $f[C]$ est un code, soient $x_1, \ldots, x_n, y_1, \ldots, y_p \in C$ tels que $x_1 \ldots x_n = y_1 \ldots y_p$, donc $f(x_1) \ldots f(x_n) = f(y_1) \ldots f(y_p)$, donc $n = p$ et $f(x_i) = f(y_i)$ pour tout i, et donc $x_i = y_i$ par injectivité.
- Si C est un code, soient $z_1, \ldots, z_n, t_1, \ldots, t_p \in f[C]$ tels que $z_1 \ldots z_n = t_1 \ldots t_p$. Il existe $x_1, \ldots, x_n, y_1, \ldots, y_p \in C$ tels que $f(x_i) = z_i$ et $f(y_j) = t_j$ pour tout i, j. Donc $x_1 \ldots x_n = y_1 \ldots y_p$, donc $n = p$ et $x_i = y_i$ pour tout i, donc $z_i = f(x_i) = f(y_i) = t_i$ pour tout i.

Soit le morphisme $f : \{0,1,2\}^* \to \{0,1,2\}^*$ tel que $f(0) = 0$, $f(1) = 1$ et $f(2) = 01$. (f est bien défini, car $\langle\{0,1,2\}\rangle = \{0,1,2\}^*$.) L'image du code $\{0,1,2\}$ n'est pas un code (et f n'est pas injectif).

Bases de monoïde

Définition (Comparer avec les espaces vectoriels)

Une partie B d'un monoïde M est appelée base de M si c'est un code engendrant M, i.e.

- $\langle B \rangle = M$.
- $\forall x_1, \ldots, x_n, y_1, \ldots, y_p \in B$,
  $\prod_{i=1}^{n} x_i = \prod_{j=1}^{p} y_j \Rightarrow (n = p \wedge \forall i \leq n,\, x_i = y_i)$

Proposition

1. L'ensemble vide est la base du monoïde trivial.
2. l'élément neutre n'appartient à aucune base.
3. Un monoïde fini non trivial n'a pas de base.
4. Un monoïde abélien non trivial avec base est du type $\{a^n \mid n \in \mathbb{N}\}$.

- $(\{0,1\}^*, \cdot, \epsilon)$ a pour base $\{0,1\}$. Et $(\Sigma^*, \cdot, \epsilon)$ a pour base Σ.
- $(\mathbb{N}, +, 0)$ a pour base $\{1\}$.

Bases de monoïde (II)

Proposition (Comparer avec les espaces vectoriels)

1. Un code C est la base du monoïde $\langle C \rangle$.
2. B est une base de M ssi tout élément de M est produit unique d'éléments de B. (Reformulation de la définition.)
3. Si un monoïde a une base, celle-ci est unique.

Preuve

Soient B et C deux bases et $b \in B \setminus C$. Il existe $c_1, \dots, c_n \in C$ tels que $b = c_1 \dots c_n$. De plus $1 < n$, car $b \notin C$. Chaque c_i s'écrit $b^i_1 \dots b^i_{k_i}$ avec $b^i_1, \dots, b^i_{k_i} \in B$. Ainsi, $b = b^1_1 \dots b^1_{k_1} \dots b^n_1, \dots, b^n_{k_n}$, le second terme étant composé d'au moins deux éléments car $n > 1$. Cela contredit l'hypothèse que B est une base. Ainsi, $B \subseteq C$ et par symétrie $B = C$.

Bases de monoïde (III)

Définition

Un monoïde avec une base est appelé monoïde libre.

Proposition (Les monoïdes de mots "simulent" les monoïdes libres)

Soit $(M, \star, e)$ un monoïde libre de base B. Alors

$$
\begin{aligned}
f : \quad (B^*, \cdot, \epsilon) &\rightarrow (M, \star, e) \\
w_1 \cdot w_2 \dots w_n &\mapsto w_1 \star w_2 \dots w_n
\end{aligned}
$$

est un isomorphisme de monoïdes.

- $f(\epsilon) = e$ par définition. Pour $w, u \in B^*$ on a $f(wu) = f(w_1 \dots w_n u_1 \dots u_k) = w_1 \star \dots \star w_n \star u_1 \star \dots \star u_k = f(w) \star f(u)$.
- f surjective : Soit $x \in M$. Soit $b_1, \dots, b_n \in B$ tel que $x = b_1 \star \dots \star b_n$. Ainsi $x = f(b_1 \dots b_n)$.
- f injective : Soient $w, u \in B^*$ tels que $f(w) = f(u)$. Donc $\prod_{i=1}^{|w|} w_i = \prod_{i=1}^{|u|} u_i$. Par unicité de décomposition, on a $w = u$.

Monoïdes libres et morphismes

Corollaire

Soit deux monoïdes M et N. Si B est une base de M et $f_B : B \to N$, il existe un unique morphisme $f : M \to N$ qui coïndice avec f_B sur B.

Preuve : (rappel) Si C est un code dans $(M, \cdot, e_M)$ et $f_C : C \to (N, \cdot, e_N)$, il existe un unique morphisme $f : \langle C \rangle \to N$ qui coïndice avec f_C sur C.

Corollaire

Un isomorphisme de monoïdes libres envoie la base sur la base.

Preuve : Par injectivité, $f : M \to N$ envoie le code B sur un code.
De plus, $\langle f[X] \rangle = f[\langle X \rangle]$, donc $\langle f[B] \rangle = f[\langle B \rangle] = f[M] = N$.

La réciproque du corollaire ci-dessus est fausse

Soit $f : \Sigma \to \mathbb{N}$ l'application constante égale à 1. Son unique extension en morphisme de monoïdes $\varphi : (\Sigma^*, \cdot, \epsilon) \to (\mathbb{N}, +, 0)$ est la fonction qui renvoie la longueur du mot, i.e. $\varphi(u) = |u|$.

Éléments simplifiables, ordre préfixe et codes

Définition

- Soit M un monoïde. $x \in M$ est dit simplifiable si pour tout $y, z \in M$ on a $(xy = xz \vee yx = zx) \Rightarrow y = z$.
- Pour tout $u, v \in \Sigma^*$ on note $u \sqsubseteq uv$ (la relation préfixe).

Proposition

Soit Σ un alphabet.

- Tous les éléments de Σ^* sont simplifiables.
- $(\Sigma^*, \sqsubseteq)$ est un ordre.
- Pour tout $u, v, u', v' \in \Sigma^*$, si $uv \sqsubseteq u'v'$, alors $u \sqsubseteq u'$ ou $u' \sqsubseteq u$.
- Pour tout $u, v, w \in \Sigma^*$, si $u \sqsubseteq vw$ et $|u| = |v|$ alors $u = v$.

Éléments simplifiables, ordre préfixe et codes (II)

Proposition

Soit Σ un alphabet. Si $X \subseteq \Sigma^* \setminus \{\epsilon\}$ n'est pas un code, il existe $x_1, \ldots, x_n, y_1, \ldots, y_p \in X$ tels que $x_1 \ldots x_n = y_1 \ldots y_p$ et $x_1 \neq y_1$.

Preuve

- Soient $x_1, \ldots, x_n, y_1, \ldots, y_p \in X$ tels que $x_1 \ldots x_n = y_1 \ldots y_p$ et $(x_1, \ldots, x_n) \neq (y_1, \ldots, y_p)$.
- Si $x_1 = y_1$, on simplifie l'égalité par x_1 à gauche et on obtient $x_2 \ldots x_n = y_2 \ldots y_p$.
- De plus $(x_2, \ldots, x_n) \neq (y_2, \ldots, y_p)$, sinon on obtiendrai $x_1 = y_1$ en simplifiant l'égalité intiale à droite, d'où
- On itère la simplification à gauche, qui termine avec un témoin, car $(x_1, \ldots, x_n) \neq (y_1, \ldots, y_p)$.

L'ordre préfixe (II)

Rappel : Soit $(E, \leq)$ un ensemble ordonné dont toute partie admet une borne supérieure. Alors $(E, \leq)$ est un treillis complet.

Définition

- Un demi-treillis est un ordre tel que toute paire d'éléments a une borne inférieure (resp. supérieure).
- Un demi-treillis complet est un ordre tel que toute partie non-vide a une borne inférieure (resp. supérieure).

Proposition

$(\Sigma^*, \sqsubseteq)$ est un demi-treillis complet. (borne inférieure)

Soit $E \subseteq \Sigma^*$ non vide. Soit M l'ensemble des minorants de E. Notons que $\epsilon \in M$. Soient u, v deux minorants de E et $w \in E$, alors $u, v \sqsubseteq w$. Donc il existe u', v' tels que $uu' = vv' = w$, donc $u \sqsubseteq v$ ou $v \sqsubseteq u$. Ainsi, M est totalement ordonné et fini, car ses mots sont préfixes de w. M a donc un plus grand élément.

Plus petite partie génératrice

Proposition

Soit M un sous-monoïde de Σ^*. Alors $X := (M \setminus \{\epsilon\}) \setminus (M \setminus \{\epsilon\})^2$ engendre M et toute partie de M qui engendre M contient X.

- Soit Y engendrant M. Donc $X \subseteq \langle Y \rangle$. Par définition, les éléments de X ne peuvent pas être décomposés, donc $X \subseteq Y \cup \{\epsilon\}$, donc $X \subseteq Y$, car $\epsilon \notin X$.
- On montre maintenant que $\langle X \rangle = M$. Comme $X \subseteq M$ et M est un monoïde, on a aussi $\langle X \rangle \subseteq M$, donc il suffit de montrer que $M \subseteq \langle X \rangle$. Soit $w \in M$. On raisonne par récurrence sur (la longueur de) w.
  - Si $|w| = 0$, alors $w = \epsilon \in \langle X \rangle$.
  - Pour le cas inductif, si $w \notin (M \setminus \{\epsilon\})^2$, alors $w \in X$, sinon w se décompose en uv avec $u, v \in M \setminus \{\epsilon\}$, i.e. $|u|, |v| < |w|$, donc par HR on a $u, v \in \langle X \rangle$, donc $w = uv \in \langle X \rangle$.

Ci-dessus, si M a une base, c'est X.

Liberté, égalité, stabilité

Définition

- Un sous-monoïde M de Σ^* est stable, si $\forall u, v, w \in \Sigma^*,\ u, v, uw, wv \in M \Rightarrow w \in M$.
- Pour $A, B \subseteq \Sigma^*$ on note $A^{-1}B := \{x \in \Sigma^* \mid \exists y \in A,\ yx \in B\}$ et $BA^{-1} := \{x \in \Sigma^* \mid \exists y \in A,\ xy \in B\}$.

Proposition

Pour tout sous-monoïde M de Σ^*, les assertions suivantes sont équivalentes.

1. M est libre.
2. M est stable.
3. $M = M^{-1}M \cap MM^{-1}$.

Dans ce cas $(M \setminus \{\epsilon\}) \setminus (M \setminus \{\epsilon\})^2$ est la base de M.

Liberté, égalité, stabilité (II)

Proposition

Pour tout sous-monoïde M de Σ^*, les assertions suivantes sont équivalentes.

1. M est libre.
2. M est stable.
3. $M = M^{-1}M \cap MM^{-1}$.

[$1 \Rightarrow 2$] Montrons que $\forall u, v, w \in \Sigma^*$, $u, v, uw, wv \in M \Rightarrow w \in M$ par récurrence sur la taille de la décomposition de u sur la base B de M.

- Le cas $u = \epsilon$ est clair.
- Pour le cas inductif, $u \neq \epsilon$, soit les décompositions $u = u_1 \dots u_n$ et $uw = x_1 \dots x_k$ avec $u_1, \dots, u_n, x_1, \dots, x_k \in B$. Alors $u(wv) = u_1 \dots u_n(wv)$ et $(uw)v = x_1 \dots x_k v$, donc $u_1 = x_1$. Soit $u' = u_2 \dots u_n \in M$, alors $u'w = x_2 \dots x_k \in M$. Par HR, $w \in M$.

Liberté, égalité, stabilité (III)

Définition

- Un sous-monoïde M de Σ^* est stable, si $\forall u, v, w \in \Sigma^*,\ u, v, uw, wv \in M \Rightarrow w \in M$.
- Pour $A, B \subseteq \Sigma^*$ on note $A^{-1}B := \{x \in \Sigma^* \mid \exists y \in A,\ yx \in B\}$ et $BA^{-1} := \{x \in \Sigma^* \mid \exists y \in A,\ xy \in B\}$.

Proposition

Pour tout sous-monoïde M de Σ^*, les assertions suivantes sont équivalentes.

1. M est libre.
2. M est stable.
3. $M = M^{-1}M \cap MM^{-1}$.

[2 $\Rightarrow$ 3] Supposons que M est stable. Alors $M \subseteq M^{-1}M$ (en composant un x avec ϵ). Réciproquement, soit $w \in M^{-1}M \cap MM^{-1}$, donc il existe $u, v \in M$ tels que $uw \in M$ et $wv \in M$. Par stabilité, $w \in M$

Liberté, égalité, stabilité (IV)

Proposition

Pour tout sous-monoïde M de Σ^*, si $M = M^{-1}M \cap MM^{-1}$ alors M est libre, et $(M \setminus \{\epsilon\}) \setminus (M \setminus \{\epsilon\})^2$ est la base de M.

Soit B la plus petite partie génératrice de M, i.e. $B = (M \setminus \{\epsilon\}) \setminus (M \setminus \{\epsilon\})^2$. Pour montrer que B est une base, montrons par récurrence sur $n + p$ que pour tout $x_1 \dots x_n = y_1 \dots y_p$ (avec éléments dans B), on a $n = p$ et $x_i = y_i$ pour tout $i \leq n$.

- Cas de base clair.
- Pour le cas inductif, supposons que $x_n \neq y_p$, e.g. il existe $w \in \Sigma^*$ tel que $x_n = wy_p$, donc $w \in MM^{-1}$ et donc $x_1 \dots x_{n-1}w = y_1 \dots y_{p-1}$ par simplification par y_p, donc $w \in M^{-1}M$. Ainsi $w \in MM^{-1} \cap M^{-1}M = M$. Or on a (encore) $x_n = wy_p$ avec $x_n, y_p \in B$ (donc $y_p \neq \epsilon$), donc $w = \epsilon$. On a donc $x_n = y_p$, et par HR et de $x_1 \dots x_{n-1} = y_1 \dots y_{p-1}$, on déduit $n - 1 = p - 1$ et $x_i = y_i$ pour tout $i \leq n - 1$.

Sous-monoïdes libres

Définition

Un sous-monoïde libre d'un monoïde est un sous-monoïde qui est libre en tant que monoïde.

Proposition

Toute intersection non vide de sous-monoïdes libres (stable) est un sous-monoïde libre (stable).

Preuve : Un sous-monoïde M de Σ^* est stable, si $\forall u, v, w \in \Sigma^*,\ u, v, uw, wv \in M \Rightarrow w \in M$.

Si L_1 et L_2 sont deux sous-monoïdes libres de bases B_1 et B_2, le sous-monoïde libre $L_1 \cap L_2$, n'a pas nécessairement $B_1 \cap B_2$ pour base.

Exemple (concernant l'alerte rouge ci-dessus)

Soit $L_1 = \langle\{1, 001\}\rangle$ et $L_2 = \langle\{10, 01\}\rangle$. Alors $L_1 \cap L_2 = \langle\{1001\}\rangle$, bien que $1001 \notin \{1, 001\} \cap \{10, 01\} = \emptyset$.

Enveloppe libre

Corollaire et Définition

Pour toute partie X de Σ^*, il existe un plus petit sous-monoïde libre contenant X. On l'appelle l'enveloppe libre de X.

Proposition

Soit X une partie de Σ^* et soit L son enveloppe libre. Alors $\langle X \rangle \subseteq L$.

En général, l'inclusion ci-dessus n'est pas une égalité.

Théorème du défaut

Théorème du défaut

Soit X une partie finie de Σ^* et soit L son enveloppe libre, de base Y. Les assertions suivantes sont équivalentes.

1. X n'est pas un code.
2. $|Y| \leq |X| - 1$
3. $X \neq Y$

Preuve

- $2 \Rightarrow 3$ par différence de cardinalité.
- $3 \Rightarrow 1$ par $\neg 1 \Rightarrow \neg 3$. Supposons que X est un code, donc $\langle X \rangle$ est libre de base X. Or $\langle X \rangle$ est le plus petit sous-monoide contenant X, donc c'est aussi le plus petit sous-monoide libre contenant X, donc $\langle X \rangle = L$, donc $X = Y$ par unicité de la base.
- $1 \Rightarrow 2$ sur la prochaine diapo.

Théorème du défaut (II)

Soit X une partie finie de Σ^* et soit L son enveloppe libre, de base Y. Si X n'est pas un code, alors $|Y| \leq |X| - 1$.

Preuve (fin sur la diapo suivante)

- Soit $f : X \setminus \{\epsilon\} \to Y$ qui à $x \in X$ associe y_1 de la décomposition de $x = y_1 \ldots y_n$ sur Y. (En effet, $x \in X \subseteq L$.)
- Supposons que f n'est pas surjective. Soit donc $y \in Y \setminus f[X]$. Soit $Z := (Y \setminus \{y\})y^* = \{zy^i \mid z \in Y \setminus \{y\} \wedge i \in \mathbb{N}\}$. Donc $\langle Z \rangle \subsetneq \langle Y \rangle = L$. De plus, $X \subseteq \langle Z \rangle$, par décomposition $z_1 y^{i_1} \ldots z_n y^{i_n}$.
- Montrons que Z est un code. Soient $z_1 y^{i_1}, \ldots, z_n y^{i_n}, t_1 y^{j_1}, \ldots, t_p y^{j_p} \in Z$ tels que $z_1 y^{i_1} \ldots z_n y^{i_n} = t_1 y^{j_1} \ldots t_p y^{j_p}$. Or Y est un code et les $z_k, t_k \in Y \setminus \{y\}$, donc $(z_1, \ldots, z_n) = (t_1, \ldots t_p)$ (d'où $n = p$), et $i_k = j_k$ pour tout $k \leq n$. Ainsi, $z_k y^{i_k} = t_k y^{j_k}$ pour tout $k \leq n$.
- Donc $\langle Z \rangle$ est un sous-monoïde libre, ce qui contredit la minimalité de $\langle Y \rangle = L$. Ainsi, f est surjective.

Théorème du défaut (II)

Soit X une partie finie de Σ^* et soit L son enveloppe libre, de base Y. Si X n'est pas un code, alors $|Y| \leq |X| - 1$.

Fin de la preuve (de $1 \Rightarrow 2$)

- $f : X \setminus \{\epsilon\} \to Y$, qui à $x \in X$ associe y_1 de la décomposition de $x = y_1 \dots y_n$ sur Y, est surjective. Donc $|Y| \leq |X \setminus \{\epsilon\}|$.
- Si $\epsilon \in X$, on obtient directement $|Y| \leq |X| - 1$. Sinon, on a juste $|Y| \leq |X|$.
- Par hypothèse, X n'est pas un code, donc il existe $x_1, \dots, x_n, x'_1, \dots x'_p \in X$ tels que $x_1 \dots x_n = x'_1 \dots x'_p$ bien que $x_1 \neq x'_1$.
- Comme $x_1 \dots x_n = x'_1 \dots x'_p$ se décomposent de la même façon sur Y, on a $f(x_1) = f(x'_1)$, donc f n'est pas injective (tout en étant surjective). Par finitude de X cela montre $|Y| \leq |X| - 1$.

Monoïdes, monoïdes libres et congruence

Proposition

Tout monoïde est le quotient d'un monoïde libre par une congruence.

Soit un monoïde $(M, \star, e_M)$. Soit la relation binaire $\sim$ sur M^* définie par $x_1 \dots x_n \sim y_1 \dots y_p$ ssi $x_1 \star \dots \star x_n = y_1 \star \dots \star y_p$. C'est une congruence, car $x_1 \star \dots \star x_n = x = y = y_1 \star \dots \star y_p$ implique $u \star x \star w = u \star y \star w$. Soit

$$\begin{array}{rrl} f: & (M, \star, e_M) & \to (M^*, \cdot, \epsilon)/\sim \\ & x & \mapsto [x] \end{array}$$

- f est injective : soit $x, y \in M$ tels que $f(x) = f(y)$. Donc $[x] = [y]$, i.e. $x \sim y$, donc $x = y$ car ce sont des mots de une lettre.
- f est surjective : soient $[w] \in M^*/\sim$ et $x = w_1 \star \dots \star w_{|w|}$. Alors $f(x) = [x] = [w]$.
- $f(e_M) = [e_M]$ (et $\epsilon \sim e_M$)
- $\forall x, y \in M$, $f(xy) = [xy] = [x][y] = f(x)f(y)$. ($\sim$ congruence)