1 Mots et langages

On introduit dans ce paragraphe quelques définitions, propriétés et notations concernant les mots et les langages.

Définition

On appelle vocabulaire (ou alphabet) un ensemble fini quelconque Σ. Les éléments d'un vocabulaire sont appelés lettres, caractères ou symboles.

Exemple

Le biologiste intéressé par l'étude de l'ADN utilisera un alphabet à quatre lettres $\{A, C, G, T\}$ pour les quatre constituants des gènes: Adénine, Cytosine, Guanine et Thymine.

Définition

• Soit Σ un alphabet, un mot sur Σ est une suite finie de symbole. Par exemple, 00110 et 110 sont deux mots sur l'alphabet $\{0, 1\}$. La longueur d'un mot w est le nombre de symboles constituant ce mot, on le note $|w|$. Ainsi, $|00110| = 5$ et $|110| = 3$.

L'unique mot de longueur 0 est le mot correspondant à la suite vide. Ce mot s'appelle le mot vide et on le note 1, ou bien ϵ.

L'ensemble des mots sur Σ est noté Σ^*.Par exemple
$\{0, 1, 2\}^* = \{\epsilon, 0, 1, 2, 00, 01, 02, 11, 12, 20, 21, 22, 000, 001, ...\}$ (ϵ est le mot vide).

• Si σ est une lettre de l'alphabet Σ, pour tout mot $w = a_1 a_2 ... a_k$ de Σ^*, on note par :

$$|w|_\sigma = card\,\{i \in \{1, 2, ..., k\} : a_i = \sigma\}.$$

le nombre d'occurrences de la lettre σ dans le mot w et $w(i)$ sa i-ème lettre. Par exemple $|00110|_0 = 3$ et $|00110|_1 = 2$, $00110\,(1) = 0$, $00110\,(4) = 1$.

Proposition

Soit Σ un alpabet,

1. l'ensemble Σ^* est infini.

2. l'ensemble Σ^* est dénombrable.

Démonstration

1. l'ensemble Σ^* est infini, en effet on a $\Sigma^* = \bigcup\limits_{n=0}^{+\infty} \Sigma^n = \Sigma^0 \cup \Sigma ... \Sigma^n \cup ....$

2. On montre que Σ^* est dénombrable. Comme Σ est fini, on peut donc numéroter ses éléments, par exemple, si $\Sigma = \{\alpha, \beta, \gamma\}$, alors $n\,(\alpha) = 1, n\,(\beta) = 2, n\,(\gamma) = 3$. Ensuite, soit u un mot de Σ^*, on considère les longueurs $|u|$ premiers nombres premiers, par exemple si $|u| = 5$, on a les 5 premiers nombres premiers sont $p(1) = 2, p(2) = 3, p(3) = 5, p(4) = 7, p(5) = 11$. On forme le nombre $f\,(u) = \prod\limits_{i=1}^{i=|u|} p(i)^{n(u(i))}$, où $u\,(i)$ désigne la ième lettre de u. Par exemple si $u = \alpha\gamma\beta\alpha\alpha$, alors
$f\,(u) = \prod\limits_{i=1}^{i=|u|} p(i)^{n(u(i))} = \prod\limits_{i=1}^{i=5} p(i)^{n(u(i))} = 2^1 \times 3^3 \times 5^2 \times 7^1 \times 11^1$. Donc on peut définir une application

$f : \Sigma^* \longrightarrow \mathbb{N}, u \longmapsto f(u) = \prod_{i=1}^{i=|u|} p(i)^{n(u(i))}$. Par l'unicité de la décomposition d'un entier en facteurs premiers, l'application f est injective. Enfin, comme f est injective et l'ensemble $\mathbb{N}$ est dénombrable, alors Σ^* est dénombrable.

Définition

La concaténation est l'opération qui associe à deux mots u et v le mot noté $u.v$ ou uv défini par: si $u = \alpha_1\alpha_2...\alpha_n$ et $v = \beta_1\beta_2...\beta_p$, alors $uv = \gamma_1\gamma_2...\gamma_{n+p}$ avec $\gamma_i = \alpha_i$ pour $i = 1, ...n$ et $\gamma_{n+i} = \beta_i$ pour $i = 1, ...p$. Par exemple, la concaténation des mots 00011 et 011 donne le mot 00011011. On vérifie facilement que la concaténation est une opération associative admettant le mot vide comme élément neutre :

$$\forall x, y, z \in \Sigma^* : (xy)z = x(yz).$$
$$\forall x \in \Sigma^* : x\epsilon = \epsilon x = x.$$

Propriété

Soit Σ un alphabet quelconque le monoïde Σ^* possède les deux propriétés suivantes:

1. tout élément de Σ^* est une suite finie d'éléments de Σ.

2. deux suites distinctes d'éléments de Σ définissent deus éléments distincts de Σ^*.

La propriété (1) distingue le monoïde Σ^* par exemple du monoïde $(\Sigma \cup \{\sigma\})^*$, avec $\sigma \notin \Sigma$.

La propriété (2) distingue le monoïde $\{\alpha, \beta\}^*$ par exemple du monoïde commutatif M obtenu en postulant que l'opération de concaténation est commutative: les deux mots $\alpha\beta$ et $\beta\alpha$ définissent alors le même élément de M.

Σ^* est le seul monoïde satisfaisant les propriétés (1) et (2), on dit que Σ^* est le monoïde libre sur Σ. On dit que Σ est une base de Σ^*.

Propriété

Soient t, u, v, w quatre mots de monoïde libre Σ^*.

1. Si $tu = vw$ et $|t| \leq |v|$ alors il existe un unique mot z de Σ^* tel que $v = tz$ et $u = zw$.
2. Si $uv = wt$ et $|u| = |w|$ alors $u = w$ et $v = t$.
3. Pour tout $i \in \mathbb{N} - \{0\}, (u^i = v^i \Rightarrow u = v)$.
4. Le monoïde libre Σ^* est simplifiable, c'est à dire,

$$4.1\ uv = uw \Rightarrow v = w;$$
$$4.2\ uv = wv \Rightarrow u = w;$$
$$4.1\ uvw = utw \Rightarrow v = t.$$

5. Les propositions suivantes sont équivalentes:

5.1 $uv = vu$,

5.2 Il existe deux entiers n et m non tous deux nuls tels que $u^n = v^m$,

5.3 Il existe un mot z et deux entiers p et q tels que $u = z^p$ et $v = z^q$.

Définition
Un langage sur un alphabet Σ est simplement un ensemble (fini ou infini) de mots sur Σ. En d'autres termes, un langage est une partie de Σ^*. On distingue en particulier le langage vide $\emptyset$ qui ne contient aucun mot.
Définition
Soient $L, M \subseteq \Sigma^*$, deux langages. La concaténation des langages L et M est le langage,

$$LM = \{uv, u \in L, v \in M\}$$

En particulier, on peut définir la puissance $n - ième$ d'un langage L, $n > 0$, par:

$$L^n = \{w_1 w_2 ... w_n, \forall i \in \{1, 2...n\}\, w_i \in L\}.$$

Et on pose $L^0 = \{\epsilon\}$.
Exemple
Soient les deux langages $L = \{u \in \Sigma^* : |u| \text{ est paire}\}$ *et* $K = \{u \in \Sigma^* : |u| \text{ est impaire}\}$.
On a alors les égalités suivantes:
$LK = KL = K$.
$LL = L$.
$KK = L \setminus \{\epsilon\}$.
Définition
On dit qu'un mot $u \in \Sigma^*$ est facteur de $w \in \Sigma^*$ s'il existe deux mots $f, g \in \Sigma^*$ tel que $w = fug$.
Exemple
Soit l'alphabet $\Sigma = \{a, b, c\}$, et le mot $w = aabc$, alors ab est un facteur de w, mais ac ne l'est pas.
Définition
Soit L est un langage sur un alphabet Σ. La congruence syntaxique de L notée $\equiv_L$ est définie par,
pour tous $u, v \in \Sigma^*, (u \equiv_L v) \Longleftrightarrow (\forall x, y \in \Sigma^*, xuy \in L \Longleftrightarrow xvy \in L)$.

2 Homomorphisme des monoïdes

Dans ce paragraphe, nous donnerons quelques propriétés sur la notion d'un homomorphisme de monoïdes.

Définition
Soient $(M, \cdot, 1_M)$, $(M', \cdot', 1_{M'})$ deux monoïdes. Une application $\varphi : M \longrightarrow K$ est un morphisme (ou encore homomorphisme) de monoïdes si:

- $\forall x, y \in M : \varphi(x \cdot y) = \varphi(x) \cdot' \varphi(y)$,
- $\varphi(1_M) = 1_{M'}$.

Un isomorphisme de monoïdes est un homomorphisme bijectif de monoïdes.
Exemple

L'application longueur $|.| : \Sigma^* \longrightarrow \mathbb{N}$ est un morphisme de monoïdes entre $(\Sigma^*, .)$ et $(\mathbb{N}, +)$. En effet,

$$\forall u, v \in \Sigma^* : |uv| = |u| + |v| \text{ et } |\epsilon| = 0.$$

Exemple

Soit $\Sigma = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ un alphabet, $n \in \mathbb{N} \setminus \{0, 1\}$.

La fonction de Parikh $\Psi : \Sigma^* \longrightarrow \mathbb{N}^n,\ \Psi(w) = (|w|_{\alpha_1}, ..., |w|_{\alpha_n})$,

est un morphisme de monoïdes entre $(\Sigma^*, .)$ et $(\mathbb{N}^n, +)$.

Exemple

Soit $\Sigma = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ un alphabet, $n \in \mathbb{N} \setminus \{0, 1\}$.

Et soit $\lambda : \Sigma \longrightarrow \mathbb{N},\ \alpha_i \longmapsto \lambda(\alpha_i)$. On définit $\widetilde{\lambda} : \Sigma^* \longrightarrow \mathbb{N}$ comme suit:

$$\widetilde{\lambda}(w) = \sum_{i=1}^{i=n} \lambda(\alpha_i) \, |w|_{\alpha_i}.$$

$\widetilde{\lambda}$ est un homomorphisme de monoïdes.

Et si $\forall 1 \leq i \leq n,\ \lambda(\alpha_i) = 1$, alors $\widetilde{\lambda} = |.|$ (le morphisme de longueur).

La proposition suivante justifie le fait que le monoïde Σ^* soit appelé monoïde libre.

Cette propriété caractérise le monoide libre engendré par Σ.

Proposition

Toute fonction $\mu : \Sigma \longrightarrow M$ de Σ dans un monoïde M se prolonge de façon unique en un morphisme de Σ^* dans M.

Démonstration

L'esistence: Posons

$\widetilde{\mu}(\epsilon) = e_M$ *et* $\widetilde{\mu}(\alpha_1\alpha_2...\alpha_n) = \mu(\alpha_1)\mu(\alpha_2)...\mu(\alpha_n),\ n \in \mathbb{N},\ \alpha_i \in \Sigma,\ 1 \leq i \leq n.$

Et facile de voir que $\widetilde{\mu}$ est bien un homomorphisme

Unicité: Soient $\widetilde{\mu}$ et $\widetilde{\lambda}$ deux homomorphismes de A^* dans M tels que:

$\forall \alpha \in A, \widetilde{\mu}(\alpha) = \widetilde{\lambda}(\alpha)$

Alors $\widetilde{\mu}(1) = \widetilde{\lambda}(1) = e_M$ et pour tout mot $w = \alpha_1\alpha_2...\alpha_n$

On a $\widetilde{\mu}(w) = \widetilde{\mu}(\alpha_1\alpha_2...\alpha_n) = \mu(\alpha_1)\mu(\alpha_2)...\mu(\alpha_n) = \widetilde{\lambda}(\alpha_1\alpha_2...\alpha_n) = \widetilde{\lambda}(w)$. $\square$

Définition

Un morphisme entre deux monoïdes libres Σ^* et Δ^* est une application $\psi : \Sigma^* \longrightarrow \Delta^*$ qui satisfait:

$$\psi(xy) = \psi(x)\psi(y) \quad \forall x, y \in \Sigma^*.$$

Notons que cet morphisme ψ est complètement déterminé ayant les images des lettres de Σ dans Δ^*, i. e, $\psi(\sigma)$ pour tout σ appartenant à Σ. Nous dirons que le morphisme ψ est non trivial s'il existe au moins une lettre $\sigma \in \Sigma$ pour laquelle $\psi(\sigma) \neq \epsilon$.

En fait remarquer que la propriété $\psi(xy) = \psi(x)\psi(y)$ implique $\psi(\epsilon) =\epsilon$.
Définition
1. Une relation binaire $\mathcal{R}$ sur un ensemble Σ^* est noethérienne s'il n'existe pas une chaine infinie d'éléments de Σ^* en relation par $\mathcal{R}$, en d'autres mots il n'existe pas une suite infinie $(w_n)_{n\in\mathbb{N}}$ d'éléments de Σ^* tel que, pour tout entier naturel n, on a $w_n\mathcal{R}w_{n+1}$.

2. Un ordre sur un ensemble Σ^* est bien fondé s'il ne contient pas de suite infini d'éléments de Σ^* strictement décroissante.
3. La partie strict d'une relation d'ordre bien fondé $\geq$ noté $>$ et définie par: $x > y$ si $x \geq y$ et $x \neq y$.
Exemples
1. La relation $\mathcal{R}_1$ définie sur $\mathbb{N}$ par $x\mathcal{R}_1y \Longleftrightarrow y = x + 1$ est bien fondé.
2. La relation $\mathcal{R}_2$ définie sur $\mathbb{N}$ par $x\mathcal{R}_2y \Longleftrightarrow x$ divise y et $x \neq y$ est bien fondé.
3. La relation usielle $\geq$ est un ordre bien fondé sur l'ensemble des entiers $\mathbb{N}$.
Proposition
1. Soit $h : \Sigma^* \longrightarrow \Gamma^*$ un morphisme, la congruence associée à h, notée $\equiv_h$, est définie par :
pour tous $u, v \in \Sigma^*, u \equiv_h v \Longleftrightarrow h(u) = h(v)$.
2. Soit $\mathcal{R}$ une relation sur Σ^* qui vérifie $h(r) = h(s)$ pour tout $(r, s) \in \mathcal{R}$, alors il existe un unique morphisme $\psi : \Sigma^*/ \underset{\mathcal{R}}{\overset{*}{\longleftrightarrow}} \longrightarrow \Gamma^*$ tel que $\psi \circ p = h$ où $\underset{\mathcal{R}}{\overset{*}{\longleftrightarrow}}$ est la congruence engendré par $\mathcal{R}$ et p est la surjection canonique.
3. Soient P et $P^{'}$ deux partitions de monoïde libre Σ^*, on dit que P est plus fine que $P^{'}$ si: $\forall p \in P, \exists p' \in P'$ tel que $p \subseteq p'$. Dans ce cas on dit que P est plus fine que P' ou bien P' est plus grossière que P.

3 Système de réécriture de mots

4 Définitions et propriétés

Définition
Un semi-système de réécriture de mots, dit aussi semi-système de Thue, est un couple $(\Sigma, \mathcal{R})$ où Σ un alphabet fini et $\mathcal{R}$ une relation binaire sur le monoïde libre Σ^*. Tout élément (α, β) de $\mathcal{R}$ est appelé règle de réécriture qu'on note $\alpha{\longrightarrow}\beta$, avec α est sa partie gauche et β sa partie droite. Des règles $\alpha{\longrightarrow}\beta_1, \alpha{\longrightarrow}\beta_2, ..., \alpha{\longrightarrow}\beta_k$ ayant même partie gauche sont souvent notées $\alpha{\longrightarrow}\beta_1 \setminus \beta_2 \setminus ... \setminus \beta_k$.
Exemple
Soient $\Sigma = \{\alpha, \beta, \gamma\}$ et $\mathcal{R} = \{\alpha\beta{\longrightarrow}\beta\alpha, \beta\alpha{\longrightarrow}\alpha\beta, \gamma{\longrightarrow} \epsilon, \epsilon {\longrightarrow}\gamma\}$, $(\Sigma, \mathcal{R})$ est un système de réécriture.
Définition
Appliquer une règle quelconque $u{\longrightarrow}v$ de $\mathcal{R}$ à un mot w contenant le facteur u consiste à remplacer u par v dans w. S'il n'y a aucune règle de $(\Sigma, \mathcal{R})$ applicable

à w, alors w est dit irréductible ou sous la forme normale. Etant données deux mots $w_1, w_2 \in \Sigma^*$, on dit que w_2 dérive directement de w_1, et on note $w_1 \underset{\mathcal{R}}{\Rightarrow} w_2$, si et seulement si, il existe une règle $u \longrightarrow v$ de $\mathcal{R}$ et $x, y \in \Sigma^*$ tels que: $w_1 = xuy$ et $w_2 = xvy$. On dit que w_2 dérive de w_1, et on note $w_1 \overset{*}{\underset{\mathcal{R}}{\Rightarrow}} w_2$, s'il existe une suite finie de mots $u_0, u_1, ..., u_n$ de Σ^* avec, $u_0 = w_1, u_i \underset{\mathcal{R}}{\Rightarrow} u_{i+1}, \forall 0 \leq i \leq n-1$ et $u_n = w_2$. Notons que la relation $\overset{*}{\underset{\mathcal{R}}{\Rightarrow}}$ est la fermeture réflexive et transitive de $\underset{\mathcal{R}}{\Rightarrow}$.

Exemples

1. Soient $\Sigma_1 = \{0, 1\}$ et $\mathcal{R}_1 = \{10 \longrightarrow 01\}$. Soient $w_1, w_2 \in \Sigma_1^*$, si $w_1 \overset{*}{\underset{\mathcal{R}_1}{\Rightarrow}} w_2$, alors w_2 est la permutation des lettres de w_1 où tous les 0 seront avant les 1. Ce semi-système de réécriture trie les mots constitués de même chiffres binaires.

2. Soient $\Sigma_2 = \{0, 1, +\}$ et $\mathcal{R}_2 = \{0 + 0 \longrightarrow 0, 0 + 1 \longrightarrow 1, 1 + 0 \longrightarrow 1, 1 + 1 \longrightarrow 0\}$.

Ce semi-système de réécriture calcul la somme (*modulo* 2) d'une suite d'entiers binaires.

3. Soient $\Sigma_3 = \{0, 1, +, E\}$ et $\mathcal{R}_3 = \{E \longrightarrow 0, E \longrightarrow 1, E \longrightarrow E + E\}$. Pour tout $w \in \{0, 1, +\}^*$, on a $E \overset{*}{\underset{\mathcal{R}_3}{\Rightarrow}} w$ si, et seulement si w est une expression construite avec les 0 et 1 et l'opérateur $+$.

4. Considérons le semi-système de réécriture sur la dérivation symbolique par rapport à x défini par:

$$\mathcal{R}_4 = \left\{ \begin{array}{c} D_x x \longrightarrow 1, D_x a \longrightarrow 0, D_x(y+z) \longrightarrow D_x y + D_x z, D_x(y*z) \longrightarrow z * D_x y + y * D_x z, \\ D_x(y-z) \longrightarrow D_x y - D_x z, D_x(-y) \longrightarrow - D_x y, D_x(y/z) \longrightarrow z * D_x y - y * D_x z)/z^2 \end{array} \right\}.$$

où a étant un symbole de constante.

Définition

Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture . Si un mot $u \in \Sigma^*$ peut se réécrire de manière non triviale, on dit qu'il est réductible. Dans le cas contraire, il est dit irréductible. On note alors $IRR(\mathcal{R})$ l'ensemble des éléments irréductibles de Σ^*.

Exemples

Soient $\Sigma = \{\alpha, \beta\}$ et $\mathcal{R} = \{\alpha\beta \longrightarrow \beta\alpha\}$. L'ensemble des mots irréductibles est

$$IRR(\mathcal{R}) = \{\beta^n \alpha^m : n, m \in \mathbb{N}\}.$$

Les mots irréductibles sont en effet les éléments de Σ^* qui ne contiennent pas $\alpha\beta$.

Définition

Soient $S_1 = (\Sigma_1, \mathcal{R}_1)$ et $S_2 = (\Sigma_2, \mathcal{R}_2)$ deux semi-systèmes de réécriture. Un morphisme de semi-systèmes de réécriture de S_1 vers S_2 est une application $\psi : \Sigma_1^* \longrightarrow \Sigma_2^*$ qui faiblement compatible avec les relations de réductions, c'est-à-dire telle que $\psi(\underset{\mathcal{R}_1}{\Rightarrow}) \subseteq \overset{*}{\underset{\mathcal{R}_2}{\Rightarrow}}$, ou encore telle que, pour tous $x, y \in \Sigma_1^*$ vérifiant $x \underset{\mathcal{R}_1}{\Rightarrow} y$, on a $\psi(x) \overset{*}{\underset{\mathcal{R}_2}{\Rightarrow}} \psi(y)$.

Un tel morphisme est dit:

• Non contractant si $\psi(\underset{\mathcal{R}_1}{\Rightarrow}) \subseteq \overset{+}{\underset{\mathcal{R}_2}{\Rightarrow}}$, ce qui équivaut à dire si $x\underset{\mathcal{R}_1}{\Rightarrow}y$, alors $\psi(x)\overset{+}{\underset{\mathcal{R}_2}{\Rightarrow}}\psi(y)$.

• Strict si $\psi(\underset{\mathcal{R}_1}{\Rightarrow}) \subseteq \underset{\mathcal{R}_2}{\Rightarrow}$, ce qui équivaut à dire si $x\underset{\mathcal{R}_1}{\Rightarrow}y$, alors $\psi(x)\underset{\mathcal{R}_2}{\Rightarrow}\psi(y)$.

5 Problème de terminaison et confluence d'un semi-système de réécriture de mots

Nous allons présenter ici deux propriétés de semi-système de réécriture telles que: la terminaison et la confluence, si un semi-système de réécriture termine, cela signifie qu'il est impossible, partant d'un certain élément, d'effectuer une infinité d'opérations de dérivation quel que soit le point de départ, on arrivera, après un nombre fini d'opérations, à un élément sur lequel on ne peut plus agir, c'est-à-dire un élément x tel qu'il n'existe pas de y vérifiant $x\underset{\mathcal{R}}{\Rightarrow}y$. Et dans un semi-système de réécriture confluent, les choix effectués n'ont pas d'importance.

Définition

On dit qu'un semi-système de réécriture $(\Sigma, \mathcal{R})$ termine ou qu'il est noethérien s'il n'existe pas de chaine de réécriture infini $w_0\underset{\mathcal{R}}{\Rightarrow}w_1...\underset{\mathcal{R}}{\Rightarrow}w_n\underset{\mathcal{R}}{\Rightarrow}...$

Exemples

Le semi-système de réécriture $(\Sigma_1, \mathcal{R}_1)$, avec $\Sigma_1 = \{\alpha, \beta\}$ et la relation $\mathcal{R}_1 = \{\alpha \longrightarrow \alpha\beta\}$, est non noethérien car la dérivation $\alpha\underset{\mathcal{R}_1}{\Rightarrow}\alpha\beta\underset{\mathcal{R}_1}{\Rightarrow}\alpha\beta\beta\underset{\mathcal{R}_1}{\Rightarrow}\alpha\beta\beta\beta\underset{\mathcal{R}_1}{\Rightarrow}...$ est bien infini dans $(\Sigma_1, \mathcal{R}_1)$. De même le semi-système de réécriture $(\Sigma_2, \mathcal{R}_2)$, avec $\Sigma_2 = \{\alpha, \beta\}$ et la relation $\mathcal{R}_2 = \{\alpha \longrightarrow \beta, \beta \longrightarrow \alpha\}$, est non noethérien car la dérivation $\alpha\underset{\mathcal{R}_2}{\Rightarrow}\beta\underset{\mathcal{R}_2}{\Rightarrow}\alpha\underset{\mathcal{R}_2}{\Rightarrow}\beta\underset{\mathcal{R}_2}{\Rightarrow}...$ est bien infini dans $(\Sigma_2, \mathcal{R}_2)$. Par contre le semi-système de réécriture $(\Sigma_3, \mathcal{R}_3)$, avec $\Sigma_3 = \{\alpha, \beta\}$ et la relation $\mathcal{R}_3 = \{\alpha\beta \longrightarrow \alpha\}$, est noethérien, car la seule règle $(\alpha\beta, \alpha)$ est applicable à un mot w de Σ_3^* si, et seulement si, $|w|_{\alpha\beta} \neq 0$, et si $|w|_{\beta} = k$, alors pas plus de k dérivations le processus de substitution termine.

Définition

Soient $(\Sigma, \mathcal{R})$ un semi-système de réécriture et deux mots $u, v \in \Sigma^*$. S'il existe $w \in \Sigma^*$ tel que $u\underset{\mathcal{R}}{\Rightarrow}w$ et $v\underset{\mathcal{R}}{\Rightarrow}w$, alors on dit que u et v sont joignables. On désignera par $u{\downarrow}v$ l'ensemble de tous les éléments $w \in \Sigma^*$ tels que $u\underset{\mathcal{R}}{\Rightarrow}w$ et $v\underset{\mathcal{R}}{\Rightarrow}w$. (Ainsi, u et v sont joignables si, et seulement si $u{\downarrow}v \neq \emptyset$.

Exemple

soient $\Sigma = \{\alpha, \beta\}$ et $\mathcal{R} = \{\alpha\beta \longrightarrow \beta\alpha\}$, $u = \alpha\beta\beta\alpha$ et $v = \beta\alpha\alpha\beta$, on a $\alpha\beta\beta\alpha\underset{\mathcal{R}}{\Rightarrow}\beta\alpha\beta\alpha$ et $\beta\alpha\alpha\beta\underset{\mathcal{R}}{\Rightarrow}\beta\alpha\beta\alpha$, donc u et v sont joignables et $\beta\alpha\beta\alpha \in u{\downarrow}v$.

Théorème

Soit $(\Sigma_1, \mathcal{R}_1)$ un semi-système de réécriture. Les assertions suivantes sont équivalentes:

1. $(\Sigma_1, \mathcal{R}_1)$ est noethèrien.

2. Il existe un ordre strict $>$ sur Σ_1^* tel que $(\Sigma_1^*, >)$ termine et tel que si $x \underset{\mathcal{R}_1}{\Rightarrow} y$ alors $x > y$.

3. Il existe un autre semi-système de réécriture $(\Sigma_2, \mathcal{R}_2)$ qui termine ainsi qu'un morphisme

Définition

Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture. On dit que le principe de récurrence est vrai dans $(\Sigma, \mathcal{R})$ si, pour toute propriété P définie sur Σ^*, on a,

si pour tout $x \in \Sigma^*$, le fait que $P(y)$ soit vraie pour tous les $y \in \Sigma^*$ tels que $x \overset{+}{\underset{\mathcal{R}}{\Rightarrow}} y$ implique que $P(x)$ est vraie, alors $P(x)$ est vraie pour tout $x \in \Sigma^*$, en symboles,

$$(\forall x \in \Sigma^*, \forall y \in \Sigma^* : \left(P(x) \text{ et } x \overset{+}{\underset{\mathcal{R}}{\Rightarrow}} y\right) \Rightarrow P(x)) \Rightarrow (\forall x \in P(x)).$$

Théorème

Un semi-système de réécriture $(\Sigma, \mathcal{R})$ est noethèrien si, et seulement si le principe de récurrence est vraie dans $(\Sigma, \mathcal{R})$.

Définition

Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture. Un branchement de $(\Sigma, \mathcal{R})$ est un triplet (x, y, z) d'éléments de Σ^* tels que $x \overset{*}{\underset{\mathcal{R}}{\Rightarrow}} y$ et $x \overset{*}{\underset{\mathcal{R}}{\Rightarrow}} z$, x est appelé la source d'un tel branchement. On dit qu'un branchement (x, y, z) est local si $x \underset{\mathcal{R}}{\Rightarrow} y$ et $x \underset{\mathcal{R}}{\Rightarrow} z$. Un branchement (x, y, z) est dit confluent s'il existe un $w \in \Sigma^*$ tel que $y \overset{*}{\underset{\mathcal{R}}{\Rightarrow}} w$ et $z \overset{*}{\underset{\mathcal{R}}{\Rightarrow}} w$. On dit d'un tel w qu'il ferme le branchement(x, y, z).

Définition

On dit qu' un semi-système de réécriture est confluent (resp. localement confluent) si tous ses branchement(resp. branchements locaux) sont confluents. On dit aussi que la relation binaire $\mathcal{R}$ est (localement) confluente.

Exemple

On considère le semi-système de réécriture $(\Sigma, \mathcal{R})$ où $\Sigma = \{\alpha, \beta\}$, $\mathcal{R} = \{\alpha\beta \longrightarrow \alpha, \beta\alpha \longrightarrow \beta\}$.

Ce système n'est pas confluent, car on a:

$\alpha\beta\alpha \overset{*}{\underset{\mathcal{R}}{\Rightarrow}} \alpha\beta \overset{*}{\underset{\mathcal{R}}{\Rightarrow}} \alpha$ et $\alpha\beta\alpha \overset{*}{\underset{\mathcal{R}}{\Rightarrow}} \alpha\alpha$, mais les mots $\alpha\alpha, \alpha$ sont en formes normaux.

Proposition

Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture.

1. Pour tout (x, y) de $\mathcal{R}$, le branchement (x, y, y) est confluent

2. Si (x, y, z) est un un branchement confluent, alors

• pour tout mot u de Σ^*, les deux branchement $(ux, u\mathrm{y}, uz)$ et (xu, yu, zu) sont confluents.

• pour tous mots u, v de Σ^*, le branchement $(uxv, u\mathrm{y}v, uzv)$ est confluent.

3. Pour tous $(x, y), (z, t)$ de $\mathcal{R}$, le branchement (xz, yz, xt) est confluent. Dans ce cas on dit que les réductions (xz, yz) et (xz, xt) sont disjointes.

Définition

Un semi-système de réécriture $S = (\Sigma, \mathcal{R})$ est dit convergent ou complet s'il termine et s'il est confluent. On dit aussi que la relation binaire $\mathcal{R}$ est convergente.

Corollaire

Soit $(\Sigma_1, \mathcal{R}_1)$ *un semi-système de réécriture tel que* $\mathcal{R}_1 = \{\alpha_i \longrightarrow \beta_i, 1 \leq i \leq n, n \in \mathbb{N}^*\}$.

Si $\forall 1 \leq i \leq n, |\alpha_i| > |\beta_i|$, *alors le semi-système* $(\Sigma_1, \mathcal{R}_1)$ *est noethérien.*

Corollaire

Soit $\Sigma = \{\sigma_1, \sigma_2, ..., \sigma_n\}$ *un alphabet,* $n \in \mathbb{N} - \{0, 1\}$. *Etant donnée l'application* $\lambda : \Sigma \longrightarrow \mathbb{N}$, $\sigma_i \longmapsto \lambda(\sigma_i)$. *On définit l'application* $\widetilde{\lambda} : \Sigma^* \longrightarrow \mathbb{N}$ *comme suit:* $\widetilde{\lambda}(w) = \sum_{i=1}^{i=n} \lambda(\sigma_i) \, |w|_{\sigma_i}$. *L'application* $\widetilde{\lambda}$ *est bien un morphisme de monoïdes.*

Soit $(\Sigma_1, \mathcal{R}_1)$ *un semi-système de réécriture avec* $\mathcal{R}_1 = \left\{\alpha_j \longrightarrow \beta_j, 1 \leq j \leq m; m \in \mathbb{N}^*\right\}$.

Si pour tout $1 \leq j \leq m : \widetilde{\lambda}(\alpha_j) > \widetilde{\lambda}(\beta_j)$, *alors* $(\Sigma_1, \mathcal{R}_1)$ *est noethérien.*