Panorama sur les variétés

Jean-Éric Pin

LIAFA, CNRS et Université Paris 7

29 janvier 2007, Paris

Outline

(1) Fermeture polynomiale
(2) Retour sur la logique
(3) Hiérarchies de concaténation

Première partie I

Fermeture polynomiale

Fermeture polynomiale d'une classe $\mathcal{C}$ de langages

La fermeture polynomiale de $\mathcal{C}$ est la classe des unions de produits de la forme $L_0a_1L_1a_2\cdots a_kL_k$ où $L_0,\ldots,L_k \in \mathcal{C}$ et $a_1,\ldots,a_k$ sont des lettres.

Un produit $L_0a_1L_1a_2\cdots a_kL_k$ est non-ambigu si chaque mot du produit admet une décomposition unique de la forme $u_0a_1u_1\cdots a_ku_k$, avec $u_0 \in L_0$, $\ldots$, $u_k \in L_k$.

La fermeture polynomiale non-ambiguë de $\mathcal{C}$ est la classe des unions de produits non-ambigus de la forme $L_0a_1L_1a_2\cdots a_kL_k$ où $L_0,\ldots,L_k \in \mathcal{C}$ et $a_1,\ldots,a_k$ sont des lettres.

Morphismes relationnels

Soient M et N des monoïdes. Un morphisme relationnel de M dans N est une application $\tau : M \to \mathcal{P}(N)$ telle que :

(1) Pour tout $s, t \in M$, $\tau(s)\tau(t) \subseteq \tau(st)$

(2) Pour tout $s \in M$, $\tau(s)$ est non vide

(3) $1 \in \tau(1)$

Produit de Mal'cev

Soit $\mathbf{V}$ une variété de monoïdes et $\mathbf{W}$ une variété de semigroupes [ordonnés]. Le produit de Mal'cev $\mathbf{W} Ⓜ \mathbf{V}$ est la classe de tous les monoïdes [ordonnés] M tels qu'il existe un morphisme relationnel

$$\tau : M \to N$$

avec $N \in \mathbf{V}$ et $\tau^{-1}(e) \in \mathbf{W}$ pour tout idempotent e de N.

Exemples :

$\mathbf{J} = \mathbf{Nil} Ⓜ \mathbf{J}_1, \quad \mathbf{R} = [es = e] Ⓜ \mathbf{J}_1, \quad \mathbf{DA} = \mathbf{LI} Ⓜ \mathbf{J}_1.$

Fermeture polynomiale d'un variété

Soit $\mathcal{V}$ une variété de langages et soit $\mathbf{V}$ la variété de monoïdes correspondante. On note Pol $\mathcal{V}$ la fermeture polynomiale et UPol $\mathcal{V}$ sa fermeture polynomiale non-ambiguë.

Théorème (Pin-Weil 1995 ; Pin 1980)

- *La variété de monoïdes ordonnés correspondant à Pol $\mathcal{V}$ est $[\![ese \leqslant e]\!] \circledM \mathbf{V}$.*
- *La variété de monoïdes correspondant à UPol $\mathcal{V}$ est $[\![ese = e]\!] \circledM \mathbf{V}$.*

Fermeture par produit d'un variété

La fermeture par produit [non ambigu] de $\mathcal{V}$ est la plus petite variété contenant $\mathcal{V}$ qui soit fermée par produit de concaténation [non ambigu].

Théorème (Straubing 1979 ; Pin 1981)

- *La variété de monoïdes correspondant à la fermeture par produit de $\mathcal{V}$ est $A \circledM V$.*
- *La variété de monoïdes correspondant à la fermeture par produit non ambigu de $\mathcal{V}$ est $LI \circledM V$.*

Deuxième partie II

Logique

Logique sur les mots

A chaque mot non vide $u = a_0 \cdots a_{|u|-1}$ on associe une structure

$$\mathcal{M}_u = (\{0, 1, \ldots, |u| - 1\}, <, (\mathbf{a})_{a \in A})$$

où $\mathbf{a}$ est interprété comme l'ensemble des positions i telles que la lettre a_i soit un a, et $<$ est l'ordre usuel sur les entiers.

Si $u = abbaab$, alors $\mathrm{Dom}(u) = \{0, 1, 2, 3, 4, 5\}$, $\mathbf{a} = \{0, 3, 4\}$ et $\mathbf{b} = \{1, 2, 5\}$.

Autres prédicats possibles : S (successeur), P (prédécesseur), $\min$, $\max$, etc.

Quelques exemples

La formule $\exists x \; \mathbf{a}x$ s'interprète ainsi :

Il existe un entier x tel que, dans u,
la lettre en position x est un a.

Ce qui définit le langage A^*aA^*.

La formule $\exists x \; \exists y \; (x < y) \wedge \mathbf{a}x \wedge \mathbf{b}y$ définit le langage $A^*aA^*bA^*$.

La formule $\mathbf{a}\min \; \wedge \; \mathbf{b}S\min$ définit le langage abA^*.

Les questions

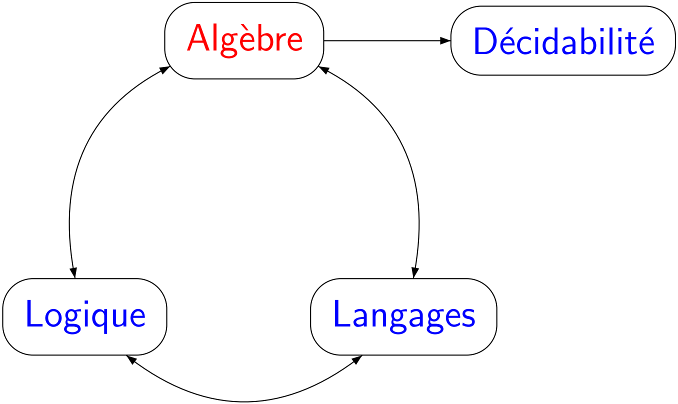
Definition

Une classe de formules $\mathcal{F}$ capture une classe de langages $\mathcal{C}$ si les langages définis par les formules de $\mathcal{F}$ sont exactement les langages de $\mathcal{C}$.

- Quels sont les languages capturés par le premier ordre (resp. le second ordre monadique, le second ordre, etc.) ?

- Peut-on décider si un langage donné est expressible au premier ordre (resp. second ordre, etc.) ?

L'idée principale



Second ordre

Théorème (Stockmeyer 1977)

Le fragment $SO(<)$ capture la hiérarchie polynomiale PH.

Notons $\Sigma_1 SO(<)$ l'ensemble des formules existentielles du second ordre : $\exists R_1 \; \exists R_2 \; \ldots \exists \; R_n \; \varphi$

Théorème (Fagin 1974)

Le fragment $\Sigma_1 SO(<)$ capture NP.

Classes de complexité

Notons TC l'opérateur qui calcule la fermeture réflexive et transitive d'une relation.
Si $\varphi(R_1, \ldots, R_k, S_1, \ldots, S_k)$ est un énoncé définissant une super-relation binaire sur des k-uplets de relations $R_1, \ldots, R_k, S_1, \ldots, S_k$, alors $TC(\varphi)$ définit la fermeture réflexive et transitive de φ. Par exemple, $TC[S(x, y)](u, v)$ est la relation $u \leqslant v$.

Théorème (Immerman 1987)

Le fragment $SO(<) + TC$ capture $PSPACE$.

Second ordre monadique

On peut quantifier sur les sous-ensembles, mais pas sur les relations n-aires pour $n > 0$.

Théorème (Büchi 1960, Elgot 1961)

Le fragment $MSO(<)$ capture les langages rationnels.

Théorème (Meyer 1975)

Il n'y a pas d'algorithme en temps élémentaire pour décider si un énoncé de MSO est vrai ou non.

Premier ordre

Théorème (McNaughton-Papert 1971)

Le fragment $FO(<)$ capture les langages *sans-étoile*.

Corollaire (Schützenberger + McNaughton)

Soit L un langage. Sont équivalents :

(1) *L est définissable au premier ordre,*

(2) *L est sans-étoile,*

(3) *le monoïde syntactique de L est apériodique.*

Complexité du premier ordre

Théorème (Cho-Huynh 1991)

Décider si la langage accepté par un automate fini est sans-étoile est un problème PSPACE-complet.

Nombre restreint de variables

Théorème (Kamp 68, Immerman-Kozen 89)

Trois variables suffisent à exprimer les langages définissables au premier ordre.

Proposition (Folklore)

Le premier ordre à une seule variable capture les langages rationnels dont le monoïde syntactique est idempotent et commutatif. Ces langages sont les combinaisons booléennes des langages A^*aA^*, avec $a \in A$.

Deux variables

Un langage est non ambigu sans étoile s'il est union finie de produits non ambigus $A_0^* a_1 A_1^* \cdots a_k A_k^*$ où $A_0, \ldots, A_k \subseteq A$ et $a_1, \ldots, a_k \in A$.

Théorème (Thérien-Wilke 1998)

Le premier ordre à deux variables capture les langages non ambigus sans étoile.

Théorème (Schützenberger 1975)

Un langage est non ambigu sans étoile ssi son monoïde syntactique est dans DA.

La variété de monoïdes finis DA

Un monoïde fini est dans DA ssi il vérifie l'une des conditions équivalentes suivantes :

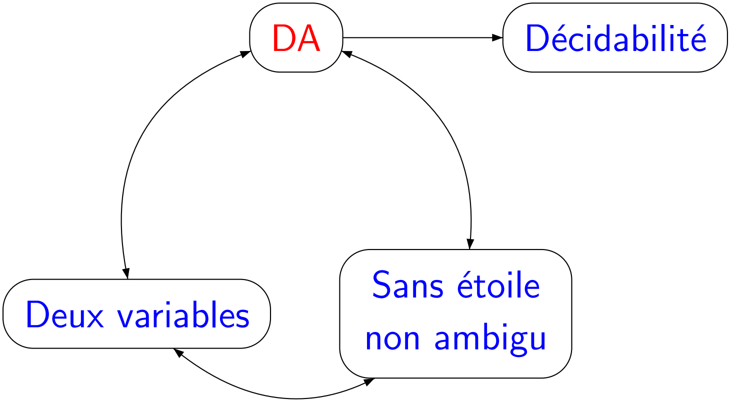
(1) tout élément $\mathcal{J}$-équivalent à un idempotent est lui-même idempotent,

(2) ses $\mathcal{J}$-classes régulières sont des semigroupes idempotents

*	*	*	*
*	*	*	*
*	*	*	*

(3) il satisfait l'identité $(xyz)^\omega y (xyz)^\omega = (xyz)^\omega$.

Résumé pour deux variables



Troisième partie III

Hiérarchies de concaténation

Hiérarchies de concaténation

Soit $\mathcal{C}$ une classe de langages. La hiérarchie de concaténation sur $\mathcal{C}$ est construite par récurrence de la façon suivante :

$\mathcal{C}_0$ est $\mathcal{C}$,

$\mathcal{C}_{n+1/2}$ est la fermeture polynomiale de $\mathcal{C}_n$,

$\mathcal{C}_{n+1}$ est la clôture booléenne de $\mathcal{C}_{n+1/2}$.

Exemples de hierarchies de concatenation

La hiérarchie de Straubing-Thérien : $\mathcal{C}$ est la classe triviale $\{\emptyset, A^*\}$,

La hiérarchie "Dot-depth" : $\mathcal{C}$ est la classe des langages testables par préfixes et suffixes (langages qui sont unions de langages de la forme $PA^*S \cup F$, où P, S et F sont des langages finis),

La hiérarchie des groupes : $\mathcal{C}$ est la classe des langages à groupe (dont le monoïde syntactique est un groupe).

La hiérarchie de Straubing-Thérien

Niveau 0 : $\emptyset$ et A^*.

Niveau $1/2$: union de langages simples (i.e. forme $A^*a_1A^* \cdots A^*a_kA^*$, où a_1, ..., a_k sont des lettres).

Niveau 1 : combinaisons booléennes de langages simples (langages testables par morceaux).

Niveau $3/2$: union de langages de la forme $A_0^*a_1A_1^* \cdots a_kA_k^*$, où chaque A_i est une partie de A et les a_i sont des lettres (Pin-Straubing 1981).

Cett hiérarchie est infinie (Brzozowski-Knast 1978).

Premiers niveaux de la dot-depth

Niveau 0 : langages testables par préfixes et suffixes.

Niveau $1/2$: union de langages de la forme $u_0A^*u_1A^* \cdots A^*u_{k-1}A^*u_k$, où les u_i sont des mots.

Niveau 1 : combinaisons booléennes de langages de la forme $u_0A^*u_1A^* \cdots A^*u_{k-1}A^*u_k$.

Niveau $3/2$: union de langages de la forme $A_0^*a_1A_1^* \cdots a_kA_k^*$, où chaque A_i est une partie de A et les a_i sont des lettres (Pin-Straubing 1981).

Cette hiérarchie est infinie (Brzozowski-Knast 1978).

Les hiérarchies Σ_n, Π_n et Δ_n

On écrit les formules en forme normale prénexe.

Σ_n : Formules $\exists^* \ \forall^* \ \exists^* \ \cdots \varphi$ avec n blocs alternés de quantificateurs.

Π_n : Formules $\forall^* \ \exists^* \ \forall^* \cdots \varphi$ avec n blocs alternés de quantificateurs.

Δ_n : Formules qui sont équivalentes à une Σ_n-formule et à une Π_n-formule.

$\mathcal{B}\Sigma_n$: combinaisons booléennes de Σ_n-formules.

Résultats de décidabilité

Théorème

(1) *Les langages* Σ_n*-définissables forment une variété positive de langages.*

(2) *Les langages* $\mathcal{B}\Sigma_n$*-définissables forment une variété de langages.*

(3) *Les langages* Δ_n*-définissables forment une variété de langages.*

Il reste à identifier les variétés de monoïdes [ordonnés] correspondantes...

Concaténation et hiérarchies logiques (1)

Théorème (Thomas 1982)

(1) *La classe* $\mathcal{B}\Sigma_n[<]$ *capture le niveau* n *de la hiérarchie de Straubing-Thérien.*

(2) *La classe* $\mathcal{B}\Sigma_n[<, \min, \max, S, P]$ *capture le niveau* n *de la hiérarchie dot-depth.*

Concaténation et hiérarchies logiques (2)

Théorème (Thomas 1982, Perrin-Pin 1986)

(1) *La classe* $\Sigma_n[<]$ *capture le niveau* $n - 1/2$ *de la hiérarchie de Straubing-Thérien.*

(2) *La classe* $\Sigma_n[<, \min, \max, S, P]$ *capture le niveau* $n - 1/2$ *de la hiérarchie dot-depth.*

Concaténation et hiérarchies logiques (3)

Théorème (Pin-Weil 1995, 1997)

(1) *La classe* $\Delta_n[<]$ *capture la fermeture polynomiale non-ambiguë du niveau* $n-1$ *de la hiérarchie de Straubing-Thérien.*

(2) *La classe* $\Delta_n[<, \min, \max, S, P]$ *capture la fermeture polynomiale non-ambiguë du niveau* $n-1$ *de la hiérarchie dot-depth.*

Les hiérarchies $FO(<)$ et de Straubing-Thérien

$$
\begin{tikzcd}[column sep=small]
 & \Sigma_1 \arrow[dr, dash] & & & \Sigma_2 \arrow[dr, dash] & & & \Sigma_3 & \cdots \\
\Delta_1 = \mathcal{B}\Sigma_0 \arrow[ur, dash] \arrow[dr, dash] & & \mathcal{B}\Sigma_1 \arrow[r, dash] & \Delta_2 \arrow[ur, dash] \arrow[dr, dash] & & \mathcal{B}\Sigma_2 \arrow[r, dash] & \Delta_3 \arrow[ur, dash] \arrow[dr, dash] & & \\
 & \Pi_1 \arrow[ur, dash] & & & \Pi_2 \arrow[ur, dash] & & & \Pi_3 & \cdots
\end{tikzcd}
$$

$$
\begin{tikzcd}[column sep=small]
 & {[x \leqslant 1]} \arrow[dr, dash] & & & \mathsf{V}_{3/2} \arrow[dr, dash] & & & \mathsf{V}_{5/2} \cdots \\
\mathsf{I} \arrow[ur, dash] \arrow[dr, dash] & & \mathsf{J} \arrow[r, dash] & \mathsf{DA} \arrow[ur, dash] \arrow[dr, dash] & & \mathsf{V}_2 \arrow[r, dash] & \mathsf{LI} \,Ⓜ\, \mathsf{V}_2 \arrow[ur, dash] \arrow[dr, dash] & \\
 & {[1 \leqslant x]} \arrow[ur, dash] & & & \tilde{\mathsf{V}}_{3/2} \arrow[ur, dash] & & & \tilde{\mathsf{V}}_{5/2} \cdots
\end{tikzcd}
$$

$$\mathsf{V}_{3/2} = [ese \leqslant e] \,Ⓜ\, \mathsf{J}_1$$

Le niveau 1 de la hiérarchie de Straubing-Thérien

Théorème (Simon, 1972)

Un langage rationnel est de niveau 1 ssi son monoïde syntactique est $\mathcal{J}$-trivial.

La variété J des monoïdes $\mathcal{J}$-triviaux est décrite par les identités $(xy)^\omega = (yx)^\omega$ et $x^{\omega+1} = x^\omega$.

Exemples de monoïdes $\mathcal{J}$-triviaux

- Le monoïde $\mathcal{C}_n$ des fonctions croissantes et extensives de $\{1, \ldots, n\}$ (fonctions f telles que $i \leqslant j$ entraîne $f(i) \leqslant f(j)$ et $i \leqslant f(i)$).

- Le monoïde $\mathcal{R}_n$ des relations réflexives sur $\{1, \ldots, n\}$. De façon équivalente, $\mathcal{R}_n$ est le monoïde des matrices booléennes $n \times n$ dont toutes les entrées diagonales sont égales à 1.

$$\begin{pmatrix} 1 & \varepsilon_{1,2} & \varepsilon_{1,2} & \cdots & \varepsilon_{1,n} \\ \varepsilon_{2,1} & 1 & \varepsilon_{2,3} & \cdots & \varepsilon_{2,n} \\ \varepsilon_{3,1} & \varepsilon_{3,2} & 1 & \cdots & \varepsilon_{3,n} \\ \vdots & \vdots & & \ddots & \vdots \\ \varepsilon_{n,1} & \varepsilon_{n,2} & \varepsilon_{n,3} & \cdots & 1 \end{pmatrix}$$

Autres exemples de monoïdes $\mathcal{J}$-triviaux

Le sous-monoïde $\mathcal{U}_n$ de $\mathcal{R}_n$ constitué par les matrices unitriangulaires de $\mathcal{R}_n$.

$$\begin{pmatrix} 1 & \varepsilon_{1,2} & \varepsilon_{1,2} & \dots & \varepsilon_{1,n} \\ 0 & 1 & \varepsilon_{2,3} & \dots & \varepsilon_{2,n} \\ 0 & 0 & 1 & \dots & \varepsilon_{3,n} \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

Caractérisation des monoïdes $\mathcal{J}$-triviaux

Théorème (Straubing 1980, Pin 1984)

Soit M un monoïde fini. Sont équivalents :

(1) M *est $\mathcal{J}$-trivial,*

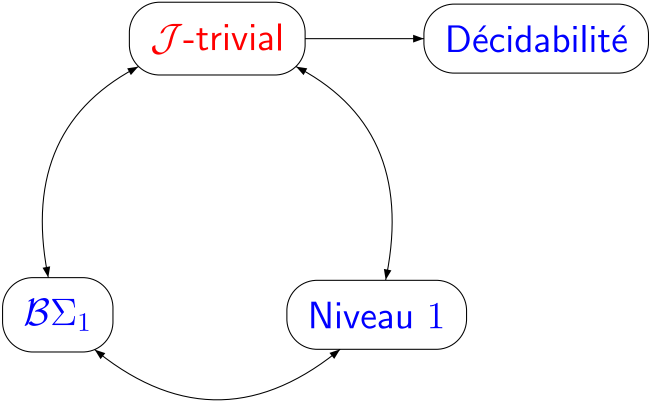
(2) M *divise $\mathcal{C}_n$ pour un certain n,*

(3) M *divides $\mathcal{R}_n$ pour un certain n,*

(4) M *divides $\mathcal{U}_n$ pour un certain n.*

Ces conditions sont décidables.

Résumé pour le niveau 1



La classe Δ_2

Théorème (Pin-Weil 97, Schützenberger 75)

Un langage est Δ_2-définissable ssi son monoïde syntactique est dans DA.

Par conséquent, Δ_2 est décidable.

Langages de niveau $3/2$

Rappel : le niveau $3/2$ correspond à Σ_2.

Théorème (Pin-Weil 1995)

Un langage est de niveau $3/2$ ssi c'est il est union finie de langages de la forme $A_0^*a_1A_1^* \cdots a_kA_k^*$ où $A_0, A_1, \dots, A_k \subseteq A$ et $a_1, \dots, a_k \in A$.

Théorème (Pin-Weil 1995)

Un langage est de niveau $3/2$ ssi son monoïde syntactique ordonné est dans la variété $[ese \leqslant e]$ Ⓜ J_1. Cette variété est décidable.

Langages de niveau 2

Rappel : le niveau 2 correspond à $\mathcal{B}\mathbf{\Sigma}_2$.

Théorème (Pin-Straubing 1981)

Un langage est de niveau 2 ssi c'est une combinaison booléenne de langages de la forme $A_0^* a_1 A_1^* \cdots a_k A_k^*$ où A_0, A_1, ..., $A_k \subseteq A$ et $a_1, \ldots, a_k \in A$.

Première description algébrique du niveau 2

Si M est un monoïde, alors $\mathcal{P}(M)$ est un monoïde pour la multiplication

$$XY = \{xy \mid x \in X,\ y \in Y\}$$

Théorème (Pin-Straubing 1981)

Un langage est de niveau 2 ssi son monoïde syntactique est dans la variété de monoïdes finis engendrée par les monoïdes $\mathcal{P}(M)$, où M est $\mathcal{J}$-trivial.

Deuxième description algébrique du niveau 2

Théorème (Pin-Straubing 1981)

Un langage est de niveau 2 ssi son monoïde syntactique divise le monoïde $\mathcal{T}_n$ des matrices triangulaires supérieures $n \times n$, pour un certain $n > 0$.

$$\begin{pmatrix} \varepsilon_{1,1} & \varepsilon_{1,2} & \varepsilon_{1,2} & \dots & \varepsilon_{1,n} \\ 0 & \varepsilon_{2,2} & \varepsilon_{2,3} & \dots & \varepsilon_{2,n} \\ 0 & 0 & \varepsilon_{3,3} & \dots & \varepsilon_{3,n} \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \varepsilon_{n,n} \end{pmatrix}$$

Décidabilité du niveau 2

Corollaire (Pin-Straubing 1981)

La décidabilité du niveau 2 est équivalente à décider si un monoïde fini donné divise $\mathcal{T}_n$ pour un certain n.

Comme on l'a vu, les problèmes correspondants pour $\mathcal{C}_n$, $\mathcal{R}_n$ et $\mathcal{U}_n$ sont décidables. Pourtant, le problème pour $\mathcal{T}_n$ est toujours ouvert !

Il suffirait de trouver un ensemble décidable d'identités pour la variété engendrée par les monoïdes $\mathcal{T}_n$.

Monoïdes de matrices unitriangulaires

Théorème (Pin-Straubing)

La variété engendrée par les monoïdes de matrices booléennes unitriangulaires est définie par les identités $(xy)^\omega = (yx)^\omega$ *and* $x^{\omega+1} = x^\omega$.

Une conjecture pour le niveau 2

Conjecture (Pin-Weil 1997)

Un langage est de niveau 2 ssi son monoïde syntactique est fini et satisfait les identités suivantes :

$$\big((x^\omega p y^\omega q x^\omega)^\omega x^\omega p y^\omega s x^\omega (x^\omega r y^\omega s x^\omega)^\omega\big) = \big((x^\omega p y^\omega q x^\omega)^\omega (x^\omega r y^\omega s x^\omega)^\omega\big)$$

pour tout $x, y, p, q, r, s \in \hat{A}^*$ tels que $c(x) = c(y) = c(p) = c(q) = c(r) = c(s)$.

Résumé des résultats de décidabilité connus

(1) Σ_0 et Π_0 sont décidables (facile)

(2) $\mathcal{B}\boldsymbol{\Sigma}_1$ est décidable (Simon 1972)

(3) Σ_2, Π_2 et Δ_2 sont décidables (Pin-Weil 1995)

(4) $\mathcal{B}\boldsymbol{\Sigma}_2$ est décidable pour un alphabet à deux lettres (Straubing 1988)

(5) Σ_3 est décidable pour un alphabet à deux lettres (Glasser-Schmidt 2001)

La décidabilité de $\mathcal{B}\boldsymbol{\Sigma}_2$ et au-delà est ouverte pour plus de deux lettres. . .

Les autres hiérarchies

Pour n entier ou demi-entier, on note

- V_n la variété de monoïdes [ordonnés] associée au niveau n de la hiérarchie de Straubing-Thérien,
- B_n la variété de monoïdes [ordonnés] associée au niveau n de la hiérarchie dot-depth,
- G_n la variété de monoïdes [ordonnés] associée au niveau n de la hiérarchie des groupes.

Les autres hiérarchies (2)

Théorème (Straubing)

Pour tout n, on a $B_n = V_n * LI$. De plus B_n est décidable ssi V_n est décidable.

Théorème (Pin 98)

Pour tout n, on a $G_n = V_n * G$.

Les variétés $\mathsf{G}_{1/2}$ et G_1

Théorème (Pin-Weil 2002)

La variété $\mathsf{G}_{1/2}$ est définie par l'identité $e \leqslant 1$.

Théorème (Margolis-Pin 1985 + Pin 1991 + Ash 1991)

La variété G_1 est définie par les identités $(x^\omega y^\omega)^\omega = (y^\omega x^\omega)^\omega$. On a aussi $G_1 = \mathsf{PG} = \mathsf{J} * \mathsf{G} = \mathsf{J} \circledM \mathsf{G} = \mathsf{BG} = \mathsf{EJ}$.

References I

J.-E. Pin et P. Weil, Polynomial closure et non-ambigu produit, *Theory Comput. Systems* **30** (1997), 1–39.