Leçon 2

Rationalité

On donne une caractérisation algébrique des relations RTF, qu'on appellera désormais relations rationnelles. Elle résume ce qu'il peut y avoir de commun entre les langages rationnels, acceptés par les automates finis, et les relations RTF. On explore ensuite par contraste ce qui les différencie, jusqu'à arriver à l'indécidabilité de l'équivalence.

Contents

2.1 Le théorème fondamental des automates finis

Les définitions et résultats de cette première section valent en toute généralité pour un monoïde M quelconque. Dans la suite, $M = A^* \times B^*$ (ou, plus généralement, $M = A_1^* \times A_2^* \times \cdots \times A_k^*$) ce qui est déjà un cas très particulier.

2.1.1 Parties rationnelles d'un monoïde

Soit M un monoïde, c'est-à-dire un ensemble muni d'une opération associative, en général appelée *produit* et notée par un $\cdot$ ou par la simple juxtaposition, et possédant un élément neutre, noté 1_M ou même 1 s'il n'y a pas ambiguïté, pour cette opération.

Le semi-anneau $\mathfrak{P}(M)$

L'ensemble des parties de M, noté $\mathfrak{P}(M)$, est muni de deux opérations :

- l'*union*, associative, commutative, et pour laquelle $\emptyset$ est un élément neutre ;
- le *produit*, extension additive du produit sur M, défini par :

$$\forall P, Q \subseteq M \qquad P \cdot Q = \{p \cdot q \mid p \in P,\, q \in Q\} \quad ,$$

et pour laquelle le singleton 1_M est un élément neutre.

Le produit est *distributif*, à gauche et à droite, sur l'union, et $\emptyset$ est un *zéro*, c'est-à-dire un élément absorbant, pour le produit : $\emptyset \cdot P = \emptyset$ pour tout P inclus dans M.

Ainsi, $\mathfrak{P}(M)$ est un *semi-anneau*. Le semi-anneau $\mathfrak{P}(M)$ a la propriété d'être *complet*, c'est-à-dire que l'union $\bigcup_{i \in I} P_i$ d'une famille quelconque de parties, même *infinie*, est bien définie et que les propriétés d'associativité et de distributivité du produit s'étendent naturellement à ces unions infinies.

L'opération $*$ On définit l'opération $*$ sur $\mathfrak{P}(M)$ par :

$$\forall P \subseteq M \qquad P^* = \bigcup_{n \in \mathbb{N}} P^n \quad ,$$

avec $P^{n+1} = P^n \cdot P$ pour tout n dans $\mathbb{N}$ et, par cohérence, $P^0 = \{1_M\}$. Il en résulte que $\emptyset^* = \{1_M\}$ (qui est le pendant du classique $0^0 = 1$).

Cette opération $*$ est susceptible d'une définition algébrique. Si $P \subseteq M$, on note $\langle P \rangle$ le *sous-monoïde engendré par P*, c'est-à-dire le plus petit sous-monoïde de M qui contient P (et 1_M) et donc aussi l'intersection de tous les sous-monoïdes qui contiennent P.

Lemme 1. $\forall P \subseteq M \qquad P^* = \langle P \rangle$. ∎

Opérations et expressions rationnelles

On appelle *opérations rationnelles sur M*, en fait sur $\mathfrak{P}(M)$, les opérations (binaires) *union* et *produit*, ainsi que l'opération (unaire) *étoile*.

Définition 2. *Une* expression rationnelle sur M *est une formule obtenue inductivement à partir des éléments de M et des symboles de fonctions binaires $+$ et $\cdot$, unaire $*$ et des constantes 0 et 1 de la manière suivante :*

(i) $\mathsf{0}$, $\mathsf{1}$, *et m, pour tout m dans M, sont des expressions rationnelles (atomiques) ;*

(ii) si E *et* F *sont des expressions rationnelles,* $(\mathsf{E}+\mathsf{F})$, $(\mathsf{E}\cdot\mathsf{F})$, *et* (E^*) *sont des expressions rationnelles.*

On note $\mathsf{Rat}\mathsf{E}\,M$ *l'ensembles des expressions rationnelles sur M.*

Exemple 3. $\mathsf{E}_1 = (((a,c)^*)\cdot((b,1)^*))$ est une expression rationnelle sur $\{a,b\}^*\times\{c\}^*$.

Définition 4. *A chaque expression rationnelle sur M, on associe une partie de M, notée* $|\mathsf{E}|$, *et définie inductivement par :*

(i) pour les expressions atomiques : $|\mathsf{0}| = \emptyset$, $|\mathsf{1}| = 1_M$, *et* $|m| = m$, *pour tout m dans M ;*

(ii) pour les expressions composées : $|(\mathsf{E}+\mathsf{F})| = |\mathsf{E}|\cup|\mathsf{F}|$, $|(\mathsf{E}\cdot\mathsf{F})| = |\mathsf{E}|\cdot|\mathsf{F}|$, *et* $|(\mathsf{E}^*)| = |\mathsf{E}|^*$.

Exemple 5. $|\mathsf{E}_1| = \{(a^n b^m, c^n) \mid n,m \in \mathbb{N}\}$.

Comme on le voit sur cet exemple, la définition formelle entraîne une multiplication des parenthèses dans les expressions qui deviennent rapidement illisibles. Pour alléger la notation, on utilise les conventions usuelles de précédence d'opérateurs : $* \gg \cdot \gg +$, l'associativité des fonctions représentées par $+$ et $\cdot$, voire même l'élision pure et simple du $\cdot$. L'expression ci-dessus devient alors : $\mathsf{E}_1 = (a,c)^*(b,1)^*$.

Sous cette forme, il n'y a plus de différence entre l'expression et la partie qu'elle dénote quand on l'écrit en utilisant les éléments de M et les symboles d'opérations rationnelles. Il faut néanmoins distinguer ces deux notions. Ainsi,

$$\mathsf{E}'_1 = \big((1,c)\big((a,1)(1,c)\big)^*(a,1)+\mathsf{1}\big)\big((b,1)(b,1)^*+\mathsf{1}\big)$$

est une autre expression, distincte de E_1, mais *équivalente* à E_1 c'est-à-dire $|\mathsf{E}'_1| = |\mathsf{E}_1|$.

Parties rationnelles de M

Définition 6. *Une partie de M est* rationnelle *si elle est dénotée par une expression rationnelle sur M. On note* $\mathrm{Rat}\,M$ *l'ensembles des partie rationnelles de M.*

Une famille de parties de M est dite *rationnellement fermée* si elle est fermée pour les opérations rationnelles. L'intersection de tout ensemble de familles de parties rationnellement fermée est une famille de parties rationnellement fermée.

Proposition 7. Rat M *est* la plus petite famille *de parties de* M
- *rationnellement fermée et*
- *qui contient les parties finies.* ■

On aurait pu énoncer que Rat M est *la plus petite famille* de parties de M rationnellement fermée qui contient l'ensemble vide, et n'importe quel ensemble générateur de M.

2.1.2 Le théorème fondamental

Rappelons qu'un *automate sur* M est un automate dont les transitions sont étiquetées par des éléments de M.

Théorème 8. *Une partie de* M *est* rationnelle *si, et seulement si, elle est acceptée par un automate* fini *sur* M.

La condition est suffisante c'est-à-dire une partie rationnelle de M est acceptée par un automate fini sur M. Il suffit pour cela, au vu de la Proposition 7, de montrer que la famille des parties acceptées par un automate fini est rationnellement fermée et que tout singleton, de même que l'ensemble vide, est accepté par un automate fini.

La condition est nécessaire c'est-à-dire qu'une partie acceptée par un automate fini est une partie rationnelle. Il suffit pour cela de montrer qu'on peut associer à chaque automate une expression rationnelle qui dénote la partie acceptée par l'automate. ■

En conséquence, une relation de A^* dans B^* est réalisée par un transducteur fini sur $A^* \times B^*$ (RTF) si, et seulement si, son graphe est une partie rationnelle de $A^* \times B^*$. Nous appellerons désormais ces relations *rationnelles* plutôt que RTF.

2.2 Rat $A^* \times B^*$, des faits

2.2.1 Intersection, complément

Contrairement aux *langages* rationnels, les relations rationnelles ne sont pas fermées par intersection et donc par complément.

Fait 9. *L'intersection de deux parties rationnelles de* $A^* \times B^*$ *n'est pas nécessairement une partie rationnelle, c'est-à-dire :*

$$R, S \in \text{Rat}\, A^* \times B^* \quad \not\Longrightarrow \quad R \cap S \in \text{Rat}\, A^* \times B^* \ .$$

Exemple 10. Les automates[1] de la Figure 1 donnent $\left|\mathcal{V}_1\right| = \{(a^n b^m, c^n) \mid n, m \in \mathbb{N}\}$ et $\left|\mathcal{W}_1\right| = \{(a^n b^m, c^m) \mid n, m \in \mathbb{N}\}$. Ainsi

$$\left|\mathcal{V}_1\right| \cap \left|\mathcal{W}_1\right| = \{(a^n b^n, c^n) \mid n \in \mathbb{N}\} \notin \operatorname{Rat} \{a, b\}^* \times \{c\}^*$$

puisque $\mathsf{Dom}\left(\left|\mathcal{V}_1\right| \cap \left|\mathcal{W}_1\right|\right) = \{a^n b^n \mid n \in \mathbb{N}\} \notin \operatorname{Rat} \{a, b\}^*$.

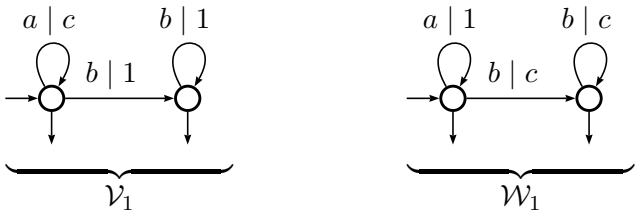

FIG. 1 – Deux automates $\mathcal{V}_1$ et $\mathcal{W}_1$ sur $\{a, b\}^* \times \{c\}^*$

Si $\theta \colon A^* \to B^*$ est une relation, on note $\complement\theta \colon A^* \to B^*$ la relation *complément* de θ, c'est-à-dire la relation dont le graphe est le complément (dans $A^* \times B^*$) du graphe de θ : $\widehat{\complement\theta} = \complement\left(\widehat{\theta}\right)$.

Corollaire 11. $\operatorname{Rat} A^* \times B^*$ *n'est pas fermée par complément.*

On a quand même :

Proposition 12. *Le complément de l'identité est une relation rationnelle.*

La preuve tient dans la construction de l'automate de la Figure 2.

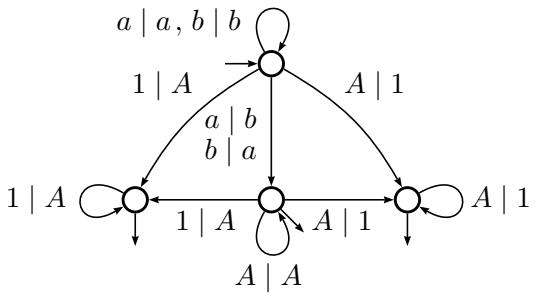

FIG. 2 – Un transducteur pour le complément de l'identité.

2.2.2 Equivalence

Une propriété essentielle des automates finis sur un monoïde libre est qu'on peut décider si deux tels automates sont *équivalents*, c'est-à-dire s'ils acceptent le même langage. Cette propriété ne s'étend pas aux relations rationnelles.

[1] A partir de cet exemple, on écrit $a \mid b$ au lieu de (a, b) pour les étiquettes des transitions, pour alléger la notation.

Théorème 13 (Rabin & Scott 1959)**.**
Soient $R, S \in \mathrm{Rat}\, A^* \times B^*$, $\|A\|, \|B\| \geq 2$ *. Il est indécidable si* $R \cap S = \emptyset$ *.*

On en déduit :

Théorème 14 (Fischer & Rozenberg 1968)**.**
L'équivalence des transducteurs finis sur $A^* \times B^*$, $\|A\|, \|B\| \geq 2$ *, est indécidable.*

On va établir ces deux résultats négatifs à la section suivante. Leurs énoncés laissent ouvert le statut des mêmes questions dans les cas où $\|A\| \geq 2, \|B\| = 1$ d'une part et $\|A\| = \|B\| = 1$ d'autre part.

Le premier cas montre une séparation intéressante entre les deux énoncés :

Théorème 15 (Gibbons & Rytter 1986)**.**
Soient $R, S \in \mathrm{Rat}\, \{a, b\}^* \times \{c\}^*$ *. On peut décider si* $R \cap S = \emptyset$ *.*

Théorème 16 (Ibarra 1978 – Lisovik 1979)**.**
L'équivalence des transducteurs finis sur $\{a, b\}^* \times \{c\}^*$ *est indécidable.*

Le deuxième cas relève d'une théorie complètement différente. On remarque que $\{a\}^* \times \{b\}^*$ est isomorphe à $\mathbb{N}^2$, le monoïde commutatif libre à deux générateurs.

Théorème 17 (Ginsburg & Spanier 1966)**.**
Pour tout entier k, $\mathrm{Rat}\, \mathbb{N}^k$ *est une algèbre de Boole effective.*

Les démonstrations de tous ces résultats dépassent le cadre de ces notes (*cf.* EAT).

2.2.3 Ambiguïté

Les transformations d'un automate $\mathcal{A}$ en une expression rationnelle E ou réciproquement d'une expression rationnelle E en un automate $\mathcal{A}$ évoquées dans la preuve du Théorème 8 donnent des objets *fortement équivalents* en ce sens que non seulement $msp|\mathcal{A}| = |\mathsf{E}|$ mais chaque élément est accepté ou dénoté avec la même « multiplicité » c'est-à-dire que le *nombre de façons* de « décomposer » un élément m selon la description donnée par l'expression E est égale au *nombre de calculs distincts* de $\mathcal{A}$ dont l'étiquette est m.

Opérations rationnelles non ambiguës

Sur $\mathfrak{P}(M)$, on définit les opérations rationnelles non ambiguës :

- l'*union disjointe* : $P \cup Q$ est disjointe si $P \cap Q = \emptyset$
- le *produit non ambigu* : $P \cdot Q$ est « non ambigu » si la décomposition d'un élément de $P \cdot Q$ en produit d'un élément de P par un élément de Q est unique, c'est-à-dire si :

$$\forall p, p' \in P\,,\ \forall q, q' \in Q \qquad p\,p' = q\,q' \quad \Longrightarrow \quad p = q \quad \text{et} \quad p' = q' \ ;$$

- l'*étoile non ambiguë* : $P^* = \bigcup_{n\in\mathbb{N}} P^n$ est non ambiguë si chacun des produits P^n est non ambigu et si l'union est non ambiguë, that is, si les P^n sont disjoints deux à deux. Autrement dit, P^* est une étoile non ambiguë si P engendre un *sous-monoïde libre* de M de base P.

La famille URat M

Une partie rationnelle de M est non ambiguë si elle est dénotée par une expression rationnelle non ambiguë. On note $\mathrm{URat}\, M$ la famille des parties rationnelles non ambiguës. On a l'énoncé analogue à la Proposition 7 : $\mathrm{URat}\, M$ est la plus petite famille de parties de M qui est fermée pour les opérations rationnelles non ambiguës et qui contient les parties finies.

Par ailleurs, un automate sur M est dit *non ambigu* si tout élément qu'il accepte est l'étiquette d'un *unique* calcul réussi. La forte équivalence évoquée ci-dessus permet d'énoncer qu'*une partie de M est* rationnelle non ambiguë *si, et seulement si, elle est acceptée par un automate* fini non ambigu *sur M*.

Un automate *déterministe* sur A^* est évidemment non ambigu et comme tout automate fini sur A^* est équivalent à un automate fini déterministe, on a donc :

$$\mathrm{URat}\, A^* = \mathrm{Rat}\, A^* \ .$$

Cette égalité n'est pas vraie en toute généralité (quand on considère d'autres monoïdes que des monoïdes libres) et en particulier dans le cas $A^* \times B^*$ qui nous occupe.

Fait 18. $\mathrm{URat}\ (\{a,b\}^* \times \{c\}^*) \subsetneq \mathrm{Rat}\ (\{a,b\}^* \times \{c\}^*)$.

Exemple 19. Ce sont encore les automates de la Figure 1 qui donnent un exemple. On peut montrer que la partie :

$$\big|\mathcal{V}_1\big| \cup \big|\mathcal{W}_1\big| = \{(a^n b^m, c^n) \mid n, m \in \mathbb{N}\} \cup \{(a^n b^m, c^m) \mid n, m \in \mathbb{N}\}$$

ne peut pas être dénotée par une expression rationnelle non ambiguë ou, ce qui revient au même, qu'il n'existe pas d'automate non ambigu sur $\{a,b\}^* \times \{c\}^*$ qui accepte cette partie.

Dans la ligne de la discussion précédente, notons que l'on a :

Théorème 20 (Eilenberg & Schützenberger 1969)**.**
Pour tout entier k, $\mathrm{URat}\, \mathbb{N}^k = \mathrm{Rat}\, \mathbb{N}^k$.

2.3 Preuve des résultats d'indécidabilité

La propriété indécidable par excellence est celle de « l'arrêt d'une machine de Turing ». Mais on peut prendre comme point de départ n'importe quelle autre, déjà

réputée indécidable. Celle que nous utiliserons dans la suite, parce qu'elle est plus simple et plus facile à mettre en œuvre, est connue sous le nom de « problème de correspondance de Post ».

Le problème de correspondance de Post (PCP)

Soit B un alphabet contenant au moins deux lettres. Étant donnés un entier k et deux ensembles de mots de B^* à k éléments : $\{u_1, u_2, \ldots, u_k\}$ et $\{v_1, v_2, \ldots, v_k\}$, existe-t-il une suite d'indices $i_1, \ldots, i_p$ dans $[k]$ telle que

$$u_{i_1} u_{i_2} \cdots u_{i_p} = v_{i_1} v_{i_2} \cdots v_{i_p} \, ?$$

Théorème 21 (Post 1946)**.** *(PCP) est récursivement indécidable.*

Cet énoncé vaut pour le problème dans toute sa généralité. Si on s'intéresse à son statut en fonction du nombre k de mots qui permettent d'en formuler une instance, la situation est plus complexe. Appelons (PCP_k) le problème précédent dans lequel l'entier k est fixé. On sait que (PCP_2) est décidable et, depuis très récemment, que (PCP_k) est indécidable pour $k \geqslant 5$. Le statut de (PCP_k) n'est pas résolu pour k égal à 3 ou 4.

Enoncé dans le langage de la théorie des langages et des automates

La raison de notre choix est que le problème de Post prend une forme particulièrement simple en termes de *morphismes entre monoïdes libres.*

Étant donné $U = \{u_1, u_2, \ldots, u_k\}$, on pose : $A_k = \{1, 2, \ldots, k\}$, et

$$\tau_U \colon A_k^* \to B^* \qquad \text{le morphisme défini par} \qquad \tau_U(i) = u_i \qquad \forall i \in [k] \ .$$

De façon analogue, si $V = \{v_1, v_2, \ldots, v_k\}$, on pose : $\tau_V \colon A_k^* \to B^*$ le morphisme défini par $\tau_V(i) = v_i$ pour tout i dans $[k]$. Une « suite d'indices », c'est un mot de A_k^* et (PCP) se reformule en :

Existe-t-il un mot w de B^* tel que $\tau_U(w) = \tau_V(w)$?

Et le Théorème 21 devient :

Théorème 22. *Soient $\theta, \mu \colon A^* \to B^*$ morphismes.*
Il est indécidable s'il existe w dans A^* tel que $\theta(w) = \mu(w)$.

Preuve des Théorème 13 et Théorème 14

Soient U et V ensembles à k éléments qui déterminent un (PCP) indécidable, et $\tau_U \colon A_k^* \to B^*$ et $\tau_V \colon A_k^* \to B^*$ les deux morphismes correspondants.

Dire qu'il est indécidable s'il existe w dans A_k^* tel que $\tau_U(w) = \tau_V(w)$ est exactement la même chose que dire qu'il est indécidable si

$$\widehat{\tau_U} \bigcap \widehat{\tau_V} = \emptyset \ ,$$

et τ_U et τ_U sont des relations rationnelles (Exemple 10 (ii)). Reste à montrer qu'on peut se ramener à un alphabet $A = \{a, b\}$ à deux lettres seulement.

Soit $\kappa\colon A_k^* \to A^*$ un *morphisme injectif* (par exemple, défini par $\kappa(i) = a^i b$). Par le Théorème 1.15, $\tau_U \circ \kappa^{-1}$ et $\tau_V \circ \kappa^{-1}$ sont des relations rationnelles et, puisque κ est injectif, on a :

$$\widehat{\tau_U \circ \kappa^{-1}} \bigcap \widehat{\tau_V \circ \kappa^{-1}} = \emptyset \quad \Longleftrightarrow \quad \widehat{\tau_U} \bigcap \widehat{\tau_V} = \emptyset \ . \qquad \blacksquare$$

Le Théorème 14 est une conséquence directe du résultat suivant plus précis.

Théorème 23.
Soit $R \in \operatorname{Rat} A^* \times B^*$, $\|A\|, \|B\| \geq 2$. *Il est indécidable si* $R = A^* \times B^*$.

On commence par prouver :

Lemme 24. *Soit* $\theta\colon A^* \to B^*$ *une relation rationnelle* fonctionnelle.
Alors $\complement\theta\colon A^* \to B^*$ *est une relation rationnelle.*

Démonstration. Notons χ le complément de l'identité sur B^*, relation rationnelle par la Proposition 12. Il vient :

$$\widehat{\complement\theta} = [(A^* \setminus \operatorname{Dom}\theta) \times B^*] \cup \widehat{\chi \circ \theta} \ .$$

Le premier terme de l'union est rationnel (Exemple 10 (i)) et le deuxième terme l'est par le Théorème 1.15. $\blacksquare$

Preuve du Théorème 23. Avec les notations de la preuve du Théorème 13, $\tau_U \circ \kappa^{-1}$ et $\tau_V \circ \kappa^{-1}$ sont des relations rationnelles fonctionnelles, et on a

$$\complement\left(\widehat{\tau_U \circ \kappa^{-1}}\right) \bigcup \complement\left(\widehat{\tau_V \circ \kappa^{-1}}\right) = A^* \times B^* \quad \Longleftrightarrow \quad \widehat{\tau_U \circ \kappa^{-1}} \bigcap \widehat{\tau_V \circ \kappa^{-1}} = \emptyset \ . \qquad \blacksquare$$

2.4 Exercices

1.— **Expressions rationnelles.**

(a) Donner des expressions rationnelles pour les graphes des relations « ordre lexicographique » et « ordre radiciel » sur $\{a, b\}^*$.

(b) Donner des expressions rationnelles pour les graphes des relations « facteurs » et « sous-mots » sur $\{a, b\}^*$.

2.— **Lemme d'itération.** Soit $\theta\colon A^* \to B^*$ une relation rationnelle.

(a) Montrer qu'il existe un entier N tel que pour couple (u, v) dans $\widehat{\theta}$ dont la longueur[2] est supérieure à N il existe une factorisation

$$(u, v) = (s, t)\,(x, y)\,(w, z)$$

telle que : (i) $1 \leqslant |x| + |y| \leqslant N$ et (ii) $(u, v) = (s, t)\,(x, y)^*(w, z) \subseteq \widehat{\theta}$.

[2]La longueur d'un couple est la somme des longueurs de ses composantes.

(b) Montrer que la fonction *miroir* $\rho\colon A^* \to A^*$:

$$\rho(a_1\, a_2 \cdots a_n) = a_n\, a_{n-1} \cdots a_1 \ ,$$

n'est pas une relation rationnelle.

3..— **Conjugaison.** Soit $\mathsf{Conj}\colon A^* \to A^*$ la relation qui à un mot w fait correspondre l'ensemble de ses *conjugués* : $\mathsf{Conj}(w) = \{v\, u \mid u, v \in A^* \quad u\, v = w\}$.

(a) Montrer que $\mathsf{Conj}(L)$ est rationnel quand L l'est.

(b) Donner un transducteur qui à un mot quelconque w de $\{a, b\}^*$ associe le mot obtenu en plaçant la première lettre de w à la fin.

(c) Composer ce transducteur avec lui-même.

(d) Montrer que Conj n'est pas une relation rationnelle.