

Éléments de théorie des automates



Jacques Sakarovitch

Vuibert Informatique

TABLE DES MATIÈRES

AVANT-PROPOS	VII
SOMMAIRE	XV
LA MACHINE À DIVISER DE MONSIEUR PASCAL	1
0 STRUCTURES FONDAMENTALES	9
1 Relations	11
2 Monoïdes	17
3 Mots et langages	21
4 Monoïdes libres	27
5 Semi-anneaux	31
6 Matrices	34
7 Vocabulaire de la théorie des graphes	37
8 Complexité et décidabilité	39
Solutions des exercices	43
Notes & références bibliographiques	51

Les trois stades de la rationalité

1 LA MACHINE LA PLUS SIMPLE...	55
1 Qu'appellerons-nous « automate » ?	57
1.1 Premières définitions — premiers exemples	57
États, transitions, etc. — Calcul, langage externe, etc. — Transposition et dualité gauche-droite	
1.2 Premières constructions — premières propriétés	66
Union — Produit cartésien — Quotient (de langages)	
1.3 Le côté graphe	73
Automates étagés — Les questions du vide et de l'infini — Critères de reconnaissabilité	
1.4 Quelques définitions supplémentaires	81
Automates non analogues — Automates complets — Automates déterministes — Automates avec transitions spontanées	
2 Langages rationnels	90
2.1 Opérations rationnelles	90
Produit de langages — Étoile d'un langage — Opérations rationnelles	
2.2 Langages rationnels	93

2.3	Les rationnels sont reconnaissables	95
	<i>Automates normalisés - Structure par produit et finale - Automates standard</i>	
2.4	Les reconnaissables sont rationnels	102
	<i>L'algorithme de McNaughton et Yamada, ou « algorithme MNY » - L'algorithme d'élimination ou « algorithme BMC » - Résolution d'équations</i>	
3	Le point de vue fonctionnel	110
3.1	Des transitions à la fonction de transition	110
3.2	Automates déterministes	112
	<i>Reformulation de la définition - Détermination - Complémentation des langages reconnaissables</i>	
3.3	Minimisation	120
	<i>L'automate des quotients d'un langage est minimal - Calcul de l'automate minimal - Une autre méthode pour la minimisation</i>	
3.4	Retour sur le lemme de l'étoile	127
	<i>Itération et simplification par blocs - Le théorème de Ramsey - Preuve du théorème 3.3</i>	
4	Expressions rationnelles	132
4.1	Expressions et langages rationnels	133
	<i>Expressions rationnelles sur un alphabet - Expressions rationnelles sur un ensemble de variables</i>	
4.2	Identités rationnelles	137
	<i>Les identités classiques - Un calcul formel</i>	
4.3	Expressions du comportement d'un automate fini	142
	<i>Algorithmes d'élimination et résolution d'équations - Algorithmes BMC et algorithme MNY, ordres identiques - Algorithmes BMC ou algorithme MNY, ordres distincts</i>	
4.4	Dérivations des expressions	148
	<i>Expressions dérivées - Un théorème de J. Brzozowski - Automates aux expressions dérivées</i>	
5	Des expressions aux automates	155
5.1	L'automate standard d'une expression	156
	<i>La construction directe - La construction de Thompson</i>	
5.2	L'automate des termes dérivés	159
	<i>Termes dérivés - Un théorème de V. Antimirov</i>	
5.3	Localisation	163
	<i>Automate de localisation d'un mot - Localisation par fenêtre glissante - Implémentation avec successeur par défaut</i>	
6	Hauteur d'étoile	169
6.1	Deux hauteurs et un degré	169
	<i>Hauteur d'étoile d'une expression - Hauteur d'étoile d'un langage - Degré d'enlacement d'un automate</i>	
6.2	Le théorème d'Eggan	173
	<i>Des expressions aux automates - Des automates aux expressions: calcul de l'index - Pas de conclusion hâtive</i>	
6.3	Une hiérarchie infinie	179
6.4	Hauteur d'étoile généralisée	181

7	Un champ d'automates	184
7.1	Le modèle de Rabin & Scott	184
7.2	Automate boustrophédon	186
7.3	Machines de Moore et de Mealy	188
8	Une moisson de propriétés	189
	Solutions des exercices	193
	Notes & références bibliographiques	230
II PUissance de l'algèbre		233
1	Automates et parties rationnelles	235
1.1	Automates sur un monoïde	235
1.2	Parties rationnelles	237
	<i>Le semi-anneau $\mathbb{P}(A^*)$ – Opérations et parties rationnelles – Expressions rationnelles – Image par morphisme – Intersection et morphisme inverse</i>	
1.3	Comportement des automates finis	242
1.4	Parties rationnelles non ambiguës	245
	<i>Définitions – La famille URat</i>	
2	Actions et parties reconnaissables	249
2.1	Actions sur un ensemble	249
	<i>Définition – Représentation matricielle des automates sur A^* – Parties reconnues par une action</i>	
2.2	Reconnaisable-ci, reconnaissable-là	255
	<i>Cohérence – Théorème de Kleene – Automate d'une action</i>	
2.3	Opérations élémentaires sur les parties reconnaissables	261
	<i>Opérations booléennes – Morphisme inverse – Quotient – Morphisme et produit</i>	
2.4	Minimisation	264
	<i>Morphismes d'actions – Action minimale – Congruence et monoïde syntactiques</i>	
2.5	L'algèbre à l'ouvrage	270
	<i>Deux exemples – Parties reconnaissables incluses dans un produit</i>	
3	Morphismes et revêtements	274
3.1	Morphismes d'automates	274
	<i>Définitions et exemples – Morphismes conjugués – Propriétés locales</i>	
3.2	Quotients d'automates	280
	<i>Morphismes localement surjectifs – Morphismes totalement surjectifs – Algorithme de Moore</i>	
3.3	Revêtements d'automates	284
	<i>Du local au global – Produit d'un automate par une action – Le langage des transitions colorées</i>	
3.4	Le revêtement de Schützenberger	290
4	Automate universel	294

4.1	Factorisations	295
	<i>Factorisations à deux termes - Sous-factorisations et factorisations - Morphismes et factorisations</i>	
4.2	Automates universels d'une partie	299
	<i>Définitions et exemples - Propriétés - Automate universel relatif à un ensemble générateur - Universalité des automates universels</i>	
4.3	Construction de l'automate universel	307
	<i>Expression d'un automate déterministe - Extraction de l'automate universel</i>	
4.4	Approximations	312
5	L'importance d'être bien ordonné	315
5.1	Dans quasi-ordres	315
5.2	Dérivations	318
	<i>Préparatifs - Démonstration du théorème 5.4</i>	
6	Rationnels dans le groupe libre	323
6.1	Reconnaisables et rationnels dans les groupes	323
	<i>Parties reconnaissables - Sous-groupes rationnels - Propriété de Fataou</i>	
6.2	Description du groupe libre	327
	<i>Congruence de Dyck et mots de Dyck - Congruence de Shirshov et mots de parenthèses - Simplifications - Réduction associée à une simplification - Factorisation non ambiguë induite par une réduction</i>	
6.3	Rationnels du groupe libre	337
	<i>Rationnels des monoïdes de simplification - Retour au groupe libre</i>	
6.4	Systèmes de Büchi	341
7	Rationnels dans les monoïdes commutatifs	347
7.1	L'ordre naturel sur $A^{\mathbb{N}}$	347
	<i>Le monoïde commutatif libre - Le lemme de Dickson</i>	
7.2	L'ordre lexicographique sur \mathbb{N}^k	350
	<i>Congruence de \mathbb{N}^k - Décomposition lexicographique</i>	
7.3	Sous-monoïdes sous-tractifs et ensembles affines	354
7.4	Ensembles semi-linéaires et semi-simples	357
7.5	Rationnels de \mathbb{N}^k	359
	<i>Le lemme de génération - Solutions positives des systèmes linéaires diophantiens - Ensembles semi-simples de \mathbb{Z}^k - Preuve des théorèmes 7.3 et 7.4</i>	
7.6	Rationnels des monoïdes commutatifs	365
8	Hauteur d'étoile des langages à groupe	367
	Solutions des exercices	373
	Notes & références bibliographiques	366
III PERTINENCE DE L'ÉNUMÉRATION		401
1	Séries formelles sur un monoïde gradué	406
1.1	Séries formelles sur M à coefficients dans K	406
	<i>Opérations sur $K\langle\langle M \rangle\rangle$ - Support d'une série - série caractéristique - Produit de Hadamard - Produit scalaire</i>	
1.2	Monoïdes gradués	409

1.3	Topologie sur $K\langle M \rangle$	412
	<i>Distance - Distance sur $K\langle M \rangle$ - Familles sommables - Morphismes continus</i>	
2	K -automates et séries K -rationnelles	420
2.1	Étoile d'une série	420
	<i>Étoile dans un semi-anneau topologique - Étoile d'une série propre - Étoile d'une série quelconque</i>	
2.2	Séries K -rationnelles	426
	<i>Opérations K-rationnelles - K-expressions rationnelles - Étoile d'une matrice</i>	
2.3	Automate avec multiplicité dans un semi-anneau	430
	<i>K-autonomie sur M - Comportement d'un K-automate - Commutateurs - Quelques autres définitions et exemples</i>	
2.4	Le théorème fondamental des automates finis	437
	<i>Automates propres - familles propres - Énoncé et preuve - Commentaires et corollaires</i>	
2.5	K -revêtements — K -quotients	444
	<i>Des revêtements aux K-revêtements - Description matricielle - K-α-revêtement - K-quotient minimal</i>	
3	Séries K -reconnaisables	454
3.1	K -représentations	454
3.2	Produits	456
	<i>Produit tensoriel de K-représentations - Produit de Hallward - Produit tensoriel de séries - Produit de mélange</i>	
3.3	Le théorème de Kleene-Schützenberger	463
4	Séries sur un monoïde libre	468
4.1	Une caractérisation des séries reconnaissables	468
	<i>Quotients des séries - Modules stables - Retour sur le théorème de Kleene-Schützenberger</i>	
4.2	Dérivation des K -expressions rationnelles	474
	<i>Polynômes de K-expressions - K-dérivée d'une K-expression - Termes dérivés - L'automate des termes dérivés</i>	
4.3	Séries sur un corps	481
	<i>Rang d'une série - Représentation réduite - Réurrence linéaire - Calculs effectifs</i>	
4.4	Les séries rationnelles et leurs supports	494
	<i>Rationalité des supports - Le théorème du polynôme f - Questions inséparables</i>	
5	Séries sur un monoïde quelconque	502
5.1	Semi-anneaux complets, semi-anneaux continus	502
5.2	Étoile d'une série	504
5.3	Séries K -rationnelles	506
6	Parties rationnelles dans les produits libres	509
6.1	Produit libre de monoïdes	509
6.2	Automate biparti sur un produit libre	511
6.3	Automate biparti déterministe	516
6.4	Automate biparti déterministe minimal	518
7	Mémento d'algèbre linéaire non commutative	523

Solutions des exercices	532
Notes & références bibliographiques	555

La rationalité dans les relations

IV RICHESSE DES TRANSDUCTEURS	559
1 Relations entre mots: une introduction	561
1.1 Relations rationnelles	561
<i>Relations rationnelles entre mots d'un libre - Relations rationnelles entre mots d'un quaternaire</i>	
1.2 Réalisation par automates	565
1.3 Réalisation par morphismes	568
<i>Réalisation - Théorème d'évaluation - Théorème de composition - Lemme de l'étoile</i>	
1.4 Relations reconnaissables	576
1.5 Réalisation par représentation	578
<i>Transducteurs à temps réel ω - Des transducteurs temps réel aux représentations - Théorème d'évaluation et complétude des représentations</i>	
1.6 Le modèle de Rabin et Scott	583
2 K-relations	585
2.1 Définitions	586
<i>L'isomorphisme canonique - K-relations - Support de relations - relations caractéristiques - Continuité</i>	
2.2 Composition	592
2.3 K-relations multiplicatives	595
3 K-relations rationnelles	598
3.1 Semi-ameses raisonnables	598
<i>Image des séries par morphismes continus - Image des séries par projections - K-extensions</i>	
3.2 Réalisations des K-relations rationnelles	602
<i>Réalisation par K-automate - Réalisation par K-représentation - Réalisation par morphismes</i>	
3.3 Théorèmes d'évaluation et de composition	604
<i>À partir de la réalisation par morphismes - À partir de la réalisation par représentation</i>	
4 Équivalence des K-transducteurs finis	610
4.1 Équivalence des B-transducteurs, cas général	610
4.2 Équivalence des B-transducteurs, cas des petits alphabets	612
4.3 Équivalence des \mathbb{N} -transducteurs	616
5 Relations rationnelles déterministes	619
5.1 Transducteurs à base	619
5.2 Transducteurs déterministes	620
<i>Définition - Unité des calculs - Presque une action</i>	
5.3 Relations déterministes	626
<i>Définitions - Complémentation - Lemme d'itération</i>	
5.4 Géographie de $\text{Rat } A^* \times B^*$, I.	631

5.5	Représentations matricielles	633
	<i>Représentation d'un transducteur déterministe - Représentation d'une relation déterministe</i>	
5.6	Un exemple: l'équivalence d'application d'un morphisme	635
6	Synchronisation des transducteurs	639
6.1	Relations rationnelles à saillie bornée	640
	<i>Définitions, notations et convention - Caractérisation des relations rationnelles à saillie bornée - Traduction en termes d'automates étiquetés</i>	
6.2	Transducteurs à décalage borné	646
	<i>Décalage dans un calcul, dans un transducteur - Algorithme de reconnaissance des transducteurs - Composition des transducteurs lettre à lettre</i>	
6.3	Relations synchronisées	653
	<i>Une nouvelle famille de relations rationnelles - Déterminisation et normalisation - Géométrie de $\text{Rat } A^* \times B^*$</i>	
7	Séries de Malcev - Neumann	661
7.1	Ordre sur le groupe libre	661
	<i>Sur les groupes ordonnés - Représentation du groupe libre - Un résultat par les anneaux ordonnés - Ordre sur le groupe libre</i>	
7.2	Séries sur un groupe ordonné	667
	<i>Le semi-anneau $\mathbb{K}_{\text{ord}}\langle\langle G \rangle\rangle$ - Semi-groupes ordonnés - Le corps $\mathbb{K}_{\text{ord}}\langle\langle G \rangle\rangle$ - Une dernière inclusion</i>	
	Solutions des exercices	672
	Notes & références bibliographiques	686
V	SIMPLICITÉ DES TRANSDUCTEURS FONCTIONNELS	689
1	Fonctionnaire	691
1.1	Décider la fonctionnalité	691
	<i>Une caractérisation effective de la fonctionnalité - Équivalence des fonctions rationnelles</i>	
1.2	Fonctions séquentielles	697
	<i>Une terminologie inadaptée - Les définitions classiques - Composition</i>	
1.3	Fonctions séquentielles pures	705
1.4	Fonctions locales	708
2	Uniformisation des relations rationnelles	712
2.1	Démonstration du théorème 2.1 (version transducteur)	714
2.2	Démonstration du théorème 2.1 (version représentation)	715
	<i>Représentation des δ-immersions d'un automate - Matrices semi-numériques - Représentation des δ-uniformisations</i>	
2.3	Décomposition des fonctions rationnelles	721
	<i>Le théorème de décomposition faible - Le théorème de décomposition fort</i>	
2.4	Le théorème du paludier, II	725
3	Transversale des fonctions rationnelles	726

3.1	La propriété de transversale rationnelle	728
	<i>Le théorème de transversale rationnelle - La propriété de transversale rationnelle pour un monoïde - Retour sur les monoïdes de simplification</i>	
3.2	Choisir son uniformisation (ou sa transversale)	733
	<i>Uniformisation des relations synchronisées - Uniformisation des relations déterministes - Le théorème 3.3 remis sur le métier</i>	
4	Fonctions séquentielles	741
4.1	Deux caractérisations	741
	<i>Translatées d'une fonction - Une caractérisation fonctionnelle - Un point de vue quasi-topologique</i>	
4.2	Décider la séquentialité	746
4.3	Minimisation	754
	<i>Conjugaison - Éloignement d'un transducteur séquentiel - Réduction - Calcul effectif</i>	
4.4	Le (grand) théorème de séquentialité	762
	<i>Différentielle d'une fonction - Preuve du théorème 4.5 (ii) \Rightarrow i) - Preuve du théorème 4.5 (ii) \Rightarrow iii) - Retour au théorème de séquentialité</i>	
4.5	Fonctions séquentielles pures et fonctions locales	768
	Solutions des exercices	770
	Notes & références bibliographiques	788
	BIBLIOGRAPHIE	791
	INDEX	500



Éléments de théorie des automates

La théorie des automates est un chapitre de base de l'informatique, essentiel pour la compréhension des méthodes formelles. Depuis cinquante ans, elle a donné lieu à une littérature abondante traitant de résultats nombreux et profonds.

Cet ouvrage veut rendre compte de cette richesse dans un cadre cohérent, aller au-delà des prémices habituelles tout en donnant des preuves complètes, mettre en perspective les différentes propriétés obtenues par des formulations de plus en plus générales. Sont traités en particulier dans cet esprit les automates avec multiplicité et les automates avec sortie (transducteurs).

Il s'adresse aux étudiants (le premier chapitre très complet est rédigé à un niveau élémentaire et couvre la partie correspondante de l'option informatique des classes préparatoires), aux enseignants et aux chercheurs en informatique. Il intéressera également les ingénieurs développeurs de logiciels comme introduction aux méthodes formelles de vérification, les linguistes pour lesquels est présentée en détail la théorie des transducteurs, les mathématiciens enfin qui y trouveront un ensemble de techniques utilisables dans d'autres domaines des mathématiques (combinatoire, groupes hyperboliques, théorie algébrique des nombres).

Plus de trois cents exercices corrigés guident et complètent la lecture de cet ouvrage.

Jacques Sakarowitch est directeur de recherche au CNRS. Membre du laboratoire Informatique théorique et programmation de 1973 à 1996, il a dirigé pendant huit ans l'Institut Blaise Pascal, qui fut la Fédération des laboratoires d'informatique du campus Jussieu. Il travaille depuis 1997 au laboratoire Traitement et communication de l'information de l'École nationale supérieure des télécommunications. Ses travaux de recherche portent sur divers aspects de la théorie des automates. Depuis 1984, il en enseigne les principaux développements dans les DEA d'informatique théorique parisiens et dans des cycles de conférences à l'étranger.

2-7117-4807-3



9 782711 748075

www.vuibert.fr