RAPPORT DE RECHERCHE

L R I

RAPPORT SCIENTIFIQUE PRESENTE POUR L'OBTENTION D'UNE HABILITATION A DIRIGER DES RECHERCHES

Jia-Yan YAO

Unité Mixte de Recherche 8623
CNRS-Université Paris Sud-LRI

07/2003

Rapport de Recherche N° 1362

CNRS – Université de Paris Sud
Centre d'Orsay
LABORATOIRE DE RECHERCHE EN INFORMATIQUE
Bâtiment 650
91405 ORSAY Cedex (France)

Laboratoire de Recherche en Informatique
Université de Paris-Sud et CNRS

Rapport scientifique présenté pour l'obtention
d'une Habilitation à Diriger les Recherches

par

Jia-Yan YAO

Théorie des automates finis et applications

Soutenu le jeudi 26 juin 2003 devant un jury constitué par

M.	Jean-Paul Allouche	Université Paris XI
M.	Jean Berstel	Université de Marne-la-Vallée
Mme	Valérie Berthé	Université Montpellier 2
M.	Dominique Gouyou-Beauchamps	Université Paris XI
M.	Michel Mendès France (président)	Université Bordeaux I
M.	Jacques Peyrière	Université Paris XI
M.	Pascal Weil	Université Bordeaux I
M.	Zhi-Ying Wen	Tsinghua University (China)

Après avis de

M.	Jean Berstel	Université de Marne-la-Vallée
Mme	Valérie Berthé	Université Montpellier 2
M.	Jeffrey Shallit	University of Waterloo (Canada)

Adresse actuelle
Université Paris Sud-CNRS
UMR 8623
LRI, Bât. 490
91405 Orsay Cedex
France
E-mail : yao@lri.fr

Adresse permanente
Department of Mathematics
Nonlinear Science Center
Wuhan University
Wuhan 430072
People's Republic of China
E-mail: yaojiaya@public.wh.hb.cn

À la mémoire de mon père Yuan-Hua YAO

À ma femme Li LIN et à notre fils Shi-Lin YAO

Remerciements

Un grand MERCI :

- à Michel Mendès France et à Zhi-Ying Wen, mes deux "pères" mathématiques et spirituels qui ont su me guider et m'encourager depuis notre première rencontre.

- à Jean-Paul Allouche pour son amitié, sa gentillesse, sa patience, sa spontanéité, et sa disponibilité : chaque fois quand je lui envoie un e-mail, je reçois sûrement sa réponse dans trois secondes; et chaque fois quand j'entre dans son bureau pour lui poser des questions, il se lève instantanément pour me répondre même s'il est très pris par son travail. Je le remercie également pour avoir lu la première version de ce mémoire et pour m'avoir suggéré de très nombreuses corrections. En fait, il m'a appris beaucoup pendant mon séjour à Orsay.

- à Jacques Peyrière qui est bien gentil d'avoir proposé de m'aider à corriger la première version de ce mémoire. Je le remercie également de m'avoir proposé de collaborer avec lui. Son amitié et sa gentillesse sont inoubliables pour moi.

- à Jean Berstel, Valérie Berthé, et Jeffrey Shallit pour avoir accepté la lourde tâche de rapporter sur mon travail, et pour m'avoir donné de très nombreuses suggestions. Je remercie également Jean Berstel et Valérie Berthé d'avoir assisté à ma soutenance, et de m'avoir posé beaucoup de questions intéressantes.

- à Dominique Gouyou-Beauchamps et Pascal Weil pour avoir accepté de faire partie de ce jury, et pour m'avoir posé des questions fort intéressantes.

- à mes collègues et amis à Wuhan, en particulier, Gong-Liang CHEN, Yan-Yan LIU, Feng PAN, Xiao-Lin Wang, Zhi-Xiong WEN, Jun WU, Min WU, Yi-Yan YU, Yi-Ping ZHANG, pour leur aide et leurs encouragements.

- à mes collègues du LRI, en particulier, Julien Albert, Stéphane Boucheron, Frédéric Magniez, Morteza Mohammed-Noori, Emmanuel Prouff, Ndoundam René, Yves Verhoeven, et sourtout Christoph Dürr et Sophie Laplante pour leur aide, leur gentillesse et leur symphatie.

- à Martine Croissant, Dominique Fontaine, et Yannis Manoussakis pour leur aide dans mes démarches administratives.

- à notre bibliothécaire Sylvie Congnard pour sa gentillesse et pour son travail impeccable.

Théorie des automates finis et applications

Jia-Yan YAO

Résumé. Ce mémoire est divisé en trois parties relativement indépendantes. Dans la première partie, nous discutons de certaines propriétés arithmétiques et topologiques des automates finis. Il sera question des automates fidèles et strictement fidèles, automates irréductibles (ou faiblement irréductibles) et automates premiers, automates homogènes, automates minimaux, automates inversibles, *etc.* Comme application, nous donnons une étude assez soigneuse des automates d'Ising, qui sera reprise dans la deuxième partie de ce mémoire, dans laquelle nous étudions les opacités des automates finis. Comme l'opacité d'un automate fini peut être interprétée comme les bruits intrinsèques du système de communication en question, cette partie peut donc être vue comme une toute nouvelle théorie de la transmission de l'information, bien différente de celle de C. E. Shannon. La troisième partie concerne la transcendance des séries formelles issues du module de Carlitz. À l'aide du célèbre théorème de G. Christol, T. Kamae, M. Mendès France, et G. Rauzy, nous montrons, entre autres, qu'une valeur de la fonction gamma de Carlitz-Goss est transcendante si et seulement si l'argument n'est pas un nombre naturel.

1. **Introduction.** Un automate fini mathématique est un modèle intuitif d'un automate fini réel. Pour décrire un automate fini réel, il n'est pas question de le démonter afin de connaître sa structure interne. En effet, même si nous connaissons déjà sa structure interne, nous ne pouvons pas dire que nous le connaissons vraiment. Tout comme dans la vie réelle, nous n'avons pas besoin de connaître comment une machine à laver fonctionne pour que nous puissions l'utiliser. Pour maîtriser un automate fini réel, nous avons seulement besoin de connaître tous ses états possibles, c'est-à-dire les fonctions possibles de la machine, et savoir en même temps comment donner des instructions pour qu'il nous offre les services commandés, ce qui revient à dire qu'il passe dans les états qui nous intéressent. À notre connaissance, le système d'éclairage est peut-être l'automate fini réel le plus simple. Un tel système est composé d'une ampoule électrique et d'un bouton de contrôle. Il possède alors deux états possibles : l'ampoule est éteinte ou allumée, ce qui sera noté respectivement a et b. À l'aide du bouton de contrôle, nous pouvons donner deux sortes d'instructions de nature opposée à l'ampoule : éteindre ou allumer, ce que nous désignerons respectivement par 0 et 1. Ainsi le système d'éclairage fonctionne en passant d'un état à un autre, en suivant notre suite d'instructions donnée qui est une suite de 0 et 1.

Un automate fini mathématique est donc un quadruplet $\mathcal{A} = (S, i, \Sigma, t)$, qui est composé, d'un alphabet S d'états (l'un de ses états, disons i, est distingué et appelé *état initial*), et d'une application $t : S \times \Sigma \to S$, appelée *fonction de transition.*

Date : Le 6 juillet 2003.

L'alphabet Σ est alors l'ensemble d'instructions, et l'automate fini $\mathcal{A}$ passe d'un état à un autre en suivant les instructions données.

À titre d'exemple, nous explicitons le système d'éclairage étudié précédemment. Dans ce cas, nous avons

$$S = \{a, b\},\ i = a,\ \Sigma = \{0, 1\},$$

et la fonction de transition t est définie par

$$t(s, 0) = a,\ \text{et}\ t(s, 1) = b,$$

pour tout $s \in S$. Nous verrons plus loin que cet automate est précisément l'automate identité qui sera discuté et étudié dans l'exemple 2.

Comme toutes les théories mathématiques, la théorie des automates finis aussi contient deux parties inséparables : théorie élémentaire, et applications. Il est donc naturel pour nous de discuter, dans la première partie (les paragraphes 5 à 10) de ce mémoire, des propriétés arithmétiques et topologiques des automates finis. Cette partie est fondée sur [121], et il sera question des automates fidèles et strictement fidèles, automates irréductibles (ou faiblement irréductibles) et automates premiers, automates homogènes, automates minimaux, automates inversibles, *etc.* Comme application, nous donnons une étude assez soigneuse des automates d'Ising, issus du modèle de physique théorique bien connu : la chaîne d'Ising unidimensionnelle. Pour leurs autres propriétés, voir [10], [78], [79], [69], [11], [120], et [121].

Les applications des automates finis sont diverses et nombreuses. Dans la suite, nous discuterons seulement deux sortes d'applications bien différentes en apparence.

Nous commençons par l'application de cette théorie à l'étude de la transmission de l'information. Pour cela, nous devons d'abord examiner de plus près les systèmes de communication usuels. Il se trouve que dans la vie réelle, un tel système sert à transférer des messages codés en mots binaires finis, qui seront décodés ensuite par le receveur en lisant les états du système apparus sucessivement pendant la transmission. Tout cela entre parfaitement dans le cadre des automates finis. En d'autres termes, un système de communication peut se simplifier en un automate fini qui consiste à transmettre des informations codées en suites de 0 et 1. Pour une raison ou une autre, le système va produire des bruits pendant la transmission qui vont perturber les informations transmises. L'étude des causes de ces bruits est importante et a occupé une place primordiale dans la théorie de l'information. Selon leurs sources, ces causes peuvent se classifier en deux catégories : celles de l'extérieur liées à des raisons physiques ou statistiques, et celles de l'intérieur liées à la structure interne du système. Grâce aux travaux remarquables, en particulier de C. E. Shannon et des autres, les facteurs extérieurs sont plus ou moins bien compris, et nous pouvons trouver dans la littérature un grand nombre d'excellents livres et articles sur ce sujet (voir par exemple [95], [94] et sa bibliographie). Cependant les causes les plus importantes ne sont pas de l'extérieur mais de l'intérieur qui proviennent de la structure interne de notre système de communication. Au premier stade de notre étude, nous pouvons ignorer complètement les bruits produits par des causes extérieures puisqu'ils sont déjà bien compris, et nous pouvons donc nous concentrer sur les facteurs intérieurs. Il se trouve que notre étude est alors liée au problème général suivant : *étant donné un système de communication $\mathcal{A}$, comment pouvons nous mesurer ses bruits intrinsèques ?*

À cette fin, nous faisons des expériences de transmission sur le système $\mathcal{A}$ en le nourrissant d'informations. Une information est alors représentée par une suite

binaire η. En appliquant η à $\mathcal{A}$, nous obtenons l'information sortante $\mathcal{A}\eta$ encodée en langage reconnaissable seulement par $\mathcal{A}$ lui-même. Ainsi pour reconnaître $\mathcal{A}\eta$, nous avons besoin d'un traducteur φ pour la traduire en langage compréhensible, et le résultat traduit sera noté $\varphi(\mathcal{A}\eta)$. Maintenant il faut comparer l'information originale η et le résultat final $\varphi(\mathcal{A}\eta)$. À cet usage, nous choisissons d'avance une méthode de comparaison $\mathbf{d}$. Alors $\mathbf{d}(\varphi(\mathcal{A}\eta), \eta)$ est la distorsion de cettte expérience de communication. Puisque nous ignorons complètement les erreurs causées par les raisons extérieures, théoriquement nous pouvons raffiner notre traducteur φ autant que possible pour exclure toutes les erreurs possibles. L'opacité

$$\Omega^{\mathbf{d}}(\mathcal{A}) = \sup_{\eta} \inf_{\varphi} \mathbf{d}(\varphi(\mathcal{A}\eta), \eta) \tag{1}$$

mesure alors les bruits intrinsèques de $\mathcal{A}$, qui met en évidence le plus grand défaut de toutes les expériences de transmission.

Une étude un peu plus poussée montre que la méthode de comparaison $\mathbf{d}$ joue un rôle crucial dans la théorie des opacités des automates finis (voir [118]), ce qui est d'ailleurs bien compréhensible. Pour l'opacité liée à la semi-norme quadratique que nous allons définir plus loin, nous avons une théorie assez satisfaisante (*cf.* [120]). Plus précisément, nous disposons dans ce cas d'un algorithme qui nous permet de calculer explicitement l'opacité de tout automate fini donné. Nous connaissons également beaucoup d'autres propriétés assez fines des opacités des automates finis. Par exemple, nous savons comment caractériser les automates transparents dont les opacités sont minimales, et les automates opaques dont les opacités sont maximales. Tout cela constitue la théorie des opacités (voir [118], [35], [120] et [122]), qui sera discutée dans la deuxième partie du mémoire (les paragraphes 11 à 18).

L'autre application de la théorie des automates finis concerne la transcendance de certaines séries formelles issues du module de Carlitz. Cette étude constitue la troisième partie de ce mémoire, et s'appuie sur le célèbre théorème de G. Christol, T. Kamae, M. Mendès France et G. Rauzy (*cf.* [36], [37], [2], et [103]), et aussi sur les diverses généralisations de ce dernier résultat (voir [93], [96], [63] et [4]).

Avant d'entrer dans les détails, il est mieux pour nous de faire une digression sur la théorie du module de Carlitz. L'approche que nous adoptons pour la présenter, n'est peut-être pas la plus intelligente, mais sans doute la plus directe et intuitive. En fait, nous allons l'aborder par une comparaison avec le cas réel classique.

Il est intéressant de retracer ici brièvement l'histoire des nombres usuels. Nos ancêtres ont découvert d'abord les entiers positifs, puis les entiers négatifs, et enfin l'élément neutre 0 pour former le groupe additif $\mathbb{Z}$. Pour faire la division, on a ensuite ajouté les inverses multiplicatifs et on a alors obtenu le corps $\mathbb{Q}$. Il se trouve que $\mathbb{Q}$ n'est pas "continu" au sens qu'il ne couvre pas la droite tout entière. Il faut donc le compléter par rapport à la value absolue usuelle pour obtenir le corps complet $\mathbb{R}$. Mais ce dernier n'est pas "parfait" non plus, car une équation aussi simple que $x^2+1=0$ n'y a pas de solution. Il faut donc y ajouter i comme solution imaginaire de cette dernière équation pour construire le corps "idéal" $\mathbb{C}$, qui est à la fois complet topologiquement et clos algébriquement. Il est à noter que le groupe multiplicatif $\mathbb{C}^\times$ est commutatif, et possède donc une structure de $\mathbb{Z}$-module qui peut être formulée comme

$$n.\exp(z) := \exp(nz) \tag{2}$$

avec $n \in \mathbb{Z}$ et $z \in \mathbb{C}$. Nous remarquons que l'élément neutre de $\mathbb{C}^\times$ est 1 (noté $\mathbf{0}$) au lieu de 0. Par ailleurs la fonction exponentielle est entière sur $\mathbb{C}$, et ses périodes, c'est-à-dire les solutions de l'équation $\exp(z) = \mathbf{0}$, forment le $\mathbb{Z}$-module $2i\pi\mathbb{Z}$. Il est intéressant de constater ici que 2 est précisément le nombre des éléments inversibles dans $\mathbb{Z}$ pour la multiplication. De plus pour tout $z \in \mathbb{C}$, nous avons, d'après le classique théorème de Weierstrass sur la factorisation des fonctions entières,

$$2\sinh(z/2) = \exp(z/2) - \exp(-z/2) = z \prod_{\alpha \in 2i\pi\mathbb{Z}\setminus\{0\}} (1 - \frac{z}{\alpha}), \tag{3}$$

où la convergence du produit infini est prise au sens de Cauchy.

La construction du module de Carlitz est tout à fait analogue à ce que nous avons fait plus haut, sauf que nous commençons par $\mathbf{A} := \mathbb{F}_q[T]$ l'anneau intègre des polynômes de la variable T à coefficients dans le corps fini $\mathbb{F}_q$ au lieu de l'anneau intègre $\mathbb{Z}$. Nous passons ensuite au corps des fractions $\mathbf{k} := \mathbb{F}_q(T)$ de $\mathbb{F}_q[T]$. Ce corps n'est pas complet pour la valeur absolue $|\cdot|_\infty$ définie par

$$\left|\frac{P}{Q}\right|_\infty = q^{\deg(P)-\deg(Q)},$$

avec P, $Q \in \mathbb{F}_q[T]$ et $Q \neq 0$, qui donne la "taille" de l'élément à mesurer, et imite la valeur absolue usuelle sur $\mathbb{Q}$. Nous le complétons par rapport à $|\cdot|_\infty$, et nous obtenons alors $\mathbf{k}_\infty := \mathbb{F}_q((1/T))$ le corps des séries formelles de Laurent sur $\mathbb{F}_q$. Mais ce dernier n'est pas clos algébriquement, il est donc nécessaire pour nous d'envisager une clôture algébrique $\overline{\mathbf{k}}_\infty$ de $\mathbf{k}_\infty$, et d'y étendre canoniquement la valeur absolue $|\cdot|_\infty$. Malheureusement $\overline{\mathbf{k}}_\infty$ n'est pas complet pour $|\cdot|_\infty$. Nous devons donc le compléter encore, et nous obtenons cette fois le corps $\mathbf{C}_\infty$ qui est enfin topologiquement complet et algébriquement clos. Ce dernier va jouer dans notre étude le rôle du corps des nombres complexes $\mathbb{C}$.

Maintenant nous définissons une nouvelle structure de $\mathbf{A}$-module sur $\mathbf{C}_\infty$ qui est en parfaite analogie avec celle sur $\mathbb{C}$ définie par la relation (2).

Pour tout $z \in \mathbf{C}_\infty$, posons $\sigma(z) = z^q$. Alors σ est un automorphisme de $\mathbf{C}_\infty$, appelé l'automorphisme de Frobenius du corps $\mathbf{C}_\infty$. Notons $\mathbf{A}[\sigma]$ l'anneau engendré sur $\mathbf{A}$ par σ, et définissons, pour tout $a = \sum_{j=0}^{k} a_j T^j \in \mathbf{A}$ avec $a_j \in \mathbb{F}_q$ $(0 \leqslant j \leqslant k)$,

$$C_a = \sum_{j=0}^{k} a_j (C_T)^j,$$

où $C_T = T + \sigma$. La nouvelle structure de $\mathbf{A}$-module sur $\mathbf{C}_\infty$, définie par

$$a.z := C_a(z), \text{ avec } a \in \mathbf{A} \text{ et } z \in \mathbf{C}_\infty,$$

est appelée le *module de Carlitz*, inventé par L. Carlitz dans les années trente du siècle dernier (*cf.* [29] et [58]). Mais souvent, l'application $a \mapsto C_a$ de $\mathbf{A}$ dans $\mathbf{A}[\sigma]$ est aussi appelée le module de Carlitz (voir par exemple [61]).

Il est démontré dans [29] (voir aussi [58] et [61]) qu'il existe une unique fonction entière e_C définie sur $\mathbf{C}_\infty$, de la forme

$$e_C(z) = \sum_{j=0}^{+\infty} \frac{z^{q^j}}{D_j},$$

avec $D_j \in \mathbf{A}$ et $D_0 = 1$, telle que pour tout $a \in \mathbf{A}$ et tout $z \in \mathbf{C}_\infty$,

$$a.e_C(z) = C_a(e_C(z)) = e_C(az). \tag{4}$$

Cette fonction e_C est appelée *la fonction exponentielle de Carlitz*, ce qui met en évidence l'analogie bien frappante entre les formules (2) et (4).

Comme $e_C(0) = 0$ et $e'_C(0) = 1$, nous pouvons en déduire formellement un inverse $\log_C$ de e_C (appelée la *fonction logarithmique de Carlitz*) par rapport à l'opération de la composition des fonctions, qui peut d'ailleurs s'exprimer comme

$$\log_C(z) = \sum_{j=0}^{+\infty} (-1)^j \frac{z^{q^j}}{L_j},$$

avec $L_j \in \mathbf{A}$ pour tout entier $j \geqslant 0$, et $L_0 = 1$.

Il est intéressant de noter que pour tout entier $j \geqslant 1$, D_j est le produit de tous les polynômes unitaires de degré j dans $\mathbf{A}$ et L_j est le plus petit multiple commun de tous les polynômes de degré j dans $\mathbf{A}$. Ainsi si nous définissons $[j] := T^{q^j} - T$, dont les zéros forment le corps fini $\mathbb{F}_{q^j}$, nous obtenons alors

$$D_j = \prod_{k=0}^{j-1} [j-k]^{q^k}, \text{ et } L_j = \prod_{k=1}^{j} [k].$$

Les polynômes $[j]$, D_j et L_j sont fondamentaux pour l'arithmétique de $\mathbf{A}$, et le lecteur se reportera par exemple à [29] et à [61] pour en savoir plus sur ce sujet.

Posons

$$\pi_C := \prod_{j=1}^{+\infty} \left(1 - \frac{[j]}{[j+1]}\right), \text{ et } \xi_C := (q-1)(-[1])^{1/q-1}\pi_C,$$

où $(-[1])^{1/q-1}$ est une racine $(q-1)$-ième de $-[1]$ dans $\mathbf{C}_\infty$. Les périodes de la fonction exponentielle e_C sont précisément les éléments de $\xi_C \mathbf{A}$, ainsi π_C joue le rôle de π, l'entier $q-1$, qui est le nombre des éléments inversibles dans $\mathbf{A}$ pour la multiplication, correspond à 2, et $2i\pi$ est analogue à ξ_C. Finalement nous remarquons que pour tout $z \in \mathbf{C}_\infty$, nous avons

$$e_C(z) = z \prod_{\alpha \in \xi_C \mathbf{A}} (1 - \frac{z}{\alpha}), \tag{5}$$

qui est la contrepartie de la formule (3), et montre que le module de Carlitz est une bonne généralisation des courbes elliptiques usuelles. Plus généralement, nous avons aussi les modules de Drinfel'd qui imitent les courbes elliptiques classiques et généralisent à leur tour le module de Carlitz, puis les T-modules qui sont analogues des variétés abéliennes, *etc.* Mais tout cela dépasse de loin le cadre de ce mémoire, et nous nous contentons d'indiquer ici quelques références [48], [49], [64], [56], [41], [66], [65], [16], [17], [110], [45], et [61] pour les lecteurs intéressés.

À partir de ces éléments fondamentaux $[j]$, D_j et L_j, nous pouvons construire, non seulement e_C et $\log_C$, qui sont les fonctions de base du module de Carlitz, mais aussi beaucoup d'autres fonctions intéressantes qui possèdent aussi des analogues classiques, comme la fonction zêta de Carlitz (voir [29], [130], et [43]), les fonctions Bessel de Carlitz ([32] et [47]), la fonction gamma de Carlitz-Goss ([30], [31], [58], [60], [99], [100], [6], [80], et [61]), *etc.* Une étude importante du module de Carlitz concerne la transcendance de valeurs de toutes ces fonctions. Sur ce plan, on a déjà obtenu beaucoup de résultats assez remarquables voire surprenants dont certains ne possèdent même pas d'analogues classiques. Cela montre que cette théorie est en général beaucoup plus réussie que la théorie classique des nombres transcendants.

À ce propos, nous disposons à l'heure actuelle de quatre méthodes appliquables. La première est due à L. I. Wade (*cf.* [106], [107], [108], [97], [42], [43], *etc.*) et connue maintenant sous son nom. Elle imite en fait l'une des méthodes classiques dans l'étude de la transcendance des nombres réels sur $\mathbb{Q}$. La deuxième est fondée sur la théorie des modules de Drinfel'd ainsi que ses diverses généralisations, et développée principalement par J. Yu (voir par exemple [125], [126], [127], [128], [129], [130], [131], [47], *etc.*). On peut la comparer avec l'étude des périodes des courbes elliptiques usuelles. La troisième est motivée par la méthode de Wade et par des considérations sur les approximations diophantiennes. Elle est exploitée surtout par B. de Mathan et marquée par son critère de transcendance (*cf.* [76], [77], [68], [46], *etc.*). La dernière est la méthode des automates finis (voir [5], [91], [21], [22], [23], [101], [102], [6], [80], [14], [113], *etc.*) qui sera discutée dans la troisième partie du mémoire. Elle a commencé avec J.-P. Allouche par la preuve élémentaire de la transcendance de π_C (voir [5]). Ce résultat fut originellement démontré par L. I. Wade par sa célèbre méthode (voir [106] et [107]).

Dans la pratique, toutes ces méthodes possèdent leur propre rayon d'influence. La méthode des modules de Drinfel'd est sans doute la plus puissante pusiqu'elle souvent nous donne des résultats de transcendance voire d'indépendance algébrique pour les valeurs des fonctions aux points algébriques non nuls. La méthode de Wade et celle de l'approximation diophantienne sont relativement plus faibles, mais ces deux-là nous permettent quand même de démontrer des résultats de transcendance pour les valeurs des fonctions aux points rationnels (voire algébriques pour des cas très exceptionels) non nuls. La méthode des automates finis est beaucoup plus restrictive, et souvent, elle nous donne seulement des résultats de transcendance pour les valeurs des fonctions au point $z = 1$! Ce dernier point est d'ailleurs bien compréhensible car la méthode des automates finis exige, en général, une bonne connaissance des coefficients des séries formelles en question.

Il est donc assez curieux pour nous de constater que la transcendance des valeurs de la fonction gamma de Carlitz-Goss (voir [102], [6], et [80]), démontrée par la méthode des automates finis, n'est pas démontrable par la méthode des modules de Drinfel'd, au moins pour l'instant. Par ailleurs J. Fresnel, M. Koskas, et B. de Mathan ont donné dans [53] une version généralisée et effective du théorème de G. Christol, T. Kamae, M. Mendès France et G. Rauzy, qui est la base de la méthode des automates finis, et ont démontré ensuite une généralisation du célèbre critère de B. de Mathan par la méthode des automates finis. De notre côté, récemment nous avons obtenu par la méthode de Wade une nouvelle preuve de la transcendance des valeurs de la fonction gamma de Carlitz-Goss (voir [124]). Ainsi la méthode de Wade, la méthode de l'approximation diophantienne, et la méthode des automates finis sont plus ou moins liées. Il sera donc intéressant, comme il a été suggéré par J.-P. Allouche, d'envisager les relations concrètes entre ces quatres méthodes.

Ce que nous venons de discuter touche seulement une toute petite partie de la théorie des automates finis. Pour en connaître plus, le lecteur peut se reporter à l'excellent livre de J.-P. Allouche et J. Shallit [13], mais aussi au très intéressant livre de N. Pytheas Fogg [88].

2. **Mots sur un alphabet.** Soit A un ensemble fini non vide. Nous l'appelons un *alphabet* et nous désignons par $\mathrm{Card}(A)$ le nombre des éléments de A. Tout membre de A est appelé *lettre*, et nous fixons ε un élément, n'appartenant pas à A, comme le *mot vide* sur A.

Notons $\mathbb{N} = \{0, 1, \ldots\}$ l'ensemble des nombres naturels. Définissons $A^0 := \{\varepsilon\}$, et pour tout entier $n \geqslant 1$, A^n comme étant l'ensemble des suites de longueur n à termes dans A. Enfin nous posons

$$A^* := \bigcup_{n=0}^{+\infty} A^n \text{ et } \overline{A} := A^* \cup A^{\mathbb{N}}.$$

Un élément w de $\overline{A}$ est appelé un *mot fini* si $w \in A^*$ et un *mot infini* si $w \in A^{\mathbb{N}}$, et la longueur de w est désignée par $|w|$. Plus précisément, nous avons $|w| = n$ pour tout $w \in A^n$, et $|w| = +\infty$ pour tout $w \in A^{\mathbb{N}}$. En particulier, nous avons $|\varepsilon| = 0$.

Soit $w = (w(n))_{0 \leqslant n < |w|} \in A^*$ et $v = (v(n))_{0 \leqslant n < |v|} \in \overline{A}$ deux mots sur A. La *concaténation* (ou le *produit*) entre w et v, notée $w * v$ (ou tout simplement wv), est encore un mot de longueur $|w| + |v|$ sur A, défini de la manière suivante :

$$(w * v)(n) = \begin{cases} w(n) & \text{si } 0 \leqslant n < |w|, \\ v(n - |w|) & \text{si } |w| \leqslant n < |w| + |v|. \end{cases}$$

Ainsi $w\varepsilon = \varepsilon w = w$, pour tout $w \in A^*$.

Il est clair que $(A^*, *)$ est un monoïde avec ε comme élément neutre. Il est aussi clair que par récurrence, nous pouvons également définir le produit d'un nombre fini ou infini des mots sur A. Par conséquent, tout mot $w = (w(n))_{0 \leqslant n < |w|} \in \overline{A}$ peut être représenté par un produit fini ou infini comme

$$w = \prod_{n=0}^{|w|-1} w(n) := w(0)w(1)\cdots.$$

Soit $w = (w(n))_{0 \leqslant n < |w|}$ et $v = (v(n))_{0 \leqslant n < |v|}$ deux mots sur A. Nous définissons

$$\mathbf{d}_A(w, v) = |A|^{-\max\{0 \leqslant n < \min(|w|, |v|) \mid w(j) = v(j),\ 0 \leqslant j \leqslant n\}}$$

si $w \neq v$, et $\mathbf{d}_A(w, v) = 0$ si $w = v$. Alors $\mathbf{d}_A$ est une distance sur $\overline{A}$. Muni de cette distance, $\overline{A}$ devient un espace métrique compact et contient A^* comme sous-ensemble dense. D'ailleurs $A^{\mathbb{N}}$ est aussi un sous-espace compact de $\overline{A}$.

3. Automates finis et suites automatiques. Commençons par la définition des automates finis (voir par exemple [50] et [40]).

Soit Σ un alphabet contenant au moins deux éléments. Un *automate fini* sur Σ, appelé un *Σ-automate fini*, est un quadruplet $\mathcal{A} = (S, i, \Sigma, t)$ composé

- d'un alphabet S des états ; l'un de ses états, disons i, est distingué et appelé *état initial*.
- d'une application $t : S \times \Sigma \to S$, appelée *fonction de transition*.

Par convention, nous posons $t(s, \varepsilon) = s$ pour tout $s \in S$, et étendons ensuite t en une application sur $S \times \Sigma^*$ (désignée toujours par t) telle que pour tout $s \in S$ et tous les $\rho, \sigma \in \Sigma^*$, nous avons $t(s, \rho\sigma) := t(t(s, \rho), \sigma)$. L'automate fini $\mathcal{A}$ induit ainsi une application (notée encore $\mathcal{A}$) de $\overline{\Sigma}$ dans $\overline{S}$ définie par

$$(\mathcal{A}\eta)(m) := t(i, \eta(0)\cdots\eta(m)),$$

pour tout $\eta \in \overline{\Sigma}$ et $m \in \mathbb{N}$ $(0 \leqslant m < |\eta|)$.

Il est utile de donner une représentation géométrique de $\mathcal{A} = (S, i, \Sigma, t)$. Les états sont représentés par des points ou noeuds ou sommets. Pour tout $s \in S$ et tout $\sigma \in \Sigma$, l'état s est lié à $t(s, \sigma)$ par une flèche orientée, étiquetée par σ. Cette flèche (appelée aussi une *arête*) est dite de *type* σ et notée $(s, \sigma, t(s, \sigma))$. Elle est

donc traitée comme un élément dans $S \times \Sigma \times S$, où s est le point de départ, σ est l'étiquette ou le type de la flèche, et $t(s,\sigma)$ est le point terminal. Nous obtenons ainsi un graphe orienté et étiqueté par les éléments de Σ, dont l'état initial i est marqué par une flèche incidente verticale. Nous l'appelons le graphe de $\mathcal{A}$ et dans la suite, nous allons constamment identifier $\mathcal{A}$ avec son graphe. Ainsi S devient l'ensemble des sommets, et Σ devient l'ensemble des étiquettes ou types des flèches.

Soit r, s deux états de l'automate fini $\mathcal{A} = (S, i, \Sigma, t)$. Nous disons que s est *accessible de* r s'il existe $\sigma \in \Sigma^*$ tel que $s = t(r,\sigma)$. En particulier, tout état s est accessible de lui-même car $t(s,\varepsilon) = s$. Un état de $\mathcal{A}$ est dit *accessible* s'il est accessible de l'état initial de $\mathcal{A}$. Si tous les états de $\mathcal{A}$ sont accessibles (resp. pour tous les états a et b de $\mathcal{A}$, l'état a est accessible de b et *vice versa*), nous appelons alors $\mathcal{A}$ un Σ-automate *accessible* (resp. *fortement accessible*). Dans la suite, nous allons nous borner à l'étude des automates accessibles.

Soit o une application définie sur S à valeurs dans un ensemble donné. Nous appelons le couple $(\mathcal{A}, o) = (S, i, \Sigma, t, o)$ un *Σ-automate avec fonction de sortie*, et o la *fonction de sortie* de $\mathcal{A}$. Comme l'automate fini $\mathcal{A}$, l'automate avec fonction de sortie $(\mathcal{A}, o)$ induit aussi une application (notée aussi $(\mathcal{A}, o)$) de $\overline{\Sigma}$ dans $\overline{o(S)}$ tel que pour tout $\eta \in \overline{\Sigma}$ et tout $m \in \mathbb{N}$ $(0 \leqslant m < |\eta|)$,

$$(\mathcal{A}, o)(\eta)(m) := o(\mathcal{A}\eta)(m) := o((\mathcal{A}\eta)(m)).$$

Ces deux applications $\mathcal{A}$ et $(\mathcal{A}, o)$ constituent le coeur de notre étude.

Finalement nous désignons par Card($\mathcal{A}$)le nombre des états de l'automate $\mathcal{A}$, par AUT(Σ)l'ensemble de tous les Σ-automates finis, et par AUTO(Σ)l'ensemble de tous lesΣ-automates avec fonction de sortie. Il est à noter que tout Σ-automate fini est aussi un Σ-automate avec fonction de sortie, dont la fonction de sortie est la fonction identité de l'ensemble des états. Ainsi nous pouvons traiter AUT(Σ) comme un sous-ensemble de AUTO(Σ).

Soit $p \geqslant 2$un entier et $\Sigma_p := \{0, 1, \ldots, p-1\}$. Une suite $u = (u(n))_{n \geqslant 0}$ est dite *p-automatique* s'il existe $(\mathcal{A}, o) = (S, i, \Sigma_p, t, o)$, un Σ_p-automate avec fonction de sortie, tel que $u(0) = o(i)$, et $u(n) = o(t(i, n_k \cdots n_0))$ pour tout entier $n \geqslant 1$ dont le développement p-adique standard est donné par

$$n = \sum_{j=0}^{k} n_j p^j.$$

Dans ce cas, nous disons aussi que u est engendré par $(\mathcal{A}, o)$. L'ensemble de toutes les suites p-automatiques sera noté AUTS(Σ_p).

Nous donnons maintenant quelques exemples simples pour illustrer les définitions et notations précédentes.

Exemple 1. *(Automate ayant un seul état) Soit $S = \{i\}$. Pour tout $\sigma \in \Sigma$, nous posons $t(i,\sigma) = i$. Alors le Σ-automate fini $\mathcal{I}_\Sigma = (S, i, \Sigma, t)$ est fortement accessible, et engendre la suite constante $iii\cdots$, si l'on a $\Sigma = \Sigma_p$ pour un certain entier $p \geqslant 2$.*

Exemple 2. *(Automate identité) Soit $S = \{a, b\}$, $i = a$, et $\Sigma = \{0, 1\}$. Nous définissons la fonction de transition t par*

$$t(s, 0) = a, \text{ et } t(s, 1) = b,$$

pour tout état $s \in S$. Il est clair que le Σ-automate fini $\mathcal{A} = (S, i, \Sigma, t)$ ainsi défini est fortement accessible, et si nous posons $o(a) = 0$ et $o(b) = 1$, alors $(\mathcal{A}, o)(\eta) = \eta$

pour tout $\eta \in \overline{\Sigma}$. *D'où vient le nom. Finalement nous remarquons que la suite 2-automatique engendrée par* $\mathcal{A}$ *est tout simplement la suite périodique* $abab\cdots$.

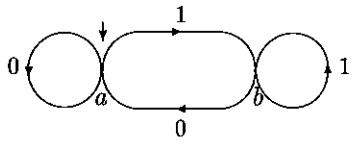


FIGURE 1. Automate identité

Exemple 3. *(Automate de Thue-Morse) Soit* $S = \{a, b\}$, $i = a$ *et* $\Sigma = \{0, 1\}$. *Nous définissons la fonction de transition* t *par*

$$t(a,0) = a,\ t(b,0) = b,\ t(a,1) = b,\ \text{et}\ t(b,1) = a.$$

Alors l'automate fini $\mathcal{A} = (S, i, \Sigma, t)$ *ainsi défini est fortement accessible et engendre la célèbre suite de Thue-Morse sur les lettres* a *et* b. *Pour en savoir plus sur cette suite et sur ses différentes généralisations, voir* [87], [105], [83], [75], [117], *et* [12].

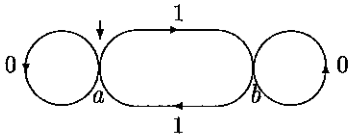


FIGURE 2. Automate de Thue-Morse

4. **Automates d'Ising.** Depuis la découverte des quasicristaux, la théorie des automates finis a trouvé une bonne place dans les recherches physiques pour simuler des systèmes apériodiques mais ordonnés. Un exemple type est la chaîne d'Ising. Une telle chaîne contient $N+1$ particules de spins $\pm$ alignées sur une droite. Pour tout $q \in \mathbb{N}$ $(0 \leqslant q \leqslant N)$, notons $\sigma(q)$ le spin de la q-ième particule. Toute suite finie de spins $\sigma = (\sigma(q))_{0 \leqslant q \leqslant N}$ détermine une unique configuration de notre système. Soit maintenant $\eta \in \{-1, +1\}^N$ une suite finie de $\pm$ qui représente par exemple la distribution de deux substances différentes ou des impuretés dans un alliage. Le hamiltonien de notre système pour la configuration $\sigma = (\sigma(q))_{0 \leqslant q \leqslant N}$ est alors défini par la formule suivante

$$\mathcal{H}_\eta(\sigma) = -J \sum_{q=0}^{N-1} \eta(q)\sigma(q)\sigma(q+1) - H \sum_{q=0}^{N} \sigma(q),$$

où $J > 0$ est la constante de couplage et $H \geqslant 0$ est le champ magnétique extérieur.

Les deux paramètres J et H étant donnés, un problème important et classique de la mécanique statistique est de chercher l'état d'équilibre du système, c'est-à-dire, trouver la configuration $\hat{\sigma}$ qui minimise le hamiltonien $\mathcal{H}_\eta(\sigma)$. Il est démontré par T. Kamae et M. Mendès France dans [69] (voir aussi [10]) qu'une telle configuration d'équilibre $\hat{\sigma}$ doit vérifier la relation de récurrence :

$$\hat{\sigma}(N) = \operatorname{sgn}(\delta(N)),\ \text{et}\ \hat{\sigma}(q) = \operatorname{sgn}\left(\delta(q) + 2\eta(q)\hat{\sigma}(q+1)\right)\ \text{pour}\ 0 \leqslant q < N,$$

où la suite finie $\delta = (\delta(q))_{0 \leqslant q \leqslant N}$ est définie par la relation de récurrence :

$$\delta(q+1) = \alpha + \eta(q)\mathrm{sgn}\,(\delta(q)) \min\{2,\ |\delta(q)|\} \quad (0 \leqslant q < N),$$

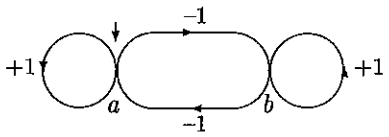
avec $\alpha = 2H/J$ et $\delta(0)$ fixé d'avance (par convention, ici sgn(0) peut prendre les deux valeurs $+1$ et -1 librement. Cela correspond au fait qu'il pourrait exister plusieurs d'états d'équilibre sous les mêmes conditions). Dans ce mémoire, nous nous bornons au cas $\delta(0) = \alpha + 2$. Alors l'étude de notre système se ramène à celle de la relation de récurrence suivante :

$$(6) \qquad \begin{cases} \delta(0) &= \alpha + 2, \\ \delta(q+1) &= \alpha + \eta(q)\mathrm{sgn}\,(\delta(q)) \min\{2, |\delta(q)|\}. \end{cases}$$

Comme la suite δ dépend de α et de η, il est donc légitime de la noter $\delta_\alpha(\eta)$. L'application $\eta \mapsto \delta_\alpha(\eta)$, définie de $\Sigma^*\backslash\{\varepsilon\}$ dans O_α^*, où $\Sigma = \{-1, +1\}$ et O_α est un sous-ensemble fini de $[\alpha - 2, \alpha + 2]$, peut être définie (voir [69] et [79]) par un automate fini avec fonction de sortie $(\mathcal{A}_\alpha, o_\alpha) = (S_\alpha, i_\alpha, \Sigma, t_\alpha, o_\alpha)$. En d'autres termes, pour tout $\eta = (\eta(j))_{0 \leqslant j < |\eta|} \in \Sigma^*$ et tout $q \in \mathbb{N}$ $(0 \leqslant q < |\eta|)$, nous avons

$$\delta_\alpha(\eta)(q+1) = o_\alpha\left(t_\alpha(i_\alpha, \eta(0)\cdots\eta(q))\right),$$

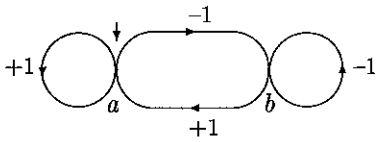
avec $\delta_\alpha(\eta)(0) = \alpha + 2$.



$$o_0(a) = +2 \quad \text{et} \quad o_0(b) = -2$$

FIGURE 3. Automate d'Ising $\mathcal{A}_0$

Pour $\alpha = 0$, la relation (6) devient $\delta(q+1) = 2\eta(0)\eta(1)\cdots\eta(q)$, et donne donc l'automate fini avec fonction de sortie défini dans la figure 3. Nous remarquons que si nous remplaçons $+1$ par 0 et -1 par 1 dans la figure 3, nous obtenons alors l'automate de Thue-Morse (voir l'exemple 3).



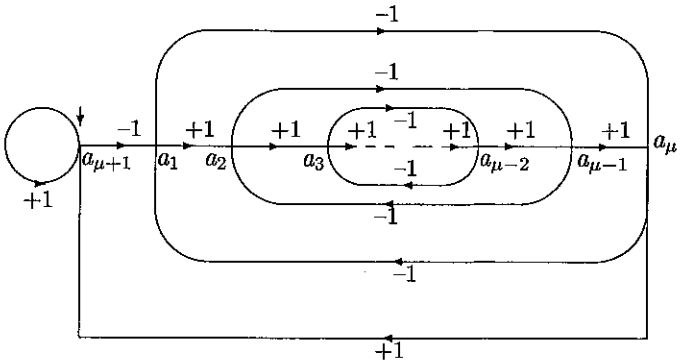
$$o_\alpha(a) = \alpha + 2 \quad \text{et} \quad o_\alpha(b) = \alpha - 2$$

FIGURE 4. Automate d'Ising $\mathcal{A}_\alpha$ avec $\alpha \geqslant 4$

Si $\alpha \geqslant 4$, la relation (6) devient $\delta(q+1) = \alpha + 2\eta(q)$, et l'automate fini avec fonction de sortie défini par la figure 4 satisfait à notre besoin. Une fois de plus, si nous remplaçons $+1$ par 0 et -1 par 1 dans la figure 4, nous obtenons alors l'automate identité (voir l'exemple 2).

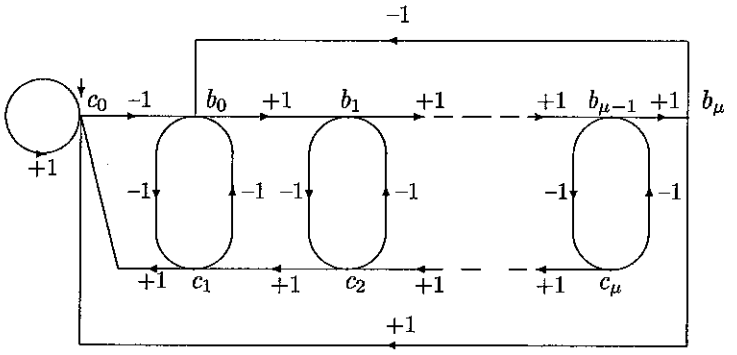
Quand $0 < \alpha < 4$, nous obtenons deux types d'automates finis avec fonction de sortie. Pour les distinguer, nous désignerons $\mathcal{A}_\alpha$ par $\mathcal{N}_\mu$ ou $\mathcal{L}_\mu$ selon que $4/\alpha \in \mathbb{N}$

ou pas, où $\mu = [4/\alpha]$ est la partie entière de $4/\alpha$. Pour plus de détails, le lecteur se reportera à la figure 5 et à la figure 6.



$$o_\alpha(a_j) = j\alpha - 2 \text{ avec } 4/\alpha \in \mathbb{N}$$

FIGURE 5. Automate d'Ising $\mathcal{A}_\alpha$ (noté $\mathcal{N}_\mu$)



$$o_\alpha(b_j) = (j+1)\alpha - 2 \text{ et } o_\alpha(c_j) = 2 - (j-1)\alpha \text{ avec } 4/\alpha \notin \mathbb{N}$$

FIGURE 6. Automate d'Ising $\mathcal{A}_\alpha$ (noté $\mathcal{L}_\mu$)

Dans la suite, nous allons présenter certaines propriétés des automates d'Ising. Pour en connaître d'autres, le lecteur peut consulter [10], [11], [69], [78] et [79].

5. Fidélité et fidélité stricte des automates finis. Étant donnée deux suites infinies $u = (u(n))_{n\geqslant 0}$ et $v = (v(n))_{n\geqslant 0}$, nous disons qu'elles sont *ultimement égales*, ce qui sera noté $u \sim v$, s'il existe $k \in \mathbb{N}$ tel que $u(n) = v(n)$, pour tout $n \geqslant k$.

Soit Σ un alphabet ayant au moins deux éléments. Nous munissons $\Sigma^{\mathbb{N}}$ de la mesure uniforme (borélienne) de Bernoulli μ_Σ, qui est déterminée par

$$\mu_\Sigma([w]) = |\Sigma|^{-|w|},$$

pour tout $w \in \Sigma^*$, où $[w]$ désigne l'ensemble de tous les éléments de $\Sigma^{\mathbb{N}}$, ayant w comme préfixe. Nous pouvons alors parler de "pour presque tout $\sigma \in \Sigma^{\mathbb{N}}$".

Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini. Nous disons que $\mathcal{A}$ est *fidèle* (*cf.* [78]) si pour presque tout $\sigma \in \Sigma^{\mathbb{N}}$, la relation $\sigma \sim \sigma'$ implique $\mathcal{A}\sigma \sim \mathcal{A}\sigma'$. Si c'est vrai

pour tout $\sigma \in \Sigma^{\mathbb{N}}$, c'est-à-dire, pour tout $\sigma \in \Sigma^{\mathbb{N}}$, $\sigma \sim \sigma'$ implique $\mathcal{A}\sigma \sim \mathcal{A}\sigma'$, nous disons alors que $\mathcal{A}$ est *strictement fidèle*.

Il est clair qu'un Σ-automate fini $\mathcal{A} = (S, i, \Sigma, t)$ est fidèle si et seulement si pour tout $s, s' \in S$ et pour presque tout $\sigma \in \Sigma^{\mathbb{N}}$, $\sigma \sim \sigma'$ implique $t(s, \sigma) \sim t(s', \sigma')$. De même, un Σ-automate fini $\mathcal{A} = (S, i, \Sigma, t)$ est strictement fidèle si et seulement si pour tout $s, s' \in S$ et tout $\sigma \in \Sigma^{\mathbb{N}}$, $\sigma \sim \sigma'$ implique $t(s, \sigma) \sim t(s', \sigma')$.

Le résultat suivant caractérise les automates fidèles (*cf.* [78]).

Proposition 1. *Un Σ-automate fini $\mathcal{A} = (S, i, \Sigma, t)$ est fidèle si et seulement s'il existe $s \in S$ et $\sigma \in \Sigma^*$ tels que $t(r, \sigma) = s$ pour tout $r \in S$.*

Ainsi l'automate d'Ising $\mathcal{A}_\alpha$ est fidèle si et seulement si $\alpha > 0$ (voir [78] dans lequel on peut aussi trouver une raison pour laquelle $\mathcal{A}_0$ n'est pas fidèle).

Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini. Un élément $\sigma \in \Sigma^*$ est appelé un *mot de synchronisation* de $\mathcal{A}$ si $t(s, \sigma)$ est indépendant de $s \in S$. Ainsi $\mathcal{A}$ est fidèle si et seulement s'il possède un mot de synchronisation. Les mots de synchronisation jouent un rôle très important dans l'étude des systèmes dynamiques symboliques. Par exemple, il est démontré dans [44], où l'auteur considère les suites bilatérales, que le système dynamique associé à une suite p-automatique, engendrée par un Σ_p-automate fini normalisé et primitif $\mathcal{A} = (S, i, \Sigma_p, t)$ (c'est-à-dire, $t(i, 0) = i$ et il existe un entier $k \geqslant 1$ tel que $[s]_k := \{t(s, \sigma) \mid \sigma \in \Sigma_p^k\} = S$ pour tout $s \in S$), possède un spectre discret si $\mathcal{A}$ a un mot de synchronisation (voir aussi [89]). Le lecteur trouvera dans [1] et [111] des discussions beaucoup plus détaillées sur les mots de synchronisation.

Pour les automates strictement fidèles, nous avons le résultat suivant (*cf.* [121]).

Proposition 2. *Un Σ-automate fini $\mathcal{A} = (S, i, \Sigma, t)$ est strictement fidèle si et seulement s'il existe un entier $k \geqslant 1$ tel que pour tout $\sigma \in \Sigma^k$ et tout état $r \in S$, l'état $t(r, \sigma)$ ne dépend que de σ mais pas de r.*

Ainsi un Σ-automate fini $\mathcal{A}$ est strictement fidèle si et seulement s'il existe un entier $k \geqslant 1$ tel que tous les mots de Σ^k sont des mots de synchronisation de $\mathcal{A}$. Par conséquent, l'automate ayant un seul état et l'automate identité sont strictement fidèles. Ainsi l'automate d'Ising $\mathcal{A}_\alpha$ est strictement fidèle pour $\alpha \geqslant 4$. Finalement nous remarquons que toute suite automatique engendrée par un automate fini strictement fidèle est nécessairement périodique (voir [121]). C'est précisément le cas de l'automate identité étudié dans l'exemple 2.

Il est aussi possible de définir et étudier les automates avec fonction de sortie qui sont fidèles ou strictement fidèles. La situation est un peu plus compliquée et sera examinée dans un travail en cours.

Pour clore ce paragraphe, nous résumons les résultats que nous avons obtenus sur la famille des automates d'Ising $(\mathcal{A}_\alpha, o_\alpha)_{\alpha \geqslant 0}$.

Soit $\alpha \geqslant 0$ un nombre réel. Pour tout $n \in \mathbb{N}$ dont le développement binaire standard est donné par

$$n = \sum_{j=0}^{k} n_j 2^j,$$

nous définissons

$$u_\alpha(n) = o_\alpha(t_\alpha(i_\alpha, (-1)^{n_k}(-1)^{n_{k-1}} \cdots (-1)^{n_0}).$$

La suite $u_\alpha = (u_\alpha(n))_{n\geqslant 0}$ est 2-automatique. Nous constatons aussi que u_0 est précisément la suite de Thue-Morse sur l'alphabet $\{-2, 2\}$, ainsi sa mesure de corrélation est continue singulière (voir par exemple [11] ou [117]), et u_0 elle-même est pseudo-aléatoire (*cf.* [24]). Soit maintenant $\alpha > 0$. Comme l'automate $\mathcal{A}_\alpha$ est primitif et fidèle, le système dynamique associé à u_α possède donc un spectre discret. En particulier, la mesure de corrélation de u_α est discrète, et la suite u_α elle-même est presque-périodique au sens de Bertrandias (voir [11]). Quand $\alpha \geqslant 4$, la conclusion est encore plus précise : u_α est en effet périodique de période 2 (voir l'exemple 2). En d'autres termes, lorsque α décroît de 4 à 0, la suite u_α est d'abord périodique, puis presque-périodique au sens de Bertrandias, puis pseudo-aléatoire. Il y a une "transition de phase" pour $\alpha = 0$. Tout cela possède une explication en physique : quand $\alpha > 0$, le champ magnétique extérieur est présent et le système est bien ordonné (la suite u_α est presque-périodique en moyenne) ; lorsque $\alpha \geqslant 4$, c'est-à-dire $H \geqslant 2J$, le champ magnétique extérieur domine les interactions intérieures, et le système devient hautement ordonné (la suite u_α est périodique). Mais quand $\alpha = 0$, le champ magnétique extérieur disparaît, et le système est alors gouverné par les interactions intérieures. Il devient donc chaotique (et la suite u_α devient pseudo-aléatoire).

Dans le paragraphe suivant, nous allons rappeler certaines définitions et résultats plus ou moins classiques (voir par exemple [50], [54], [55], [20], [69], [34], [92], et leurs bibliographies). Nous les appliquerons ensuite aux automates D'Ising.

6. **Certains aspects arithmétiques des automates finis.** Étant donné deux Σ-automates finis $\mathcal{A} = (S, i, \Sigma, t)$ et $\mathcal{A}' = (S', i', \Sigma, t')$, nous appelons $\mathcal{A}'$ un *facteur* de $\mathcal{A}$ (*cf.* [69] ou [50]), s'il existe une application surjective λ définie sur S à valeurs dans S' telle que $i' = \lambda(i)$, et pour tout $s \in S$ et tout $\sigma \in \Sigma$, nous avons

$$t'(\lambda(s), \sigma) = \lambda(t(s, \sigma)).$$

Dans ce cas, nous disons que λ est un *homomorphisme de* $\mathcal{A}$ et notons $\mathcal{A}' = \lambda(\mathcal{A})$. Un Σ-automate fini $\mathcal{A}$ possède au moins deux facteurs : $\mathcal{I}_\Sigma$ et $\mathcal{A}$ lui-même. Ces deux facteurs seront appelés les *facteurs triviaux* de $\mathcal{A}$, et l'ensemble de tous les facteurs de $\mathcal{A}$ sera noté $\mathrm{FAC}(\mathcal{A})$. Nous allons voir que $\mathrm{FAC}(\mathcal{A})$ est fermé pour le produit d'automates finis défini dans le paragraphe suivant.

Soit $\mathcal{A}$ un Σ-automate fini et λ un homomorphisme de $\mathcal{A}$. Si λ est aussi injective, alors l'application inverse λ^{-1} est un homomorphisme de $\lambda(\mathcal{A})$. Dans ce cas, nous disons que λest un *isomorphisme de* $\mathcal{A}$, et que $\mathcal{A}$et $\mathcal{A}'$sont *isomorphes*, ce qui sera noté $\mathcal{A} \simeq \mathcal{A}'$. Intuitivement deux automates finis sont isomorphes, si et seulement si, à la notation des états près, ils possèdent le même graphe. Nous obtenons ainsi sur $\mathrm{AUT}(\Sigma)$ une relation d'équivalence. Dans la suite nous identifierons toujours les Σ-automates isomorphes et utiliserons, s'il n'y a pas de confusion possible, les mêmes symboles $\mathcal{A}$,$\mathcal{B}$,... pour désigner les Σ-automates finis et les classes des Σ-automates isomorphes. En particulier, à isomorphisme près, il n'y a qu'un seul Σ-automate qui est composé d'un seul état, c'est-à-dire leΣ-automate fini $\mathcal{I}_\Sigma$.

Finalement nous remarquons que pour tout Σ-automate fini $\mathcal{A} = (S, i, \Sigma, t)$, toute application injective λdéfinie sur S peut être traitée comme un isomorphisme de $\mathcal{A}$. En fait, nous avons

$$\mathcal{A} \simeq \lambda(\mathcal{A}) := (\lambda(S), \lambda(i), \Sigma, \lambda \circ t \circ \tilde{\lambda})$$

où l'application $\tilde{\lambda}$ est définie sur $\lambda(S) \times \Sigma$ par

$$\tilde{\lambda}(\lambda(s), \sigma) := (s, \sigma),$$

pour tout $s \in S$ et tout $\sigma \in \Sigma$.

Proposition 3. *Soit $\mathcal{A}$ et $\mathcal{A}'$ deux Σ-automates finis. Si $\mathcal{A}'$ est un facteur de $\mathcal{A}$ et $\mathcal{A}$ est un facteur de $\mathcal{A}'$, alors $\mathcal{A} \simeq \mathcal{A}'$.*

Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini. Soit π une partition de S. Nous allons utiliser le même symbole π pour désigner la relation d'équivalence sur S induite par la partition π. Pour tout $s \in S$, notons $\pi(s)$ la classe d'équivalence de s sous π, et écrivons $r \equiv s \pmod{\pi}$ si $r \in \pi(s)$. Nous appelons π une *partition automatique* de l'automate fini $\mathcal{A}$ si pour tous les $r, s \in S$, la relation $r \equiv s \pmod{\pi}$ implique que

$$t(r, \sigma) \equiv t(s, \sigma) \pmod{\pi},$$

pour tout $\sigma \in \Sigma$. Par cette définition, nous obtenons tout de suite que les partitions triviales (S) et $(\{s\})_{s \in S}$ sont des partitions automatiques de $\mathcal{A}$. Finalement nous remarquons que les partitions automatiques sont en effet les partitions vérifiant la propriété de substitution définies dans [55, p. 22], et que dans la littérature, elles sont aussi appelées *partitions régulières à droite* (voir par exemple [20, p. 18]).

Soit π une partition automatique de $\mathcal{A}$. À partir de π, nous pouvons déduire un nouveau Σ-automate $\mathcal{A}/\pi = (\pi, \pi(i), \Sigma, t')$ (appelé le *Σ-automate quotient* de $\mathcal{A}$ par rapport à π), où la fonction de transition t' est définie par

$$t'(\pi(s), \sigma) = \pi(t(s, \sigma)),$$

pour tout $s \in S$ et tout $\sigma \in \Sigma$. Nous remarquons que $\mathcal{A}/\pi$ est un facteur de $\mathcal{A}$, dont l'homomorphisme correspondant est l'application $s \mapsto \pi(s)$ $(s \in S)$.

Réciproquement si $\mathcal{A}' = (S', i', \Sigma, t')$ est un facteur de $\mathcal{A}$, il existe alors un homomorphisme λ de $\mathcal{A}$, défini de S sur S', tel que $\mathcal{A}' = \lambda(\mathcal{A})$. Posons

$$\pi(\lambda) := \{\lambda^{-1}(\lambda(s)) \mid s \in S\}.$$

Alors $\pi(\lambda)$ est une partition automatique de $\mathcal{A}$ telle que $\mathcal{A}/\pi(\lambda) \simeq \mathcal{A}'$. Ainsi les facteurs et les Σ-automates quotients de $\mathcal{A}$ coïncident.

En d'autres termes, nous avons le résultat suivant (voir aussi [55]).

Proposition 4. *Soit $\mathcal{A} = (S, i, \Sigma, t)$ un automate fini. Il existe alors une bijection entre les facteurs et les partitions automatiques de $\mathcal{A}$. En particulier, le facteur trivial $\mathcal{I}_\Sigma$ (resp. $\mathcal{A}$) correspond à la partition triviale (S) (resp. $(\{s\})_{s \in S}$).*

Il est à noter que si π est une partition automatique de $\mathcal{A}$, et si Π est une partition automatique de $\mathcal{A}/\pi$, alors $(\mathcal{A}/\pi)/\Pi \simeq \mathcal{A}/\pi'$, où π' est définie par

$$\pi' = \left\{ \bigcup_{\sigma \in \mathbf{E}} \sigma \mid \mathbf{E} \in \Pi \right\}.$$

De la proposition 4, nous obtenons immédiatement

Corollaire 1. *Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini. Une application λ définie sur S est un homomorphisme de $\mathcal{A}$ si et seulement si $\pi(\lambda) := \{\lambda^{-1}(\lambda(s)) \mid s \in S\}$ est une partition automatique de $\mathcal{A}$.*

Corollaire 2. *Tout automate fini ne possède qu'un nombre fini de facteurs.*

Bien sûr, tout comme nous sommes déjà convenus dans ce paragraphe, nous devons aussi identifier les facteurs isomorphes dans le résultat précédent.

Maintenant nous allons définir et étudier les produits d'automates finis. Pour des définitions plus générales, le lecteur peut se reporter par exemple à [50], [54], [55], [69], et aux références qu'ils contiennent.

Soit $\mathcal{A} = (S, i, \Sigma, t)$ et $\mathcal{A}' = (S', i', \Sigma, t')$ deux Σ-automates finis. *L'automate produit* $\mathcal{A} \times \mathcal{A}'$ (noté aussi $\mathcal{A}\mathcal{A}'$) est défini ci-dessous (*cf.* [69]) :

- l'ensemble des états est $S \otimes S' := \{(t(i,\sigma), t'(i',\sigma)) \mid \sigma \in \Sigma^*\}$, dont (i, i') est l'état initial,
- la fonction de transition $t \otimes t'$ est définie par $t \otimes t'(s, \sigma) := (t(s_1, \sigma), t'(s_2, \sigma))$, pour tout $s = (s_1, s_2) \in S \otimes S'$ et tout $\sigma \in \Sigma$.

L'opération binaire $\times$ est associative, commutative et idempotente, c'est-à-dire, pour tous les Σ-automates finis $\mathcal{A}$, $\mathcal{A}'$, et $\mathcal{A}''$, nous avons

$$(\mathcal{A} \times \mathcal{A}') \times \mathcal{A}'' \simeq \mathcal{A} \times (\mathcal{A}' \times \mathcal{A}''),\ \mathcal{A} \times \mathcal{A}' \simeq \mathcal{A}' \times \mathcal{A},\ \text{et}\ \mathcal{A} \times \mathcal{A} \simeq \mathcal{A}.$$

Muni du produit $\times$, l'ensemble $\mathrm{AUT}(\Sigma)$ devient un monoïde commutatif, avec $\mathcal{I}_\Sigma$ comme élément neutre. D'ailleurs $\mathcal{I}_\Sigma$ est aussi le seul élément inversible pour $\times$.

Le résultat suivant justifie la définition des facteurs des automates finis.

Proposition 5. *Soit $\mathcal{A}$ et $\mathcal{A}'$ deux Σ-automates finis. Alors $\mathcal{A}$ et $\mathcal{A}'$ sont facteurs du produit $\mathcal{A} \times \mathcal{A}'$.*

Proposition 6. *Si $\mathcal{A}$ est un Σ-automate fini et $\mathcal{A}'$ est un facteur de $\mathcal{A}$, alors*

$$\mathcal{A} \simeq \mathcal{A} \times \mathcal{A}'.$$

Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini, et π_1 et π_2 deux partitions automatiques de $\mathcal{A}$. Alors l'intersection

$$\pi_1 \cap \pi_2 = \{\mathbf{s} \cap \mathbf{s}' \mid \mathbf{s} \in \pi_1,\ \mathbf{s}' \in \pi_2,\ \text{et}\ \mathbf{s} \cap \mathbf{s}' \neq \emptyset\}$$

est une nouvelle partition automatique de $\mathcal{A}$. En plus, nous avons aussi

$$\pi_1 \cap \pi_2 = \{\pi_1(s) \cap \pi_2(s) \mid s \in S\}.$$

Proposition 7. *Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini. Si π_1 et π_2 sont deux partitions automatiques de $\mathcal{A}$, alors*

$$\mathcal{A}/\pi_1 \times \mathcal{A}/\pi_2 \simeq \mathcal{A}/(\pi_1 \cap \pi_2).$$

Ce résultat signifie que la bijection entre $\mathrm{FAC}(\mathcal{A})$ et l'ensemble de toutes les partitions automatiques de $\mathcal{A}$, est en effet un homomorphisme du produit. En d'autres termes, le produit de deux facteurs de $\mathcal{A}$ correspond à l'intersection des deux partitions automatiques correspondantes de $\mathcal{A}$.

Soit $\mathcal{A} = (S, i, \Sigma, t)$ et $\mathcal{A}' = (S', i', \Sigma, t')$ deux Σ-automates finis. Nous disons que $\mathcal{A}$ *est divisible par* $\mathcal{A}'$ ou $\mathcal{A}$ *est un multiple de* $\mathcal{A}'$ (ce qui sera noté $\mathcal{A}' \mid \mathcal{A}$), s'il existe un Σ-automate fini $\mathcal{A}''$ tel que $\mathcal{A} \simeq \mathcal{A}' \times \mathcal{A}''$.

De ces deux propositions précédentes, nous obtenons aisément qu'un Σ-automate fini $\mathcal{A}$ est divisible par un autre Σ-automate fini $\mathcal{A}'$ si et seulement si $\mathcal{A}'$ est un facteur de $\mathcal{A}$. Il est clair que la divisibilité a défini un ordre partiel sur $\mathrm{AUT}(\Sigma)$, qui est réticulé pour ce dernier.

En fait, pour deux Σ-automates finis $\mathcal{A}'$ et $\mathcal{A}''$, $\mathcal{A}' \times \mathcal{A}''$ est le plus petit multiple commun de $\mathcal{A}'$ et $\mathcal{A}''$ ($\mathcal{A}' \times \mathcal{A}''$ divise tout multiple commun de $\mathcal{A}'$ et $\mathcal{A}''$), et le

produit de tous les facteurs communs de $\mathcal{A}'$ et $\mathcal{A}''$ est le plus grand facteur commun de $\mathcal{A}'$ et $\mathcal{A}''$ (c'est-à-dire, tout facteur commun de $\mathcal{A}'$ et $\mathcal{A}''$ le divise).

Un automate fini $\mathcal{A}$ est dit *irréductible* s'il ne possède que des facteurs triviaux. D'après la proposition 4, nous obtenons qu'un automate fini est irréductible si et seulement si toutes ses partitions automatiques sont triviales. Par conséquent, tout automate composé de deux états est irréductible. En particulier, l'automate de Thue-Morse (voir l'exemple 3) et l'automate identité (voir l'exemple 2) sont irréductibles. Ainsi les automates d'Ising $\mathcal{A}_0$ et $\mathcal{A}_\alpha$ ($\alpha \geqslant 4$) sont irréductibles.

En général, nous ne pouvons pas décomposer un automate arbitrairement donné en produit d'automates irréductibles. Cela complique la structure arithmétique des automates finis. Dans la suite, nous expliciterons $\mathrm{FAC}(\mathcal{N}_\mu)$ et $\mathrm{FAC}(\mathcal{L}_\mu)$ ($\mu \geqslant 1$), et montrons que les automates d'Ising $\mathcal{N}_\mu$ ($\mu \geqslant 2$) et $\mathcal{L}_\upsilon$ ($\upsilon \geqslant 1$) ne peuvent pas être décomposés en produits de facteurs irréductibles.

Pour $\mu = 1$, $\mathcal{N}_1$ est égal à $\mathcal{A}_4$, donc irréductible. Mais si $\mu \geqslant 2$, alors

$$\mathrm{FAC}(\mathcal{N}_\mu) = \{\mathcal{I}_\Sigma, \mathcal{N}'_\mu, \mathcal{N}_\mu\},$$

où $\mathcal{N}'_\mu$ est le facteur de $\mathcal{N}_\mu$, qui correspond à la partition automatique

$$\pi_\mu = \{\{a_{\mu+1}, a_\mu\}, \{a_1\}, \ldots, \{a_{\mu-1}\}\}$$

de $\mathcal{N}_\mu$. Ainsi $\mathcal{N}_\mu$ n'est pas irréductible car il contient un (seul) facteur non trivial. Ce simple fait nous conduit à introduire une nouvelle notion, appelée automates faiblement irréductibles. Plus précisément, nous disons qu'un automate fini est *faiblement irréductible* si toute décomposition de la forme $\mathcal{A} \simeq \mathcal{A}' \times \mathcal{A}''$ implique que $\mathcal{A}'$ ou $\mathcal{A}''$ est un facteur trivial de $\mathcal{A}$. Il est clair que tout automate irréductible est aussi faiblement irréductible. Mais la réciproque est évidemment fausse. C'est le cas de $\mathcal{N}_\mu$ ($\mu \geqslant 2$) : $\mathcal{N}_\mu$ est faiblement irréductible mais pas irréductible, car il contient $\mathcal{N}'_\mu$ comme un facteur non trivial.

Par récurrence sur le nombre des états, nous pouvons facilement montrer que tout automate fini peut se décomposer en produit de facteurs faiblement irréductibles. Cependant la décomposition n'est pas unique en général, comme nous allons le voir dans le cas de $\mathcal{L}_\mu$ ($\mu \geqslant 1$), qui est beaucoup plus compliqué que celui de $\mathcal{N}_\mu$.

Pour $\mu = 1$, $\mathrm{FAC}(\mathcal{L}_1)$ est composé des sept facteurs suivants :

$$\begin{aligned}
\pi_0 &= \{c_0,\ c_1,\ b_0,\ b_1\}\ (\mathcal{I}_\Sigma),\\
\pi_1 &= \{\{c_0\},\ \{b_0\},\ \{c_1,\ b_1\}\}\ (\mathcal{N}_2),\\
\pi_2 &= \{\{c_0,\ c_1\},\ \{b_0\},\ \{b_1\}\}\ (\mathcal{L}'_1),\\
\pi_3 &= \{\{c_0,\ c_1,\ b_1\},\ \{b_0\}\}\ (\mathcal{N}'_2),\\
\pi_4 &= \{\{c_0,\ b_1\},\ \{c_1\},\ \{b_0\}\}\ (\mathcal{N}_1 \times \mathcal{N}'_2),\\
\pi_5 &= \{\{c_0,\ b_1\},\ \{c_1,\ b_0\}\}\ (\mathcal{N}_1),\\
\pi_6 &= \{\{c_0\},\ \{c_1\},\ \{b_0\},\ \{b_1\}\}\ (\mathcal{L}_1).
\end{aligned}$$

Nous pouvons seulement décomposer $\mathcal{L}_1$ comme

$$\mathcal{L}_1 = \mathcal{N}_1 \times \mathcal{N}_2 = \mathcal{N}_1 \times \mathcal{L}'_1.$$

Mais ni $\mathcal{N}_2$ ni $\mathcal{L}'_1$ n'est irréductible. En fait, tous les deux contiennent $\mathcal{N}'_2$ comme unique facteur non trivial, ils sont donc faiblement irréductibles.

Pour $\mu \geqslant 2$, $\mathrm{FAC}(\mathcal{L}_\mu)$ est composé de dix éléments :

$$\begin{aligned}
\pi_0 &= \{c_j, b_j; 0 \leqslant j \leqslant \mu\}\ (\mathcal{I}_\Sigma),\\
\pi_1 &= \{\{c_0\}, \{c_j, b_{\mu-j+1}\}, \{b_0\}; 1 \leqslant j \leqslant \mu\}\ (\mathcal{N}_{\mu+1}),\\
\pi_2 &= \{\{c_0\}, \{c_1, b_\mu\}, \{c_j\}, \{b_{j-1}\}, \{b_0\}; 2 \leqslant j \leqslant \mu\}\ (\mathcal{N}'_\mu \times \mathcal{N}_{\mu+1}),\\
\pi_3 &= \{\{c_0, c_1\}, \{c_j\}, \{b_0\}, \{b_1\}, \{b_j\}; 2 \leqslant j \leqslant \mu\}\ (\mathcal{L}'_\mu),\\
\pi_4 &= \{\{c_0, c_1, b_{\mu-1}, b_\mu\}, \{c_j, b_{\mu-j}\}; 2 \leqslant j \leqslant \mu\}\ (\mathcal{N}'_\mu),\\
\pi_5 &= \{\{c_0, c_1, b_\mu\}, \{c_{j+1}\}, \{b_j\}; 0 \leqslant j \leqslant \mu-1\}\ (\mathcal{N}'_\mu \times \mathcal{N}'_{\mu+1}),\\
\pi_6 &= \{\{c_0, c_1, b_\mu\}, \{c_j, b_{\mu+1-j}\}, \{b_0\}; 2 \leqslant j \leqslant \mu\}\ (\mathcal{N}'_{\mu+1}),\\
\pi_7 &= \{\{c_0, b_\mu\}, \{c_j\}, \{b_{j-1}\}; 1 \leqslant j \leqslant \mu\}\ (\mathcal{N}_\mu \times \mathcal{N}'_{\mu+1}),\\
\pi_8 &= \{\{c_j, b_{\mu-j}\}; 0 \leqslant j \leqslant \mu\}\ (\mathcal{N}_\mu),\\
\pi_9 &= \{\{c_j\}, \{b_j\}; 0 \leqslant j \leqslant \mu\}\ (\mathcal{L}_\mu).
\end{aligned}$$

D'où nous obtenons immédiatement

$$\mathrm{FAC}(\mathcal{L}'_\mu) = \{\mathcal{I}_\Sigma, \mathcal{N}'_\mu, \mathcal{N}'_{\mu+1}, \mathcal{N}'_\mu \times \mathcal{N}'_{\mu+1}, \mathcal{L}'_\mu\},$$

ainsi $\mathcal{L}'_\mu$ est faiblement irréductible, et la décomposition en facteurs faiblement irréductibles de $\mathcal{L}_\mu$ est donnée par

$$\mathcal{L}_\mu = \mathcal{N}_\mu \times \mathcal{N}_{\mu+1} = \mathcal{L}'_\mu \times \mathcal{N}_{\mu+1} = \mathcal{N}_\mu \times \mathcal{L}'_{\mu+1}.$$

Une fois de plus, la décomposition n'est pas unique. Ici nous indiquons que la première décomposition a déjà été signalée dans [69].

En fait, le problème d'unicité est lié à une autre notion que nous discutons maintenant. Tout comme dans le cas classique des nombres premiers, nous disons qu'un automate fini $\mathcal{A}$ est *premier* si $\mathcal{A} \mid \mathcal{A}' \times \mathcal{A}''$ implique $\mathcal{A} \mid \mathcal{A}'$ ou $\mathcal{A} \mid \mathcal{A}''$. Il est clair que les automates faiblement irréductibles $\mathcal{N}_\mu$ et $\mathcal{L}'_\mu$ ($\mu \geqslant 2$) ne sont pas premiers. Cela explique pourquoi les décompositions précédentes ne sont pas uniques. Cependant nous avons quand même le résultat suivant, bien qu'à l'heure actuelle, nous ne sachions toujours pas s'il existe des automates premiers ou non.

Proposition 8. *Tout automate premier est faiblement irréductible.*

La réciproque est fausse. En effet, il existe des automates irréductibles qui ne sont pas premiers (voir le paragraphe 7).

7. **Automates homogènes.** Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate, $s \in S$ et $\sigma \in \Sigma$. Nous appelons s un *état homogène* de type σ de $\mathcal{A}$ si sur le graphe de $\mathcal{A}$, toutes les flèches incidentes à s sont de type σ. En d'autres termes, s'il existe $r \in S$ et $\rho \in \Sigma$ tels que $t(r, \rho) = s$, alors $\rho = \sigma$. Finalement nous appelons $\mathcal{A}$ un *automate homogène* si tous les états de $\mathcal{A}$ sont homogènes (cependant il ne faut pas confondre les automates homogènes discutés ici avec ceux étudiés dans [112]).

Notons que les automates homogènes étudiés ici sont appelés aussi *automates purs* dans [69], qui sont des objets assez différents de ceux introduits dans [25], bien qu'ils portent le même nom. Nous remarquons également que cette notion peut se généraliser aux automates généraux (non nécessairement déterministes), et que les automates de Glushkov sont homogènes (voir par exemple [33]).

Il est clair que l'automate identité étudié dans l'exemple 2 est homogène. Aussi pour tout $\alpha \geqslant 4$, l'automate d'Ising $\mathcal{A}_\alpha$ est homogène. Plus généralement, pour tout $\rho \in \Sigma$, si nous définissons $\mathcal{P}_\rho = (\Sigma, \rho, \Sigma, t_\rho)$, où la fonction de transition t_ρ est

donnée par $t_\rho(s,\sigma)=\sigma$, pour tout $s\in\Sigma$ et tout $\sigma\in\Sigma$, alors $\mathcal{P}_\rho$ est un Σ-automate homogène. Finalement nous remarquons que nous avons aussi $\mathrm{Card}(\mathcal{A})\geqslant\mathrm{Card}(\Sigma)$, pour tout Σ-automate homogène $\mathcal{A}$. Ainsi dans un certain sens, les Σ-automates homogènes $\mathcal{P}_\rho$ ($\rho\in\Sigma$) sont les Σ-automates homogènes "minimaux". Le résultat suivant précise ce point de vue, généralise et améliore un résultat de [69].

Proposition 9. *Un Σ-automate fini $\mathcal{A}=(S,i,\Sigma,t)$ est homogène si et seulement s'il existe $\rho\in\Sigma$ tel que $\mathcal{P}_\rho$ divise $\mathcal{A}$.*

Comme l'automate d'Ising $\mathcal{N}_1$ est homogène, ainsi l'automate d'Ising $\mathcal{L}_1$ est aussi homogène car il contient $\mathcal{N}_1$ comme un facteur.

Les automates homogènes aussi jouent un rôle important dans la théorie des opacités des auomates finis, que nous discuterons dans la deuxième partie de ce mémoire. En fait, nous pouvons montrer qu'un automate fini fortement accessible est transparent si et seulement s'il est homogène (*cf.* [118] et [35]).

Soit $\rho\in\Sigma$. Comme la fonction de transition t_ρ de $\mathcal{P}_\rho$ est indépendante de sa première variable, toute partition de Σ est alors automatique pour $\mathcal{P}_\rho$. Par conséquent, $\mathrm{FAC}(\mathcal{P}_\rho)$ est en bijection avec l'ensemble des partitions de Σ.

Pour tout $\sigma\in\Sigma$, posons $\pi_\sigma=\{\{\sigma\},\Sigma\backslash\{\sigma\}\}$. L'automate quotient P_ρ/π_σ est composé de deux états, donc irréductible. De la proposition 7, nous obtenons aussi

$$P_\rho\simeq\prod_{\sigma\in\Sigma}P_\rho/\pi_\sigma.$$

Ainsi P_ρ peut être décomposé en automates irréductibles.

Maintenant nous sommes en position de donner un exemple afin de montrer qu'un automate irréductible n'est pas forcément premier.

Exemple 4. *Soit $\Sigma=\{\alpha,\beta,\gamma,\delta\}$. Soit $\pi=\{\{\alpha,\beta\},\{\gamma,\delta\}\}$. Le Σ-automate quotient P_α/π est composé de deux états, c'est donc un facteur irréductible de P_α. Comme il est différent de tous les P_α/π_σ ($\sigma\in\Sigma$), il n'est donc pas premier.*

En d'autres termes, le produit de deux automates finis peut contenir des facteurs qui ne sont facteurs ni l'un ni l'autre de ces deux automates originaux.

Soit $\mathcal{A}=(S,i,\Sigma,t)$ un Σ-automate fini et π une partition de Σ. Un état s de $\mathcal{A}$ est appelé un *état π-homogène* de $\mathcal{A}$ si les types des flèches incidentes à s sont à valeurs dans une même classe de π, c'est-à-dire, il existe une classe $\mathbf{s}\in\pi$ telle que si $\sigma\in\Sigma$ et $r\in S$ satisfont à $t(r,\sigma)=s$, alors $\sigma\in\mathbf{s}$. Enfin nous appelons $\mathcal{A}$ un *automate π-homogène* si tous ses états sont π-homogènes. L'homogénéité est alors une spéciale π-homogénéité avec $\pi=\{\{\sigma\}\mid\sigma\in\Sigma\}$.

Comme dans le cas des automates homogènes, nous avons aussi un résultat similaire pour les automates π-homogènes.

Proposition 10. *Soit $\mathcal{A}$ un Σ-automate fini et π une partition de Σ. Alors $\mathcal{A}$ est π-homogène si et seulement s'il existe $\rho\in\Sigma$ tel que $\mathcal{P}_\rho/\pi$ divise $\mathcal{A}$.*

8. **Automates minimaux.** Soit $(\mathcal{A},o)$ et $(\mathcal{A}',o')$ deux Σ-automates finis avec fonction de sortie. Si nous avons $(\mathcal{A},o)(\eta)=(\mathcal{A}',o')(\eta)$ pour tout $\eta\in\overline{\Sigma}$, nous disons alors que $(\mathcal{A},o)$ et $(\mathcal{A}',o')$ sont *équivalents*, ce qui sera noté $(\mathcal{A},o)\approx(\mathcal{A}',o')$. Si en plus $\mathcal{A}\simeq\mathcal{A}'$, nous disons qu'ils sont *isomorphes* et écrivons $(\mathcal{A},o)\cong(\mathcal{A}',o')$. Cette relation d'isomorphisme entre les Σ-automates finis avec fonction de sortie, induit une relation d'équivalence sur $\mathrm{AUTO}(\Sigma)$. Dans la suite, nous identifierons toujours les Σ-automates avec fonction de sortie qui sont isomorphes.

Soit $(\mathcal{A}, o) = (S, i, \Sigma, t, o)$ un Σ-automate fini avec fonction de sortie. Nous disons que deux états r, s de $\mathcal{A}$ sont *indiscernables* si

$$o(t(r, \sigma)) = o(t(s, \sigma)),$$

pour tout $\sigma \in \Sigma^*$. Dans le cas où tous les états de $\mathcal{A}$ sont discernables, nous disons alors que $(\mathcal{A}, o)$ est un Σ-*automate minimal*. Il est clair que tout automate fini est minimal car la fonction de sortie correspondante est la fonction identité de l'ensemble des états, donc elle est injective.

Proposition 11. *Deux automates minimaux équivalents sont isomorphes.*

Il est bien connu que tout automate fini avec fonction de sortie est équivalent à un automate minimal (voir par exemple [40]). Le théorème suivant améliore ce résultat en montrant qu'en fait, tout automate minimal est le plus petit facteur commun de tous les automates avec fonction de sortie qui lui sont équivalents.

Proposition 12. *Pour tout Σ-automate fini avec fonction de sortie $(\mathcal{A}, o)$, il existe un unique Σ-automate minimal $(\mathcal{A}', o')$ tel que $(\mathcal{A}, o) \approx (\mathcal{A}', o')$ et $\mathcal{A}' \mid \mathcal{A}$.*

En fait, l'automate $\mathcal{A}'$ est le facteur de $\mathcal{A}$ correspodant à la partition de Nérode.

Dès lors, nous pouvons identifier $\mathrm{AUTO}(\Sigma)$ à l'ensemble de tous les Σ-automates minimaux, et ne considérons dans la suite que les automates minimaux.

Soit $p \geqslant 2$ un entier. Un Σ_p-automate fini $\mathcal{A} = (S, i, \Sigma_p, t)$ est dit *normalisé* si l'on a $t(i, 0) = i$. L'ensemble de tous les Σ_p-automates normalisés avec fonction de sortie sera noté $\mathrm{NAUTO}(\Sigma_p)$.

Il est intéressant de noter que l'homogénéité est une "propriété de produit". En d'autres termes, le produit avec un automate homogène donne un automate homogène. Cela nous rappelle bien sûr les idéaux de l'algèbre. En même temps, être normalisé est une "propriété de facteur" dans le sens que tout facteur d'un automate normalisé est aussi normalisé. Ces deux sortes de propriétés seront examinées du plus près dans un travail en cours.

Soit $p \geqslant 2$ un entier. Il est facile de voir que toute suite p-automatique peut être engendrée par un Σ_p-automate normalisé avec fonction de sortie. Plus précisément, on peut montrer qu'il existe une bijection Θ de $\mathrm{AUTS}(\Sigma_p)$ sur $\mathrm{NAUTO}(\Sigma_p)$, par laquelle toutes les propriétés de $\mathrm{NAUTO}(\Sigma_p)$ pourront être transférées à $\mathrm{AUTS}(\Sigma_p)$ et *vice versa* (voir [121]). Ce point de vue est bien important pour notre étude.

Proposition 13. *Soit $u_1, u_2, \ldots, u_k$ des suites p-automatiques complexes. Si elles sont linéairement dépendantes sur $\mathbb{C}$, alors l'un des $\mathcal{A}_j$ divise le produit de tous les autres $\mathcal{A}_j$, où nous posons $\Theta(u_j) = (\mathcal{A}_j, o_j)$ $(1 \leqslant j \leqslant k)$.*

Comme application, on obtient tout de suite que la suite de Thue-Morse, la suite de Rudin-Shapiro, la suite de Baum-Sweet, la suite de pliage de papier, et la suite constante 1 sont linéairement indépendantes sur $\mathbb{C}$ (voir par exemple [2] pour les définitions de toutes ces suites). Bien entendu, on peut aussi vérifier aisément ce résultat directement à partir de la définition de l'indépendance linéaire.

9. **Automates inversibles.** Soit $(\mathcal{A}, o) = (S, i, \Sigma, t, o)$ un automate fini avec fonction de sortie. Nous disons que $(\mathcal{A}, o)$ est *inversible à gauche* (resp. *inversible*) si l'application $\sigma \mapsto (\mathcal{A}, o)(\sigma)$ $(\sigma \in \overline{\Sigma}\backslash\{\varepsilon\})$ est injective (resp. bijective). Il est clair que $(\mathcal{A}, o)$ est inversible à gauche si et seulement si pour tout $s \in S$, toutes les valeurs $o(t(s, \sigma))$ $(\sigma \in \Sigma)$ sont différentes. Nous remarquons que dans ce cas, nous

avons $\mathrm{Card}(\Sigma) \leqslant \mathrm{Card}(o(S))$. Ainsi $\mathcal{I}_\Sigma$, l'automate ayant un seul état, n'est pas inversible à gauche bien qu'il soit inversible pour le produit d'automates finis. Nous remarquons également que tous les automates homogènes, en particulier l'automate identité, sont inversibles à gauche.

Le résultat suivant justifie la définition de l'inversibilité à gauche.

Proposition 14. *Un Σ-automate avec fonction de sortie $(\mathcal{A}, o) = (S, i, \Sigma, t, o)$ est inversible à gauche si et seulement s'il existe un $o(S)$-automate avec fonction de sortie $(\mathcal{A}', o')$ tel que pour tout $\sigma \in \overline{\Sigma}\backslash\{\varepsilon\}$, on a $(\mathcal{A}', o') \circ (\mathcal{A}, o)(\sigma) = \sigma$.*

Pour les automates inversibles, nous avons un résultat analogue.

Proposition 15. *Soit $(\mathcal{A}, o) = (S, i, \Sigma, t, o)$ un Σ-automate avec fonction de sortie. Il est alors inversible si et seulement s'il existe un $o(S)$-automate avec fonction de sortie $(\mathcal{A}', o')$ tel que pour tout $\sigma \in \overline{\Sigma}\backslash\{\varepsilon\}$ et tout $\delta \in \overline{o(S)}\backslash\{\varepsilon\}$, on a*

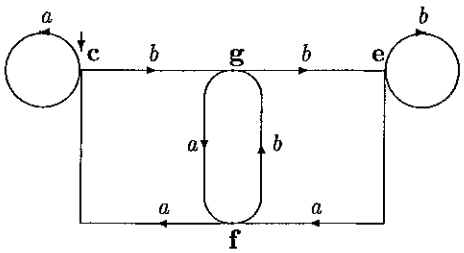
$$(\mathcal{A}', o') \circ (\mathcal{A}, o)(\sigma) = \sigma \text{ et } (\mathcal{A}, o) \circ (\mathcal{A}', o')(\delta) = \delta.$$

Il existe aussi une caractérisation assez simple des automates inversibles.

Proposition 16. *Un Σ-automate avec fonction de sortie $(\mathcal{A}, o) = (S, i, \Sigma, t, o)$ est inversible si et seulement s'il est inversible à gauche et* $\mathrm{Card}(o(S)) = \mathrm{Card}(\Sigma)$.

Ainsi l'automate de Thue-Morse, et l'automate identité ou plus généralement les Σ-automates homogènes "minimaux" $\mathcal{P}_\rho$ ($\rho \in \Sigma$) sont inversibles. Par conséquent, les automates d'Ising $\mathcal{A}_0$, $\mathcal{A}_\alpha$ ($\alpha \geqslant 4$), et $\mathcal{N}_1$ sont inversibles. Cependant nous pouvons démontrer que les automates d'Ising $\mathcal{N}_\mu$ ($\mu \geqslant 2$) et $\mathcal{L}_\nu$ ($\nu \geqslant 1$) sont inversibles à gauche, mais non inversibles.

Soit $(\mathcal{A}, o) = (S, i, \Sigma, t, o)$ et $(\mathcal{A}', o') = (S', i', o(S), t', o')$ deux automates avec fonction de sortie. Si $(\mathcal{A}', o') \circ (\mathcal{A}, o)(\sigma) = \sigma$ pour tout $\sigma \in \overline{\Sigma}\backslash\{\varepsilon\}$, nous disons alors que $(\mathcal{A}', o')$ est *un inverse à gauche* de $(\mathcal{A}, o)$, et que $(\mathcal{A}, o)$ est *un inverse à droite* de $(\mathcal{A}', o')$. Finalement nous appelons $(\mathcal{A}', o')$ *un inverse bilatéral* de $(\mathcal{A}, o)$ si $(\mathcal{A}', o')$ est un inverse à gauche et un inverse à droite de $(\mathcal{A}, o)$. Un automate avec fonction de sortie peut avoir plusieurs inverses à gauche ou à droite, mais il peut seulement avoir un inverse bilatéral au plus.



$$o'(\mathbf{c}) = o'(\mathbf{e}) = 0, \text{ et } o'(\mathbf{f}) = o'(\mathbf{g}) = 1$$

FIGURE 7. L'inverse bilatéral de l'automate de Thue-Morse

À titre d'exemple, nous donnons ici l'inverse bilatéral $(\mathcal{A}', o')$ de l'automate de Thue-Morse. Il est à noter que si nous redéfinissons la fonction de sortie o' par

$$o'(\mathbf{c}) = o'(\mathbf{f}) = 0, \text{ et } o'(\mathbf{e}) = o'(\mathbf{g}) = 1,$$

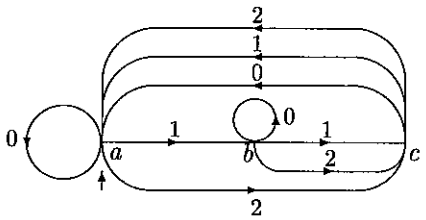
nous obtenons également l'inverse bilatéral de l'automate identité.

En général, si $\mathcal{A}_1$ et $\mathcal{A}_2$ sont deux automates inversibles ayant le même ensemble d'états, leurs inverses bilatéraux se distinguent seulement par les fonctions de sortie.

Ainsi les proposition 14 et proposition 15 peuvent-elles être reformulées comme suit : tout automate fini avec fonction de sortie possède un inverse à gauche (resp. un inverse bilatéral) si et seulement s'il est inversible à gauche (resp. inversible). Nous obtenons donc un analogue exact du résultat bien connu qu'une application g est injective (resp. bijective) si et seulement s'il existe une application h telle que la composition $h \circ g$ est l'application identité (resp. $h \circ g$ et $g \circ h$ sont les applications identités correspondantes).

Soit $(\mathcal{A}, o)$ un Σ-automate avec fonction de sortie. Si $(\mathcal{A}, o)$ possède un inverse à droite, alors l'application $\sigma \mapsto (\mathcal{A}, o)(\sigma)$ $(\sigma \in \overline{\Sigma}\backslash\{\varepsilon\})$ est surjective. Inspirés par les résultats précédents, nous pouvons nous demander si la réciproque est aussi vraie. Malheureusement la réponse est négative, comme l'exemple suivant le montre.

Exemple 5. *Soit $\Sigma = \{0, 1, 2\}$. Pour le Σ-automate avec fonction de sortie défini ci-dessous, l'application $\sigma \mapsto (\mathcal{A}, o)(\sigma)$ $(\sigma \in \overline{\Sigma}\backslash\{\varepsilon\})$ est surjective, mais $(\mathcal{A}, o)$ n'a aucun inverse à droite.*



$o(a) = +$ et $o(b) = o(c) = -$

FIGURE 8. Un contre-exemple

Soit $(\mathcal{A}, o) = (S, i, \Sigma, t, o)$ un Σ-automate avec fonction de sortie. Lorsque l'application $\sigma \mapsto (\mathcal{A}, o)(\sigma)$ $(\sigma \in \overline{\Sigma}\backslash\{\varepsilon\})$ est surjective, nous avons nécessairement

$$\mathrm{Card}(o(S)) \leqslant \mathrm{Card}(\Sigma).$$

Cette propriété n'est évidemment pas suffisante. Pour le moment, nous ne savons même pas comment caractériser les Σ-automates avec fonction de sortie $(\mathcal{A}, o)$ tels que l'application $\sigma \mapsto (\mathcal{A}, o)(\sigma)$ $(\sigma \in \overline{\Sigma}\backslash\{\varepsilon\})$ soit surjective. Nous ne savons pas non plus quand $(\mathcal{A}, o)$ peut posséder un inverse à droite. Cependant nous pouvons quand même remarquer que si o est injective, alors $\sigma \mapsto (\mathcal{A}, o)(\sigma)$ $(\sigma \in \overline{\Sigma}\backslash\{\varepsilon\})$ est une application surjective si et seulement si pour tout $s \in S$, nous avons

$$\{t(s, \sigma) \mid \sigma \in \Sigma\} = S,$$

et si cette condition est satisfaite, alors $(\mathcal{A}, o)$ possède un inverse à droite.

10. **Aspects topologiques des automates finis.** Désignons par $\mathrm{AUTO}_{\mathbb{C}}(\Sigma)$ l'ensemble des Σ-automates minimaux $(\mathcal{A}, o) = (S, i, \Sigma, t, o)$ vérifiant $o(S) \subseteq \mathbb{C}$. Sans perte de généralité, nous pouvons aussi supposer dans la suite que $\Sigma \subseteq \mathbb{C}$ et que la fonction de sortie o est définie sur $\mathbb{C}$ tout entier.

Soit $(\mathcal{A}_1, o_1)$ et $(\mathcal{A}_2, o_2)$ deux Σ-automates minimaux dans $\mathrm{AUTO}_{\mathbb{C}}(\Sigma)$. Pour tous les $a, b \in \mathbb{C}$ et tout état (r, s) de $\mathcal{A}_1 \times \mathcal{A}_2$, nous définissons

$$o_1 o_2((r, s)) = o_1(r) o_2(s), \text{ et } (a o_1 + b o_2)((r, s)) = a o_1(r) + b o_2(s),$$

et nous désignons par $(\mathcal{A}_1, o_1) \times (\mathcal{A}_2, o_2)$ (resp. $a(\mathcal{A}_1, o_1) + b(\mathcal{A}_2, o_2)$) l'unique Σ-automate minimal, équivalent à $(\mathcal{A}_1 \times \mathcal{A}_2, o_1 o_2)$ (resp. $(\mathcal{A}_1 \times \mathcal{A}_2, ao_1 + bo_2)$). Muni de ces deux opérations binaires, $\mathrm{AUTO}_{\mathbb{C}}(\Sigma)$ est une $\mathbb{C}$-algèbre, dont $(\mathcal{I}_\Sigma, 0)$ est élément zéro, $(\mathcal{I}_\Sigma, 1)$ est élément neutre pour la multiplication. Finalement nous remarquons qu'un élément $(\mathcal{A}, o) = (S, i, \Sigma, t, o) \in \mathrm{AUTO}_{\mathbb{C}}(\Sigma)$ est inversible pour la multiplication si et seulement si $0 \notin o(S)$.

Soit $(\mathcal{A}, o) \in \mathrm{AUTO}_{\mathbb{C}}(\Sigma)$. Pour tout $\sigma \in \Sigma^*$, nous posons

$$f_\sigma((\mathcal{A}, o)) = o(\mathcal{A}\sigma).$$

Alors f_σ est une application à valeurs complexes définie sur $\mathrm{AUTO}_{\mathbb{C}}(\Sigma)$. Désignons par $\mathcal{W}_{\mathbb{C}}(\Sigma)$ la topologie la plus faible (appelée *topologie faible*) sur $\mathrm{AUTO}_{\mathbb{C}}(\Sigma)$ telle que toutes les f_σ ($\sigma \in \Sigma^*$) soient continues. L'espace $(\mathrm{AUTO}_{\mathbb{C}}(\Sigma), \mathcal{W}_{\mathbb{C}}(\Sigma))$ est séparé (*cf.* [27, Ch. 10]). Mais il n'est pas complet.

Désignons par Φ l'application définie sur $\mathrm{AUTO}_{\mathbb{C}}(\Sigma)$, qui envoie chaque $(\mathcal{A}, o)$ de $\mathrm{AUTO}_{\mathbb{C}}(\Sigma)$ sur l'application $\sigma \mapsto f_\sigma((\mathcal{A}, o))$. Il est clair que l'application Φ est un homéomorphisme de $(\mathrm{AUTO}_{\mathbb{C}}(\Sigma), \mathcal{W}_{\mathbb{C}}(\Sigma))$ sur $\Phi(\mathrm{AUTO}_{\mathbb{C}}(\Sigma)) \subseteq \mathbb{C}^{\Sigma^*}$, muni de la topologie produit. D'ailleurs l'espace topologique $(\mathrm{AUTO}_{\mathbb{C}}(\Sigma), \mathcal{W}_{\mathbb{C}}(\Sigma))$ est métrisable et $\Phi(\mathrm{AUTO}_{\mathbb{C}}(\Sigma))$ est dense dans $\mathbb{C}^{\Sigma^*}$, qui est complet et métrisable.

Soit $(\mathcal{A}, o) = (S, i, \Sigma, t, o)$ un élément de $\mathrm{AUTO}_{\mathbb{C}}(\Sigma)$. Définissons

$$\|(\mathcal{A}, o)\| = \sup_{s \in S} |o(s)|.$$

Alors $\|\cdot\|$ est une norme sur $\mathrm{AUTO}_{\mathbb{C}}(\Sigma)$, et la topologie induite sur $\mathrm{AUTO}_{\mathbb{C}}(\Sigma)$, appelée *topologie uniforme*, est strictement plus forte que la toplogie faible $\mathcal{W}_{\mathbb{C}}(\Sigma)$. Malheureusement elle n'est pas complète non plus.

Proposition 17. *Soit $((\mathcal{A}_n, o_n))_{n \geqslant 0}$ une suite dans $\mathrm{AUTO}_{\mathbb{C}}(\Sigma)$, qui converge pour la topologie uniforme vers $(\mathcal{A}, o) \in \mathrm{AUTO}_{\mathbb{C}}(\Sigma)$. Il existe alors un entier $k \geqslant 0$ tel que $\mathcal{A}$ divise $\mathcal{A}_n$, pour tout entier $n \geqslant k$.*

Définissons maintenant la topologie forte $\mathcal{S}_{\mathbb{C}}(\Sigma)$ sur $\mathrm{AUTO}_{\mathbb{C}}(\Sigma)$ telle que l'espace vectoriel topologique $(\mathrm{AUTO}_{\mathbb{C}}(\Sigma), \mathcal{S}_{\mathbb{C}}(\Sigma))$ soit localement convexe et complet.

Pour tout entier $n \geqslant 1$, nous désignons par $\mathrm{AUTO}_{\mathbb{C}}^{(n)}(\Sigma)$ le sous-espace vectoriel de $\mathrm{AUTO}_{\mathbb{C}}(\Sigma)$, qui est engendré par les Σ-automates minimaux $(\mathcal{A}, o)$ satisfaisant à $\mathrm{Card}(\mathcal{A}) \leqslant n$, où $\mathrm{Card}(\mathcal{A})$ est le nombre des états de $\mathcal{A}$. Nous pouvons montrer aisément que la dimension de $\mathrm{AUTO}_{\mathbb{C}}^{(n)}(\Sigma)$ est finie. Comme le corps $\mathbb{C}$ est complet pour la valeur absolue usuelle, toutes les topologies séparées et compatibles avec la structure $\mathbb{C}$-vectorielle de $\mathrm{AUTO}_{\mathbb{C}}^{(n)}(\Sigma)$ coïncident (voir [26, EVT I, p. 14]). En particulier, la topologie faible et la topologie uniforme coïncident sur $\mathrm{AUTO}_{\mathbb{C}}^{(n)}(\Sigma)$. Et la topologie induite sera notée $\mathcal{S}_{\mathbb{C}}^{(n)}(\Sigma)$. Il est clair qu'elle est localement convexe. Il est aussi clair que les espaces de Banach $(\mathrm{AUTO}_{\mathbb{C}}^{(n)}(\Sigma), \mathcal{S}_{\mathbb{C}}^{(n)}(\Sigma))$ forment une suite strictement inductive d'espaces vectoriels topologiques localement convexes, dont la limite $(\mathrm{AUTO}_{\mathbb{C}}(\Sigma), \mathcal{S}_{\mathbb{C}}(\Sigma))$ est un espace $\mathbb{C}$-vectoriel localement convexe et complet (voir par exemple [26, EVT II, p. 35]). Finalement nous constatons que le dual algébrique de $\mathrm{AUTO}_{\mathbb{C}}(\Sigma)$ est égal au dual topologique de $(\mathrm{AUTO}_{\mathbb{C}}(\Sigma), \mathcal{S}_{\mathbb{C}}(\Sigma))$. En d'autres termes, toutes les formes linéaires sur $\mathrm{AUTO}_{\mathbb{C}}(\Sigma)$ sont continues pour la topologie forte $\mathcal{S}_{\mathbb{C}}(\Sigma)$ (voir [114, p. 58]).

La topologie $\mathcal{S}_{\mathbb{C}}(\Sigma)$ est certainement plus forte que la topologie uniforme. En particulier, la proposition 17 est aussi valable dans $(\mathrm{AUTO}_{\mathbb{C}}(\Sigma), \mathcal{S}_{\mathbb{C}}(\Sigma))$. D'ailleurs cette topologie est caractérisée par les deux propriétés suivantes.

Proposition 18. *Une suite $((\mathcal{A}_n, o_n))_{n\geqslant 0}$ est convergente dans $\mathrm{AUTO}_{\mathbb{C}}(\Sigma)$ pour la topologie forte si et seulement s'il existe un entier $k \geqslant 1$ tel que la même suite est convergente dans $(\mathrm{AUTO}^{(k)}_{\mathbb{C}}(\Sigma), \mathcal{S}^{(k)}_{\mathbb{C}}(\Sigma))$.*

La réciproque est aussi vraie.

Proposition 19. *Soit $((\mathcal{A}_n, o_n))_{n\geqslant 0}$ une suite de Cauchy dans $\mathrm{AUTO}_{\mathbb{C}}(\Sigma)$ pour la topologie faible $\mathcal{W}_{\mathbb{C}}(\Sigma)$. Si la suite $(\mathrm{Card}(\mathcal{A}_n))_{n\geqslant 0}$ est bornée, alors $((\mathcal{A}_n, o_n))_{n\geqslant 0}$ est convergente pour la topologie forte.*

Revenons à la famille des automates d'Ising $((\mathcal{A}_\alpha, o_\alpha))_{\alpha\geqslant 0}$.

Soit $\alpha_0 > 0$ un nombre réel. Pour tous les nombres réels α, β dans $[\alpha_0, +\infty[$, nous avons (voir le théorème 4 dans [69])

$$\|(\mathcal{A}_\alpha, o_\alpha) - (\mathcal{A}_\beta,\ o_\beta)\| \leqslant \left(1 + \left[\frac{4}{\alpha_0}\right]\right) |\alpha - \beta|,$$

l'application $\alpha \mapsto (\mathcal{A}_\alpha, o_\alpha)$ est donc uniformément continue de $[\alpha_0, +\infty[$ dans l'espace $(\mathrm{AUTO}_{\mathbb{C}}(\Sigma), \|\cdot\|)$. Mais comme pour tout $\alpha \geqslant \alpha_0$, nous avons aussi

$$\mathrm{Card}(\mathcal{A}_\alpha) \leqslant 2[4/\alpha] + 1 \leqslant 2[4/\alpha_0] + 1,$$

alors l'application $\alpha \mapsto (\mathcal{A}_\alpha, o_\alpha)$ est uniformément continue dans $[\alpha_0, +\infty[$ pour la topologie forte $\mathcal{S}_{\mathbb{C}}(\Sigma)$ (en vertu de la proposition 19), donc continue sur $]0, +\infty[$ pour cette même topologie. Elle est aussi faiblement continue au point $\alpha = 0$. Cependant elle n'est pas fortement continue en ce point car $\mathcal{A}_0$ ne divise pas $\mathcal{A}_\alpha$, même si α est proche de 0 (voir la proposition 17). En fait, au voisinage de $\alpha = 0$, la fonction $\alpha \mapsto \mathrm{Card}(\mathcal{A}_\alpha)$ n'est pas bornée (*cf.* proposition 18).

Le lecteur peut se reporter à [69] pour une autre approche de ce qui précède.

Soit $p \geqslant 2$ un entier. Nous désignons par $\mathrm{AUTS}_{\mathbb{C}}(\Sigma_p)$ (resp. $\mathrm{NAUTO}_{\mathbb{C}}(\Sigma_p)$) l'ensemble des suites p-automatiques complexes (resp. le sous-espace vectoriel des automates minimaux normalisés de $\mathrm{AUTO}_{\mathbb{C}}(\Sigma_p)$). Alors $\mathrm{AUTS}_{\mathbb{C}}(\Sigma_p)$ est un espace vectoriel sur $\mathbb{C}$ et la restriction de l'application Θ à $\mathrm{AUTS}_{\mathbb{C}}(\Sigma_p)$ (notée $\Theta_{\mathbb{C}}$) est un isomorphisme d'espaces vectoriels sur $\mathbb{C}$. Ainsi toutes les propriétés topologiques de $\mathrm{NAUTO}_{\mathbb{C}}(\Sigma_p)$ peuvent être transférées via $\Theta_{\mathbb{C}}$ sur $\mathrm{AUTS}_{\mathbb{C}}(\Sigma_p)$.

Nous disons qu'une famille de suites p-automatiques $(u_k)_{k\geqslant 0}$ est faiblement (resp. uniformément ou fortement) convergente vers une suite p-automatique u, si $(\Theta(u_k))_{k\geqslant 0}$ converge faiblement (resp. uniformément ou fortement) vers $\Theta(u)$.

Il est clair que la famille $(u_k)_{k\geqslant 0}$ converge faiblement vers u si et seulement si pour tout $n \in \mathbb{N}$, nous avons

$$\lim_{k\to\infty} u_k(n) = u(n).$$

De manière similaire, cette famille converge uniformément vers u si et seulement si

$$\lim_{k\to\infty} \sup_k |u_k(n) - u(n)| = 0.$$

Ainsi même si u n'est pas p-automatique, il a toujours un sens de dire que $(u_k)_{k\geqslant 0}$ converge faiblement (resp. uniformément) ou non vers u.

La caractérisation des suites p-automatiques fortement convergentes est un peu plus compliquée et nécessite une nouvelle notion, celle de p-noyau.

Pour toute suite $u = (u(n))_{n\geqslant 0}$, nous définissons

$$\mathcal{N}_p(u) := \left\{ \left(u(p^b n + a)\right)_{n\geqslant 0} \mid 0 \leqslant a < p^b, \text{ et } a, b \in \mathbb{N} \right\},$$

et l'appelons le *p-noyau* de u. Il est bien connu qu'une suite u est p-automatique si et seulement si $\mathcal{N}_p(u)$ est fini, et dans ce cas, nous avons aussi (*cf.* [2])

$$\mathrm{Card}(\mathcal{N}_p(u)) = \mathrm{Card}(\Theta_{\mathbb{C}}(u)).$$

Ainsi la proposition 18 peut se reformuler comme suit : une famille de suites p-automatiques $(u_n)_{n\geqslant 0}$ converge fortement vers une suite p-automatique u si et seulement si $(\mathrm{Card}(\mathcal{N}_p(u_n)))_{n\geqslant 0}$ est borné et $(u_n)_{n\geqslant 0}$ converge faiblement vers u.

Un problème important dans l'étude des suites p-automatiques concerne leur clôture topologique. Plus précisément, nous voulons savoir quand la limite d'une suite de suites p-automatiques est encore p-automatique. Il est clair que la topologie en question joue un rôle capital dans ce problème. Par exemple, la limite d'une suite de suites p-automatiques faiblement ou uniformément convergente n'est pas p-automatique en général. À propos de ce problème, nous avons le résultat suivant qui provient directement de la proposition 19.

Proposition 20. *Soit $(u_n)_{n\geqslant 0}$ une suite de suites p-automatiques complexes qui converge faiblement vers une suite complexe u. Si la suite $(\mathrm{Card}(\mathcal{N}_p(u_n)))_{n\geqslant 0}$ est bornée, alors u est p-automatique.*

11. **Opacité quadratique des automates finis.** À partir de ce paragraphe, nous entrons dans la deuxième partie du mémoire qui étudie la théorie des opacités des automates finis, commencée par M. Mendès France en 1991 (voir [79]).

Comme nous l'avons déjà indiqué dans l'introduction, nous traiterons dans cette partie tout automate fini comme un système de communication, qui consiste à transférer des informations. Un problème important de la théorie de la transmission de l'information concerne la relation entre les informations d'entrée et celles de sortie. Nous remarquons que ce problème est déjà abordé plus ou moins dans les paragraphes 5 et 9, dont l'étude est relativement locale au sens que nous cherchons les relations précises entre les suites d'entrée et celles de sortie. La théorie des opacités que nous allons discuter touche un autre aspect du problème. En fait, elle s'intéresse aux bruits intrinsèques produits par notre système, qui décrivent une relation plutôt globale entre les informations originales et celles de sortie.

Nous discutons d'abord l'opacité quadratique liée à la semi-norme $\|\cdot\|_2$ dont la définition suit. C'est la partie la plus réussie de notre théorie. Nous envisageons ensuite des opacités plus générales et en tirons quelques propriétés fondamentales. Nous verrons que la méthode de comparaison choisie joue un rôle crucial dans notre étude, comme nous l'avons bien signalé dans l'introduction.

Pour toute suite bornée à valeurs complexes $u = (u(m))_{m\geqslant 0}$, nous définissons

$$\|u\|_2 := \limsup_{k\to\infty} \left(\frac{1}{k} \sum_{m=0}^{k-1} |u(m)|^2 \right)^{1/2}.$$

Il est clair que $\|\cdot\|_2$ est une semi-norme sur l'espace de toutes les suites complexes bornées, que nous appelons *semi-norme quadratique*.

Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini. Sans perte de généralité, nous supposons toujours $\Sigma \subseteq \mathbb{C}$ dans cette partie. *L'opacité quadratique* de $\mathcal{A}$ est alors définie par

$$\Omega_2(\mathcal{A}) = \sup_{\eta} \inf_{\varphi} \|\varphi(\mathcal{A}\eta) - \eta\|_2,$$

où η parcourt l'ensemble des suites infinies sur Σ, et φ parcourt l'ensemble des applications complexes définies sur S.

En général, il est difficile voire impossible de calculer $\Omega_2(\mathcal{A})$ directement à partir de sa définition. On est donc conduit à introduire *l'opacité quadratique restreinte*

$$\omega_2(\mathcal{A}) = \sup_{\eta \ u.p.} \inf_{\varphi} \|\varphi(\mathcal{A}\eta) - \eta\|_2,$$

où η *u.p.* signifie que η parcourt l'ensemble des suites ultimement périodiques sur Σ, et où φ parcourt l'ensemble des applications complexes définies sur S.

C'ést cette quantité que M. Mendès France a étudiée en 1991 (*cf.* [79]) dans le cas où $S = \{-1, +1\}$. Quant à la définition de $\Omega_2(\mathcal{A})$, elle est apparue dans [115] pour la première fois. On verra plus loin qu'en fait, on a $\omega_2(\mathcal{A}) = \Omega_2(\mathcal{A})$ (voir [118] et [120]), qui résout un problème posé par M. Mendès France.

Pour mieux comprendre $\omega_2(\mathcal{A})$ et $\Omega_2(\mathcal{A})$, il est nécessaire pour nous d'avoir une bonne connaissance des circuits sur le graphe d'un automate fini. C'est ce que nous allons présenter dans le paragraphe suivant.

12. Circuits sur le graphe d'un automate fini. Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini. Un *chemin* (orienté) $\mathcal{P}$ sur (le graphe de) $\mathcal{A}$ est une suite finie ou infinie des flèches successives orientées sur $\mathcal{A}$. La longueur de $\mathcal{P}$ (notée $\ell(\mathcal{P})$) est le nombre des flèches orientées contenues dans $\mathcal{P}$. Comme toute flèche orientée sur $\mathcal{A}$ est traitée comme un élément de $S \times \Sigma \times S$, tout chemin $\mathcal{P}$ sur $\mathcal{A}$ peut alors être représenté par une suite sur $S \times \Sigma \times S$, et par simplicité, nous identifions souvent $\mathcal{P}$ et cette suite. Intuitivement nous pouvons identifier tout chemin $\mathcal{P}$ à l'ensemble de ses flèches orientées, comptées avec multiplicité. En d'autres termes, quand nous marchons sur $\mathcal{P}$, si nous sommes passés m fois sur la même flèche, nous la comptons comme m flèches différentes.

Tout chemin $\mathcal{P}$ sur $\mathcal{A}$ est déterminé par son point de départ, et par la suite des étiquettes apparues successivement dans $\mathcal{P}$, qui sera notée $\eta[\mathcal{P}]$, et appelée l'étiquette de $\mathcal{P}$. Réciproquement, tout $\eta = (\eta(m))_{m \geqslant 0} \in \overline{\Sigma}$ engendre un chemin

$$\mathcal{P}(\eta) := (i, \eta(0), (\mathcal{A}\eta)(0))((\mathcal{A}\eta)(0), \eta(1), (\mathcal{A}\eta)(1)) \ldots$$

sur le graphe de $\mathcal{A}$, qui décrit les flèches visitées en suivant η à partir de l'état initial. L'étiquette du chemin $\mathcal{P}(\eta)$ est alors la suite η elle-même.

Un *circuit* $\mathcal{C}$ sur $\mathcal{A}$ est un chemin orienté cyclique sur $\mathcal{A}$. Tout comme ci-dessus, tout circuit $\mathcal{C}$ peut aussi être représenté par une suite finie sur $S \times \Sigma \times S$, et nous identifions souvent $\mathcal{C}$ avec cette suite finie. Un circuit possède un point de base ou point de départ ; changer le point de base, c'est changer de circuit, lequel se déduit du premier par une permutation circulaire (cependant dans le calcul pratique des opacités, une telle distinction n'est pas nécessaire. Voir les paragraphes 13 et 15). Désignons par $\mathfrak{C}(\mathcal{A})$ l'ensemble de tous les circuits sur $\mathcal{A}$. Il est évident que $\mathfrak{C}(\mathcal{A})$ est non vide et denombrable, car $\mathcal{A}$ est accessible et ne possède qu'un nombre fini d'états. On verra que cet ensemble a une structure assez simple.

Soit C' et C'' deux circuits de $\mathcal{A}$ dont s' et s'' sont les points de base respectifs. Si s'' est aussi un sommet de C', par concaténation, nous allons définir un nouveau circuit de $\mathcal{A}$ (noté $C'C''$). Écrivons

$$C' = L_1 \cdots L_k \cdots L_m,$$

avec $L_j \in S \times \Sigma \times S$ $(1 \leqslant j \leqslant m)$, où s' est le point initial de L_1, s'' est le point terminal de L_k, et s'' n'apparaît pas parmi les L_j $(1 \leqslant j < k)$. Définissons alors

$$C'C'' := L_1 \cdots L_k C'' L_{k+1} \cdots L_m.$$

Cette définition peut s'expliquer intuitivement : nous partons de s', pris comme le point de départ de $C'C''$, et marchons le long de C' jusqu'à la première rencontre du sommet initial s'' de C''. Nous quittons ensuite C' pour rejoindre C'', et nous parcourons C'' tout entier jusqu'à son sommet terminal s''. Puis nous parcourons tout le reste de C' et nous nous retrouvons finalement à son sommet initial s'.

Soit C un circuit de $\mathcal{A}$. Nous appelons C un *circuit simple* si tout sommet de C n'a qu'une flèche incidente et qu'une flèche sortante. Comme l'automate fini $\mathcal{A}$ n'a qu'un nombre fini de sommets, il ne possède qu'un nombre fini de circuits simples, disons $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_n$. Considérons le $\mathbb{Z}$-module libre engendré par l'ensemble de tous les circuits simples sur $\mathcal{A}$, dont les éléments sont représentés par des sommes formelles finies $\sum_{j=1}^{n} d_j \mathcal{C}_j$, avec $d_j \in \mathbb{Z}$. Un circuit C de l'automate fini $\mathcal{A}$ est dit représentable par une somme formelle $\sum_{j=1}^{n} d_j \mathcal{C}_j$ avec $d_j \in \mathbb{N}$ (par simplicité, souvent nous écrivons directement $C = \sum_{j=1}^{n} d_j \mathcal{C}_j$), s'il existe une décomposition de cette somme formelle en circuits simples sous la forme

$$\mathcal{C}_{i_1} + \mathcal{C}_{i_2} + \cdots + \mathcal{C}_{i_m}$$

(l'ordre d'écriture étant significatif), où pour tout entier j $(1 \leqslant j \leqslant n)$, le circuit simple $\mathcal{C}_j$ apparaît exactement d_j fois, de sorte que par concaténation, nous avons

$$C = \mathcal{C}_{i_1} \mathcal{C}_{i_2} \cdots \mathcal{C}_{i_m}.$$

Dans ce cas, nous disons aussi que le circuit C parcourt la somme formelle. Par récurrence sur la longueur du circuit en question, nous pouvons montrer aisément que tout circuit sur $\mathcal{A}$ peut être représenté par une somme formelle de circuits simples. Cependant la représentation n'est pas forcément unique. En d'autres termes, pour tout circuit C sur $\mathcal{A}$, il existe toujours un point $d(C) = (d_j(C))_{1 \leqslant j \leqslant n}$ dans $\mathbb{N}^n \setminus \{O\}$ (où O est l'origine de $\mathbb{N}^n$) tel que le circuit C parcourt la somme formelle $\sum_{j=1}^{n} d_j(C) \mathcal{C}_j$, mais un tel point $d(C)$ n'est pas unique en général (*cf.* [118]). Heureusement cette non-unicité ne gênera pas la poursuite de notre étude.

Soit $\mathcal{P} = P_0 P_1 \cdots$ avec $P_j \in S \times \Sigma \times S$ un chemin infini sur l'automate fini $\mathcal{A}$. Soit $C = L_0 L_1 \cdots L_{m-1}$ $(L_j \in S \times \Sigma \times S)$ un circuit de $\mathcal{A}$. Nous disons que $\mathcal{P}$ s'enroule ultimement sur le circuit C s'il existe un entier $h \geqslant 0$ tel que pour tous les entiers $j, k \geqslant 0$ vérifiant $j \equiv k \pmod{m}$, nous avons $P_{j+h} = L_k$. Il est clair que cette définition n'est qu'une reformulation mathématique de notre vision géométrique.

Soit C un circuit sur $\mathcal{A}$ avec $s \in S$ comme point de base. Comme $\mathcal{A}$ est accessible, il existe donc un mot fini σ sur Σ tel que $s = t(i, \sigma)$. Désignons par δ l'étiquette du circuit C. Alors $\eta_C := \sigma\delta^\infty := \sigma\delta\delta\cdots$ est une suite ultimement périodique telle que le chemin infini $\mathcal{P}(\eta_C)$ (engendré par η_C) s'enroule ultimement sur C. Réciproquement, pour toute suite ultimement périodique η sur Σ, nous pouvons facilement montrer qu'il existe un circuit C_η sur $\mathcal{A}$ tel que le chemin infini $\mathcal{P}(\eta)$

(engendré par η) s'enroule ultimement sur $\mathcal{C}_\eta$ (voir [118]). Dans la suite, ce résultat sera utilisé implicitement en différentes occasions.

13. **Calcul de l'opacité quadratique des automates finis.** Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini dont les circuits simples sont $\mathcal{C}_1, \ldots, \mathcal{C}_n$. Soit $s \in S$ et $\sigma \in \Sigma$. Pour tout entier j $(1 \leqslant j \leqslant n)$, nous définissons $\delta^j_\sigma(s)$ ainsi : $\delta^j_\sigma(s) := 1$ si s est un sommet de $\mathcal{C}_j$ et si sur $\mathcal{C}_j$, la flèche incidente à s est de type σ ; sinon $\delta^j_\sigma(s) := 0$.

Soit $d = (d_1, \ldots, d_n) \in \mathbb{R}^n_+ \setminus \{O\}$, c'est-à-dire, $d_j \geqslant 0$ $(1 \leqslant j \leqslant n)$ et d est différent de l'origine O. Pour tout $s \in S$ et tout $\sigma \in \Sigma$, nous définissons

$$\lambda_{s,\sigma}(d) = \sum_{j=1}^{n} d_j \delta^j_\sigma(s), \text{ et } \lambda_s(d) = \sum_{\eta \in \Sigma} \lambda_{s,\eta}(d). \tag{7}$$

Finalement nous posons

$$\lambda(d) = \sum_{s \in S} \lambda_s(d) \tag{8}$$

Il est clair que pour tout entier j $(1 \leqslant j \leqslant n)$ et tout $s \in S$, $\sum_{\sigma \in \Sigma} \delta^j_\sigma(s)$ est précisément le nombre de flèches sur $\mathcal{C}_j$, incidentes à s. Il est égal à 1 ou 0 selon que s est un sommet de $\mathcal{C}_j$ ou non. Ainsi la longueur du circuit $\mathcal{C}_j$ vérifie

$$\ell(\mathcal{C}_j) = \sum_{s \in S} \sum_{\sigma \in \Sigma} \delta^j_\sigma(s).$$

Par conséquent, pour tout $d = (d_1, \ldots, d_n) \in \mathbb{R}^n_+ \setminus \{O\}$, nous avons

$$\lambda(d) = \sum_{s \in S} \lambda_s(d) = \sum_{s \in S} \sum_{\sigma \in \Sigma} \sum_{j=1}^{n} d_j \delta^j_\sigma(s) = \sum_{j=1}^{n} d_j \ell(\mathcal{C}_j). \tag{9}$$

Soit $\mathcal{C}$ un circuit sur $\mathcal{A}$. Il existe alors un point $d(\mathcal{C}) = (d_j(\mathcal{C}))_{1 \leqslant j \leqslant n} \in \mathbb{N}^n_+ \setminus \{O\}$ tel que l'on a $\mathcal{C} = \sum_{j=1}^{n} d_j(\mathcal{C}) \mathcal{C}_j$. On peut facilement voir que $\lambda(d(\mathcal{C}))$ est la longueur de $\mathcal{C}$ et que $\lambda_{s,\sigma}(d(\mathcal{C}))$ (avec $\sigma \in \Sigma$ et $s \in S$) est le nombre des flèches de type σ sur $\mathcal{C}$ incidentes à s. Tous ces nombres ne dépendent que de $\mathcal{C}$, mais ni du choix spécial de $d(\mathcal{C})$ ni du point de base de $\mathcal{C}$. Cette remarque est importante et explique pourquoi le fait que la décomposition d'un circuit générique en circuits simples n'est pas unique ne trouble pas notre étude sur les opacités.

Soit s un sommet de $\mathcal{A}$. Pour tout $d = (d_1, \ldots, d_n) \in \mathbb{R}^n_+ \setminus \{O\}$, définissons

$$F_s(d) := \inf_{x \in \mathbb{C}} \sum_{\sigma \in \Sigma} \lambda_{s,\sigma}(d) \, |x - \sigma|^2 .$$

L'infimum est atteint au point $x = \varphi_d(s)$ défini par

$$\varphi_d(s) := \frac{1}{\lambda_s(d)} \sum_{\sigma \in \Sigma} \lambda_{s,\sigma}(d) \sigma$$

si $\lambda_s(d) > 0$, et $\varphi_d(s) := 0$ sinon (en fait dans ce dernier cas, $\varphi_d(s)$ peut être choisi arbitrairement). De cette manière, nous avons défini sur S une fonction à valeurs complexes φ_d, qui sera utile dans notre calcul.

La fonction F_s est rationnelle et continue sur $\mathbb{R}^n_+ \setminus \{O\}$. Mais en général, elle n'est pas différentiable. En fait, elle possède seulement des dérivées partielles faibles.

Soit f une fonction définie sur $\mathbb{R}_+^n \setminus \{O\}$. Nous disons que f possède une dérivée partielle faible au point $d^0 = (d_1^0, \ldots, d_n^0) \in \mathbb{R}_+^n \setminus \{O\}$ par rapport à sa j-ième variable d_j $(1 \leqslant j \leqslant n)$, si la limite suivante existe (elle sera notée $\frac{\partial f}{\partial d_j}(d^0)$),

$$\lim_{x \to 0} \frac{1}{x} \left(f(d_1^0, \ldots, d_j^0 + x, \ldots, d_n^0) - f(d_1^0, \ldots, d_j^0, \ldots, d_n^0) \right)$$

où x varie dans $\mathbb{R}$ de sorte que $(d_1^0, \ldots, d_j^0 + x, \ldots, d_n^0) \in \mathbb{R}_+^n \setminus \{O\}$.

Enfin pour tout $d = (d_1, \ldots, d_n) \in \mathbb{R}_+^n \setminus \{O\}$ et pour toute fonction à valeurs complexes φ définie sur S, nous posons

$$G(d, \varphi) := \sum_{s \in S} \sum_{\sigma \in \Sigma} \lambda_{s,\sigma}(d) |\varphi(A) - \sigma|^2, \text{ et } \nu(d) := \inf_{\phi \in \mathbb{C}^S} G(d, \phi).$$

Il est clair que pour tout $d \in \mathbb{R}_+^n \setminus \{O\}$, nous avons $\nu(d) = G(d, \varphi_d)$. Ainsi la fonction ν possède aussi des dérivées partielles faibles sur $\mathbb{R}_+^n \setminus \{O\}$.

Avec ces notations et définitions, nous avons le théorème suivant (voir [120]) qui généralise, complète et corrige un résultat de [79]. Il est à noter que nos présentes notations ne coïncident pas exactement avec celles de M. Mendès France dans [79].

Théorème 1. *Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini dont les circuits simples sont $\mathcal{C}_1, \ldots, \mathcal{C}_n$. Nous avons alors*

$$\omega_2(\mathcal{A}) = \sup_{\mathcal{C} \in \mathfrak{C}(\mathcal{A})} \sqrt{\frac{\nu(d(\mathcal{C}))}{\lambda(d(\mathcal{C}))}} = \sup_{d \in \mathbb{R}_+^n \setminus \{O\}} \sqrt{\frac{\nu(d)}{\lambda(d)}}. \tag{10}$$

Comme conséquence directe, nous obtenons le résultat suivant (*cf.* [120]).

Corollaire 3. *Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini dont les circuits simples sont $\mathcal{C}_1, \ldots, \mathcal{C}_n$. Il existe alors un point $d \in \mathbb{R}_+^n \setminus \{O\}$ tel que nous avons*

$$\omega_2(\mathcal{A}) = \sqrt{\nu(d)/\lambda(d)}.$$

Ainsi pour calculer l'opacité restreinte $\omega_2(\mathcal{A})$, nous avons seulement besoin de trouver la plus grande valeur de la fonction ν/λ prise sur $\mathbb{R}_+^n \setminus \{O\}$. Pour cela, nous introduisons, pour tout $\omega \in \mathbb{R}_+$, une fonction auxiliaire H^ω définie sur $\mathbb{R}_+^n \setminus \{O\}$ telle que pour tout $d \in \mathbb{R}_+^n \setminus \{O\}$, nous avons

$$H^\omega(d) = \lambda(d)\omega^2 - \nu(d).$$

Il est évident que pour tout $\omega \in \mathbb{R}_+$, tout comme les deux fonctions ν et λ, la fonction auxiliaire H^ω possède aussi des dérivées partielles faibles sur $\mathbb{R}_+^n \setminus \{O\}$.

Maintenant nous sommes prêts à présenter l'algorithme suivant qui nous servira à calculer les opacités des automates finis (*cf.* [120]).

Théorème 2. *Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini dont les circuits simples sont $\mathcal{C}_1, \ldots, \mathcal{C}_n$. Soit $\omega \geqslant 0$ un nombre réel. Alors $\omega = \omega_2(\mathcal{A})$ si et seulement s'il existe un point $d^\omega = (d_1^\omega, \ldots, d_n^\omega) \in \mathbb{R}_+^n \setminus \{O\}$ tel que*

$$\frac{\partial H^\omega}{\partial d_j}(d^\omega) \geqslant 0,$$

pour tout entier j $(1 \leqslant j \leqslant n)$, et si en particulier $d_j^\omega > 0$, nous avons alors

$$\frac{\partial H^\omega}{\partial d_j}(d^\omega) = 0.$$

Nous en déduisons immédiatement le résultat suivant (*cf.* [120]).

Corollaire 4. *Pour tout Σ-automate fini $\mathcal{A} = (S, i, \Sigma, t)$, l'opacité restreinte $\omega_2(\mathcal{A})$ est algébrique sur le corps $\mathbb{Q}_\Sigma$, et son degré sur ce dernier est une puissance de 2. Ici $\mathbb{Q}_\Sigma$ est l'extension de $\mathbb{Q}$ engendrée par les nombres réels $|\sigma - \eta|^2$ $(\sigma, \eta \in \Sigma)$.*

Il est à noter qu'en général, ni $\omega_2(\mathcal{A})$ ni $(\omega_2(\mathcal{A}))^2$ ne sont rationnels même si l'on a $Q_\Sigma = Q$. Pour plus de détails, voir le paragraphe 15.

14. **Quelques propriétés élémentaires de l'opacité quadratique.** Avant de nous servir du théorème 2 pour calculer les opacités des automates d'Ising, nous en tirons d'abord quelques propriétés générales de ω_2 et Ω_2.

Dans un certain sens, un automate fini, ainsi que son opacité, est déterminé par ses circuits simples. Le théorème 2 nous a déjà confirmé ce point de vue. Mais nous pouvons faire beaucoup mieux en nous servant du résultat suivant (*cf.* [120]) dont la preuve est fondée sur le théorème 2.

Théorème 3. *Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini dont les circuits simples sont $\mathcal{C}_1, \ldots, \mathcal{C}_n$. Alors on a*

$$\omega_2(\mathcal{A}) = \min_{\varphi \in \mathbb{C}^S} \max_{1 \leqslant j \leqslant n} \left(\frac{1}{\ell(\mathcal{C}_j)} \sum_{s \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^j(s) \, |\varphi(s) - \sigma|^2 \right)^{1/2}.$$

Comme conséquence, nous en déduisons immédiatement (*cf.* [35] et [120]).

Corollaire 5. *Pour $\mathcal{I}_\Sigma$ le Σ-automate ayant un seul état, nous avons*

$$\omega_2(\mathcal{I}_\Sigma) = \min_{x \in \mathbb{C}} \max_{\sigma \in \Sigma} |x - \sigma|.$$

Nous remarquons que pour tout Σ-automate fini $\mathcal{A}$, nous avons (voir [120])

$$0 \leqslant \omega_2(\mathcal{A}) \leqslant \omega_2(\mathcal{I}_\Sigma).$$

Plus généralement, si $\mathcal{A}'$ est un facteur de $\mathcal{A}$, alors $\omega_2(\mathcal{A}) \leqslant \omega_2(\mathcal{A}')$ (*cf.* [118]).

Un Σ-automate fini $\mathcal{A}$ est alors appelé *transparent* ou *opaque* selon que $\omega_2(\mathcal{A})$ est égal à 0 ou à $\omega_2(\mathcal{I}_\Sigma)$. Le problème de la caractérisation des automates transparents est assez facile à résoudre (voir [118]). Celui des automates opaques est beaucoup plus compliqué car la géométrie de Σ y joue un rôle déterminant. Ce dernier problème a été abordé dans [118], et résolu complètement dans [35]. Nos résultats obtenus sur ce sujet seront exposés dans le paragraphe 17.

À partir du théorème 3 et d'un lemme fondamental (voir [120]), nous pouvons montrer, comme nous l'avons déjà signalé dans le paragraphe 11, l'égalité suivante.

Théorème 4. *Pour tout Σ-automate fini $\mathcal{A}$, nous avons*

$$\omega_2(\mathcal{A}) = \Omega_2(\mathcal{A}).$$

Une autre preuve de cette égalité a été donnée dans [118] dans un cadre beaucoup plus général. Le lecteur peut aussi consulter [74] pour une troisième preuve fondée directement sur le théorème 2.

Nous pouvons nous demander si le théorème 4 peut se déduire du fait que les suites ultimement périodiques sont denses dans $\Sigma^{\mathbb{N}}$. La réponse est malheuresement négative, et le lecteur peut se reporter à [120] pour une explication.

Une autre conséquence du théorème 3 est le résultat suivant (*cf.* [118] et [120]).

Théorème 5. *Pour tout Σ-automate fini $\mathcal{A}$, nous avons*

$$\Omega_2(\mathcal{A}) = \inf_{\varphi\in\mathbb{C}^S} \sup_{\eta\in\Sigma^{\mathbb{N}}} \|\varphi(\mathcal{A}\eta) - \eta\|_2 .$$

Ce résultat possède une interprétation assez intéressante. Dans l'introduction du mémoire, nous avons expliqué comment définir l'opacité $\Omega^{\mathbf{d}}(\mathcal{A})$ d'un système de communication $\mathcal{A}$. Or dans la pratique, nous pouvons évidemment intervertir le procédé que nous avons adopté pour $\Omega^{\mathbf{d}}(\mathcal{A})$. En d'autres termes, nous pouvons fixer d'abord le traducteur φ et chercher la plus grande distorsion $\sup_\eta \mathbf{d}(\varphi(\mathcal{A}\eta), \eta)$ de nos expériences, puis nous raffinons les traducteurs autant que possible pour enlever les bruits qu'ils produisent ; à la fin nous obtenons

$$\Phi^{\mathbf{d}}(\mathcal{A}) = \inf_{\varphi} \sup_{\eta} \mathbf{d}(\varphi(\mathcal{A}\eta), \eta),$$

qui est une nouvelle opacité de nature légèrement différente. Il est clair que nous avons $\Phi^{\mathbf{d}}(\mathcal{A}) \geqslant \Omega^{\mathbf{d}}(\mathcal{A})$. D'ailleurs l'inégalité peut devenir stricte (voir [118]), ce qui contredit, bien sûr, notre connaissance pragmatique. Heureusement ce n'est pas le cas de l'opacité quadratique, comme le théorème 5 nous l'a bien confirmé.

Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini. De la définition de $\omega(\mathcal{A})$, nous pouvons demander s'il existe une suite ultimement périodique $\eta \in \Sigma^{\mathbb{N}}$ telle que

$$\omega_2(\mathcal{A}) = \inf_{\varphi\in\mathbb{C}^S} \|\varphi(\mathcal{A}\eta) - \eta\|_2 . \tag{11}$$

Si la réponse était positive, alors $(\omega(\mathcal{A}))^2$ serait dans $\mathbb{Q}_\Sigma$, donc rationnel si tous les nombres $|\sigma - \eta|^2$ $(\sigma, \eta \in \Sigma)$ étaient rationnels. Or dans le paragraphe 15, nous allons voir que ce n'est pas le cas même si $\Sigma \subset \mathbb{Q}$. Cependant nous avons quand même le résultat suivant ([120]), qui ne contredit évidemment pas $\Omega_2 = \omega_2$.

Théorème 6. *Pour tout Σ-automate fini $\mathcal{A}$, il existe une suite $\eta \in \Sigma^{\mathbb{N}}$ telle que*

$$\Omega(\mathcal{A}) = \inf_{\varphi\in\mathbb{C}^S} \|\varphi(\mathcal{A}\eta) - \eta\|_2.$$

La preuve de ce résultat est fondée sur les théorèmes 3 et 4, mais aussi sur une version améliorée (voir [120]) de la construction des suites écrasantes, inventée originellement par N. Loraud dans [74].

15. **Opacités des automates d'Ising.** Pour les automates d'Ising $\mathcal{A}_\alpha$ $(\alpha \geqslant 0)$, nous avons $\Sigma = \{+1, -1\}$, donc $\omega_2(\mathcal{I}_\Sigma) = 1$. Désignons par n_α le nombre des circuits simples de l'automate d'Ising $\mathcal{A}_\alpha = (S_\alpha, i_\alpha, \Sigma, t_\alpha)$ (bien sûr, ici nous n'avons pas besoin de distinguer les circuits simples, qui se distinguent seulement par leurs points de base). Alors pour tout $d \in \mathbb{R}_+^{n_\alpha} \setminus \{O\}$ et tout $s \in S_\alpha$, nous avons

$$G_s(d) = \frac{4\lambda_{s,+1}(d)\lambda_{s,-1}(d)}{\lambda_s(d)}.$$

Par conséquent, pour tout nombre réel $\omega \geqslant 0$ et tout $d \in \mathbb{R}_+^{n_\alpha} \setminus \{O\}$, nous avons

$$H^\omega(d) = \lambda(d)\omega^2 - \sum_{s\in S_\alpha} \frac{4\lambda_{s,+1}(d)\lambda_{s,-1}(d)}{\lambda_s(d)}. \tag{12}$$

Dans la suite, nous allons distinguer quatres cas pour calculer $\omega^{(\alpha)} := \omega_2(\mathcal{A}_\alpha)$, en nous servant de l'algorithme donné dans le théorème 2.

Cas 1 : $\alpha = 0$. Dans ce cas, nous avons $n_0 = 3$ (voir la figure 9).

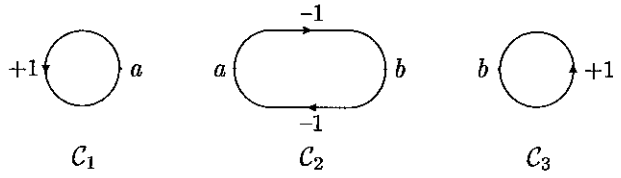


FIGURE 9. Circuits simples de $\mathcal{A}_0$

Pour tout $d = (d_1, d_2, d_3) \in \mathbb{R}^3_+ \setminus \{O\}$, nous avons

$$\lambda_{a,+1}(d) = d_1,\ \lambda_{a,-1}(d) = d_2,\ \text{et}\ \lambda_{b,+1}(d) = d_3,\ \lambda_{b,-1}(d) = d_2.$$

Ainsi pour tout nombre réel $\omega \geqslant 0$,

$$H^\omega(d) = (d_1 + 2d_2 + d_3)\omega^2 - \frac{4d_1d_2}{d_1 + d_2} - \frac{4d_2d_3}{d_2 + d_3},$$

d'où nous obtenons

$$\begin{aligned}
\frac{\partial H^\omega}{\partial d_1}(d) &= \omega^2 - \frac{4d_2^2}{(d_1 + d_2)^2}, \\
\frac{\partial H^\omega}{\partial d_2}(d) &= 2\omega^2 - \frac{4d_1^2}{(d_1 + d_2)^2} - \frac{4d_3^2}{(d_2 + d_3)^2}, \\
\frac{\partial H^\omega}{\partial d_3}(d) &= \omega^2 - \frac{4d_2^2}{(d_2 + d_3)^2}.
\end{aligned}$$

Posons

$$\frac{\partial H^\omega}{\partial d_1}(d) = \frac{\partial H^\omega}{\partial d_2}(d) = \frac{\partial H^\omega}{\partial d_3}(d) = 0.$$

Nous obtenons alors $\omega = 1$, c'est-à-dire $\omega^{(0)} = 1$. L'automate d'Ising $\mathcal{A}_0$ est donc opaque. Ce résultat a déjà été remarqué par M. Mendès France (*cf.* [79]), et peut être aussi démontré par notre critère sur les automates opaques (voir [118] ou [35]).

Cas 2 : $\alpha \geqslant 4$. Dans ce cas, nous avons aussi $n_\alpha = 3$ (voir la figure 10).

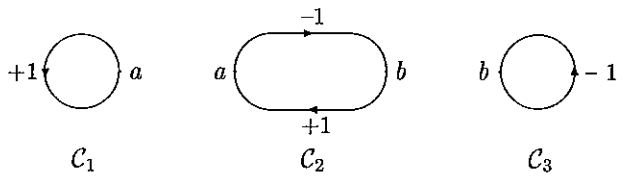


FIGURE 10. Circuits simples de $\mathcal{A}_\alpha$ (avec $\alpha \geqslant 4$)

Pour tout $d = (d_1, d_2, d_3) \in \mathbb{R}^3_+ \setminus \{O\}$, nous avons alors

$$\lambda_{a,+1}(d) = d_1 + d_2,\ \lambda_{a,-1}(d) = 0,\ \text{et}\ \lambda_{b,+1}(d) = 0,\ \lambda_{b,-1}(d) = d_2 + d_3.$$

Ainsi pour tout nombre réel $\omega \geqslant 0$, la fonction auxiliaire H^ω est donnée par

$$H^\omega(d) = (d_1 + 2d_2 + d_3)\omega^2,$$

et nous obtenons par suite

$$\frac{\partial H^{\omega}}{\partial d_1}(d) = \omega^2, \ \frac{\partial H^{\omega}}{\partial d_2}(d) = 2\omega^2, \ \frac{\partial H^{\omega}}{\partial d_3}(d) = \omega^2.$$

Du système d'équations

$$\frac{\partial H^{\omega^{(\alpha)}}}{\partial d_1}(d) = \frac{\partial H^{\omega^{(\alpha)}}}{\partial d_2}(d) = \frac{\partial H^{\omega^{(\alpha)}}}{\partial d_3}(d) = 0,$$

nous obtenons $\omega^{(\alpha)} = 0$. Ainsi l'automate d'Ising $\mathcal{A}_\alpha$ est transparent pour $\alpha \geqslant 4$. Ce résultat est aussi signalé dans [79], et peut être démontré également par notre critère sur les automates transparents (voir [118]).

Cas 3 : $4/\alpha \notin \mathbb{N}$ $(0 < \alpha < 4)$. Alors $\mathcal{A}_\alpha = \mathcal{L}_\mu$, et nous avons (voir la figure 11).

$$n_\alpha = 3 + \mu + \frac{1}{2}\mu(\mu+1), \text{ avec } \mu = [4/\alpha].$$

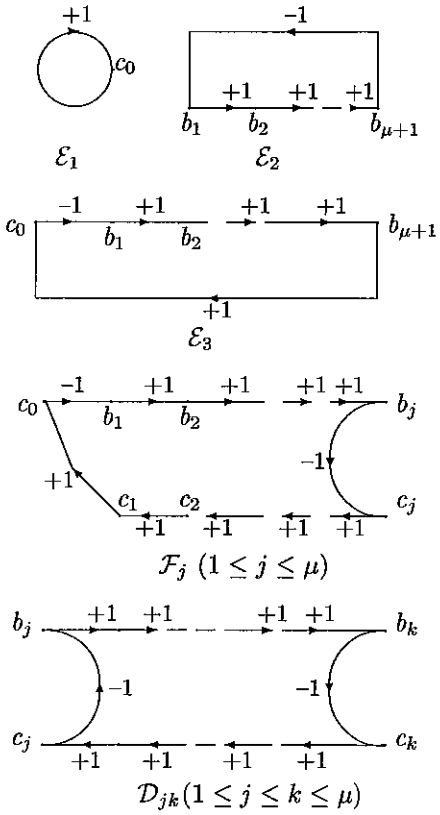


FIGURE 11. Circuits Simples de $\mathcal{L}_\mu$

Pour tout $d = (d_l)_{1 \leqslant l \leqslant n_\alpha} \in \mathbb{R}_+^{n_\alpha} \setminus \{O\}$ et tout $j, k \in \mathbb{N}$ $(1 \leqslant j \leqslant k \leqslant \mu)$, posons

$$e_1 := d_1, \ e_2 := d_2, \ e_3 := d_3, \ f_j := d_{j+3}, \text{ et } d_{jk} := d_{j\mu - \frac{1}{2}(j-1)j+k+3}.$$

En d'autres termes, nous renumérotons les coordonnées du point d, selon les indices de nos circuits simples présentés ci-dessus.

Avec ces nouvelles notations, nous avons alors

$$
\begin{array}{lrcl}
1). & \lambda_{c_0,+1}(d) & = & e_1+e_3+\sum_{j=1}^{\mu} f_j,\\
 & \lambda_{c_0,-1}(d) & = & 0,\\
2). & \lambda_{b_1,+1}(d) & = & 0,\\
 & \lambda_{b_1,-1}(d) & = & e_2+e_3+\sum_{j=1}^{\mu} f_j+\sum_{k=1}^{\mu} d_{1k},\\
3). & \lambda_{b_j,+1}(d) & = & e_2+e_3+\sum_{k=j}^{\mu} f_k+\sum_{k=1}^{j-1}\sum_{l=j}^{\mu} d_{kl},\\
 & \lambda_{b_j,-1}(d) & = & \sum_{k=j}^{\mu} d_{jk}\ (2\leqslant j\leqslant \mu),\\
4). & \lambda_{b_{\mu+1},+1}(d) & = & e_2+e_3,\\
 & \lambda_{b_{\mu+1},-1}(d) & = & 0,\\
5). & \lambda_{c_j,+1}(d) & = & \sum_{k=j+1}^{\mu} f_k+\sum_{k=1}^{j}\sum_{l=j+1}^{\mu} d_{kl},\\
 & \lambda_{c_j,-1}(d) & = & f_j+\sum_{k=1}^{j} d_{kj}\ (1\leqslant j\leqslant \mu-1),\\
6). & \lambda_{c_\mu,+1}(d) & = & 0,\\
 & \lambda_{c_\mu,-1}(d) & = & f_\mu+\sum_{l=1}^{\mu} d_{l\mu}.
\end{array}
$$

Ainsi pour tout nombre réel $\omega\geqslant 0$ et tout $d\in\mathbb{R}_+^{n_\alpha}\setminus\{O\}$, nous avons

$$\lambda(d)=e_1+(\mu+1)e_2+(\mu+2)e_3+\sum_{j=1}^{\mu}(2j+1)f_j+\sum_{k=1}^{\mu}\sum_{l=k}^{\mu}2(l-k+1)d_{kl},$$

$$H^\omega(d)=\lambda(d)\omega^2-\sum_{j=2}^{\mu}\frac{4\lambda_{b_j,+1}(d)\lambda_{b_j,-1}(d)}{\lambda_{b_j}(d)}-\sum_{k=1}^{\mu-1}\frac{4\lambda_{c_k,+1}(d)\lambda_{c_k,-1}(d)}{\lambda_{c_k}(d)}.$$

Pour simplifier les notations, posons, pour tout entier j $(1\leqslant j\leqslant\mu)$,

$$\beta_j^{(\pm)}=\lambda_{b_j,\pm1}(d),\ \beta_j=\lambda_{b_j}(d),\text{ et }\gamma_j^{(\pm)}=\lambda_{c_j,\pm1}(d),\ \gamma_j=\lambda_{c_j}(d).$$

En prenant les dérivées partielles faibles de H^ω, nous obtenons

$$
\begin{array}{lrcl}
7). & \frac{\partial H^\omega}{\partial e_1}(d) & = & \omega^2,\\
8). & \frac{\partial H^\omega}{\partial e_2}(d) & = & (\mu+1)\omega^2-4\sum_{j=2}^{\mu}(\frac{\beta_j^{(-)}}{\beta_j})^2,\\
9). & \frac{\partial H^\omega}{\partial e_3}(d) & = & (\mu+2)\omega^2-4\sum_{j=2}^{\mu}(\frac{\beta_j^{(-)}}{\beta_j})^2,\\
10). & \frac{\partial H^\omega}{\partial f_1}(d) & = & 3\omega^2-4(\frac{\gamma_1^{(+)}}{\gamma_1})^2,\\
11). & \frac{\partial H^\omega}{\partial f_j}(d) & = & (2j+1)\omega^2-4\sum_{k=2}^{j}(\frac{\beta_k^{(-)}}{\beta_k})^2\\
 & & & -4\sum_{k=1}^{j-1}(\frac{\gamma_k^{(-)}}{\gamma_k})^2-4(\frac{\gamma_j^{(+)}}{\gamma_j})^2\ (2\leqslant j\leqslant\mu),\\
12). & \frac{\partial H^\omega}{\partial d_{11}}(d) & = & 2\omega^2-4(\frac{\gamma_1^{(+)}}{\gamma_1})^2,\\
13). & \frac{\partial H^\omega}{\partial d_{1j}}(d) & = & 2j\omega^2-4\sum_{k=2}^{j}(\frac{\beta_k^{(-)}}{\beta_k})^2\\
 & & & -4\sum_{k=1}^{j-1}(\frac{\gamma_k^{(-)}}{\gamma_k})^2-4(\frac{\gamma_j^{(+)}}{\gamma_j})^2\ (2\leqslant j\leqslant\mu),\\
14). & \frac{\partial H^\omega}{\partial d_{jj}}(d) & = & 2\omega^2-4(\frac{\beta_j^{(+)}}{\beta_j})^2-4(\frac{\gamma_j^{(+)}}{\gamma_j})^2\ (2\leqslant j\leqslant\mu-1),\\
15). & \frac{\partial H^\omega}{\partial d_{jk}}(d) & = & 2(k-j+1)\omega^2-4\sum_{l=j+1}^{k}(\frac{\beta_l^{(-)}}{\beta_l})^2-4(\frac{\beta_j^{(+)}}{\beta_j})^2\\
 & & & -4\sum_{l=j}^{k-1}(\frac{\gamma_l^{(-)}}{\gamma_l})^2-4(\frac{\gamma_k^{(+)}}{\gamma_k})^2\ (2\leqslant j<k\leqslant\mu),\\
16). & \frac{\partial H^\omega}{\partial d_{\mu\mu}}(d) & = & 2\omega^2-4(\frac{\beta_\mu^{(+)}}{\beta_\mu})^2.
\end{array}
$$

Pour tout nombre réel $\omega \in [0,1]$ et tout $x \in [0, \omega^2/2]$, définissons

$$\mathbf{f}_\omega(x) = 1 - \sqrt{\frac{1}{2}\omega^2 - x^2}.$$

Posons $\mathbf{g}_0(\omega) := 0$ pour tout $\omega \in [0,1]$. Par récurrence sur l'entier μ ($\mu \geqslant 0$), nous pouvons définir une suite de fonctions réelles $(\mathbf{g}_\mu)_{\mu \geqslant 0}$ par $\mathbf{g}_\mu := \mathbf{f}_\omega \circ \mathbf{g}_{\mu-1}$, et montrer que pour tout entier μ ($\mu \geqslant 1$), il existe un unique $\varpi_\mu \geqslant 0$ vérifiant

$$\mathbf{g}_{\mu-1}(\varpi_\mu) = \varpi_\mu/\sqrt{2}.$$

Fixons $\mu \geqslant 1$ un entier. Pour tout entier j ($1 \leqslant j \leqslant \mu + 1$), définissons

$$x_j = \mathbf{g}_{j-1}(\varpi_\mu).$$

Nous pouvons montrer que pour tout entier j ($1 \leqslant j \leqslant \mu$), nous avons $x_j < x_{j+1}$. Nous en déduisons par suite $0 < x_j < 1$ ($2 \leqslant j \leqslant \mu$).

Posons $z_1 = 1$, et

$$z_j = (1 - x_{j+1}) z_{j-1}/x_j, \ (2 \leqslant j \leqslant \mu - 1).$$

Posons ensuite $d_{11} := x_2 z_1/(1 - x_2)$, $d_{kl} := 0$ ($1 \leqslant k \leqslant l - 2 \leqslant \mu - 2$), et

$$d_{(j-1)j} := z_{j-1}, \ d_{jj} := \frac{x_{j+1} - x_j}{x_j} z_{j-1} \ (2 \leqslant j \leqslant \mu).$$

Définissons maintenant $d^{\varpi_\mu} = (d_j)_{1 \leqslant j \leqslant n_\alpha} \in \mathbb{R}_+^{n_\alpha} \setminus \{O\}$ par

$$d_j := 0 \ (1 \leqslant j \leqslant \mu + 3), \text{ et } d_{k\mu - \frac{1}{2}(k-1)k+l+3} := d_{kl} \ (1 \leqslant k \leqslant l \leqslant \mu).$$

En nous servant des formules 7)–16), nous pouvons montrer que le couple $(\varpi_\mu, d^{\varpi_\mu})$ satisfait aux conditions du théorème 2. Ainsi $\omega^{(\alpha)} = \varpi_\mu$, avec $\mu = [4/\alpha]$.

Cas 4 : $4/\alpha \in \mathbb{N}$ $(0 < \alpha < 4)$. Posons $\mu = 4/\alpha$. Alors $\mathcal{A}_\alpha = \mathcal{N}_\mu$, et nous pouvons montrer, tout comme dans le cas précédent, que nous avons aussi $\omega_2(\mathcal{N}_\mu) = \varpi_\mu$.

En conclusion, nous avons le résultat suivant.

Théorème 7. *Pour tout entier μ ($\mu \geqslant 1$), l'opacité $\varpi_\mu := \omega(\mathcal{L}_\mu) = \omega(\mathcal{N}_\mu)$ est déterminée par l'équation $\mathbf{g}_{\mu-1}(\varpi_\mu) = \varpi_\mu/\sqrt{2}$. En plus, la suite positive $(\varpi_\mu)_{\mu \geqslant 1}$ est strictement croissante et converge vers* 1.

Posons $\varpi_0 = 0$ et $\varpi_\infty = 1$. Alors $\omega^{(\alpha)} := \omega_2(\mathcal{A}_\alpha) = \varpi_{[4/\alpha]}$, pour tout $\alpha \geqslant 0$, où $[4/0] = \infty$ par convention. Ainsi

$$\lim_{\alpha \to 0} \omega^{(\alpha)} = \omega^{(0)},$$

ce qui signifie que la fonction $\alpha \to \omega^{(\alpha)}$ est continue en $\alpha = 0$. On remarque que ce résultat est en parfaite harmonie avec la continuité de la famille des automates d'Ising, signalée dans le paragraphe 10.

Quelques résultats numériques :

$$\varpi_0 = 0, \ \varpi_1 = 0, \ \varpi_2 = \frac{\sqrt{2}}{2}, \ \varpi_3 = 2(\sqrt{2} - 1), \ \varpi_4 = \frac{5}{8}\sqrt{2}, \ \ldots, \ \varpi_\infty = 1.$$

En fait, à l'aide du logiciel Maple, il est relativement facile de résoudre l'équation

$$\mathbf{g}_{\mu-1}(\varpi_\mu) = \varpi_\mu/\sqrt{2} \ (\mu \geqslant 1).$$

Enfin nous remarquons que $\varpi_3^2 = 4(3 - 2\sqrt{2}) \notin \mathbb{Q}$, malgré $\Sigma = \{1, -1\} \subset \mathbb{Q}$.

Le lecteur se reportera à [120] pour tous les détails omis de ce paragraphe.

16. **Opacités générales des automates finis.** Ayant présenté la théorie de l'opacité quadratique, nous envisageons maintenant des généralisations, dont la plus immédiate est sans doute l'opacité liée à la semi-norme $\|\cdot\|_q$ suivante.

Fixons $q \geqslant 1$. Pour toute suite complexe bornée $u = (u(m))_{m\geqslant 0}$, définissons

$$\|u\|_q := \limsup_{k\to\infty} \left(\frac{1}{k}\sum_{m=0}^{k-1} |u(m)|^q\right)^{1/q}.$$

Il est clair que $\|\cdot\|_q$ est une semi-norme sur l'espace de toutes les suites complexes bornées, et notre semi-norme quadratique correspond à $q = 2$.

Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini. L'opacité de l'automate fini $\mathcal{A}$ par rapport à la semi-norme $\|\cdot\|_q$ est alors définie par

$$\Omega_q(\mathcal{A}) = \sup_{\eta}\inf_{\varphi} \|\varphi(\mathcal{A}\eta) - \eta\|_q,$$

où η parcourt l'ensemble des suites infinies sur Σ, et φ parcourt l'ensemble des applications complexes définies sur S.

Pour le moment, nous ne savons pas comment calculer explicitement Ω_q, sauf dans le cas $q = 2$ que nous avons déjà traité dans le paragraphe 13. La difficulté est plutôt technique et se trouve principalement dans le fait qu'en général, il n'existe pas de formule explicite pour la fonction réelle ψ, définie sur $\mathbb{R}_+^\Sigma$ par

$$\forall\, s = (s_\sigma)_{\sigma\in\Sigma} \in \mathbb{R}_+^\Sigma,\ \psi(s) = \inf_{x\in\mathbb{C}} \sum_{\sigma\in\Sigma} s_\sigma |x - \sigma|^q.$$

En d'autres termes, nous n'avons pas d'analogue du théorème 2 en général sauf dans le cas $q = 2$. Cependant tous les autres résultats que nous avons présentés dans les paragraphes 13 et 14 sont encore valables (voir [118]). En particulier, nous avons le théorème suivant qui repose sur une belle application du célèbre théorème de minimax de J. von Neumann (voir par exemple [51] ou [84]).

Théorème 8. *Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini. Nous avons alors*

$$\Omega_q(\mathcal{A}) = \sup_{\eta\ u.p.}\inf_{\varphi} \|\varphi(\mathcal{A}\eta) - \eta\|_q = \inf_{\varphi}\sup_{\eta} \|\varphi(\mathcal{A}\eta) - \eta\|_q.$$

Nous avons aussi le résultat suivant (*cf.* [118]) qui généralise dans un certain sens le théorème 1 du paragraphe 13.

Théorème 9. *Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini dont les circuits simples sont $\mathcal{C}_1, \ldots, \mathcal{C}_n$. Nous avons alors*

$$\Omega_q(\mathcal{A}) = \sup_{\mathcal{C}\in\mathfrak{C}(\mathcal{A})}\inf_{\varphi\in\mathbb{C}^S} \left(\frac{G_q(d(\mathcal{C}), \varphi)}{\lambda(d(\mathcal{C}))}\right)^{1/q} = \sup_{d\in\mathbb{R}^n\setminus\{O\}}\inf_{\varphi\in\mathbb{C}^S} \left(\frac{G_q(d,\varphi)}{\lambda(d)}\right)^{1/q},$$

où la fonction G_q est définie sur $\mathbb{R}_+^n\setminus\{O\}\times\mathbb{C}^S$ par

$$G_q(d,\varphi) := \sum_{s\in S}\sum_{\sigma\in\Sigma} \lambda_{s,\sigma}(d)|\varphi(s) - \sigma|^q,$$

pour tout $d = (d_1, \ldots, d_n) \in \mathbb{R}_+^n\setminus\{O\}$ et tout $\varphi \in \mathbb{C}^S$.

En particulier, il existe $d \in \mathbb{R}_+^n\setminus\{O\}$ et $\varphi^0 \in \mathbb{C}^S$ tels que

$$\Omega_q(\mathcal{A}) = \left(\frac{G_q(d,\varphi^0)}{\lambda(d)}\right)^{1/q} = \inf_{\varphi\in\mathbb{C}^S}\left(\frac{G_q(d,\varphi)}{\lambda(d)}\right)^{1/q}.$$

À l'aide du théorème précédent, nous pouvons montrer tout de suite le résultat suivant (*cf.* [120]) qui est la bonne généralisation du théorème 3.

Théorème 10. *Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini dont les circuits simples sont $C_1, \ldots, C_n$. Nous avons alors*

$$\Omega_q(\mathcal{A}) = \min_{\varphi \in \mathbb{C}^S} \max_{1 \leqslant j \leqslant n} \left(\frac{1}{\ell(C_j)} \sum_{s \in S} \sum_{\sigma \in \Sigma} \delta_\sigma^j(s) |\varphi(s) - \sigma|^q \right)^{1/q}. \tag{6}$$

Comme conséquence, nous obtenons le résultat suivant.

Corollaire 6. *Pour $\mathcal{I}_\Sigma$ le Σ-automate ayant un seul état, nous avons*

$$\Omega_q(\mathcal{I}_\Sigma) = \min_{x \in \mathbb{C}} \max_{\sigma \in \Sigma} |x - \sigma|.$$

Comme dans le cas de l'opacité quadratique (voir le paragraphe 14), pour tout Σ-automate fini $\mathcal{A}$, nous avons aussi (voir [120])

$$0 \leqslant \Omega_q(\mathcal{A}) \leqslant \Omega_q(\mathcal{I}_\Sigma) = \Omega_2(\mathcal{I}_\Sigma).$$

Un Σ-automate fini $\mathcal{A}$ sera appelé *transparent* ou *opaque* selon que $\Omega_q(\mathcal{A})$ est égal à 0 ou $\Omega_q(\mathcal{I}_\Sigma)$ (en fait, le nombre réel q ne joue aucun rôle ici). Dans le paragraphe suivant, nous allons caractériser tous ces automates bien particuliers.

Il y a aussi un analogue du théorème 6 dont la preuve est presque identique.

Théorème 11. *Pour tout Σ-automate fini $\mathcal{A}$, il existe une suite $\eta \in \Sigma^{\mathbb{N}}$ telle que*

$$\Omega_q(\mathcal{A}) = \inf_{\varphi \in \mathbb{C}^S} \|\varphi(\mathcal{A}\eta) - \eta\|_q.$$

17. **Caractérisations des automates transparents et opaques.** Commençons par la caractérisation des automates transparents.

Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini. Soit s un sommet de $\mathcal{A}$ et σ une flèche incidente à s sur le graphe de $\mathcal{A}$. La flèche σ est dite *fidèle* à s sur $\mathcal{A}$ si elle appartient à un circuit sur $\mathcal{A}$. Du théorème 9, nous pouvons déduire facilement le critère suivant (*cf.* [118]) :

Théorème 12. *Un Σ-automate fini $\mathcal{A}$ est transparent si et seulement si pour tout sommet s de $\mathcal{A}$, les flèches fidèles à s sont de même type.*

Comme application directe, nous avons le résultat suivant.

Corollaire 7. *Soit $\mathcal{A}$ un Σ-automate fortement accessible. Alors $\mathcal{A}$ est transparent si et seulement s'il est homogène.*

La caractérisation des automates opaques est relativement plus compliquée. En fait, comme nous l'avons déjà signalé, la structure géométrique de l'ensemble des étiquettes Σ va y jouer un rôle important.

Fixons $c \in \mathbb{C}$ et $r \in \mathbb{R}$ ($r \geqslant 0$). Nous définissons

$$\mathbb{D}(c, r) := \{x \in \mathbb{C} \mid |x - c| \leqslant r\}$$

et l'appelons disque (de centre c et de rayon r) dans le plan complexe. Notons ensuite $\mathcal{D}(\Sigma)$ l'ensemble de tous les disques qui contiennent Σ. Dans $\mathcal{D}(\Sigma)$, il y a un et un seul disque (noté $\mathbb{D}(\Sigma)$) dont le rayon est minimal. Désignons par $c(\Sigma)$ le centre et par $r(\Sigma)$ le rayon du disque $\mathbb{D}(\Sigma)$. Nous avons alors

$$r(\Sigma) = \min_{x \in \mathbb{C}} \max_{\sigma \in \Sigma} |x - \sigma|.$$

Ainsi $\Omega_q(\mathcal{I}_\Sigma) = r(\Sigma)$ pour tout $q \geqslant 1$. Notons $\partial\mathbb{D}(\Sigma)$ le bord du disque $\mathbb{D}(\Sigma)$. Il est clair que $\partial\mathbb{D}(\Sigma)$ contient au moins deux points de Σ.

Soit Σ' un sous-ensemble de Σ. Nous appelons Σ' un *sous-ensemble essentiel* de Σ si $\mathbb{D}(\Sigma') = \mathbb{D}(\Sigma)$. Soit mainenant Σ' un sous-ensemble essentiel de Σ. Nous disons que Σ' est un *sous-ensemble minimal* de Σ, si Σ' n'a aucun sous-ensemble essentiel propre. De la géométrie élémentaire, nous pouvons facilement démontrer qu'un sous-ensemble essentiel Σ' de Σ est minimal si et seulement si Σ' est composé de deux points a, b (dans ce cas, nous avons $c(\Sigma) = (a+b)/2$), ou trois points qui forment un triangle acutangle, avec $\partial\mathbb{D}(\Sigma)$ comme cercle circonscrit.

Soit Σ' un sous-ensemble essentiel de Σ. Nous appelons Σ' un *sous-ensemble extrémal* de Σ si $\Sigma' \subseteq \partial\mathbb{D}(\Sigma)$. Il est clair que tout sous-ensemble minimal de Σ est aussi extrémal. Réciproquement, tout sous-ensemble extrémal de Σ contient un sous-ensemble minimal de Σ car il est un sous-ensemble essentiel de Σ. Enfin nous désignons par $\mathbb{E}(\Sigma)$ la collection de tous les sous-ensembles extrémaux de Σ.

Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini dont les circuits simples sont $\mathcal{C}_1, \ldots, \mathcal{C}_n$. Pour tout $d \in \mathbb{R}_+^n \setminus \{O\}$, nous définisons

$$S(d) := \{s \in S \mid \lambda_s(d) > 0\}.$$

Avec ces définitions et notations, nous avons le critère suivant, dont la preuve est fondée principalement sur le théorème 9 (voir [35]).

Théorème 13. *Soit $\mathcal{A} = (S, i, \Sigma, t)$ un Σ-automate fini dont les circuits simples sont $\mathcal{C}_1, \ldots, \mathcal{C}_n$. Alors $\mathcal{A}$ est opaque si et seulement s'il existe $d \in \mathbb{R}_+^n \setminus \{O\}$ tel que pour tout $s \in S(d)$, nous avons*

$$\sum_{\sigma \in \Sigma} \lambda_{s,\sigma}(d)(\sigma - c(\Sigma)) = 0, \text{ et } \Sigma_s(d) := \{\sigma \in \Sigma \mid \lambda_{s,\sigma}(d) \neq 0\} \in \mathbb{E}(\Sigma).$$

À partir de ce résultat, nous pouvons déduire une caractérisation géométrique des automates opaques, qui généralise le théorème 8 de [118]. Malheureusement cette caractérisation géométrique n'est valable que sous certaines conditions bien restrictives. À l'origine nous voulions caractériser les automates opaques par leurs propriétés géométriques, tout comme le théorème 8 dans [118]. Nous n'y sommes pas parvenu complètement. Cependant comme toutes les équations apparues dans notre critère sont linéaires, nous obtenons en fait un algorithme théorique, par lequel et à l'aide d'un ordinateur, il n'est donc pas très difficile de juger si un automate fini est opaque ou non.

Soit $\mathcal{A} = (S, \Sigma, i, t)$ et $\mathcal{A}' = (S', \Sigma', i', t')$ deux automates finis. Nous appelons $\mathcal{A}'$ un *sous Σ'-automate fini* de $\mathcal{A}$ si $S' \subseteq S$, $\Sigma' \subseteq \Sigma$, et $t' = t\,|_{S' \times \Sigma'}$. En d'autres termes, $\mathcal{A}'$ est un sous-automate de $\mathcal{A}$ si et seulement si le graphe de $\mathcal{A}'$ est un sous-graphe de celui de $\mathcal{A}$. Il est clair que si $\mathcal{A}'$ est sous-automate de $\mathcal{A}$, nous avons alors $\Omega_q(\mathcal{A}') \leqslant \Omega_q(\mathcal{A})$. En particulier, si $\mathcal{A}'$ est un sous Σ'-automate opaque de $\mathcal{A}$ et si $r(\Sigma') = r(\Sigma)$, alors $\mathcal{A}$ est aussi opaque.

Soit $\mathcal{A} = (S, \Sigma, i, t)$ un Σ-automate fini. Nous disons que $\mathcal{A}$ est un Σ-*automate équilibré* si sur le graphe de $\mathcal{A}$, tout sommet reçoit exactement $\mathrm{Card}(\Sigma)$ flèches incidentes et les types de toutes ces flèches sont distinctes. Un exemple type est le Σ-automate $\mathcal{I}_\Sigma$, qui est composé d'un seul état.

Maintenant supposons que $\mathbb{E}(\Sigma)$ ne contient qu'un seul élément (noté $\mathrm{Ex}(\Sigma)$). Alors $\mathrm{Ex}(\Sigma)$ est un sous-ensemble minimal de Σ. Il est donc composé de deux

points, ou trois points qui forment un triangle acutangle, avec $\partial\mathbb{D}(\Sigma)$ comme cercle circonscrit. Dans ce cas, les graphes des automates opaques possèdent une structure géométrique assez simple (voir [35]).

Proposition 21. *Tout Σ-automate opaque a un sous $\mathrm{Ex}(\Sigma)$-automate équilibré.*

Pour la réciproque, nous avons le résultat partiel suivant (*cf.* [35]).

Théorème 14. *Supposons que $\mathrm{Ex}(\Sigma)$ est composé de deux points, ou trois points qui forment un triangle équilatéral. Dans ce cas, un Σ-automate fini est opaque si et seulement s'il a un sous $\mathrm{Ex}(\Sigma)$-automate équilibré.*

Si $\mathrm{Ex}(\Sigma)$ est composé de trois points qui forment un triangle acutangle Δ, il est intéressant de demander si la condition que Δ est équilatéral est aussi nécessaire pour que le théorème 14 soit vrai.

Finalement nous remarquons que si Σ est extrémal et si $c(\Sigma)$ est son barycentre, alors tout Σ-automate équilibré est opaque. La preuve est en effet identique à celle du théorème 14.

18. **Opacités associées à des pseudo-distances.** Comme nous l'avons signalé dans l'introduction, la méthode de comparaison **d** joue un rôle crucial dans notre étude des opacités. En fait, à chaque méthode de comparaison choisie, correspond une théorie de l'opacité relativement indépendante. En particulier, pour toute pseudo-distance (dont notre semi-norme $\|\cdot\|_q$ est un cas spécial), nous pouvons lui associer une opacité et étudier les diverses propriétés de cette dernière. Il se trouve que certaines propriétés bien importantes présentées dans les paragraphes précédents, de l'opacité attachée à la semi-norme $\|\cdot\|_q$, ne sont plus valables pour d'autres opacités, mais heureusement d'autres propriétés intéressantes surgissent dans ce cas. Pour en savoir plus sur ce sujet, le lecteur peut se reporter à [118].

Jusqu'à présent, nous avons seulement étudié les automates déterministes. Il est aussi possible de généraliser la théorie des opacités présentée dans les paragraphes 11 à 18 aux automates non déterministes, et aux transducteurs. Tout cela sera discuté et examiné dans un travail en cours [122].

19. **Séries formelles et transcendance.** Dès maintenant, nous entrons dans la troisième partie de notre mémoire qui se consacre à l'étude de la transcendance des séries formelles sur des corps finis, issues du module de Carlitz.

Nous commençons par des définitions et notations.

Soit p ($p \geqslant 2$) un nombre premier et q une puissance entière de p. Nous désignons par $\mathbb{F}_q$ le corps fini à q éléments et par $\mathbb{F}_q[T]$ l'anneau (intègre) des polynômes à coefficients dans $\mathbb{F}_q$. Nous notons $\mathbb{F}_q(T)$ le corps de fractions de $\mathbb{F}_q[T]$. Pour tous les P, $Q \in \mathbb{F}_q[T]$ avec $Q \neq 0$, nous définissons

$$v_\infty(P/Q) = -(\deg P - \deg Q).$$

Il est clair que v_∞ est une valuation discrète sur $\mathbb{F}_q(T)$. La complétion de $\mathbb{F}_q(T)$ par rapport à v_∞ sera notée $\mathbb{F}_q((1/T))$, et appelée le corps des séries formelles de Laurent sur $\mathbb{F}_q$. Nous étendons ensuite canoniquement v_∞ au corps $\mathbb{F}_q((1/T))$. Alors tout $f \in \mathbb{F}_q((1/T))$ peut s'écrire d'une manière unique comme

$$f = \sum_{m=k}^{+\infty} a(m)T^{-m},$$

avec $a(m) \in \mathbb{F}_q$ pour tout $m \in \mathbb{Z}$ ($m \geqslant k$) et $a(k) \neq 0$. Ainsi $v_\infty(f) = k$.

Comme $\mathbb{F}_q((1/T))$ n'est pas algébriquement clos, il est nécessaire pour nous de considérer une clôture algébrique Ω de $\mathbb{F}_q(1/T)$ et d'y étendre canoniquement la valuation v_∞. Mais malheureusement, à son tour Ω n'est pas complet pour v_∞. Nous devons donc le compléter encore, et nous obtenons le corps $\mathbf{C}_\infty$ qui est à la fois topologiquement complet (par rapport à la valeur absolue $|\cdot|_\infty$ associée à v_∞) et algébriquement clos. Ce dernier va jouer dans notre étude le rôle du corps des nombres complexes $\mathbb{C}$.

Un élément $z \in \mathbf{C}_\infty$ est dit *algébrique* sur $\mathbb{F}_q(T)$ s'il existe $c_0, c_1, \ldots, c_k \in \mathbb{F}_q[T]$, des polynômes non tous nuls, tels que

$$\sum_{j=0}^{k} c_j z^j = 0.$$

Sinon nous disons que z est *transcendant* sur $\mathbb{F}_q(T)$.

En 1980, C. Christol, T. Kamae, M. Mendès France, et G. Rauzy ont démontré le surprenant résultat suivant (voir [36], [37], et [2] pour plus de détails), qui établit un lien étroit entre les suites automatiques et les séries formelles algébriques, et a constitué la pierre angulaire de la théorie arithmétique des suites automatiques.

Théorème 15. *Soit $u = (u(m))_{m\geqslant 0}$ une suite à valeurs dans le corps fini $\mathbb{F}_q$. Alors la série formelle de Laurent*

$$\sum_{m=0}^{+\infty} u(m) T^{-m}$$

est algébrique sur $\mathbb{F}_q(T)$ si et seulement si la suite u est q-automatique.

Nous remarquons qu'une version légèrement différente de ce résultat était déjà parue un an plus tôt dans [36].

Avant de poursuivre, il est mieux pour nous de résumer quelques résultats élémentaires sur les suites automatiques (voir par exemple [2], [88] et [13] pour plus de détails). Le plus important d'entre eux est sans doute la caractérisation suivante des suites automatiques.

Théorème 16. *Soit $r \geqslant 2$ un entier. Une suite $u = (u(m))_{m\geqslant 0}$ est r-automatique si et seulement si son r-noyau*

$$\mathcal{N}_r(u) := \{(u(r^b m + a))_{m\geqslant 0} \mid b \geqslant 0,\ 0 \leqslant a < r^b\}$$

est un ensemble fini.

Il semble que le théorème 16 soit apparu sous la présente forme dans [2] pour la première fois. Cependant nous pouvons également trouver une version ancienne un peu déguisée de ce résultat dans [50] (voir le théorème 8.1, p. 55). Finalement nous remarquons que la dénomination de r-noyau a été proposée par O. Salon.

Comme conséquences immédiates, nous obtenons les corollaires faciles suivants.

Corollaire 8. *Toute suite ultimement périodique est r-automatique.*

Corollaire 9. *Une suite est r-automatique si et seulement si elle est r^k-automatique pour tout entier $k \geqslant 1$.*

À ce sujet, nous avons aussi le remarquable résultat démontré par A. Cobham dans [38] : si une suite est à la fois r-automatique et s-automatique, avec $r, s \geqslant 2$ deux entiers multplicativement indépendants, alors elle est ultimement périodique.

Corollaire 10. *Soit $u = (u(n))_{n\geqslant 0}$ et $v = (v(n))_{n\geqslant 0}$ deux suites r-automatiques à valeurs dans un semigroupe. Alors le r-noyau de la suite $w = (u(n)v(n))_{n\geqslant 0}$ est un ensemble fini. Par conséqunt, la suite w est aussi r-automatique.*

Soit

$$f = \sum_{m=k}^{+\infty} a(m)T^{-m},$$

avec $a(m) \in \mathbb{F}_q$ pour tout $m \in \mathbb{Z}$ $(m \geqslant k)$, une série formelle de Laurent. Nous définissons sa dérivée formelle par rapport à T par la formule suivante

$$f' = -\sum_{m=k}^{+\infty} ma(m)T^{-m-1}.$$

Il est facile de voir que cette dérivation formelle vérifie toutes les propriétés usuelles.

Enfin nous remarquons que si la série formelle f est algébrique sur $\mathbb{F}_q(T)$, la suite $(a(m))_{m\geqslant 0}$ est q-automatique, ainsi $(ma(m))_{m\geqslant 0}$ est q-automatique puisque la suite $(m \pmod p)_{m\geqslant 0}$ est ultimement périodique, donc q-automatique. D'où, nous obtenons le résultat bien connu suivant.

Proposition 22. *La dérivée d'une série formelle algébrique de Laurent sur $\mathbb{F}_q$ est encore une série formelle algébrique.*

En fait, cette proposition est vraie, non seulement pour le corps fini $\mathbb{F}_q$, mais aussi pour tous les corps commutatifs.

20. **Critères de non-automaticité et applications.** La théorie des nombres transcendants a été inaugurée par J. Liouville en 1844 dans son mémoire [73], dans lequel, il a obtenu, pour la première fois, une classe très étendue de nombres transcendants, appelés maintenant nombres de Liouville.

La construction de J. Liouville est en fait fondée principalement sur le résultat suivant (*cf.* [73] ou [18]) :

Théorème 17. *Soit α un nombre algébrique de degré $m > 1$. Il existe alors une constante $c > 0$ telle que pour tout couple d'entiers (r, s) avec $s > 0$, nous avons*

$$\left|\alpha - \frac{r}{s}\right| > \frac{c}{s^m}.$$

Soit β un nombre réel. À l'aide du théorème précédent, il est facile de voir que si pour tout entier $m \geqslant 1$, il existe un couple d'entiers (r, s) avec $s > 0$ tel que

$$\left|\beta - \frac{r}{s}\right| < \frac{1}{s^m},$$

alors le nombre β est transcendant. C'est ce genre de nombres que nous appelons *nombres de Liouville* (voir [18]). En 1844, J. Liouville a utilisé précisément ce résultat pour construire les premiers nombres transcendants, dont l'un des plus connus est sans doute le nombre suivant

$$\xi = \sum_{m=1}^{+\infty} 10^{-m!}.$$

En fait, tout nombre irrationnel dont le développement décimal contient des plages de zéros suffisamment longues est un nombre de Liouville, donc transcendant. Inspirés par ce fait, mais aussi par le critère de B. de Mathan (voir [76] et [77]), ainsi

que par des considérations diophantiennes, nous allons donner une série de critères de non-automaticité, qui pourront être ensuite traduits facilement, au moyen du théorème 15, en critères de transcendance (*cf.* [116]).

Dans la suite, nous fixons S un alphabet, a un élément dans S, $u = (u(m))_{m\geqslant 0}$ une suite à valeurs dans S, et $r \geqslant 2$ un entier.

Théorème 18. *Soit* $(\mathbf{l}(m))_{m\geqslant 0}$ *et* $(\mathbf{h}(m))_{m\geqslant 0}$ *deux suites strictement croissantes d'entiers telles que pour tout entier* $m \geqslant 0$, *nous avons* $\mathbf{h}(m) \leqslant \mathbf{l}(m)$, *et* $u(k) = a$ *pour* $\mathbf{h}(m) \leqslant k \leqslant \mathbf{l}(m)$, *mais* $u(\mathbf{h}(m) - 1) \neq a$. *Si en plus,*

$$\lim_{n\to\infty} \mathbf{h}(n) = +\infty, \text{ et } \lim_{n\to\infty} \frac{\mathbf{l}(n)}{\mathbf{h}(n)} = +\infty,$$

alors la suite u *n'est pas automatique.*

Théorème 19. *Soit* $(\mathbf{l}(m))_{m\geqslant 0}$ *et* $(\mathbf{h}(m))_{m\geqslant 0}$ *deux suites strictement croissantes d'entiers telles que pour tout entier* $m \geqslant 0$, *nous avons* $\mathbf{h}(m) \leqslant \mathbf{l}(m)$, *et* $u(k) = a$ *pour* $\mathbf{h}(m) \leqslant k \leqslant \mathbf{l}(m)$, *mais* $u(\mathbf{h}(m) - 1) \neq a$. *Si pour tout entier* $s \geqslant 1$,

$$\lim_{m\to\infty} (r^s\mathbf{l}(m-s) - \mathbf{h}(m)) = +\infty, \text{ et } \lim_{m\to\infty} (\mathbf{h}(m) - r^s\mathbf{h}(m-s)) = +\infty,$$

alors la suite u *n'est pas* r*-automatique.*

Théorème 20. *Soit* $(\mathbf{l}(m))_{m\geqslant 0}$ *et* $(\mathbf{h}(m))_{m\geqslant 0}$ *deux suites strictement croissantes d'entiers telles que pour tout entier* $m \geqslant 0$, *nous avons* $\mathbf{h}(m) \leqslant \mathbf{l}(m)$, *et* $u(k) = a$ *pour* $\mathbf{h}(m) \leqslant k \leqslant \mathbf{l}(m)$, *mais* $u(\mathbf{h}(m) - 1) \neq a$. *Si pour tout entier* $s \geqslant 1$,

$$\lim_{m\to\infty} (\mathbf{l}(m+s) - r^s\mathbf{h}(m)) = +\infty, \text{ et } \lim_{m\to\infty} (r^s\mathbf{h}(m) - \mathbf{h}(m+s)) = +\infty,$$

alors la suite u *n'est pas* r*-automatique.*

Dans les deux théorèmes précédents, nous avons utilisé constamment le fait

$$u(\mathbf{h}(m) - 1) \neq a,$$

pour tout entier $m \geqslant 0$, et introduit pour cela une relation entre $\mathbf{h}(m)$ et $\mathbf{h}(m+1)$. Par contre, nous n'avons besoin d'aucune relation entre $\mathbf{l}(m)$ et $\mathbf{l}(m+1)$. Nous envisageons maintenant un autre type de critère de non-automaticité qui consiste à intervertir les rôles joués par les deux suites $(\mathbf{h}(m))_{m\geqslant 0}$ et $(\mathbf{l}(m))_{m\geqslant 0}$.

Théorème 21. *Soit* $(\mathbf{l}(m))_{m\geqslant 0}$ *et* $(\mathbf{h}(m))_{m\geqslant 0}$ *deux suites strictement croissantes d'entiers telles que pour tout entier* $m \geqslant 0$, *nous avons* $\mathbf{h}(m) \leqslant \mathbf{l}(m)$, *et* $u(k) = a$ *pour* $\mathbf{h}(m) \leqslant k \leqslant \mathbf{l}(m)$, *mais* $u(\mathbf{l}(m) + 1) \neq a$. *Si pour tout entier* $s \geqslant 1$,

$$\lim_{m\to\infty} (r^s\mathbf{l}(m) - \mathbf{h}(m+s)) = +\infty, \text{ et } \lim_{m\to\infty} (\mathbf{l}(m+s) - r^s\mathbf{l}(m)) = +\infty,$$

alors la suite u *n'est pas* r*-automatique.*

Théorème 22. *Soit* $(\mathbf{l}(m))_{m\geqslant 0}$ *et* $(\mathbf{h}(m))_{m\geqslant 0}$ *deux suites strictement croissantes d'entiers telles que pour tout entier* $m \geqslant 0$, *nous avons* $\mathbf{h}(m) \leqslant \mathbf{l}(m)$, *et* $u(k) = a$ *pour* $\mathbf{h}(m) \leqslant k \leqslant \mathbf{l}(m)$, *mais* $u(\mathbf{l}(m) + 1) \neq a$. *Si pour tout entier* $s \geqslant 1$,

$$\lim_{m\to\infty} (\mathbf{l}(m+s) - r^s\mathbf{h}(m)) = +\infty, \text{ et } \lim_{m\to\infty} (r^s\mathbf{l}(m) - \mathbf{l}(m+s)) = +\infty,$$

alors la suite u *n'est pas* r*-automatique.*

Le théorème 19 est en fait motivé par le célèbre critère de transcendance suivant, dû à B. de Mathan (*cf.* [76] et [77]), qui a été ensuite généralisé respectivement par Y. Hellegouarch (voir [68]) et par L. Denis (voir [46]).

Théorème 23. *Soit $\alpha \in \mathbb{F}_q((T^{-1}))$. Supposons qu'il existe une suite $(P_m/Q_m)_{m\geqslant 0}$ d'approximations rationnelles de α, où $P_m, Q_m \in \mathbb{F}_q[T]$, avec $P_mQ_m \neq 0$, et P_m et Q_m ne sont pas forcément premiers entre eux, vérifiant les conditions :*

(1) $\exists\ \Lambda \in \mathbb{F}_q[T]$ *tel que* $Q_m = \Lambda Q_{m-1}^q$, *pour tout entier* $m \geqslant 1$,

(2) *il existe une constante* $C > 0$ *telle que pour tout entier* $m \geqslant 1$,

$$\left|\alpha - \frac{P_m}{Q_m}\right|_\infty < C|Q_m|_\infty^{-1},$$

(3) $\exists\ \Delta \in \mathbb{F}_q[T]$ *irréductible unitaire tel que*

$$\lim_{m\to\infty} (qv_\Delta(P_{m-1}) - v_\Delta(P_m)) = +\infty,$$

où pour tout $P \in \mathbb{F}_q[T]$, $v_\Delta(P)$ *désigne le plus grand entier* k *tel que* Δ^k *divise* P *dans* $\mathbb{F}_q[T]$.

Alors la série formelle de Laurent α est transcendante sur $\mathbb{F}_q(T)$.

Dans [71], M. Koskas a montré que dans le cas où $Q_0 = 1$, $\Lambda = T^s$, et $\Delta = T$, le critère de B. de Mathan précédent peut être traité facilement par la méthode des automates finis. En réalité, c'est cette découverte de M. Koskas qui nous a vraiment conduit aux théorèmes 19 et 20, dont le dernier nous a guidé à son tour au résultat suivant, qui est un critère de transcendance dans le style de celui de B. de Mathan, mais avec une condition plutôt opposée.

Théorème 24. *Soit $\alpha \in \mathbb{F}_q((T^{-1}))$. Supposons qu'il existe une suite $(P_m/Q_m)_{m\geqslant 0}$ d'approximations rationnelles de α, où $P_m, Q_m \in \mathbb{F}_q[T]$, avec $P_mQ_m \neq 0$, et P_m et Q_m ne sont pas forcément premiers entre eux, vérifiant les conditions :*

(1) $\exists\ \Lambda \in \mathbb{F}_q[T]$ *tel que* $Q_m = \Lambda Q_{m-1}^q$, *pour tout entier* $m \geqslant 1$,

(2) *il existe une constante* $C > 0$ *telle que pour tout entier* $m \geqslant 1$,

$$\left|\alpha - \frac{P_m}{Q_m}\right|_\infty < C|Q_m|_\infty^{-1},$$

(3) $\exists\ \Delta \in \mathbb{F}_q[T]$ *irréductible unitaire tel que*

$$\lim_{m\to\infty} (v_\Delta(P_m) - qv_\Delta(P_{m-1})) = +\infty.$$

Alors la série formelle de Laurent α est transcendante sur $\mathbb{F}_q(T)$.

Tous ces critères précédents possèdent de nombreuses applications. Dans la suite, nous nous contentons d'en donner une, en nous servant du théorème 20 pour montrer que la suite des quotients partiels de la série formelle de Baum-Sweet n'est pas automatique. Il est à noter que ce résultat a été démontré initialement par M. Mkaouar dans [82] par une méthode différente.

21. **Série formelle de Baum-Sweet et fractions continues.** Tout comme dans le cas réel, les séries formelles de Laurent à coefficients dans $\mathbb{F}_q$ peuvent aussi se développer en fraction continue, dont les quotients partiels sont des polynômes à coefficients dans $\mathbb{F}_q$ (voir par exemple [3] et ses références).

Rappelons que jusqu'à présent, nous ne connaissons aucun nombre réel algébrique de degré $\geqslant 3$, dont le développement en fraction continue est à quotients partiels bornés. Plus de choses sont connues dans le cas des séries formelles algébriques : en 1976, L. E. Baum et M. M. Sweet ont donné dans [19] le premier exemple d'une série formelle cubique, dont les quotients partiels ne prennent qu'un nombre fini

de valeurs, ainsi que des exemples dont les quotients partiels prennent une infinité de valeurs. Tenant compte du théorème 15, M. Mendès France a posé la question suivante : si la suite des quotients partiels d'une série formelle algébrique ne prend qu'un nombre fini de valeurs, est-ce qu'elle est aussi automatique? On voit que la réponse à cette question suppose que l'on sache, d'une part déterminer les séries formelles algébriques à quotients partiels dans un ensemble fini, d'autre part, pour chaque série formelle algébrique à quotients partiels dans un ensemble fini, donner une expression (explicite) de ces quotients partiels, enfin démontrer l'automaticité de cette suite en utilisant ce développement explicite.

En 1986, W. H. Mills et D. P. Robbins ont montré des exemples de telles séries avec des développements en fractions continues explicites (*cf.* [81]). D'ailleurs ils sont les seuls exemples connus en caractéristique $p \geqslant 3$, et J.-P. Allouche *et al.* ont montré que pour chaque exemple donné, la suite des quotients partiels est automatique (voir [3] et [8]). Mais malheureusement, la méthode qu'ils ont utilisée ne permettait pas d'étudier l'exemple initial donné en caractéristique 2 par L. E. Baum et M. M. Sweet. En fait, dans ce cas, la suite des quotients partiels n'est pas automatique. Ce résultat a été démontré par M. Mkaouar dans [82]. Nous allons en présenter maintenant une autre preuve (voir [116]).

Posons $\mathbf{B} = \{T, T+1, T^2, T^2+1\} \subseteq \mathbb{F}_2[T]$. Pour tout mot $w = (w(j))_{0 \leqslant j \leqslant m}$ sur $\mathbf{B}$, nous définissons

$$w^+ := w(m) \cdots w(1)w(0), \text{ et } \mathbf{t}(w) := (w(0)+1)w(1) \cdots w(m).$$

Enfin pour tout entier $k \geqslant 1$, nous désignons par $(w)^k$ le mot composé de k fois w. Avec ces notations, nous allons définir une suite infinie Γ_∞.

Soit $m \geqslant 3$ un entier. Si m est impair, nous posons

$$\Lambda_m := T, T+1, T^2, (T,\ T^2)^{(2^{m-1}-4)/3}, T+1, T.$$

Dans le cas contraire où m est pair et $m \geqslant 4$, nous posons

$$\Lambda_m := T+1, T^2+1, (T, T^2)^{(2^{m-1}-5)/3}, T, T^2+1, T+1.$$

Finalement nous définissons par récurrence la suite de mots $(F_m)_{m \geqslant 0}$ par :

$$\begin{aligned}
&F_0 := T+1,\\
&F_1 := F_0, T^2+1,\\
&F_2 := F_1, T, T^2, T+1,\\
&F_m := F_{m-1}, \mathbf{t}(F_{m-3}^+), \Lambda_m, F_{m-3}, \text{ pour } m \geqslant 3.
\end{aligned}$$

Il a été démontré dans [82] que pour tout entier $m \geqslant 0$,

$$|F_m| = \frac{1}{3}2^{m+2} + \lambda_1 r_1^m + \lambda_2 r_2^m + \lambda_3 r_3^m + \frac{1}{12}(-1)^{m+1} - 1,$$

où pour tout entier $1 \leqslant k \leqslant 3$,

$$\lambda_k = \frac{1}{116}(26 + 10r_1 - r_k^2),$$

et où r_1, r_2, r_3 sont les trois solutions de l'équation $r^3 - r^2 - 2 = 0$.

Plus précisément, nous avons les expressions explicites suivantes :

$$\begin{aligned} r_1 &= \frac{(28-\sqrt{(28)^2-1})^{1/3}}{3}+\frac{(28+\sqrt{(28)^2-1})^{1/3}}{3}+\frac{1}{3}, \\ r_2 &= \frac{(28-\sqrt{(28)^2-1})^{1/3}}{3}\omega+\frac{(28+\sqrt{(28)^2-1})^{1/3}}{3}\omega^2+\frac{1}{3}, \\ r_3 &= \frac{(28-\sqrt{(28)^2-1})^{1/3}}{3}\omega^2+\frac{(28+\sqrt{(28)^2-1})^{1/3}}{3}\omega+\frac{1}{3}, \end{aligned}$$

où le nombre ω est défini par

$$\omega = -\frac{1}{2}+\frac{\sqrt{3}}{2}i.$$

Il est clair que nous avons $1 < |r_2| = |r_3| < r_1 < 2$ et $\lambda_1 > 0$. Comme pour tout entier $m \geqslant 1$, le mot F_m commence par F_{m-1}, la suite de mots $(F_m)_{m\geqslant 0}$ admet une limite faible, notée F_∞. Enfin nous remarquons que le développement en fraction continue de la série formelle de Baum-Sweet f est donné par

$$f = [1, T, F_\infty],$$

et elle est solution de l'équation $Tf^3 + f + T = 0$ (voir [81]).

Pour la suite F_∞, nous pouvons montrer que les conditions du théorème 20 sont bien vérifiées avec $r = 2$. Ainsi F_∞ n'est pas 2-automatique. Le fait que cette suite n'est pas r-automatique, pour tout entier r qui n'est pas une puissance de 2, peut se déduire du critère suivant, qui est dû essentiellement à M. Mkaouar (*cf.* [82]) et qui a été démontré sous cette forme dans [116].

Théorème 25. *Soit S un alphabet et $a \in S$. Soit $u = (u(m))_{m\geqslant 0}$ une suite à valeurs dans S telle que*

$$\overline{d}(u,a) := \limsup_{N\to\infty} \frac{1}{N}\mathrm{Card}\,(\{0 \leqslant m < N \mid u(m) = a\}) = 0.$$

Soit $(b(m))_{m\geqslant 0}$ une suite strictement croissante d'entiers vérifiant $u(b(m)) = a$, pour tout entier $m \geqslant 0$. S'il existe un entier $r \geqslant 2$ et une constante $c > 0$ tels que

$$b(m) \sim cr^m, \text{ lorsque } m \to \infty,$$

alors la suite u n'est pas s-automatique, pour tout entier $s \geqslant 2$ tel que s et r soient multiplicativement indépendants.

En fait, ce résultat est fondé sur le célèbre critère de Weyl concernant les suites équiréparties modulo 1 (*cf.* [72]), et aussi sur le théorème suivant (voir [39]).

Théorème 26. *Soit $r \geqslant 2$ un entier et u une suite r-automatique à valeurs dans un alphabet S. Fixons $a \in S$. Alors $\overline{d}(u,a) = 0$ si, et seulement si, il existe deux entiers $s \geqslant 1$ et $t \geqslant 1$ tels que $r^{s-1} \leqslant t < r^s$, et $u(m) \neq a$ pour tout entier m de la forme $m = jr^{s+k} + tr^k + l$, avec $j, k \geqslant 0$ et $0 \leqslant l < r^k$.*

22. **Fonction gamma de Carlitz-Goss.** Dans ce paragraphe, nous discutons de la fonction gamma de Carlitz-Goss et étudions la transcendance de ses valeurs.

Pour tout entier $n \in \mathbb{N}$, dont le développement q-adique est

$$n = \sum_{j=0}^{k} n_j q^j \ (0 \leqslant n_j \leqslant q-1),$$

nous définissons

$$\Pi(n) := \prod_{j=0}^{k} D_j^{n_j}$$

et appelons Π *fonction factorielle* attachée à l'anneau intègre $\mathbb{F}_q[T]$. Cette fonction a été introduite par L. Carlitz dans [30]. La fonction gamma de Carlitz Γ est alors définie par $\Gamma(n) := \Pi(n-1)$, pour tout entier $n \geqslant 1$.

Soit P un polynôme irréductible unitaire dans $\mathbb{F}_q[T]$. Nous désignons par v_P la valuation P-adique sur $\mathbb{F}_q[T]$. En d'autres termes, pour tout $Q \in \mathbb{F}_q[T]$, $v_P(Q)$ est le plus grand entier k tel que P^k divise Q dans $\mathbb{F}_q[T]$. Avec ces notations et définitions, nous avons, pour tout entier $n \geqslant 0$,

$$\Pi(n) = \prod_{P \text{ irréductible unitaire}} P^{n_P}, \tag{13}$$

où pour tout polynôme irréductible unitaire $P \in \mathbb{F}_q[T]$,

$$n_P := v_P(\Pi(n)) = \sum_{l=1}^{+\infty} [n/N(P)^l],$$

ici $N(P) = q^{\deg P}$ est le cardinal du corps quotient $\mathbb{F}_q[T]/P\mathbb{F}_q[T]$.

La relation (13), signalée initialement par W. Sinnott, explique partiellement pourquoi Π a été appelée fonction factorielle. Cette factorisation en polynômes irréductibles unitaires est en fait un analogue précis de la formule classique de la factorisation en nombres premiers

$$n! = \prod_{r \text{ premier}} r^{n_r}, \tag{14}$$

où pour tout nombre premier r,

$$n_r = \sum_{l=1}^{+\infty} [n/N(r)^l],$$

cette fois $N(r)$ désigne le cardinal du corps quotient $\mathbb{Z}/r\mathbb{Z}$, c'est-à-dire $N(r) = r$.

L'analogie entre (13) et (14) nous révèle un aspect de la similarité frappante entre les deux anneaux intègres $\mathbb{F}_q[T]$ et $\mathbb{Z}$. Remarquons en particulier que les groupes multiplicatifs correspondants sont ${\mathbb{F}_q}^\times = \mathbb{F}_q \backslash \{0\}$ et $\mathbb{Z}^\times = \{1, -1\}$; ainsi les polynômes unitaires correspondent aux entiers strictement positifs, et les polynômes irréductibles unitaires aux nombres premiers. Le lecteur peut consulter par exemple [100], [61], et leurs bibliographies pour en connaître plus sur ce sujet.

Nous définissons maintenant la fonction gamma de Carlitz-Goss $\overline{\Pi}$, introduite par D. Goss pour interpoler la fonction factorielle Π (voir [60], [62], [100], [61], et leurs références), comme suit.

Pour tout entier p-adique $n \in \mathbb{Z}_p$, dont le développement q-adique est

$$n = \sum_{j=0}^{+\infty} n_j q^j \ (0 \leqslant n_j \leqslant q-1),$$

nous posons

$$\overline{\Pi}(n) := \prod_{j=0}^{+\infty} \left(\frac{D_j}{T^{\deg D_j}} \right)^{n_j},$$

qui est un élément dans $\mathbb{F}_q((T^{-1}))$, car pour tout entier $j \geqslant 1$, nous avons

$$v_\infty\left(\left(\frac{D_j}{T^{\deg D_j}}\right)-1\right) = (q-1)q^{j-1},$$

qui tend évidemment vers $+\infty$. Il est à noter que $\overline{\Pi}$ n'est pas la "vraie" fonction gamma de Carlitz-Goss (il est peut-être mieux de l'appeler *fonction factorielle de Carlitz-Goss*), et que la "vraie" fonction est $\overline{\Gamma}$, qui est définie, tout comme Γ déduite de Π, par $\overline{\Gamma}(n) = \overline{\Pi}(n-1)$, pour tout $n \in \mathbb{Z}_p$.

À propos des résultats de transcendance des valeurs de la fonction gamma de Carlitz-Goss $\overline{\Pi}$, D. S. Thakur a montré dans [99] que les valeurs de cette fonction aux entiers strictement négatifs sont transcendantes. Bien sûr, les valeurs aux entiers positifs sont rationnelles, c'est-à-dire, éléments de $\mathbb{F}_q(T)$.

D. S. Thakur a aussi montré que $\overline{\Pi}(-1/2)$ (si $p \neq 2$) et $\overline{\Pi}(a/1-q)$ $(0 < a < q)$ sont transcendantes (voir [98], [99], et [100]), en reliant ces valeurs à la série formelle

$$\pi_C = \prod_{j=1}^{+\infty}\left(1-\frac{[j]}{[j+1]}\right) = \prod_{j=1}^{+\infty}\left(1-\frac{T^{q^j}-T}{T^{q^{j+1}}-T}\right),$$

qui a été introduite par L. Carlitz dans [29] (voir aussi l'introduction de ce mémoire), et dont la transcendance a été démontrée d'être par L. I. Wade (*cf.* [106] et [107]).

J. Yu dans [131] et A. Thiery dans [104] ont démontré par des méthodes différentes que $\overline{\Pi}(1/1-q^2)$ est transcendante.

En utilisant la méthode des automates finis, D. S. Thakur a montré (voir [102]) que $\overline{\Pi}(r)$ est transcendante, si $r \in \mathbb{Z}_p$ est congru modulo $\mathbb{Z}$ à une fraction propre, qui s'écrit comme $c/(1-q^\mu)$, avec $0 < c < q^\mu - 1$, et $c = \sum_{l=0}^{\mu-1} \alpha_l q^l$ $(0 \leqslant \alpha_l < q)$, tel qu'il existe un entier h $(0 \leqslant h \leqslant \mu - 1)$ vérifiant

$$\mu \sum_{l=0}^{\mu-1} \beta_{l-h} q^l < q^\mu - 1,$$

où par définition, nous avons $\beta_{l-h} = \alpha_k$, avec k un entier compris entre 0 et $\mu - 1$ tel que $k \equiv l - h \pmod{\mu}$.

Il a été indiqué dans [6] que L. Denis a montré que $\overline{\Pi}(n)$ est irrationnel pour tout $n \in (\mathbb{Q} \cap \mathbb{Z}_p)\backslash\mathbb{N}$ si $q > 3$.

Il a été aussi signalé dans [6] qu'à l'aide de son critère de transcendance de [77], B. de Mathan a obtenu une autre preuve (voir également [68] et [53]) du résultat de D. S. Thakur [102].

En combinant la méthode des automates finis et la dérivation logarithmique des séries formelles, J.-P. Allouche a montré dans [6] que $\overline{\Pi}(n)$ est transcendante pour tout $n \in (\mathbb{Q} \cap \mathbb{Z}_p)\backslash\mathbb{N}$. En suivant son idée mais améliorant sa méthode, finalement nous avons montré (voir [80]), avec M. Mendès France, le résultat suivant qui résout complètement le problème de transcendance des valeurs prises par la fonction gamma de Carlitz-Goss.

Théorème 27. *Soit $n \in \mathbb{Z}_p$. La série formelle de Laurent $\overline{\Pi}(n)$ est transcendante sur le corps $\mathbb{F}_q(T)$ si et seulement si $n \notin \mathbb{N}$.*

Nous remarquons que ce résultat ne possède pas de correspondant dans le cas réel, au moins pour le moment. D'ailleurs ce n'est pas un phénomène isolé, et la fonction zêta de Carlitz (voir [130] et [43]) nous en a offert un autre exemple. Ainsi dans un

certain sens, la théorie classique est en retard sur la théorie de transcendance sur des corps de fonctions.

En fait, le théorème 27 est fondé sur le théorème suivant, qui donne une réponse positive à une question soulevée par J.-P. Allouche dans [5].

Théorème 28. *Soit $u = (u(m))_{m\geqslant 1}$ une suite à valeurs dans le corps fini $\mathbb{F}_q$. Alors la série formelle de Laurent*

$$f := \sum_{m=1}^{+\infty} \frac{u(m)}{T^{q^m} - T}$$

est transcendante sur $\mathbb{F}_q(T)$ si et seulement si u n'est pas ultimement nulle.

Pour cela, nous traitons, à titre d'exemple, le cas où $q = p$. Pour tout $n \in \mathbb{Z}_p$, dont le développement q-adique est

$$n = \sum_{j=0}^{+\infty} n_j q^j \ (0 \leqslant n_j \leqslant q-1),$$

nous avons, en dérivant par rapport à la variable T,

$$\begin{aligned} \frac{\left(\overline{\Pi}(n)\right)'}{\overline{\Pi}(n)} &= \sum_{j=1}^{+\infty} n_j \left(\frac{D_j'}{D_j} - \frac{jq^j}{T}\right) \\ &= -\sum_{j=1}^{+\infty} \frac{n_j}{T^{q^j} - T}. \end{aligned}$$

Ainsi si $n \notin \mathbb{N}$, la suite $(n_j \pmod p)_{j\geqslant 0}$ n'est pas ultimement nulle, $\left(\overline{\Pi}(n)\right)'/\overline{\Pi}(n)$ est donc transcendante en vertu du théorème 28. Par conséquent, $\overline{\Pi}(n)$ est aussi transcendante, d'après la proposition 22.

En nous appuyant sur le théorème 28, nous pouvons aussi démontrer facilement les résultats suivants (voir [80]).

Théorème 29. *Soit $k \geqslant 1$ un entier et $(n_j)_{j\geqslant 0}$ une suite d'entiers tels que la suite $(n_j \pmod{p^k})_{j\geqslant 0}$ n'est pas ultimement nulle. Alors le produit infini*

$$\prod_{j=1}^{+\infty} \left(\frac{D_j}{T^{\deg D_j}}\right)^{n_j}$$

est une série formelle de Laurent transcendante sur $\mathbb{F}_q(T)$.

Théorème 30. *Soit $(\lambda_v)_v$ une famille finie d'entiers et $n^{(v)} = \sum_{j=0}^{+\infty} n_j^{(v)} q^j$ des entiers p-adiques, avec $0 \leqslant n_j^{(v)} \leqslant q-1$. Alors $\prod_v \left(\overline{\Pi}(n^{(v)})\right)^{\lambda_v}$ est rationnelle si la suite $(\sum_v \lambda_v n_j^{(v)})_{j\geqslant 0}$ est ultimement nulle, et transcendante dans le cas contraire.*

23. **Fonction gamma de Carlitz-Goss généralisée.** Inspirés par [67] et [91], nous allons généraliser la fonction gamma de Carlitz-Goss $\overline{\Pi}$, et étudier la nature algébrique des valeurs prises par ces nouvelles fonctions. Ce paragraphe peut être vu comme un complément à ce qui précède.

Soit $\nu = (\nu_j)_{j\geqslant 0}$ une suite d'entiers > 0. Pour tout entier $j \geqslant 1$, nous définissons

$$\mu_j := \sum_{k=0}^{j-1} \nu_k, \ [j]_\nu := T^{p^{\mu_j}} - T, \text{ et } D_j^{(\nu)} := \prod_{l=0}^{j-1} [j-l]^{p^{\mu_j - \mu_{j-l}}}.$$

Par convention, nous posons $D_0^{(\nu)} := 1$.

Pour tout $j \in \mathbb{N}$, posons $\overline{D}_j^{(\nu)} := D_j^{(\nu)}/T^{\deg D_j^{(\nu)}}$. Si $j \geqslant 2$, nous avons alors

$$v_\infty(\overline{D}_j^{(\nu)} - 1) = p^{\mu_j} - p^{\mu_{j-1}} = (p^{\nu_j} - 1)p^{\mu_{j-1}}.$$

Ainsi $\overline{D}_j^{(\nu)}$ tend vers 1 dans $\mathbb{F}_q((T^{-1}))$. Par suite, pour tout $n \in \mathbb{Z}_p$, dont le développement q-adique est

$$n = \sum_{j=0}^{+\infty} n_j q^j \ (0 \leqslant n_j \leqslant q-1),$$

le produit infini

$$\overline{\Pi}_\nu(n) := \prod_{j=0}^{+\infty} (\overline{D}_j^{(\nu)})^{n_j} := \lim_{k \to +\infty} \prod_{j=0}^{k} (\overline{D}_j^{(\nu)})^{n_j}$$

converge dans $\mathbb{F}_q((T^{-1}))$, et nous appelons $\overline{\Pi}_\nu$ *fonction gamma de Carlitz-Goss généralisée*, associée à la suite ν (comme plus haut, la "vraie" fonction gamma de Carlitz-Goss généralisée est $\overline{\Gamma}_\nu$, définie par $\overline{\Gamma}_\nu(n) := \overline{\Pi}_\nu(n-1)$, pour tout $n \in \mathbb{Z}_p$).

Nous remarquons que si $s = \log q/\log p$, et si v est la suite constante dont la valeur commune est s, nous avons alors $\overline{\Gamma}_\nu = \overline{\Gamma}$.

Aussi à l'aide du théorème 28, nous pouvons démontrer les résultats suivants.

Théorème 31. *Soit $n \in \mathbb{Z}_p$ et $\nu = (\nu_j)_{j \geqslant 0}$ une suite d'entiers strictement positifs. Alors $\overline{\Pi}_\nu(n)$ est transcendante sur $\mathbb{F}_q(T)$ si et seulement si $n \notin \mathbb{N}$.*

Théorème 32. *Soit $k \geqslant 1$ un entier et $(n_j)_{j \geqslant 0}$ une suite d'entiers tels que la suite $(n_j \pmod{p^k})_{j \geqslant 0}$ n'est pas ultimement nulle. Alors pour toute suite ν d'entiers strictement positifs, le produit infini $\prod_{j=0}^{+\infty} (\overline{D}_j^{(\nu)})^{n_j}$ est transcendant sur $\mathbb{F}_q(T)$.*

Théorème 33. *Soit $\lambda_1, \lambda_2, \ldots, \lambda_k$ des entiers naturels, et $n^{(i)} = \sum_{j=0}^{+\infty} n_j^{(i)} q^j$ des entiers p-adiques, avec $0 \leqslant n_j^{(i)} < q$ $(1 \leqslant i \leqslant k)$. Alors pour toute suite ν d'entiers > 0, le produit fini des séries formelles de Laurent $\prod_{i=1}^{k} (\overline{\Pi}_\nu(n^{(i)}))^{\lambda_i}$ est ou bien rationnel ou bien transcendant sur $\mathbb{F}_q(T)$, et il est transcendant sur $\mathbb{F}_q(T)$ si et seulement si la suite $(\sum_{i=1}^{k} \lambda_i n_j^{(i)})_{j \geqslant 0}$ n'est pas ultimement nulle.*

Le théorème précédent nous révèle la nature du produit des valeurs d'une seule fonction $\overline{\Pi}_\nu$ aux arguments différents. Il est aussi possible d'examiner le produit des valeurs de différentes fonctions $\overline{\Pi}_\nu$ aux arguments différents. Sur ce plan, nous avons le résultat partiel suivant.

Théorème 34. *Soit $\lambda_1, \lambda_2, \ldots, \lambda_k$ des entiers naturels, et $n^{(i)} = \sum_{j=0}^{+\infty} n_j^{(i)} q^j$ des entiers p-adiques, avec $0 \leqslant n_j^{(i)} < q$ $(1 \leqslant i \leqslant k)$. Soit $\nu^{(1)}, \nu^{(2)}, \ldots, \nu^{(k)}$ des suites d'entiers strictement positifs. Pour tous les entiers $i, j, m \geqslant 1$ $(1 \leqslant i \leqslant k)$, posons*

$$\mu_j^{(i)} := \sum_{l=0}^{j-1} \nu_l^{(i)} \text{ et } u(m) := \sum_{\mu_j^{(i)} = m} \lambda_i n_j^{(i)}.$$

Si la suite $(u(m) \pmod{p})_{m \geqslant 0}$ n'est pas ultimement nulle, alors $\prod_{i=1}^{k} (\overline{\Pi}_{\nu^{(i)}}(n^{(i)}))^{\lambda_i}$ est transcendant sur $\mathbb{F}_q(T)$.

Discutons maintenant de la généralisation de π_C.

Pour toute suite d'entiers strictement positifs $\nu = (\nu_j)_{j\geqslant 0}$, nous définissons

$$\pi_\nu := \prod_{j=1}^{+\infty}\left(1-\frac{[j]_\nu}{[j+1]_\nu}\right).$$

Dans [91], F. Recher a examiné le cas où ν est une suite purement périodique, et a montré dans ce cas, par la méthode de J.-P. Allouche (voir [5]) qui lui a servi à démontrer la transcendance de π_C à l'aide des automates finis, que π_ν est transcendant sur $\mathbb{F}_q(T)$. Plus généralement, nous avons

Théorème 35. *Pour toute suite d'entiers strictement positifs $\nu = (\nu_j)_{j\geqslant 0}$, π_ν est transcendant sur le corps $\mathbb{F}_q(T)$.*

La preuve est assez simple et mérite d'être mentionnée ici.

Prenant la dérivée logarithmique de π_ν par rapport à T, nous obtenons

$$\begin{aligned}\frac{\pi'_\nu}{\pi_\nu} &= \sum_{j=1}^{+\infty}\left(\frac{[j+1]'_\nu-[j]'_\nu}{[j+1]_\nu-[j]_\nu}-\frac{[j+1]'_\nu}{[j+1]_\nu}\right)\\ &= \sum_{j=1}^{+\infty}\left(\frac{p^{\mu_{j+1}}T^{p^{\mu_{j+1}}-1}-p^{\mu_j}T^{p^{\mu_j}-1}}{[j+1]_\nu-[j]_\nu}-\frac{p^{\mu_{j+1}}T^{p^{\mu_{j+1}}-1}-1}{[j+1]_\nu}\right)\\ &= \sum_{j=1}^{+\infty}\frac{1}{[j+1]_\nu}.\end{aligned}$$

Ainsi π'_ν/π_ν est transcendant sur $\mathbb{F}_q(T)$, d'après le théorème 28. Par suite, π_ν est transcendant sur $\mathbb{F}_q(T)$ en vertu de la proposition 22.

24. **Fonction gamma de Carlitz-Goss P-adique.** En dualité avec la fonction gamma de Carlitz-Goss $\overline{\Pi}$ qui est l'interpolation ∞-adique de Π, D. Goss a aussi introduit l'interpolation P-adique Π_P, pour tout polynôme P irréductible unitaire à coefficients dans $\mathbb{F}_q$ (voir [59] et [60]), que nous étudions maintenant.

Fixons P un polynôme irréductible unitaire dans $\mathbb{F}_q[T]$ de degré $h \geqslant 1$. Nous désignons par v_P la valuation P-adique sur $\mathbb{F}_q[T]$, que nous étendons canoniquement au corps $\mathbb{F}_q(T)$. Notons $\mathbb{F}_q(T)_P$ la complétion P-adique de $\mathbb{F}_q(T)$, c'est-à-dire la complétion de $\mathbb{F}_q(T)$ par rapport à la valuation v_P. Les éléments de $\mathbb{F}_q(T)_P$ sont aussi appelés des séries formelles sur $\mathbb{F}_q$.

Pour tout entier $j \geqslant 0$, nous désignons par $D_{j,P}$ le produit de tous les polynômes unitaires dans $\mathbb{F}_q[T]$ de degré j, qui sont premiers avec P. Nous avons alors

$$D_{j,P} = D_j \text{ pour } 0 \leqslant j < h, \text{ et } D_{j,P} = D_j/P^{q^{j-h}}D_{j-h} \text{ pour } j \geqslant h.$$

Il est démontré dans [59] (voir aussi [60]) que $-D_{j,P}$ tend P-adiquement vers 1, lorsque $j \to +\infty$. Ainsi pour tout $n \in \mathbb{Z}_p$, dont le développement q-adique est

$$n = \sum_{j=0}^{+\infty} n_j q^j \ (0 \leqslant n_j \leqslant q-1),$$

le produit infini

$$\Pi_P(n) := \prod_{j=0}^{+\infty}(-D_{j,P})^{n_j}$$

converge et définit une série formelle dans $\mathbb{F}_q(T)_P$.

Par une méthode tout à fait analogue à celle du théorème 27, nous pouvons aussi démontrer le résultat suivant (*cf.* [113]).

Théorème 36. *Soit $P \in \mathbb{F}_q[T]$ un polynôme irréductible unitaire. Soit $n \in \mathbb{Z}_p$ un entier p-adique dont le développement q-adique est donné par*

$$n = \sum_{j=0}^{+\infty} n_j q^j \ (0 \leqslant n_j \leqslant q-1).$$

Supposons qu'il existe un entier $a \geqslant 0$ tel que pour tout entier $j \geqslant a$,

$$n_{jh+k} = n_k \ (1 \leqslant k < h).$$

Alors $\Pi_P(n)$ est algébrique sur le corps $\mathbb{F}_q(T)$ si et seulement si la suite $(n_j)_{j\geqslant 0}$ est ultimement périodique de période d.

Comme corollaire, nous obtenons tout de suite le théorème suivant (voir [113]).

Théorème 37. *Soit $P \in \mathbb{F}_q[T]$ un polynôme unitaire de degré 1. Soit $n \in \mathbb{Z}_p$ un entier p-adique dont le développement q-adique est donné par*

$$n = \sum_{j=0}^{+\infty} n_j q^j \ (0 \leqslant n_j \leqslant q-1).$$

Alors $\Pi_P(n)$ est algébrique sur le corps $\mathbb{F}_q(T)$ si et seulement si la suite $(n_j)_{j\geqslant 0}$ est ultimement constante.

De manière similaire, nous avons aussi obtenu les résultats suivants (voir [113]).

Théorème 38. *Soit $P \in \mathbb{F}_q[T]$ un polynôme unitaire de degré 1. Soit $k \geqslant 1$ un entier et $(n_j)_{j\geqslant 0}$ une suite d'entiers tels que la suite $(n_j \pmod{p^k})_{j\geqslant 0}$ n'est pas ultimement constante. Alors le produit infini*

$$\prod_{j=0}^{+\infty} (-D_{j,P})^{n_j}$$

est transcendant sur le corps $\mathbb{F}_q(T)$.

Théorème 39. *Soit $\lambda_1, \lambda_2, \ldots, \lambda_k$ des entiers naturels, et $n^{(i)} = \sum_{j=0}^{+\infty} n_j^{(i)} q^j$ des entiers p-adiques, avec $0 \leqslant n_j^{(i)} < q$ $(1 \leqslant i \leqslant k)$. Soit $P \in \mathbb{F}_q[T]$ un polynôme unitaire de degré 1. Alors le produit fini $\prod_{i=1}^{k} (\Pi_P(n^{(i)}))^{\lambda_i}$ est ou bien rationnel ou bien transcendant sur $\mathbb{F}_q(T)$, et il est transcendant sur $\mathbb{F}_q(T)$ si et seulement si la suite $(\sum_{i=1}^{k} \lambda_i n_j^{(i)})_{j\geqslant 0}$ n'est pas ultimement constante.*

Inspirés par le théorème 37, nous conjecturons le résultat suivant.

Conjecture 1. *Soit $P \in \mathbb{F}_q[T]$ un polynôme unitaire de degré $h \geqslant 1$. Soit $n \in \mathbb{Z}_p$ un entier p-adique dont le développement q-adique est donné par*

$$n = \sum_{j=0}^{+\infty} n_j q^j \ (0 \leqslant n_j \leqslant q-1).$$

Alors $\Pi_P(n)$ est algébrique sur le corps $\mathbb{F}_q(T)$ si et seulement si la suite $(n_j)_{j\geqslant 0}$ est ultimement périodique de période h.

En fait, la preuve que la condition sur la suite $(n_j)_{j\geqslant 0}$ est suffisante est assez facile (voir [100] et [113]). C'est la réciproque qui nous pose des problèmes.

25. **Quelques fonctions transcendantes.** Dans ce paragraphe, nous définirons trois familles de fonctions et étudierons leur nature algébrique.

Soit $\mathbf{k} := \mathbb{F}_q(T)$. Nous désignons par $\mathbf{k}[t]$ l'anneau (intègre) des polynômes de la variable t à coefficients dans $\mathbf{k}$, et par $\mathbf{k}(t)$ le corps de fractions de $\mathbf{k}[t]$. Notons ω_t la valuation t-adique sur $\mathbf{k}[t]$. En d'autres termes, pour tout $P \in \mathbf{k}[t]$, $\omega_t(P)$ désigne le plus grand entier k tel que t^k divise P dans $\mathbf{k}[t]$. Nous étendons ensuite ω_t au corps $\mathbf{k}(t)$, et désignons par $\mathbf{k}((t))$ la complétion topologique de $\mathbf{k}(t)$ par rapport à la valuation ω_t. Il est clair que pour tout $f \in \mathbf{k}((t))$, nous pouvons écrire

$$f = \sum_{m=k}^{+\infty} a(m)t^m,$$

avec $a(m) \in \mathbf{k}$ pour tout $m \in \mathbb{Z}$ $(m \geqslant k)$. En particulier, $\omega_t(f) = k$ si $a(k) \neq 0$.

Soit $\gamma \geqslant 1$ un entier et $u = (u(j))_{j\geqslant 0}$ une suite à valeurs dans $\mathbb{F}_q$. Nous posons

$$\psi_u^{(\gamma)} := \sum_{j=0}^{+\infty} \frac{u(j)}{D_j^\gamma}\, t^{q^j},\ \lambda_u^{(\gamma)} := \sum_{j=0}^{+\infty} \frac{u(j)}{L_j^\gamma} t^{q^j},\ \text{et } \varphi_u^{(\gamma)} := \sum_{j=1}^{+\infty} \frac{u(j)}{[j]^\gamma} t^{q^j},$$

et nous nous intéressons à la nature algébrique de toutes ces fonctions.

Exemple 6. *D'abord soit* $u = ((-1)^j)_{j\geqslant 0}$. *Alors*

$$\psi_u^{(1)} = \sum_{j=0}^{+\infty} (-1)^j \frac{t^{q^j}}{D_j} = e_C$$

est précisément la fonction exponentielle de Carlitz. Soit maintenant v *la suite constante* 1. *Cette fois nous obtenons la fonction logarithmique de Carlitz*

$$\lambda_v^{(1)} = \sum_{k=0}^{+\infty} \frac{t^{q^k}}{L_k} = \log_C .$$

Ces deux fonctions, introduites par L. Carlitz dans [29], *ont marqué le début de la théorie du module de Carlitz.*

Exemple 7. *Pour tout entier* γ *compris entre* 1 *et* q, *posons* $u_\gamma = ((-1)^{j\gamma})_{j\geqslant 0}$. *Nous avons alors (voir* [98]*)*

$$\lambda_{u_\gamma}^{(\gamma)}(1) = \sum_{k=0}^{+\infty} \frac{(-1)^{k\gamma}}{L_k^\gamma} = \zeta_C(\gamma),$$

où ζ_C *est la fonction zêta de Carlitz définie par*

$$\zeta_C(s) := \sum_{P\in\mathbb{F}_q[T]\ \textit{unitaire}} \frac{1}{P^s},$$

pour tout entier $s \geqslant 1$.

Exemple 8. *Pour tout* $n \in \mathbb{Z}_p$ *dont le développement* q*-adique est donné par*

$$n = \sum_{j=0}^{+\infty} n_j q^j \ (0 \leqslant n_j \leqslant q-1),$$

nous avons alors

$$\frac{\left(\overline{\Pi}(n)\right)'}{\overline{\Pi}(n)} = -\sum_{j=1}^{+\infty} \frac{n_j}{T^{q^j} - T} = \varphi_u^{(1)}(-1), \text{ avec } u = (n_j)_{j \geqslant 0}.$$

Tous ces exemples montrent que les trois familles de fonctions $\psi_u^{(\gamma)}$, $\lambda_u^{(\gamma)}$, et $\varphi_u^{(\gamma)}$ sont bien omniprésentes dans notre étude du module de Carlitz.

Théorème 40. *Soit $\gamma \geqslant 1$ un entier et u une suite à valeurs dans $\mathbb{F}_q$. Alors la fonction $\psi_u^{(\gamma)}$ est transcendante sur le corps $\mathbf{k}(t)$ si et seulement si la suite u n'est pas ultimement nulle. En particulier, la fonction exponentielle de Carlitz e_C est transcendante sur le corps $\mathbf{k}(t)$.*

Théorème 41. *Soit $\gamma \geqslant 1$ un entier et u une suite à valeurs dans $\mathbb{F}_q$. Alors la fonction $\lambda_u^{(\gamma)}$ est transcendante sur le corps $\mathbf{k}(t)$ si et seulement si la suite u n'est pas ultimement nulle. En particulier, la fonction logarithmique de Carlitz $\log_C$ est transcendante sur le corps $\mathbf{k}(t)$.*

Il est bien connu que e_C et $\log_C$ sont des fonctions transcendantes. D'ailleurs le théorème 40 est un cas spécial d'un résultat général de L. I. Wade (voir [109]), établi par une méthode purement analytique. Mais comme la fonction $\lambda_u^{(\gamma)}$ n'est pas entière, il est donc difficile pour nous de raisonner de la même manière afin de démontrer le théorème 41. Dans [119], nous avons donné une méthode algébrique mais élémentaire pour traiter $\psi_u^{(\gamma)}$, $\lambda_u^{(\gamma)}$, ainsi que des problèmes similaires. En fait, les deux théorèmes précédents sont des conséquences faciles du résultat suivant (voir [96], [63], et [4]), qui généralise le théorème 15.

Théorème 42. *Soit $v = (v(m))_{m \geqslant 0}$ une suite à valeurs dans un corps $\mathbf{K}$. Nous fixons $\overline{\mathbf{K}}$ une clôture algébrique de $\mathbf{K}$. Alors la série formelle*

$$\sum_{m=0}^{+\infty} v(m) t^m$$

est algébrique sur $\mathbf{K}(t)$ si et seulement si le $\overline{\mathbf{K}}$-espace vectoriel engendré par

$$\left\{ \left(v^{1/q^a}(q^a m + b) \right)_{m \geqslant 0} \mid a,\ b \in \mathbb{N},\ 0 \leqslant b < q^a \right\}$$

est de dimension finie sur $\overline{\mathbf{K}}$.

Ce théorème a été démontré par H. Sharif et C. Woodcock (voir [96]), et par T. Harase (voir [63]) indépendamment. La présente version est la reformulation due à J.-P. Allouche (*cf.* [4]).

Dans le cas où la suite $v = (v(m))_{m \geqslant 0}$ prend une forme bien particulière, nous avons le critère simplifié suivant (*cf.* [119]).

Théorème 43. *Soit $w = (w(m))_{m \geqslant 0}$ une suite à valeurs dans un corps $\mathbf{K}$. Alors la série formelle $\sum_{m=0}^{+\infty} w(m) t^{q^m}$ est algébrique sur le corps $\mathbf{K}(t)$ si et seulement si le $\overline{\mathbf{K}}$-espace vectoriel engendré par les suites $(w^{1/q^k}(m+k))_{m \geqslant 0}$ $(k \in \mathbb{N})$ est de dimension finie sur $\overline{\mathbf{K}}$.*

Dans le cas où $\mathbf{K}$ est un corps fini, le lecteur peut trouver dans [28] une première version du théorème 43. Enfin nous remarquons que les théorèmes 40 et 41 sont fondés sur le théorème 43 et sur le simple fait que k vecteurs sont linéairement indépendants si un mineur d'ordre k de la matrice formée par ces vecteurs est non nul. Pour plus de détails, voir [119].

Pour la fonction $\varphi_u^{(\gamma)}$, nous avons le résultat analogue suivant qui donne une réponse affirmative à la conjecture posée à la fin de [119].

Théorème 44. *Soit $\gamma \geqslant 1$ un entier et u une suite à valeurs dans $\mathbb{F}_q$. Alors la fonction $\varphi_u^{(\gamma)}$ est transcendante sur le corps $\mathbf{k}(t)$ si et seulement si la suite u n'est pas ultimement nulle.*

Il semble que la méthode précédente n'est pas valable pour le théorème 44, et nous ne savons pas pourquoi. Heureusement à l'aide du théorème 28, nous pouvons démontrer, en utilisant la dérivation par rapport à T, que si la suite u n'est pas ultimement nulle, alors $\varphi_u^{(\gamma)}(1)$ est transcendant sur $\mathbb{F}_q[T]$ (voir [123]), d'où la preuve du théorème 44.

Dans [106], L. I. Wade a montré que la valeur de la fonction exponentielle (resp. logarithmique) de Carlitz est transcendante pour un argument algébrique non nul. Inspiré par ce théorème et d'autres faits, nous conjecturons le résultat suivant.

Conjecture 2. *Soit u une suite à valeurs dans $\mathbb{F}_q$ et $\alpha \in \mathbf{C}_\infty$ un élément algébrique non nul. Si u n'est pas ultimement nulle, alors pour tout entier $\gamma \geqslant 1$, les valeurs $\psi_u^{(\gamma)}(\alpha)$, $\lambda_u^{(\gamma)}(\alpha)$, et $\varphi_u^{(\gamma)}(\alpha)$ sont transcendantes sur $\mathbb{F}_q(T)$.*

Bien sûr, dans le cas de $\lambda_u^{(\gamma)}$ ou $\varphi_u^{(\gamma)}$, nous devons supposer en plus que α est dans le domaine de convergence de la fonction en question.

Il semble que pour l'instant, cette conjecture est hors de notre portée. Cependant en utilisant la méthode de Wade, celle de l'approximation diophantienne, ainsi que la méthode des automates finis, nous avons quand même pu examiner la nature algébrique de ces trois fonctions aux arguments rationnels, au moins pour certaines valeurs. Tout cela sera discuté et traité dans [123] (voir aussi [124]).

Finalement nous constatons que jusqu'à présent, nous avons seulement discuté de la transcendance des séries formelles, et nous n'avons guère mentionné la théorie de transcendance des nombres réels liés aux suites automatiques ou plus généralement aux suites substitutives par des procédés classiques (par exemple, développement binaire ou en fraction continue), qui dépasse le cadre de ce mémoire. À cette fin, nous renvoyons le lecteur intéressé à [85], [52], [15], [90], [86], [7], [9], et bien sûr aussi à l'excellent livre [13].

26. **Perspectives.** À l'avenir, plusieurs directions de recherches sont possibles.

À propos de notre étude sur les propriétés élémentaires des automates finis, il reste encore beaucoup de questions ouvertes. Actuellement nous savons comment caractériser les automates fidèles et strictement fidèles. Nous pouvons évidemment poser ces mêmes questions pour les automates avec fonction de sortie. Nous savons qu'un automate premier est faiblement irréductible. Cependant nous ne savons pas s'il existe une relation entre les automates irréductibles et les automates premiers. En fait, nous ne savons même pas s'il existe un automate premier. Nous ne savons pas non plus quand un automate fini peut se décomposer en automates irréductibles, et quand la décomposition est unique. Il est facile de savoir si un automate fini

est irréductible ou pas (la proposition 4). Mais pour l'instant, nous ne disposons d'aucune caractérisation simple des automates finis faiblement irréductibles. Tout cela complique l'arithmétique des automates finis.

Nous remarquons que l'homogénéité est une "propriété de produit", c'est-à-dire, le produit avec un automate homogène nous donne encore un automate homogène. Cela nous rappelle bien sûr les idéaux de l'algèbre. En même temps, être normalisé est une "propriété de facteur" dans le sens où tout facteur d'un automate normalisé est aussi normalisé. Il sera intéressant de caractériser ces deux sortes de propriétés par les structures des automates en question, comme ce que nous avons fait dans la proposition 9. Les automates avec fonction de sortie inversibles ou inversibles à gauche sont déjà bien compris. Mais pour le moment, nous n'avons aucune idée sur les automates avec fonction de sortie qui sont inversibles à droite. Nous ne savons pas non plus comment caractériser les automates avec fonction de sortie qui sont surjectifs. Un problème important dans l'étude des suites p-automatiques concerne leur clôture topologique. En d'autres termes, nous voulons savoir quand la limite d'une suite de suites p-automatiques est encore p-automatique. Sur ce sujet, nous avons déjà obtenu une condition suffisante. Mais elle est trop forte, donc peu utile. Il est donc nécessaire d'envisager des conditions plus souples.

À côté de la théorie des opacités des automates finis, nous pouvons, d'une part, généraliser tous ce que nous avons fait plus haut aux automates finis généraux non nécessairement déterministes (voir [122]), et d'autre part, examiner avec plus de minutie l'opacité attachée à la pseudo-distance de Hamming, et discuter ensuite l'opacité de plusieurs automates finis enchaînés. Il est à noter que dans ce dernier cas, nous n'aurons pas des fonctions faiblement dérivables. Ainsi la situation sera beaucoup plus compliquée que dans le cas de l'opacité quadratique.

À côté de l'étude de la transcendance des séries formelles issues du module de Carlitz, nous avons obtenu tout récemment un critère de transcendance qui contient tous les critères mentionnés dans ce mémoire, et possède de nombreuses applications intéressantes (voir [123]). D'ailleurs ce critère peut être démontré par l'approximation diophantienne, et par la méthode de Wade respectivement. Cela laisse supposer que ces deux méthodes sont plus ou moins équivalentes. En même temps, nous avons aussi obtenu une nouvelle preuve par la méthode de Wade de la transcendance des valeurs de la fonction gamma de Carlitz-Goss, un résultat démontré initialement à l'aide des automates finis. Nous rappelons que J. Fresnel, M. Koskas, et B. de Mathan ont aussi montré qu'il existe un passage entre la méthode de l'approximation diophantienne et celle des automates finis (voir [53]). Tout cela confirme la suggestion de J.-P. Allouche que les quatres méthodes citées dans l'introduction de ce mémoire sont peut-être équivalentes. Bien sûr, il reste encore beaucoup de travail à faire pour arriver à ce résultat.

Bibliographie

[1] R. L. Adler, L. W. Goodwyn and B. Weiss, *Equivalence of topological Markov shifts.* Israel J. Math. **27** (1977), 48-63.

[2] J.-P. Allouche, *Automates finis en théorie des nombres.* Exposition. Math. **5** (1987), 239-266.

[3] J.-P. Allouche, *Sur le développement en fraction continue de certaines séries formelles.* C. R. Acad. Sci. Paris, Sér. I, Math., **307** (1988), 631-633.

[4] J.-P. Allouche, *Note sur un article de Sharif et Woodcock.* Sém. Théor. Nombres Bordeaux, Sér. 2, **1** (1989), 163-187.

[5] J.-P. Allouche, *Sur la transcendance de la série formelle* II. Sém. Théor. Nombres Bordeaux, Sér. 2, **2** (1990), 103-117.
[6] J.-P. Allouche, *Transcendence of the Carlitz-Goss gamma function at rational arguments.* J. Number Theory **60** (1996), 318-328.
[7] J.-P. Allouche, *Nouveaux résultats de transcendance de réels à développement non aléatoire.* Gaz. Math. **84** (2000), 19-34.
[8] J.-P. Allouche, J. Bétréma, et J. Shallit, *Sur des points fixes de morphismes d'un monoïde libre.* RAIRO, Inform. Théor. Appl. **23** (1989), 235–249.
[9] J.-P. Allouche, J. L. Davison, M. Queffélec, and L. Q. Zamboni, *Transcendence of Sturmian or morphic continued fractions.* J. Number Theory **91** (2001), 39-66.
[10] J.-P. Allouche and M. Mendès France, *Quasicrystal Ising chain and automata theory.* J. Stat. Phys. **42** (1986), 809-821.
[11] J.-P. Allouche and M. Mendès France, *Automata and automatic sequences,* dans *Beyond Quasicrystals* (Les Houches, 1994), 293-367, Springer (1995).
[12] J.-P. Allouche and J. O. Shallit, *The ubiquitous Prouhet-Thue-Morse sequence,* dans *Sequences and Their Applications* (Singapore, 1998), 1-16. Springer Ser. Discrete Math. Theor. Comput. Sci., Springer, London (1999).
[13] J.-P. Allouche and J. O. Shallit, *Automatic Sequences. Theory, Applications, Generalizations.* To be published by Cambridge University Press (2003).
[14] J.-P. Allouche and D. S. Thakur, *Automata and transcendence of the Tate period in finite characteristic.* Proc. Amer. Math. Soc. **127** (1999), 1309-1312.
[15] J.-P. Allouche and L. Q. Zamboni, *Algebraic irrational binary numbers cannot be a fixed points of non-trivial constant-length or primitive morphisms.* J. Number Theory **69** (1998), 119-124.
[16] G. W. Anderson, *t-motives.* Duke Math. J. **53** (1986), 457-502.
[17] G. W. Anderson and D. S. Thakur, *Tensor powers of the Carlitz module and zeta values.* Ann. of Math. **132** (1990), 159-191.
[18] A. Baker, *Transcendental Number Theory.* Cambridge University Press (1975).
[19] L. E. Baum and M. M. Sweet, *Continued fractions of algebraic power series in characteristic* 2. Ann. of Math. **103** (1976), 593-610.
[20] J. Berstel, *Transductions and Context-free Languages.* Teubner verlagsgesellschaft (1979).
[21] V. Berthé, *Fonction ζ de Carlitz et automates.* J. Théor. Nombres Bordeaux **5** (1993), 53-77.
[22] V. Berthé, *Automates et valeurs de transcendance du logarithme de Carlitz.* Acta Arith. **66** (1994), 369-390.
[23] V. Berthé, *Combinaisons linéaires de $\zeta(s)/\Pi^s$ sur $F_q(x)$, pour $1 \leqslant s \leqslant q-2$.* J. Number Theory **53** (1995), 272-299.
[24] J.-P. Bertrandias, *Espaces de fonctions bornées et continues en moyenne asymptotique d'ordre p.* Bull. Soc. Math. France, Mémoire **5** (1966), 106 pp.
[25] J.-C. Birget, S. Margolis, J. Meakin, and P. Weil, *PSPACE-completeness of certain algorithmic problems on the subgroups of free groups.* Theoret. Comput. Sci. **242** (2000), 247-281.
[26] N. Bourbaki, *Éléments de Mathématique. Espaces Vectoriels Topologiques.* Masson (1981).
[27] N. Bourbaki, *Éléments de Mathématique. Topologie Générale.* Hermann (1971).
[28] C. Cadic, *Interprétations p-automatique des groupes formels de Lubin-Tate et des modules de Drinfel'd réduits* (Thèse). Université de Limoges (1999).
[29] L. Carlitz, *On certain functions connected with polynomials in a Galois field.* Duke Math. J. **1** (1935), 137-168.
[30] L. Carlitz, *An analogue of the von Staudt-Clausen theorem.* Duke Math. J. **3** (1937), 503-517.
[31] L. Carlitz, *An analogue of the Staudt-Clausen theorem.* Duke Math. J. **7** (1940), 62-67.
[32] L. Carlitz, *Some special functions over GF(q,x).* Duke Math. J. **27** (1960), 139-158.
[33] P. Caron and D. Ziadi, *Characterization of Glushkov automata.* Theoret. Comput. Sci. **233** (2000), 75-90.
[34] C. Choffrut, *Minimizing subsequential transducers: a survey.* Prétirage (2003). Accessible sur http://www.liafa.jussieu.fr/~cc.
[35] G.-L. Chen and J.-Y. Yao, *Characterization of opaque automata.* Discrete Math. **247** (2002), 65-78.
[36] G. Christol, *Ensembles presque périodiques k-reconnaissables.* Theoret. Comput. Sci. **9** (1979), 141-145.

[37] G. Christol, T. Kamae, M. Mendès France et G. Rauzy, *Suites algébriques, automates et substitutions*. Bull. Soc. Math. France **108** (1980), 401-419.
[38] A. Cobham, *On the base-dependence of sets of numbers recognizable by finite automata*. Math. Systems Theory **3** (1969), 186-192.
[39] A. Cobham, *Uniform tag sequences*. Math. Systems Theory **6** (1972), 164-192.
[40] J. H. Conway, *Regular Algebra and Finite Machines*. Chapman and Hall Ltd. (1971).
[41] P. Deligne and D. Husemöller, *Survey of Drinfel'd modules*. Contemp. Math. **67** (1987), 25-91.
[42] G. Damamme et Y. Hellegouarch, *Propriétés de transcendance des valeurs de la fonction zêta de Carlitz*. C. R. Acad. Sci. Paris, Séri. I, Math., **307** (1988), 635-637.
[43] G. Damamme et Y. Hellegouarch, *Transcendence of the values of the Carlitz zeta function by Wade's method*. J. Number Theory **39** (1991), 257-278.
[44] F. M. Dekking, *The spectrum of dynamical systems arising from substitutions of constant length*. Z. Wahrscheinlichkeitstheorie und Verw. Gebiete **41** (1977/78), 221-239.
[45] L. Denis, *Transcendance et dérivées de l'exponentielle de Carlitz*. Sém. Théor. Nombres Paris (1993), 1-21.
[46] L. Denis, *Un critère de transcendance en caractéristique finie*. J. Algebra **182** (1996), 522-533.
[47] L. Denis, *Valeurs transcendantes des fonctions de Bessel-Carlitz*. Ark. Mat. **36** (1998), 73-85.
[48] V. G. Drinfel'd, *Elliptic modules*. Math. USSR Sbornik **23** (1974), 561-592.
[49] V. G. Drinfel'd, *Elliptic modules II*. Math. USSR Sbornik **31** (1977), 159-170.
[50] S. Eilenberg, *Automata, Languages and Machines*. Vol. A. Academic Press (1974).
[51] I. Ekeland, *La théorie des Jeux et Ses Applications à l'Économie Mathématique*. Presses Universitaires de France (1974).
[52] S. Ferenczi and C. Mauduit, *Transcendence of numbers with a low complexity expansion*. J. Number Theory **67** (1997), 146-161.
[53] J. Fresnel, M. Koskas, and B. de Mathan, *Automata and transcendence in positive characteristic*. J. Number Theory **80** (2000), 1-24.
[54] F. Gécseg, *Composition of automata*. Lecture Notes in Computer Science **14** (1974), 351-363.
[55] F. Gécseg, *On products of abstract automata*. Acta Sci. Math. (Szeged) **38** (1976), 21-43.
[56] E.-U. Gekeler, *Drinfel'd Modular Curves*. Lecture Notes in Math. **1231**. Springer (1986).
[57] A. Ginzburg, *Algebraic Theory of Automata*. Academic Press, New York (1968).
[58] D. Goss, *von-Staudt for* $\mathbb{F}_q[T]$. Duke Math. J. **45** (1978), 885-910.
[59] D. Goss, *Modular forms for* $\mathbb{F}_r[T]$. J. Reine Angew. Math. **317** (1980), 16-39.
[60] D. Goss, *The* Γ *function in the arithmetic of function fields*. Duke Math. J. **56** (1988), 163-191.
[61] D. Goss, *Basic Structures of Function Field Arithmetic*. Second edition. Springer (1998).
[62] D. Goss, D. R. Hayes and M. I. Rosen (Eds.), *The Arithmetic of Function Fields*. Walter de Gruyter, Berlin/New York (1992).
[63] T. Harase, *Algebraic elements in formal power series rings*. Israel J. Math. **63** (1988), 281-288.
[64] D. R. Hayes, *Explicit class field theory in global function fields*, dans *Studies in Algebra and Number Theory*, 173-217, Adv. in Math. Suppl. Stud., **6**. Academic Press, New York-London (1979).
[65] D. R. Hayes, *A brief introduction to Drinfel'd modules*, dans [62] ci-dessus, 1-32.
[66] Y. Hellegouarch, *Modules de Drinfel'd généralisés*, dans *Approximations Diophantiennes et Nombres Transcendants*, Luminy 1990 (P. Philippon éd.). Walter de Gruyter, Berlin (1992).
[67] Y. Hellegouarch, *Un analogue d'un théorème d'Euler*. C. R. Acad. Sci. Paris, Sér. I, Math., **313** (1991), 155-158.
[68] Y. Hellegouarch, *Une généralisation d'un critère de de Mathan*. C. R. Acad. Sci. Paris, Sér. I, Math., **321** (1995), 677-680.
[69] T. Kamae and M. Mendès France, *A continuous family of automata: the Ising automata*. Ann. Inst. H. Poincaré, Phys. Théor. **64** (1996), 349-372.
[70] Y. Katznelson, *An Introduction to Harmonic Analysis*. John Wiley and Sons, Inc. (1968).
[71] M. Koskas, *Complexité de suites - Fonctions de Carlitz* (Thèse). Université Bordeaux I (1995).

[72] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences.* John Wiley and Sons, Inc. (1974).
[73] J. Liouville, *Sur des classes très étendues de quantités dont la valeur n'est ni rationnelle ni même réductible à des irrationnelles algébriques.* C. R. **18** (1844), 883-885, 910-911
[74] N. Loraud, *Numérations généralisées, langages et automates* (Thèse). Université de Provence (1996).
[75] K. Mahler, *On the translation properties of a simple class of arithmetical functions.* J. Math. and Phys. **6** (1927), 158-163.
[76] B. de Mathan, *Un critère de transcendance en caractéristique positive.* C. R. Acad. Sci. Paris, Sér. I, Math., **319** (1994), 427-432.
[77] B. de Mathan, *Irrationality measures and transcendence in positive characteristic.* J. Number Theory **54** (1995), 93-112.
[78] M. Mendès France, *The Ising transducer.* Ann. Inst. H. Poincaré, Phys. Théor. **52** (1990), 259-265.
[79] M. Mendès France, *Opacity of an automaton. Application to the inhomogeneous Ising chain.* Comm. Math. Phys. **139** (1991), 341-352.
[80] M. Mendès France and J.-Y. Yao, *Transcendence and the Carlitz-Goss gamma function.* J. Number Theory **63** (1997), 396-402.
[81] W. H. Mills and D. P. Robbins, *Continued fractions for certain algebraic power series.* J. Number Theory **23** (1986), 388-404.
[82] M. Mkaouar, *Sur le développement en fraction continue de la série de Baum et Sweet.* Bull. Soc. Math. France **123** (1995), 361-374 .
[83] M. Morse, *Recurrent geodesics on a surface of negative curvature.* Trans. Amer. Math. Soc. **22** (1921), 84-100.
[84] H. Moulin, *Fondation de la Théorie des Jeux.* Hermann (1979).
[85] K. Nishioka, *New approach in Mahler's method.* J. Reine Angew. Math. **407** (1990), 202-219.
[86] K. Nishioka, T.-A. Tanaka, and Z.-Y. Wen, *Substitution in two symbols and transcendence.* Tokyo J. Math. **22** (1999), 127-136.
[87] E. Prouhet, *Mémoire sur quelques relations entre les puissances des nombres.* C. R. Acad. Sci. Paris **33** (1851), 225..
[88] N. Pytheas Fogg (V. Berthé, S. Ferenczi, C. Mauduit, A. Siegel, éditeurs) *Substitutions in Dynamics, Arithmetics and Combinatorics.* Lecture Notes in Math. **1794**. Springer (2002).
[89] M. Queffélec, *Substitution Dynamical Systems — Spectral Analysis.* Lecture Notes in Math. **1294**. Springer-Verlag (1987).
[90] M. Queffélec, *Transcendance des fractions continues de Thue-Morse.* J. Number Theory **73** (1998), 201-211.
[91] F. Recher, *Propriétés de transcendance de séries formelles provenant de l'exponentielle de Carlitz.* C. R. Acad. Sci. Paris, Sér. I, Math., **315** (1992), 245-250.
[92] J. Sakarovitch, *Éléments de Théorie des Automates.* À paraître chez Vuilber (2003).
[93] O. Salon, *Suites automatiques à multi-indices et algébricité.* C. R. Acad. Sci. Paris, Sér. I, Math., **305** (1987), 501-504.
[94] M. Schwartz, *Information Transmission, Modulation, and Noises.* McGraw-Hill, Inc (1970).
[95] C. E. Shannon, *A mathematical theory of communication.* The Bell System Technical Journal **27** (1948), 379-423, 623-656.
[96] H. Sharif and C. F. Woodcock, *Algebraic functions over a field of positive characteristic and Hadamard products.* J. Lond. Math. Soc. **37** (1988), 395-403.
[97] S. M. Spencer, Jr., *Transcendental numbers over certain function fields.* Duke Math. J. **19** (1952), 93-105.
[98] D. S. Thakur, *Gamma functions and Gauss sums for function fields and periods of Drinfel'd modules* (Thesis). Harvard University (1987).
[99] D. S. Thakur, *Gamma functions for function fields and Drinfel'd modules.* Ann. of Math. **134** (1991), 25-64.
[100] D. S. Thakur, *On Gamma functions for function fields,* dans [62] ci-dessus (1992), 75-86.
[101] D. S. Thakur, *Automata-style proof of Voloch's result on transcendence.* J. Number Theory **58** (1996), 60-63.
[102] D. S. Thakur, *Transcendence of gamma values for $F_q[T]$.* Ann. of Math. **144** (1996), 181-188.

[103] D. S. Thakur, *Automata and transcendence.* Dans : Number theory (Tiruchirapalli, 1996), Contemp. Math. Vol. **210**, American Mathematical Society (1998), 387-399.
[104] A. Thiery, *Indépendance algébrique des périodes et quasi-périodes d'un module de Drinfel'd,* dans [62] ci-dessus (1992), 265-284.
[105] A. Thue, *Über unendliche Zeichenreihen.* Norskevid. Selsk. Skr. I. Mat. Nat. Kl., Christiana, **7** (1906), 1-22.
[106] L. I. Wade, *Certain quantities transcendental over $GF(p^n, x)$.* Duke Math. J. **8** (1941), 701-720.
[107] L. I. Wade, *Certain quantities transcendental over $GF(p^n, x)$, II.* Duke Math. J. **10** (1943), 587-594.
[108] L. I. Wade, *Two types of function field transcendental numbers.* Duke Math. J. **11** (1944), 755-758.
[109] L. I. Wade, *Remarks on the Carlitz ψ-functions.* Duke Math. J. **13** (1946), 71-78.
[110] M. Waldschmidt, *Transcendence problems connected with Drinfel'd modules.* International Symposium on Algebra and Number Theory (Silivri, 1990). Istanbul Üniv. Fen Fak. Mat. Derg. **49** (1990), 57-75.
[111] P. Walters, *Symbolic Dynamics and Its Applications.* Contemp. Math. Vol. **135**. American Mathematical Society (1992).
[112] M. W. Warner, *Semi-group, group quotient and homogeneous automata.* Inform. and Control **47** (1980), 59-66.
[113] Z.-Y. Wen and J.-Y. Yao, *Transcendence, automata theory and gamma functions for polynomial rings.* Acta Arith. **101** (2002), 39-51.
[114] K. Vo-Khac, *Distributions. Analyse de Fourier. Opérateurs aux Dérivées Partielles.* Tome 1. Vuibert (1972).
[115] J.-Y. Yao, *Contribution à l'étude des automates finis* (Thèse). Université Bordeaux I (1996).
[116] J.-Y. Yao, *Critères de non-automaticité et leurs applications.* Acta Arith. **80** (1997), 237-248.
[117] J.-Y. Yao, *Généralisations de la suite de Thue-Morse.* Ann. Sci. Math. Québec **21** (1997), 177-189.
[118] J.-Y. Yao, *Opacités des automates finis.* Discrete Math. **202** (1999), 279-298.
[119] J.-Y. Yao, *Some transcendental functions over function fields with positive characteristic.* C. R. Math. Acad. Sci. Paris **334** (2002), 939-943.
[120] J.-Y. Yao, *Opacity of a finite automaton, method of calculation and the Ising Chain.* Discrete Appl. Math. **125** (2003), 289-318.
[121] J.-Y. Yao, *Some properties of Ising automata.* Prétirage (2003).
[122] J.-Y. Yao, *Finite automata and information transmission.* En préparation (2003).
[123] J.-Y. Yao, *A transcendence criterion in positive characteristic and applications in the study of Carlitz module.* Prétirage (2003).
[124] J.-Y. Yao, *Carlitz-Goss gamma function, Wade's method, and transcendence.* Prétirage (2003).
[125] J. Yu, *Transcendental numbers arising from Drinfel'd modules.* Mathematika **30** (1983), 61-66.
[126] J. Yu, *Transcendence theory over function fields.* Duke Math. J. **52** (1985). 517-527.
[127] J. Yu, *A six exponentials theorem in finite characteristic.* Math. Ann. **272** (1985), 91-98.
[128] J. Yu, *Transcendence and Drinfel'd modules.* Invent. Math. **83** (1986), 507-517.
[129] J. Yu, *Transcendance and Drinfel'd modules: several variables.* Duke Math. J. **58** (1989), 559-575.
[130] J. Yu, *Transcendence and special zeta values in characteristic p.* Ann. of Math. **134** (1991), 1-23.
[131] J. Yu, *Transcendence in finite characteristic,* dans [62] ci-dessus (1992), 253-264.

INDEX

RAPPORTS INTERNES AU LRI - ANNEE 2003

N°	Nom	Titre	Nbre de pages	Date parution
1345	FLANDRIN E LI H WEI B	A SUFFICIENT CONDITION FOR PANCYCLABILITY OF GRAPHS	16 PAGES	01/2003
1346	BARTH D BERTHOME P LAFOREST C VIAL S	SOME EULERIAN PARAMETERS ABOUT PERFORMANCES OF A CONVERGENCE ROUTING IN A 2D-MESH NETWORK	30 PAGES	01/2003
1347	FLANDRIN E LI H MARCZYK A WOZNIAK M	A CHVATAL-ERDOS TYPE CONDITION FOR PANCYCLABILITY	12 PAGES	01/2003
1348	AMAR D FLANDRIN E GANCARZEWICZ G WOJDA A P	BIPARTITE GRAPHS WITH EVERY MATCHING IN A CYCLE	26 PAGES	01/2003
1349	FRAIGNIAUD P GAURON P	THE CONTENT-ADDRESSABLE NETWORK D2B	26 PAGES	01/2003
1350	FAIK T SACLE J F	SOME b-CONTINUOUS CLASSES OF GRAPH	14 PAGES	01/2003
1351	FAVARON O HENNING M A	TOTAL DOMINATION IN CLAW-FREE GRAPHS WITH MINIMUM DEGREE TWO	14 PAGES	01/2003
1352	HU Z LI H	WEAK CYCLE PARTITION INVOLVING DEGREE SUM CONDITIONS	14 PAGES	02/2003
1353	JOHNEN C TIXEUIL S	ROUTE PRESERVING STABILIZATION	28 PAGES	03/2003
1354	PETITJEAN E	DESIGNING TIMED TEST CASES FROM REGION GRAPHS	14 PAGES	03/2003
1355	BERTHOME P DIALLO M FERREIRA A	GENERALIZED PARAMETRIC MULTI-TERMINAL FLOW PROBLEM	18 PAGES	03/2003
1356	FAVARON O HENNING M A	PAIRED DOMINATION IN CLAW-FREE CUBIC GRAPHS	16 PAGES	03/2003
1357	JOHNEN C PETIT F TIXEUIL S	AUTO-STABILISATION ET PROTOCOLES RESEAU	26 PAGES	03/2003
1358	FRANOVA M	LA "FOLIE" DE BRUNELLESCHI ET LA CONCEPTION DES SYSTEMES COMPLEXES	26 PAGES	04/2003
1359	HERAULT T LASSAIGNE R MAGNIETTE F PEYRONNET S	APPROXIMATE PROBABILISTIC MODEL CHECKING	18 PAGES	01/2003
1360	HU Z LI H	A NOTE ON ORE CONDITION AND CYCLE STRUCTURE	10 PAGES	04/2003
1361	DELAET S DUCOURTHIAL B TIXEUIL S	SELF-STABILIZATION WITH r-OPERATORS IN UNRELIABLE DIRECTED NETWORKS	24 PAGES	04/2003